Electronic Colloquium on Computational Complexity, Report No. 137 (2020)

Deterministic and Efficient Interactive Coding from Hard-to-Decode Tree Codes

Zvika Brakerski*
Weizmann Institute of Science

Yael Tauman Kalai
Microsoft and MIT

Raghuvansh R. Saxena†
Princeton University

Abstract

The field of Interactive Coding studies how an interactive protocol can be made resilient to channel errors. Even though this field has received abundant attention since Schulman's seminal paper (FOCS 92), constructing interactive coding schemes that are both deterministic and efficient, and at the same time resilient to adversarial errors (with constant information and error rates), remains an elusive open problem.

An appealing approach towards resolving this problem is to show efficiently encodable and decodable constructions of a combinatorial object called tree codes (Schulman, STOC 93). After a lot of effort in this direction, the current state of the art has deterministic constructions of tree codes that are efficiently encodable but require a logarithmic (instead of constant) alphabet (Cohen, Haeupler, and Schulman, STOC 18). However, we still lack (even heuristic) candidate constructions that are efficiently decodable.

In this work, we show that tree codes that are efficiently encodable, *but not efficiently decodable*, also imply deterministic and efficient interactive coding schemes that are resilient to adversarial errors. Our result immediately implies a deterministic and efficient interactive coding scheme with a logarithmic alphabet (*i.e.*, $1/\log\log$ rate). We show this result using a novel implementation of hashing through *deterministic* tree codes that is powerful enough to yield interactive coding schemes.

*Supported by the Binational Science Foundation (Grant No. 2016726), and by the European Union Horizon 2020 Research and Innovation Program via ERC Project REACT (Grant 756482) and via Project PROMETHEUS (Grant 780701).

†Part of this work was done while visiting Microsoft Research New England.

ISSN 1433-8092

Contents

1 Introduction

In a sequence of groundbreaking works, Schulman [Sch92, Sch93, Sch96], defined interactive error-correcting codes. An interactive error correcting code starts with a two party communication protocol that is built to work over the *noiseless* channel, and compiles it to a *noise resilient* two-party protocol that is only a constant factor longer than the noiseless protocol. A protocol is said to be noise-resilient if it works even when a constant fraction of the symbols communicated during the protocol are adversarially corrupted.

Ever since Schulman's works, the hunt for deterministic and efficient interactive codes has remained an elusive open problem. An interactive code is said to be efficient if the 'next message' functions of the noise resilient protocol are efficiently (and deterministically) computable given oracle access to the next message functions of the noiseless protocol.

The main line of attack towards getting deterministic and efficient interactive coding schemes is to construct efficiently encodable and decodable combinatorial objects known as *tree codes* [Sch93]. Essentially, a tree code is an error correcting code with an "online" encoding function. That is, for all i, the i^{th} symbol computed by the tree code depends only on the first i symbols of the message it is encoding. The success in this line of attack has been partial. On the one hand, there has been a lot of progress in the direction of getting tree codes that are efficiently encodable [Pec06, MS14, CHS18] but on the other hand, the problem of constructing efficiently decodable tree codes seems to be extremely hard.

1.1 Our Result

We show that efficient interactive codes can be constructed from tree codes that are not efficiently decodable (but are efficiently encodable). An informal statement of our main result is below (for a formal statement, see Theorem 3.8).

Theorem 1.1 (Informal)**.** *There is an efficient and deterministic transformation from an efficiently encodable tree-code to an interactive-coding scheme for two party communication protocols.*

Our result makes a fundamental conceptual contribution, showing that efficiently decoding tree codes is not a bottleneck in the path towards getting deterministic and efficient interactive coding schemes. Furthermore, by combining it with known results on tree codes, we obtain interactive coding schemes in regimes where none were known prior to our work. For example, combining our result with the slightly sub-constant rate tree codes of [CHS18] yields a new deterministic and efficient interactive coding scheme with slightly super-linear communication overhead.

Corollary 1.2 (Combining our result with [CHS18])**.** *There exists a deterministic interactive coding scheme against adversarial noise that takes a two party protocol of length n and obtains a two party protocol of length $\mathcal{O}(n \log \log n)$ that is resilient to a constant fraction of errors.*

Additionally, although the parameters of the tree codes that we use are slightly different, we believe that our techniques can also be combined with those in the work of [MS14] where the authors show efficiently encodable tree codes based on a conjecture about exponential sums. This will lead to the first full fledged deterministic and efficient interactive coding scheme that has a constant communication blowup and is resilient to a constant fraction of errors based on the same conjecture.

1.2 Related Work

A lot of work has been done in the field of interactive coding in the past few decades, and our description of the field in the introduction barely scratched the surface. The long line of work [GMS11, BR11, BK12, BE14, BKN14, GMS14, EGH16, BGMO17, to cite a few] focuses on building better and better (in various aspects) interactive codes in different regimes. We only elaborate on a few that are the closest to ours and refer the reader to [Gel17] for an excellent survey.

Efficient randomized interactive coding schemes. The relaxed problem of constructing efficient *randomized* interactive coding schemes has also received a lot of attention. For our setting of adversarial noise, [BK12], followed by [GH14], construct a hash-function based interactive coding scheme. Their coding scheme can also be implemented deterministically in the non-uniform setting, where a non-deterministic "advice" string, linear in the length of the protocol, is given to the communicating parties and the adversary [BKN14] (see also [GH14]). For the easier setting of random noise, such schemes have been known since [Sch92].

Other interactive coding variants. Many other variants of interactive coding have been studied in the literature, including multi-party interactive coding [RS94, JKL15, HS16, EKS18, GKR19] and list decodable interactive coding [BE14, GH14]. Non-adversarial error models were also considered, most notably the binary symmetric channel (BSC) model, where each bit going over the channel is flipped with some small constant probability [Sch92, GMS11, GHK+16].

Tree Codes. Efficiently encodable tree codes are known to be constructible probabilistically with high probability [Sch93, Pec06], or heuristically based on conjectures on exponential sums [MS14]. Very recently, an explicit construction with constant error rate and slightly sub-constant $(1/\log\log(n))$ information rate was presented by Cohen, Haeupler and Schulman [CHS18]. Narayanan and Weidner [NW19] later showed that the tree code of [CHS18] can be efficiently decoded using a randomized algorithm, but only against sub-constant error rate. Also related is the construction of tree codes in sub-exponential time by [Bra12] and the construction of a weaker object called 'potent tree codes' in [GMS11].

1.3 Our Techniques

It is well known [BK12] that efficient interactive coding schemes are possible given access to hash functions. In our scheme, we use the same blueprint as [BK12] but we design a novel way to substitute the *randomized* hash functions with *deterministic* tree codes. It turns out that ensuring that the parties never need to decode the tree code requires the parties to maintain not one, but *several* tree codes in a stack and encode different parts of their state using different tree codes. Matters are further complicated by the fact that the stack needs to be very small almost all the time so that the communication complexity of our simulation does not blow up too much.

We then plug this deterministic tree code based hashing mechanism into the consistency checks of [BK12] to get an interactive coding scheme. In our scheme, instead of sending hashes of their local state like in [BK12], the parties encode their state using various tree codes and exchange these encodings with each other. At first sight, this may seem natural as tree codes, like hash functions, are guaranteed to 'disagree' in many coordinates once the encoded states start becoming different. However, there is a major difference.

Unlike hash functions that are "memoryless" (any invocation of a hash function will detect an inconsistency with high probability), tree codes are static, deterministic objects. It is true that they guarantee a large distance on average, but there may be large 'unprotected' regions of the tree code where they provide no distance guarantees. A lot of work goes behind ensuring that the unprotected regions of different tree codes in our stack do not overlap and we have some protection at all points in our simulation. We next present a detailed overview of our solution. We believe that our approach may be useful in derandomizing other similar interactive tasks.

2 Overview of Our Interactive Coding Scheme

We provide a high level overview of our construction and describe the main ideas behind the proof of security. At a very high level, our construction follows the blueprint of [BK12], while instantiating the consistency checks using efficiently encodable tree codes instead of hash functions.

2.1 A Blueprint for Interactive Coding Schemes

In interactive coding, there are two parties, Alice and Bob, that wish to reconstruct the transcript π of a *noiseless* protocol while communicating over a *noisy* channel. This reconstruction is done gradually, where at each point, the parties maintain a local view of π that has been reconstructed thus far. The goal of the parties is to make sure that these (potentially inconsistent) local views eventually converge to the actual transcript π.

In [BK12], the authors present the following two-layer blueprint for efficient interactive coding schemes:

- **Inner Layer:** The first step in [BK12] is to break the transcript π into logarithmic sized chunks. In the 'inner layer' of the blueprint, the parties simulate each chunk of π separately using a standard (inefficient) interactive coding scheme. As each chunk is only logarithmic in length, we can afford to simulate these chunks inefficiently while making sure that the overall simulation is efficient.

- **Outer Layer:** In the outer layer, the parties stitch together chunks obtained from the inner layer to get the actual transcript π. Namely, the parties maintain a local view of the sequence of chunks that have been simulated so far and in each iteration of the outer layer, they attempt to extend this sequence by simulating the next chunk. At the end of each iteration, the parties execute a *consistency check* to make sure that the chunk they are adding to their local sequence is consistent with what the other party is adding and fix inconsistencies (if any).

  The consistency check plays two roles. Firstly, the parties check whether they are 'synchronized' by exchanging with each other the number of chunks that they have simulated so far. If the parties are not in sync, *i.e.*, one party has a simulated more chunks than the other, then the party that has simulated more chunks rewinds one chunk, and the other party keeps their transcript as is.

  Besides the number of chunks, the parties also hash the sequence of chunks that they have locally and exchange these hashes with each other. These hash values come into play when the parties are synchronized, and are a means to detect if their local sequences are the same. If they are, then the parties proceed to simulate the next chunk. Otherwise, *both* the parties rewind one chunk.

Analyzing the outer layer. Due to the inner layer, we can assume in our analysis of the outer layer, that each iteration is either fully corrupted (and thus contains adversarial content), or not corrupted at all. We need, therefore, to ensure that if at most a constant fraction of iterations are corrupted then the parties output the correct transcript π.

The analysis of the outer layer is usually done using a potential function, whose goal is to quantify the intuition that "progress" is made in each iteration of the interactive coding scheme. Here, "progress" could either mean that the local views of the parties are now closer to the desired output π, or that some damage done by the adversary in previous iterations is being undone, or (importantly) that the adversary introduced new errors. The latter is considered as "progress" since the budget of the adversary is limited, and the coding scheme benefits from the adversary using up its budget. In order to get an interactive coding scheme with constant blowup in communication, the prime principle to keep in mind is that all communication by the parties needs to be "paid for" by the progress being made. Additionally, if one is interested in constant error rate, then each error inserted by the adversary is "detected and fixed" after a constant amount of communication.

In [BK12], these two layers are composed to get the final interactive coding scheme. We emphasize that randomness is only used in the Outer Layer, and in particular in the hashes inside the consistency checks at the end of each iteration.

2.2 Our Approach: Tree Code Based Consistency Checks

In this work, we replace the randomized consistency checks of [BK12] with a deterministic tree-code based one. This task is far from trivial. In particular, as we explain below, the number of bits sent in each of our deterministic consistency checks will not be fixed. Rather, in our deterministic solution, the length of each consistency check can be arbitrarily long, depending on the adversarial errors introduced so far. To simplify our description of our consistency checks, we first assume that the parties are always synchronized. In Subsection 2.3 we show how to deal with synchronization issues.

2.2.1 Basic Idea: A Stack of Tree Codes

Replacing hash functions with tree codes is a natural approach. The purpose of the hashing mechanism is to provide a signal for the event that the two local sequences of chunks disagree. The property of this signal is that once a disagreement occurs, a constant fraction of the iterations result in the parties receiving an indication of this disagreement (with overwhelming probability). Observe that a tree code naturally provides such a mechanism, simply encoding the local view with a tree code does exactly this, since we will still get an indication of the disagreement in a constant fraction of the iterations, and in order to avoid the detection of this discrepancy, the adversary needs to keep investing new errors.

A closer look, however, reveals a very significant difference between detection on a *large but fixed subset* of the iterations, as offered by tree codes, and detection at *every iteration* with large probability, as offered by hash functions. Let us illustrate this using an example.

Suppose that, in some iteration i, the local sequences of chunks of the parties disagree, and even though iteration i was not corrupted, the parties did not detect this disagreement. Such failure can happen in the hash setting due to its probabilistic nature, and in the tree code setting because it only guarantees detection on a large subset of (and not all) iterations. Further, assume (optimistically) that in iteration $i+1$, the disagreement is detected and the parties rewind their local state, reaching the same state as they had in iteration i. Now, in the hash-based solution, we get a second chance to detect the past disagreement, since we use a fresh hash function. The naive tree-code based solution, however, is doomed to repeat the mis-detection due to the deterministic nature of the tree code. This allows the adversary to invest a sufficient amount of errors to place the parties in a vicious loop, and then the adversary can just sit back and watch the protocol never converging.

Our Approach: Rather than simply rewinding one step and then continuing forward (which may lead to an infinite loop), our protocol guarantees that the rewinding process

removes an actual disagreement. At a high level, this is done by ensuring that the parties keep rewinding till they find a place where their sequences disagree. Such a rewinding procedure is implemented using "backwards tree codes". Namely, as the parties rewind, they send the sequence of chunks, starting from the last chunk, that they have rewound encoded using a tree code to each other. The parties will end the rewind stage and continue going 'forward' only after a point of disagreement is found while going backwards.

Unfortunately, this fix is only partial, and the reason again is the deterministic nature of tree codes. Suppose that the adversary inserts a lot of errors at the beginning to create a large "unprotected region" (*i.e.*, a region of the tree code lacking good distance). When they are in an unprotected region, it may take a lot of iterations for the parties to detect that a disagreement exists in their sequences of chunks. Consequently, when they eventually detect this disagreement, the parties may have to rewind a lot of chunks in order to reach this point of disagreement. Once this point of disagreement is reached, the parties start going forward again.

However, even when going forward a second time, the parties are still in the unprotected region, and it may take them a lot of iterations to detect any errors that the adversary inserts now. This slow detection means that the adversary wastes a lot of communication for each error he inserts, derailing our interactive coding scheme.

We fix this problem by "patching" the unprotected region of the tree code, as follows. After a disagreement is removed, we add to the original (forward) tree-code, which may be in an unprotected region, a new forward tree-code. We use this new tree-code to encode the suffix of the transcript starting from the point of disagreement found by the backward tree code. This encoding is in addition to the original tree code encoding. As the new tree code is in a protected region (the first levels of any tree code are protected), the parties will quickly detect any new errors inserted by the adversary and continue the simulation.

Observe that adding new tree codes each time a point of disagreement is found can result in the parties having a stack of multiple tree codes. This is because sometimes we will need to "patch the patch" by adding forward tree codes again and again. We refer to this as "the stack of tree codes". As the communication in each iteration will be proportional to the number of tree codes in the stack, we need to make sure to control the size of the stack so as to keep it from blowing up the information rate. Besides, there are multiple other issues that need to be resolved. We address these in the detailed description below.

2.2.2 Analyzing the Stack of Tree Codes

We now cover the remaining issues with our stack of tree codes, and also provide a taste of our analysis. Recall from Subsection 2.1 that, in order to have a constant blowup in the communication and a constant error rate, one needs to make sure that the communication during the rewind and patching phases is proportional to the number of errors inserted by the adversary.

- **The master tree code:** The protocol starts as in the basic idea above. The parties

maintain locally, a sequence of chunks that they have simulated, and in each consistency check they send the tree code symbol that stems from encoding this sequence of chunks. While this is not a complete solution (as we explained), this simple consistency check still provides the guarantee that as soon as a disagreement arises, the adversary must keep inserting new errors in order to keep the parties from detecting the disagreement. The conclusion is that the existence of a discrepancy will eventually be detected, and the time spent in detecting this disagreement can be charged to the adversary's budget.

- **Backwards tree codes:** Recall that once a disagreement is detected the parties start a backwards tree code to reach the point of disagreement. Can the communication spent in detecting this disagreement be charged to the adversary's budget?

  Intuitively, it seems that the answer should be yes, since the rewinding should be paid for by the errors that created and hid the disagreement from the parties. This intuition can indeed be formalized, except for the following two cases:

  - **Fake disagreements:** Recall that the rewind process is triggered by detecting a disagreement in the master tree code. However, it is possible that this disagreement is "fake" in the sense that the parties think there is a disagreement due to adversarial error, even when there is no disagreement. In this case, the parties will continue to rewind all the way to the first chunk, since they will never find a point of disagreement, as none exists.

    We get around this issue by having the parties verify the "reason" of entering the rewind process at each step of the rewind process. Namely, when the parties are rewinding, then, in the consistency check, they not only exchange the backward tree-code encodings, but they also exchange the point and value of the master tree code that caused the rewinding. If at some point these values agree and there is no reason to go backwards, the parties reverse the backtracking process, one step at a time.

    Adding the reasons to the rewind process ensures that the adversary needs to corrupt the reasons at each step of the rewind process in case of a fake disagreement, thereby, getting around the above problem.

  - **Too many disagreements:** The other case where the adversary's budget fails to pay for the rewinding is in case the adversary inserted a lot of disagreements and it is infeasible to correct them one at a time[1]. To understand this case, suppose that the adversary generated a burst of "ancient" errors resulting in a large unprotected region, and then inserted another burst of errors inside this unprotected region. As the region is unprotected, the parties only detect the second burst of errors after a lot of iterations, when they go back and remove the last disagreement in this burst.

    Once they remove this disagreement, the parties start going forward using a patching tree code. We claim that even if the adversary does not insert any more errors, it

[1]Note that disagreements can only be corrected one at a time as after reaching the first point of disagreement, the parties are not even sure whether a second point of disagreement exists or not.

will take the parties a lot of iterations to get rid of the second burst of errors. This is because they will remove these errors one at a time, and may potentially go forward a lot after any such removal. Indeed, the master tree code does not protect them, and the patching tree code does not either because it starts after the burst of errors, and is therefore oblivious to the errors in the burst.

To ensure that error correction happens quickly enough, we "double" the rewind process (for example, if we detect a disagreement 5 chunks in the past, we will rewind to remove 10 chunks from the local transcript). On the one hand, this is only a constant factor, so if there were no ancient errors, then we did not lose too much from this doubling. On the other hand, if there is an ancient burst of errors, then due to the doubling of the rewind process, we make progress fast enough towards correcting all the disagreements in the local view of the parties.

- **Patching tree codes:** Suppose that a rewind just concluded, and the parties would now like to start going forward and rebuild their local transcript. Recall that, when the parties start going forward again, they add a patching tree code to their stack of tree codes that runs in parallel with the master tree code as they go forward. The purpose of this patching tree code is to provide extra protection to the parties in case they are in an unprotected region of the master tree code. With this patching tree code, two encodings are sent in the consistency check for every new chunk that is added to the local view of the parties. These encodings are those of the master tree code and the patching tree code respectively. The encoding of the master tree code corresponds to the all the chunks in the parties' local view, whereas the encoding of the patching tree code corresponds to the suffix of the chunks starting from the point where the rewind process ended.

  Similar to the analysis of the backwards tree codes, the analysis of the patching tree codes gets stuck in two cases. Both these cases parallel the analogous cases in the analysis of the backwards tree codes and we only provide a brief description.

  - **Fake patches:** The first bad case for the analysis is when the adversary makes the parties add a patching tree code even though they did not reach a point of disagreement in the rewind phase. This is problematic because when it happens, the parties erase all of the progress they made in the rewind phase due to just one extra error inserted by the adversary (namely, the one that caused the patching tree code to start).

    We fix this problem by having a "reason" for the patching tree code that is "verified" every time a new symbol is sent on the patching tree code. This reason is the location and the value of the backward tree codes where the disagreement was found. With this reason, if the adversary wants to create a long fake patching tree code, he needs to insert errors at every step of this patching tree code in order to fail the verification done by the parties at every step. This needs a lot of errors that the adversary cannot afford for too long.

– **Too many patches:** The other bad case occurs when the adversary creates multiple patches on the same master tree code. Recall that the purpose of a patch is to provide protection in the unprotected regions of the master tree code. Once the parties are outside the unprotected region, they must drop the patching tree codes to save on the communication in the consistency check. Indeed, the communication needed in the consistency checks increases with the number of tree codes in the stack.

  However, the parties do not know where the unprotected regions are, and we need some other criterion to drop the patching tree codes. One natural candidate is to drop the patching tree code at the point where the rewind process started, *i.e.*, if the parties rewound x chunks before going forward again, then the patching tree code will be dropped after x iterations. This idea, however, does not work, and it is possible to create a pathological example where the adversary can make the parties waste a lot of communication in the patching and rewind processes by carefully inserting a small number of corruptions.

  The solution is twofold. Firstly, we double the length of the patching tree codes. Namely, instead of dropping them after x iterations, the parties drop them after $2x$ iterations. On the one hand, it is only a constant factor, and therefore still can be charged to the adversary's budget while on the other hand, now the parties will be able to escape the unprotected region much faster and reach a point where the master tree code again protects them. Besides doubling the length of the patching tree codes, we will also need the patching tree codes deeper in the stack to be more secure than the tree codes higher up in our stack. We do this by adding more and more redundancy to tree code symbols as we go deeper and deeper in the stack. Specifically, we ensure that the size of the encoding of a tree code is a small exponential in the position of the tree code in the stack. This extra redundancy in deeper tree codes allows us to finish our argument.

In conclusion, our consistency check maintains a stack of tree codes consisting of the master code, backtracking codes, and patching codes. We use the term forward tree codes to refer to the master and the patching tree codes together. The number of bits sent in each consistency check depends on the number of tree codes in the stack. Importantly, the consistency check only requires *efficiently encodable* tree codes and does not require any randomness.

2.3 Our Outer Layer: An Error-Resilient Protocol in Model LONG

Recall that we assumed the parties are always synchronized in Subsection 2.2 when describing our tree code based consistency checks. We next remove this assumption and show how the parties can synchronize themselves and finish our Outer Layer.

Recall that synchronization is needed in [BK12] because if the parties are not synchronized, then they think they are simulating different chunks of the noiseless transcript

and the resulting communication is meaningless. For our consistency checks, synchronization is also needed in order to make sure that tree code encodings exchanged by the parties in the consistency checks can be compared to each other. Indeed, it only makes sense to compare two tree code encodings if they come from the same 'level' in the tree code, as otherwise, the distance property is not guaranteed to hold.

In order to make sure that they are synchronized, the parties exchange the following synchronization information: The total number of chunks (forward and backward) that the parties have simulated so far, the number of tree codes they have in their stack, the number of chunks in the parties' local sequence when each tree code was added to the stack, and the length of their forward transcript and backward transcript (the length of the backward transcript is non-zero only if they are in the process of backtracking). This synchronization information adds only a constant multiplicative overhead to the number of bits sent in the consistency checks, and therefore blows up the length of our interactive coding scheme by only a constant factor.

The model `LONG`. Observe that the number of bits required to encode our synchronization information and the number of tree code encodings exchanged by the parties depends on the number of tree codes in the parties' stack. Correspondingly, the number of bits sent by the parties in the consistency check in the Outer Layer will vary from iteration to iteration. In order to capture this neatly, we present our outer layer in an artificial model, called model `LONG`. In our Inner Layer, we convert a protocol in model `LONG` to one in the standard two party model.

In model `LONG`, the protocol proceeds in "iterations" of $P + 1$ rounds, where P is the time it takes to simulate one chunk of the noiseless transcript. Each iteration consists of P "standard/short" rounds where parties send each other one symbol per round followed by one "long" round where the parties may send arbitrarily long messages. The long rounds correspond to the consistency check in our Outer Layer, where the parties may be sending a lot of bits based on the number of tree codes currently in their stack. In model `LONG`, we consider adversaries that either corrupt an entire iteration, and are charged by the communication complexity of that iteration, or leave the iteration completely uncorrupted. This is similar to the adversaries in [BK12], except that for us, the communication complexity of an iteration is not fixed, and depends on the adversarial error.

Synchronizing Alice and Bob. The presence of a stack of tree codes instead of a single hash function and fact that the communication complexity of an iteration is not fixed makes our synchronization procedure more complicated than [BK12]. Firstly, in order to detect which party is ahead of the other, the parties can no longer rely on the length of their local sequence of chunks. Indeed, this length is not a good estimate because the parties can go both forward and backwards in the sequence. Instead, the parties determine who is further ahead based on the *total* number of chunks, both forward and backward, simulated so far and this number is exchanged as a part of the synchronization information.

Furthermore, because the communication in each iteration is different, when the parties detect that they are out of sync (say Alice is ahead of Bob), then instead of Alice going back one iteration in time, as in [BK12], she needs to go back an amount proportional to the communication in this iteration. For example, suppose that Alice and Bob detect a synchronization error in iteration i, when the length of the synchronization information received by Alice from Bob is b bits. Also suppose that in all the iterations 1 through i Alice sent a bits of synchronization information to Bob. Then, in iteration i, Alice will need to go back (roughly) b/a iterations, so that the total amount of communication that she rewound is around $a \cdot b/a = b$. Rewinding in this way ensures that the amount of communication it takes to get back in sync is upper bounded by a constant times the amount of errors invested by the adversary to make the parties fall out of sync.

Finally, just like [BK12], if the parties are synchronized, then they continue the consistency check as described in the foregoing section.

2.4 Our Inner Layer: From Model LONG to the Standard Model

In our Inner Layer, we convert a protocol in model LONG to a protocol in the standard model, with essentially the same error resilience properties (up to constant factors). The fact that the long messages exchanged after every P rounds in model LONG are arbitrarily long makes this part quite tedious[2]. We do this in two steps:

1. First, we convert the protocol in model LONG into another protocol in model LONG, which has the guarantee that all the long messages are of the same fixed length which is a constant times P.

2. Then, we convert the protocol obtained in Step 1 above into one in the standard model.

Observe that Step 2 is quite straightforward and is very similar to the Inner Layer of [BK12] described in Subsection 2.1, and it simply applies a deterministic tree code based interactive coding scheme to each iteration separately. Since each iteration is only of length $\mathcal{O}(P)$ after Step 1, which is logarithmic in the length of the noiseless transcript, the tree codes required in this step are computationally efficient.

However, Step 1 is tedious, and is roughly carried out as follows. When a party needs to send a long message, the party first encodes the message using a standard error correcting code resilient to insertions and deletions. Then the party breaks this encoded message (which may be way too long) into blocks, each of length P. The parties will then send these blocks one at a time, along with some metadata, which includes which block number it is, and whether it is the last block or not, *etc.*. This metadata will help the receiving party stitch the individual blocks together in the right order.

[2]Dealing with variable message-length in interactive coding was already considered in previous works [EHK18] (although our case is simpler in some aspects since we do not seek to preserve round complexity).

The reason we use error correcting codes resilient to insertion and deletion errors is to simulate the guarantee in model LONG that says that corrupting any part of the long message or the P standard rounds before it requires the adversary to spend a number of errors proportional to the length of the long message. Error correcting codes resilient to insertions and deletions provide this abstraction (up to constant factors) even if certain blocks are lost in the transmission and reconstruction.

However, even these error correcting codes do not make sure that corrupting any of the P standard rounds requires as many corruptions as the length of the long message. To ensure this, we repeat these P standard rounds before every block in the long message and only proceed if all these repetitions are consistent with each other, *i.e.* they yield the same transcript. If there are blocks where these P rounds are not consistent with each other, we rewind one block and repeat to (hopefully) get consistency. Ensuring that the repetitions are mutually consistent in turn ensures that the adversary needs to invest a lot of corruptions if he wants to corrupt the P standard rounds. In turn, this ensures that our requirements from the Inner Layer are satisfied.

3 Definitions and Models

3.1 Notations and Preliminaries

Notation. For $d > 0$, the notation $[d] = \{1, 2, \cdots, d\}$ will denote the set of integers at most d. The notation $[a : b)$ will denote the set $[a, b) \cap \mathbb{Z}$, and $(a : b)$, $(a : b]$, and $[a : b]$ are defined analogously. For $n > 0$ and a set S, the set $S^{\leq n}$ is defined to be $\bigcup_{i=0}^{n} S^i$ where S^i denotes the set $\underbrace{S \times S \times \cdots \times S}_{i \text{ times}}$. We also define $S^* = \bigcup_{i \geq 0} S^i$. We use $\|$ to denote concatenation.

For a string $s = s_1 s_2 \cdots s_n$ of length $n > 0$ and $i \in [n]$, we use $s_{\leq i}$ to denote the string $s_1 s_2 \cdots s_i$. We define $s_{<i}$, $s_{>i}$, and $s_{\geq i}$ analogously. For $i_1 < i_2 \in [n]$, we use $s_{(i_1:i_2]}$ or $s(i_1 : i_2]$ to denote $s_{i_1+1} s_{i_1+2} \cdots i_{i_2}$ and $s_{(i_1:i_2)}, s(i_1 : i_2)$ *etc.* are defined analogously. Similarly, for a function $f : X \to Y^n$ (for some sets X, Y, and $n > 0$) and $i \in [n]$, we use f_i to denote the function that on input $x \in X$ outputs the i^{th} coordinate of $f(x)$, and $f_{\leq i}$ to denote the function that outputs the first i coordinates. We similarly define $f_{<i}$, $f_{>i}$, and $f_{\geq i}$. We shall use A and B to denote Alice and Bob respectively, and if $C \in \{A, B\}$, then $\overline{C}$ will denote the unique element in $\{A, B\}$ that is not C. For any vector v, we denote by $|v|$ the number of elements in v.

A distance metric over strings. Let Σ be an alphabet. Consider strings $u, v \in \Sigma^*$. We define the function $\Delta : \Sigma^* \times \Sigma^* \to \mathbb{N}$ as:

$$\Delta(u, v) = ||u| - |v|| + \sum_{i \in [\min(|u|,|v|)]} \mathbb{1}\left(u_i \neq v_i\right).$$

Observe that Δ reduces to the well known notion of Hamming distance when $|u| = |v|$. Just like the Hamming distance, the function Δ defines a metric.

Lemma 3.1. *The function $\Delta(\cdot, \cdot)$ defines a metric over strings.*

Proof. Clearly $\Delta(u, u) = 0$ for all strings u and the function Δ is symmetric. It remains to show the triangle inequality. Let u, v, w be strings. Define $k = \min(|u|, |w|)$. If $|v| \leq k$, we have that:

$$\begin{aligned}
\Delta(u, w) &= ||u| - |w|| + \sum_{i \in [k]} \mathbb{1}(u_i \neq w_i) \\
&= ||u| - |v|| + ||v| - |w|| - 2 \cdot (k - |v|) + \sum_{i \in [k]} \mathbb{1}(u_i \neq w_i) && (\text{As } |v| \leq k) \\
&\leq ||u| - |v|| + ||v| - |w|| + \sum_{i \in [|v|]} \mathbb{1}(u_i \neq w_i) && (\text{As } |v| \leq k) \\
&\leq \Delta(u, v) + \Delta(v, w).
\end{aligned}$$

On the other hand, if $|v| > k = \min(|u|, |v|, |w|)$, we have that:

$$\begin{aligned}
\Delta(u, w) &= ||u| - |w|| + \sum_{i \in [k]} \mathbb{1}(u_i \neq w_i) \\
&\leq ||u| - |v|| + ||v| - |w|| + \sum_{i \in [k]} \mathbb{1}(u_i \neq v_i) + \sum_{i \in [k]} \mathbb{1}(v_i \neq w_i) \\
&\leq \Delta(u, v) + \Delta(v, w),
\end{aligned}$$

where the last step uses $k = \min(|u|, |v|, |w|)$. □

Lemma 3.2. *Let k, l_1, l_2 be integers such that $k \leq l_1$. For strings $s_1 \in \Sigma^{l_1}, s_2 \in \Sigma^{l_2}, t \in \Sigma^k$, we have*

$$\Delta(s_1, t) - \Delta(s_1 \| s_2, t) = -l_2.$$

Proof. Note that

$$\begin{aligned}
\Delta(s_1, t) - \Delta(s_1 \| s_2, t) &= l_1 - k + \sum_{i \in [k]} \mathbb{1}(s_{1,i} \neq t_i) - (l_1 + l_2 - k) - \sum_{i \in [k]} \mathbb{1}(s_{1,i} \neq t_i) \\
&= -l_2.
\end{aligned}$$

□

Lemma 3.3. *Let k, l_1, l_2 be integers such that $l_1 + l_2 \leq k$. For strings $s_1 \in \Sigma^{l_1}, s_2 \in \Sigma^{l_2}, t \in \Sigma^k$, we have*

$$\Delta(s_1 \| s_2, t) \leq \Delta(s_1, t).$$

Proof. Note that

$$\Delta(s_1 \| s_2, t) = k - l_1 - l_2 + \sum_{i \in [l_1]} \mathbb{1}(s_{1,i} \neq t_i) + \sum_{i \in [l_2]} \mathbb{1}(s_{2,i} \neq t_{l_1 + i})$$

$$\leq k - l_1 + \sum_{i \in [l_1]} \mathbb{1}\left(s_{1,i} \neq t_i\right)$$
$$= \Delta(s_1, t).$$

□

3.2 Error Correcting Codes and Tree Codes

We will use error correcting codes, and tree codes extensively in this paper, and we recall these notions in this section.

Error Correcting Codes. We will use the following error correcting codes promised by [SZ99, GL16]. Recall the function $\Delta(v, w)$ defined in Subsection 3.1.

Theorem 3.4. *Fix any finite alphabet Σ and any $\gamma \in (0, 1/2)$. There exists an integer $K_0 = K_0(\gamma)$ and functions $\mathsf{ECC}_\gamma : \Sigma^* \to \Sigma^*$ and $\mathsf{DECC}_\gamma : \Sigma^* \to \Sigma^*$ that can be computed in time polynomial in the length of their input such that the following holds for all $t > 0$:*

- *For all $u \in \Sigma^t$, we have $\mathsf{ECC}_\gamma(u) \in \Sigma^{K_0 t}$. (Rate condition)*
- *For all $u \in \Sigma^t$ and all $\tilde{E} \in \Sigma^*$, we have $\Delta(\tilde{E}, \mathsf{ECC}_\gamma(u)) \leq \gamma K_0 t \implies \mathsf{DECC}_\gamma(\tilde{E}) = u$. (Distance condition)*

We mention that the requirement in Theorem 3.4 is strictly weaker than the 'edit distance' requirement in the works of [SZ99, GL16] as our metric $\Delta(\cdot)$ is larger than edit distance. This weaker requirement will be sufficient for our needs. Additionally working with $\Delta(\cdot)$ allows us to use Lemma 3.2 which will simplify the presentation of some of our arguments.

Remark 3.5. *Let Σ be as in Theorem 3.4. For notational ease, in the rest of this paper, we denote $\mathsf{ECC} = \mathsf{ECC}_{\frac{1}{3}}$, $\mathsf{DECC} = \mathsf{DECC}_{\frac{1}{3}}$, and $K_0 = K_0(1/3)$. Observe that we can assume, without loss of generality, for all $s \in \Sigma^*$ such that $|s| \geq K_0$, we have $\frac{|s|}{2} \leq K_0 \cdot |\mathsf{DECC}(s)| \leq 2|s|$.*

Tree Codes. Tree codes, first introduced by Schulman [Sch93], are 'online' error correcting codes that work even when the input is streaming. We use the following version defined in [BR11].

Definition 3.6 ((α, d, n, Σ)-tree code)**.** *Let $d, n > 0$ be integers and let $\alpha > 0$ be a parameter. Let Σ be a finite set. A d-ary tree code of depth n and distance $\alpha > 0$ over alphabet Σ is defined by an encoding function $\mathsf{TC}_{\alpha,d,n,\Sigma} : [d]^{\leq n} \to \Sigma$ that satisfies the following:*

For all integers $k \leq n$, if we define, for $v = v_1 v_2 \cdots v_k \in [d]^k$, the function $\overline{\mathsf{TC}}_{\alpha,d,n,\Sigma}(v)$ to be $\mathsf{TC}_{\alpha,d,n,\Sigma}(v_1) \| \mathsf{TC}_{\alpha,d,n,\Sigma}(v_1, v_2) \| \cdots \| \mathsf{TC}_{\alpha,d,n,\Sigma}(v_1, v_2, \cdots, v_k)$, then, it holds for all $u = u_1 \cdots u_k, v = v_1 \cdots v_k \in [d]^k$ that

$$\Delta(\overline{\mathsf{TC}}_{\alpha,d,n,\Sigma}(u), \overline{\mathsf{TC}}_{\alpha,d,n,\Sigma}(v)) \geq \alpha \cdot (k - |\mathsf{LCP}(u, v)|).$$

In the above definition, $\mathsf{LCP}(u, v)$ denotes the longest common prefix of the strings u, v. Observe that the way $\overline{\mathsf{TC}}_{\alpha,d,n,\Sigma}$ is defined, it holds that $\overline{\mathsf{TC}}_{\alpha,d,n,\Sigma}(u)$ and $\overline{\mathsf{TC}}_{\alpha,d,n,\Sigma}(v)$ are of length k and agree on the first $|\mathsf{LCP}(u, v)|$ coordinates. Thus, the definition implies that at least a α fraction of the remaining coordinates are different in $\overline{\mathsf{TC}}_{\alpha,d,n,\Sigma}(u)$ and $\overline{\mathsf{TC}}_{\alpha,d,n,\Sigma}(v)$.

The following theorem was first proved by [Sch96]:

Theorem 3.7. *For every $n, d \in \mathbb{N}$, and $0 < \alpha < 1$, there exists a $(\alpha, d, n, [d^{\mathcal{O}_{1-\alpha}(1)}])$-tree code.*

3.3 Communication Models

In this section, we define the two communication models that we work with and establish a connection between these models.

3.3.1 The Communication Model STANDARD

We begin by defining the model STANDARD that captures the 'standard' two party setting with adversarial noise found in the literature. Namely, the protocols in STANDARD have a fixed, predetermined number of rounds such that in every round, Alice sends a message to Bob and then, Bob sends a message to Alice (that may depend on the message he just received). Furthermore, the messages sent by the parties to each other come from a constant sized alphabet Σ.

Note that the execution of a protocol in model STANDARD takes place in the presence of adversarial noise. This means that a small number of messages sent by the parties may be corrupted before they reach the other party. The corruptions are adversarial in the sense that we only record the total number of messages corrupted, and the protocol should work regardless of where these corruptions are (as long as they are below the total number of corruptions allowed).

Next, we formally define the notion of a protocol and an adversary in model STANDARD:

Definition of a protocol. Let $T > 0$ be an integer and Σ be a finite non-empty set. Let X^A, X^B be the set of inputs of Alice and Bob respectively. Similarly, let Y^A, Y^B be the set of outputs of Alice and Bob respectively.

A protocol Π with T rounds and alphabet Σ in model STANDARD is defined by a tuple $\Pi = \{f^C, g^C\}_{C\in\{A,B\}}$. Here[3], the function f^A has type $f^A : X^A \times \Sigma^{<T} \to \Sigma$ and the function f^B has type $f^B : X^B \times \Sigma^{\leq T} \to \Sigma$. Also, for $C \in \{A, B\}$, the function g^C has type $g^C : X^C \times \Sigma^{\leq 2T} \to Y^C$.

[3]Note that the difference of '$<$' *vs.* '$\leq$' in the definition of f^A and f^B above is owing to our convention that Alice speaks first in every round.

Definition of an adversary. Using the same notation as above, we define an adversary $\mathcal{A}$ for the protocol Π. The adversary $\mathcal{A}$ is defined by a pair of functions $(\mathcal{A}^A, \mathcal{A}^B)$ of the type $\mathcal{A}^A, \mathcal{A}^B : X^A \times X^B \to \Sigma^T$.

Recall that we use $\mathcal{A}^A_i$ to denote i^{th} coordinate of $\mathcal{A}^A$ and $\mathcal{A}^A_{\leq i}$ to denote the first i coordinates of $\mathcal{A}^A$, *etc.* We finish this section, by describing how a protocol Π is executed in the presence of adversary $\mathcal{A}$.

Execution of a protocol. The protocol Π proceeds in T rounds. At the beginning of the protocol, Alice has an input $x^A \in X^A$ while Bob has an input $x^B \in X^B$. We maintain the invariant that before she speaks in round i, Alice can compute $\mathcal{A}^A_{<i}(x^A, x^B)$ and before Bob speaks in round i, he can compute $\mathcal{A}^B_{\leq i}(x^A, x^B)$. Additionally, we maintain that after round i, Alice and Bob have transcripts $\pi^A, \pi^B \in \Sigma^{2i}$ respectively. At the beginning of the protocol, $\pi^A = \pi^B = \varepsilon$, the empty string

In round $i \in [T]$, Alice sends the symbol $f^A(x^A, \mathcal{A}^A_{<i}(x^A, x^B))$ to Bob and Bob receives the symbol $\mathcal{A}^B_i(x^A, x^B)$. This is followed by Bob sending the symbol $f^B(x^B, \mathcal{A}^B_{\leq i}(x^A, x^B))$ to Alice and Alice receiving $\mathcal{A}^A_i(x^A, x^B)$. Alice appends $f^A(x^A, \mathcal{A}^A_{<i}(x^A, x^B))$ and $\mathcal{A}^A_i(x^A, x^B)$ to π^A (in that order) while Bob appends $\mathcal{A}^B_i(x^A, x^B)$ and $f^B(x^B, \mathcal{A}^B_{\leq i}(x^A, x^B))$ to π^B.

Observe how the execution preserves our invariant above. Also, note that if $f^A(x^A, \mathcal{A}^A_{<i}(x^A, x^B)) \neq \mathcal{A}^B_i(x^A, x^B)$, then the message from Alice to Bob was corrupted in round i. Similarly, if $f^B(x^B, \mathcal{A}^B_{\leq i}(x^A, x^B)) \neq \mathcal{A}^A_i(x^A, x^B)$, then the message from Bob to Alice was corrupted in round i.

After T rounds are over, the parties output $g^C(x^C, \pi^C)$, where, as usual, $C = A$ for Alice and $C = B$ for Bob.

Observe that the entire execution described above is determined by Π, $\mathcal{A}$, x^A, and x^B. For $C \in \{A, B\}$, we sometimes simply say $\Pi^C_{\mathcal{A}}(x^A, x^B)$ to denote the value of $g^C(x^C, \pi^C)$ in the execution above.

Corruptions. For $r \in [T]$, we define:

$$\mathsf{corr}^{A\to B}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, r) = \mathbb{1}(f^A(x^A, \mathcal{A}^A_{<r}(x^A, x^B)) \neq \mathcal{A}^B_r(x^A, x^B)).$$
$$\mathsf{corr}^{B\to A}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, r) = \mathbb{1}(f^B(x^B, \mathcal{A}^B_{\leq r}(x^A, x^B)) \neq \mathcal{A}^A_r(x^A, x^B)).$$

(S in the aboved notation stands for the model `STANDARD`.) Observe that $\mathsf{corr}^{A\to B}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, r) = 1$ if and only if the message from Alice to Bob was corrupted in round r. Similarly $\mathsf{corr}^{B\to A}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, r) = 1$ if and only if the message from Bob to Alice was corrupted in round r. Also, define:

$$\mathsf{corr}^{A\to B}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, \leq r) = \sum_{i\in[r]} \mathsf{corr}^{A\to B}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, i).$$
$$\mathsf{corr}^{B\to A}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, \leq r) = \sum_{i\in[r]} \mathsf{corr}^{B\to A}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, i).$$

The total number of corruptions is defined to be:

$$\mathsf{corr}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, \leq r) = \mathsf{corr}^{A\to B}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, \leq r) + \mathsf{corr}^{B\to A}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, \leq r).$$

Finally, we define $\mathsf{corr}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B) = \mathsf{corr}_{\mathrm{S},\Pi,\mathcal{A}}(x^A, x^B, \leq T)$. We omit the subscripts from the above definition when they are clear from context.

Noiseless Adversary. Observe that for every protocol Π, there is a unique adversary $\mathcal{A}^*$ that satisfies $\mathsf{corr}_{\mathrm{S},\Pi,\mathcal{A}^*}(x^A, x^B) = 0$. We call this the *noiseless adversary* for Π and define $\Pi^C(x^A, x^B) = \Pi^C_{\mathcal{A}^*}(x^A, x^B)$ for $C \in \{A, B\}$.

3.3.2 The Communication Model `LONG`

To improve the presentation of our interactive coding scheme, we define a new communication model called model `LONG`. We remark that the model `LONG` is somewhat unrealistic and we only use it to make the proof of correctness of our interactive coding scheme simpler.

The key difference between the model `LONG` and the model `STANDARD` is that the former has an additional parameter that we call the 'period' and denote by P. The total number of rounds in any protocol in model `LONG` will be a multiple of $P + 1$. These rounds will be exactly like the rounds in a protocol in model `STANDARD`, except that every $(P+1)^{\text{th}}$ round, the parties can send arbitrarily many symbols from Σ (based on the transcript so far).

Due to the fact that there are rounds where the parties can send more than one symbol from Σ, the total number of symbols sent in the protocol may not be determined by the number of rounds. We will use R to denote the number of rounds in the protocol and have an additional parameter, S, to capture the number of symbols exchanged by any party during the protocol (We will define S formally later).

We now proceed to define the notion of a protocol and an adversary more formally. Note that the adversaries in model `LONG` can insert/delete symbols in the rounds that are multiples of $P + 1$. This is done to avoid signaling, as the messages in these rounds can be of different lengths (see [GK17] and references therein for a good discussion of signaling).

We also note that in model `LONG`, the corruptions inserted by the adversary are counted in a way such that even if the adversary corrupts only one symbol in the rounds $(c(P + 1) : (c+1)(P+1)]$, for some $c \geq 0$, it has to spend as many corruptions as the total communication in rounds $(c(P + 1) : (c + 1)(P + 1)]$. This way of counting the corruptions is justified by using appropriate (interactive) error correction.

Definition of a protocol. Let Σ be a finite set with a special symbol $\perp$ and let $P, R, S > 0$ be integers such that S is a multiple of P and R is a multiple of $P+1$. As before, let X^A, X^B be the set of inputs of Alice and Bob respectively. Similarly, let Y^A, Y^B be the set of outputs of Alice and Bob respectively.

A protocol Π with R rounds, period P, with alphabet Σ, and a length of S symbols in

model LONG is defined by a tuple $\Pi = \{f^C, g^C\}_{C\in\{A,B\}}$. Here[4], the function f^A has type $f^A : X^A \times (\Sigma^*)^{<R} \to \Sigma^*$ and the function f^B has type $f^B : X^B \times (\Sigma^*)^{\leq R} \to \Sigma^*$. Also, for $C \in \{A, B\}$, the function g^C has type $g^C : X^C \times (\Sigma^*)^{\leq R} \to Y^C$.

To reflect the fact that in every $(P+1)^{\text{th}}$ round, the parties can send arbitrarily long messages to each other, we make sure that the functions f^A and f^B satisfy an additional property. For the function f^A, we require that unless the second input is in $(\Sigma^*)^{k(P+1)-1}$, for some integer k, the function will only take values in Σ, and for the function f^B, we require that unless the second input is in $(\Sigma^*)^{k(P+1)}$, for some integer k, the function will only take values in Σ.

Similarly, to reflect the fact that the parties communicate at most S symbols, we ensure that after S symbols have been communicated (sent/received) by any party, the party can only send and receive $\perp$. This is done by ensuring that, for all $\pi \in (\Sigma^*)^{<R}$ and $i \in [R]$, we have:

$$\begin{aligned}
&\sum_{i'<i}|\pi_{i'}| + \sum_{i'<i}|f^A(x^A, \pi_{<i'})| < S \implies \sum_{i'<i}|\pi_{i'}| + \sum_{i'\leq i}|f^A(x^A, \pi_{<i'})| \leq S. \\
&\sum_{i'<i}|\pi_{i'}| + \sum_{i'<i}|f^A(x^A, \pi_{<i'})| \geq S \implies f^A(x^A, \pi_{<i}) = \begin{cases} \perp^P & , (P+1) \text{ divides } i \\ \perp & , \text{ otherwise} \end{cases}.
\end{aligned} \tag{1}$$

In the foregoing equation, $\perp^P$ denotes $\perp$ concatenated to itself P times. Analogous constraints hold for Bob as well.

Definition of an adversary. Using the same notations as above, we define an adversary $\mathcal{A}$ for Π. The adversary $\mathcal{A}$ is defined by a pair of functions $(\mathcal{A}^A, \mathcal{A}^B)$ where $\mathcal{A}^A, \mathcal{A}^B : X^A \times X^B \to (\Sigma^*)^R$. As before, for $i \in [R]$, we use $\mathcal{A}^A_i$ (resp. $\mathcal{A}^B_i$) and $\mathcal{A}^A_{\leq i}$ (resp. $\mathcal{A}^B_{\leq i}$) to denote the i^{th} coordinate and the first i coordinates of $\mathcal{A}^A$ (resp. $\mathcal{A}^B$) respectively.

We require that if $i \in [R]$ is not a multiple of $P+1$, then $\mathcal{A}^A_i, \mathcal{A}^B_i$ take values in Σ. This ensures that if i is not a multiple of $P+1$, then the parties receive exactly one symbol in round i.

Execution of a protocol. We now describe an execution of a protocol Π in model LONG in the presence of adversary $\mathcal{A}$. We use the same notation as above. At the beginning of the protocol, Alice and Bob have inputs $x^A \in X^A$ and $x^B \in X^B$ respectively. We will maintain the invariant that before Alice speaks in round $i \in [R]$, she knows the value of $\mathcal{A}^A_{<i}(x^A, x^B)$. Similarly, we will maintain that before Bob speaks in round i, he knows the value of $\mathcal{A}^B_{\leq i}(x^A, x^B)$.

In round $i \in [R]$, Alice sends $f^A(x^A, \mathcal{A}^A_{<i}(x^A, x^B))$ to Bob while Bob receives $\mathcal{A}^B_i(x^A, x^B)$. This is followed by Bob sending $f^B(x^B, \mathcal{A}^B_{\leq i}(x^A, x^B))$ to Alice and Alice receiving $\mathcal{A}^A_i(x^A, x^B)$. Observe how this execution maintains are invariant above.

[4]Again, the difference of '$<$' *vs.* '$\leq$' in the definition of f^A and f^B above is owing to our convention that Alice speaks first in every round.

Finally, after round R, for all $C \in \{A, B\}$, party C outputs $g^C(x^C, \mathcal{A}^C_{\leq R}(x^A, x^B))$. Recall that $C = A$ for Alice and $C = B$ for Bob.

Observe that the entire execution described above is determined by Π, $\mathcal{A}$, x^A, and x^B. For $C \in \{A, B\}$, we sometimes simply say $\Pi^C_{\mathcal{A}}(x^A, x^B)$ to denote the value of $g^C(x^C, \mathcal{A}^C_{\leq R}(x^A, x^B))$ in the execution above.

Corruptions. To finish this section, for $r \in [R/(P+1)]$, we define the function $\mathsf{corr}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r)$ that measures the number of corruptions inserted by the adversary in the rounds $((r-1)(P+1) : r(P+1)]$ (L in these definitions stands for the model LONG). We have:

$$\mathsf{disc}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) = \mathbb{1}\left(\exists i' \in [P+1] : f^A(x^A, \mathcal{A}^A_{<(r-1)(P+1)+i'}(x^A, x^B)) \neq \mathcal{A}^B_{(r-1)(P+1)+i'}(x^A, x^B)\right).$$
$$\mathsf{disc}^{B\to A}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) = \mathbb{1}\left(\exists i' \in [P+1] : f^B(x^B, \mathcal{A}^B_{\leq(r-1)(P+1)+i'}(x^A, x^B)) \neq \mathcal{A}^A_{(r-1)(P+1)+i'}(x^A, x^B)\right).$$
$$\mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) = \mathsf{disc}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) \cdot \max\left(|f^A(x^A, \mathcal{A}^A_{<r(P+1)}(x^A, x^B))|, |\mathcal{A}^B_{r(P+1)}(x^A, x^B)|\right).$$
$$\mathsf{corr}^{B\to A}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) = \mathsf{disc}^{B\to A}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) \cdot \max\left(|f^B(x^B, \mathcal{A}^B_{\leq r(P+1)}(x^A, x^B))|, |\mathcal{A}^A_{r(P+1)}(x^A, x^B)|\right).$$
$$\mathsf{corr}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) = \mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) + \mathsf{corr}^{B\to A}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r).$$

(In the above notation disc stands for discrepancy.) We omit the subscripts from the above definition when they are clear from context and define $\mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, \leq r) = \sum_{i\in[r]} \mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, i)$ and $\mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B) = \mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, \leq R/(P+1))$. We define $\mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, \leq 0) = 0$ for convenience and use analogous definitions for $\mathsf{corr}^{B\to A}_{\mathrm{L},\Pi,\mathcal{A}}$ and $\mathsf{corr}_{\mathrm{L},\Pi,\mathcal{A}}$.

3.4 Formal Statement of the Main Theorem

Having defined our communication models, we are ready to formally state our main theorem.

Theorem 3.8 (Formal statement of Theorem 1.1)**.** *There exists constant η, η', θ such that the following holds:*

Let $\Sigma, X^A, X^B, Y^A, Y^B$ be sets as in Subsection 3.3. Let $\Pi = \{f^C, g^C\}_{C\in\{A,B\}}$ be a protocol in model STANDARD *with $T > 2^{200K_0+10^5\theta_2}$ rounds and alphabet Σ. Furthermore, the input and output sets of Alice (resp. Bob) in Π are X^A and Y^A (resp. X^B and Y^B) respectively.*

Then, there is a protocol $\Pi' = \{f'^C, g'^C\}_{C\in\{A,B\}}$ in model STANDARD *with $T' = \eta T$, alphabet Σ, and the same input and outputs sets for the two parties such that for every adversary $\mathcal{A}'$ for Π' in model* STANDARD*, and all inputs $x^A \in X^A$ and $x^B \in X^B$, and $C \in \{A, B\}$, we have that*

$$\mathsf{corr}_{\mathrm{S},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta T' \implies \Pi'^C_{\mathcal{A}'}(x^A, x^B) = \Pi^C(x^A, x^B).$$

Furthermore, the functions f'^C and g'^C, for $C \in \{A, B\}$ make use of the function $\mathsf{TC} = \mathsf{TC}_{1-10^{-5},|\Sigma|^{2\log(\eta' T)},\eta' T/\log(\eta' T),\Sigma^{K\log(\eta' T)}}(\cdot)$ (for a large enough constant K so that Theorem 3.7 holds) and can be computed in time polynomial in T given oracle access to the functions f^C and g^C, where $C \in \{A, B\}$, and oracle access to the function TC.

Remark 3.9. *There exists $\eta_0 > 0$ such that Theorem 3.8 holds for $\eta = \eta_0$ and $\theta = \frac{1}{10}$ for the weaker requirement that the functions f'^C and g'^C, for $C \in \{A, B\}$ can be computed in time exponential in T. For this weaker requirement, oracle access to TC is not necessary for the furthermore part.*

For the rest of this paper, we reserve η_0 to denote the constant from Remark 3.9.

4 Relation Between Model STANDARD and model LONG

Recall that our goal in Theorem 3.8 is to describe an interactive coding scheme in model STANDARD. Instead of showing such a scheme, we actually show an interactive coding scheme in model LONG and a general transformation from protocols in model LONG to protocols in model STANDARD. This section formalizes and proves the transformation (see Theorem 4.1), while the next section constructs the interactive coding scheme in model LONG.

Theorem 4.1. *For all $\theta_2 > 10^{-20}$, there exist constant η_1, θ_1 such that for $\eta_2 = 10^5\theta_2 + 100K_0$, the following holds:*

Let $\Sigma, X^A, X^B, Y^A, Y^B$ be sets as in Subsection 3.3 above. Let $P, R, S > 0$ be integers such that $2\log S > P \geq \log S > 100(K_0 + \log\eta_2)$. Let $\Pi = \{f^C, g^C\}_{C\in\{A,B\}}$ be a protocol in model LONG with R rounds, period P, alphabet Σ and length of S symbols. Furthermore, the input and output sets of Alice (resp. Bob) in Π are X^A and Y^A (resp. X^B and Y^B) respectively.

Then, there is a protocol $\Pi' = \{f'^C, g'^C\}_{C\in\{A,B\}}$ in model STANDARD with $T = \eta_1 S$ rounds and alphabet Σ with the same input and output sets for the two parties such that for every adversary $\mathcal{A}'$ for Π' in model STANDARD, there is an adversary $\mathcal{A}$ for Π in model LONG such that for all inputs $x^A \in X^A$ and $x^B \in X^B$, we have

1. *For all $C \in \{A, B\}$, we have that $\Pi^C_{\mathcal{A}}(x^A, x^B) = \Pi'^C_{\mathcal{A}'}(x^A, x^B)$. Furthermore, the functions f'^C and g'^C, for $C \in \{A, B\}$ can be computed in time polynomial in S assuming oracle access to the functions f^C and g^C, where $C \in \{A, B\}$.*
2. *It holds that $\mathsf{corr}_{\mathrm{S},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta_1 T \implies \mathsf{corr}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B) \leq \theta_2 S$.*

We devote the rest of this section to proving Theorem 4.1. We shall use the following claim:

Claim 4.2. *For all $\theta_2 > 10^{-20}$, if $\eta_2 = 10^5\theta_2 + 100K_0$, then the following holds:*

Let $\Sigma, X^A, X^B, Y^A, Y^B$ be sets as in Subsection 3.3 above. Let $P, R, S > 0$ be integers such that $2\log S > P \geq \log S > 100(K_0 + \log\eta_2)$. Let $\Pi = \{f^C, g^C\}_{C\in\{A,B\}}$ be a protocol

in model LONG *with R rounds, period P, alphabet Σ and length of S symbols. Furthermore, the input and output sets of Alice (resp. Bob) in Π are X^A and Y^A (resp. X^B and Y^B) respectively. Then, there is a protocol $\hat{\Pi} = \{\hat{f}^C, \hat{g}^C\}_{C\in\{A,B\}}$ in model* LONG *such that:*

1. *The protocol $\hat{\Pi}$ has a length of $\hat{S} = \eta_2 S$ symbols, $\hat{R} = \frac{\hat{S}(P+1)}{10P}$ rounds, and period $\hat{P} = P$.*

2. *For all $r \in [\hat{R}/(P+1)]$, the number of symbols transmitted by the parties in round $r(P+1)$ in $\hat{\Pi}$ is $4P$ regardless of the inputs of Alice and Bob. This means that, without loss of generality, we can assume that the number of symbols received by Alice and Bob is also $4P$.*

3. *For every adversary $\hat{\mathcal{A}}$ for $\hat{\Pi}$ in model* LONG*, there is an adversary $\mathcal{A}$ for Π in model* LONG *such that for all inputs $x^A \in X^A$ and $x^B \in X^B$, we have*

   (a) *For all $C \in \{A, B\}$, we have that $\Pi^C_{\mathcal{A}}(x^A, x^B) = \hat{\Pi}^C_{\hat{\mathcal{A}}}(x^A, x^B)$. Furthermore, the functions $\hat{f}^C$ and $\hat{g}^C$, for $C \in \{A, B\}$ can be computed in time polynomial in S assuming oracle access to the functions f^C and g^C, where $C \in \{A, B\}$.*

   (b) *It holds that $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B) \le \theta_2 S/100 \implies \mathsf{corr}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B) \le \theta_2 S$.*

We prove this claim in Subsection 4.1 and first show how Theorem 4.1 follows from it.

Proof of Theorem 4.1 assuming Claim 4.2. Let $\theta_2 > 10^{-20}$ be fixed. Define $\eta_1 = \frac{\eta_0+8K_0}{10}$ and $\theta_1 = \frac{\theta_2}{800\eta_1} \cdot \min(\eta_0/10, K_0)$. Let $\hat{\Pi}$ in model LONG be as promised by Claim 4.2. Define a protocol Π' in model STANDARD with $T' = \eta_1 S$ rounds and the same input and output sets and alphabet as Π as follows:

When the inputs to the parties are x^A and x^B, then, in protocol Π', Alice and Bob execute the protocol in Algorithm 1 $\hat{R}/(P+1)$ times, where the transcripts input to any execution are the outputs of the previous execution. After $\hat{R}/(P+1)$ executions, the parties output $\hat{g}^C(x^C, \hat{\tau}^C)$, where $\hat{\tau}^C$ is output of the last, *i.e.*, the $(\hat{R}/(P+1))^{\text{th}}$ execution.

We claim that Π' satisfies Theorem 4.1. Consider any adversary $\mathcal{A}'$ for Π' in model STANDARD and let x^A and x^B be inputs for Alice and Bob. From Algorithm 1, this adversary defines a value $\hat{\tau}^C \in (\Sigma^*)^*$ for $C \in \{A, B\}$, which is the transcript output by the $(\hat{R}/(P+1))^{\text{th}}$ execution. Furthermore, observe from Algorithm 1 that $|\hat{\tau}^A_r| = |\hat{\tau}^B_r| = 4P$, if r is a multiple of $P+1$, and $|\hat{\tau}^A_r| = |\hat{\tau}^B_r| = 1$ otherwise. Define an adversary $\hat{\mathcal{A}}$ for $\hat{\Pi}$ in model LONG such that $\hat{\mathcal{A}}^C(x^A, x^B) = \hat{\tau}^C$ for $C \in \{A, B\}$. Finally, define $\mathcal{A}$ for Π in model LONG to be the one promised by item 3 above.

We claim that $\mathcal{A}$ satisfies Theorem 4.1. Indeed, the first part holds because, by item 3a, we have $\Pi^C_{\mathcal{A}}(x^A, x^B) = \hat{\Pi}^C_{\hat{\mathcal{A}}}(x^A, x^B) = \hat{g}^C(x^C, \hat{\tau}^C) = \Pi'^C_{\mathcal{A}'}(x^A, x^B)$. The furthermore part follows straightforwardly from the definition of Algorithm 1 and the furthermore part of item 3a together with Theorem 3.4 and Remark 3.9. The second part also holds because if $\mathsf{corr}_{\mathrm{S},\Pi',\mathcal{A}'}(x^A, x^B) \le \theta_1 T = \theta_1\eta_1 S$, then

$$\mathsf{corr}_{\mathrm{S},\Pi',\mathcal{A}'}(x^A, x^B, \le \frac{10\eta_1}{\eta_2} i) - \mathsf{corr}_{\mathrm{S},\Pi',\mathcal{A}'}(x^A, x^B, \le \frac{10\eta_1}{\eta_2}(i-1)) > \frac{800\theta_1\eta_1}{\theta_2} P,$$

for at most $\theta_2 S/(800P)$ values of $i \in [\hat{R}/(P+1)]$. Due to Remark 3.9 and Theorem 3.4, if i is not one of these values, we have that $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i) = 0$. This means that $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B) \leq \theta_2 S/100$ implying that $\mathsf{corr}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B) \leq \theta_2 S$, as required.

□

Algorithm 1 Compiling one block of the protocol $\hat{\Pi}$.

Input: For $C \in \{A, B\}$, party C has an input $x^C \in X^C$ and a transcript $\hat{\pi}^C \in (\Sigma^*)^*$. It holds that the $|\hat{\pi}^C|$ is a multiple of $P+1$.

Output: For $C \in \{A, B\}$, the party C outputs a transcript $\hat{\tau}^C \in (\Sigma^*)^*$. It holds that $|\hat{\tau}^C| = |\hat{\pi}^C| + P + 1$.

1: Alice and Bob simulate the next P rounds of the protocol $\hat{\Pi}$ assuming inputs x^C and transcript $\hat{\pi}^C$, as follows: Let $\mathfrak{C} = \{f^C_{\mathfrak{C}}, g^C_{\mathfrak{C}}\}_{C \in \{A,B\}}$ be a protocol in model `STANDARD` with P rounds such that, for $C \in \{A, B\}$, we have

- $f^C_{\mathfrak{C}}(x^C, \varsigma) = \hat{f}^C(x^C, \hat{\pi}^C \| \varsigma)$ for all $\varsigma \in \Sigma^*$. (Here, on the right hand side, we consider ς to be an element of $(\Sigma^*)^*$, by considering each of its coordinates to be an element of Σ^*.)
- $g^A_{\mathfrak{C}} : X^C \times \Sigma^{2P} \to (\Sigma^*)^P$ (resp. $g^B_{\mathfrak{C}}$) is the function that outputs all the even (resp. odd) coordinates of its second argument (seen as elements of Σ^*).

Let $\mathfrak{C}'$ be the protocol with $\eta_0 P$ rounds promised by Remark 3.9 when applied to $\mathfrak{C}$. The parties execute $\mathfrak{C}'$ for $\eta_0 P$ rounds and get output τ_1^C.

2: For the next $4K_0P$ rounds, Bob sends $\perp$ while Alice sends the symbols in $\mathsf{ECC}(\hat{f}^A(x^A, \hat{\pi}^A \| \tau_1^A))$ one by one. Let $\tau_2^B \in \Sigma^*$ denote the string of symbols received by Bob and define $\hat{\tau}^B \leftarrow \hat{\pi}^B \| \tau_1^B \| \mathsf{DECC}(\tau_2^B)$.

3: For the next $4K_0P$ rounds, Alice sends nothing while Bob sends the symbols in $\mathsf{ECC}(\hat{f}^B(x^B, \hat{\tau}^B))$ one by one. Let $\tau_2^A \in \Sigma^*$ denote the string of symbols received by Alice and define $\hat{\tau}^A \leftarrow \hat{\pi}^A \| \tau_1^A \| \mathsf{DECC}(\tau_2^A)$.

4: Alice outputs $\hat{\tau}^A$ and Bob outputs $\hat{\tau}^B$.

4.1 Proof of Claim 4.2

Henceforth, we concentrate on proving Claim 4.2. Let Π be a protocol as in the statement of Claim 4.2. As Π is in model `LONG` with period P, the players can send arbitrarily long messages every $(P+1)^{\text{th}}$ round. Define the set of messages:

$$\mathsf{Long} = \{z \mid \exists k > 0 : z = 2k(P+1) \text{ or } z = 2k(P+1) - 1\}, \tag{2}$$

and note that an integer z is in the definition of Long if and only if the z^{th} message in Π can be arbitrarily long. We emphasize that in Long, we count the number of *messages*, and not the number of rounds, which explains the factor of 2. We assume that the number of symbols sent by the parties in the long messages is a multiple of P. This is without loss of

generality as it can be ensured by blowing up the total number of symbols sent by a factor of at most 2.

We define the protocol $\hat{\Pi}$ in Algorithm 2. In fact, Algorithm 2 only describes Alice's side of $\hat{\Pi}$. Bob's side of $\hat{\Pi}$ is symmetric. Before we analyze Algorithm 2, we give some intuition behind its definition.

4.1.1 Intuition and Description of Algorithm 2

Many of the ideas in Algorithm 2 are similar to ideas we've already described in Section 2, and we keep this part brief and simple.

In order to compile the protocol Π to the protocol $\hat{\Pi}$, we replace the long messages in Π by messages in Σ^P. We do this by encoding these long messages using an error-correcting code resilient to insertion deletion errors and the breaking the encoded messages into smaller messages in Σ^P. Our assumption that the number of symbols sent by the parties in the long messages is a multiple of P kicks in here, and allows us to break the long messages into *blocks* of length P without having to worry about rounding issues.

Along with sending each message block by block, we also send some auxiliary information with the blocks. This auxiliary information consists of the message number m, the block number c, a Boolean variable e, that indicates whether or not this block is the last one in the message, and another Boolean variable $flag$ whose purpose we describe later.

The auxiliary information sent with each message requires at most logarithmic (in S) number of symbols to share (up to constant factors). This is where our assumption that $P \geq \log(S)$ kicks in. Since the parties only send the auxiliary information once per block, and $P \geq \log(S)$, this information only adds a constant factor to the total communication.

In addition to the long messages in Π, the parties also need to send messages consisting of a single symbol from Σ. In our protocol, these messages are sent in the rounds that are not multiples of $P + 1$ and are repeated before each block in the long message (Line 9). Moreover, a block is only added to the long message if the short messages received before the block are consistent with those received previously. This is controlled by the variable $flag$.

Once the parties receive these long and short messages, they check in Line 19 if the auxiliary information matches. If yes, they add these messages to the variable msgs, which records the transcript of Π. If not, then the parties resynchronize (using ideas similar to those described in Subsection 2.3 and Subsection 2.4 (see also Subsubsection 5.1.2).

Notation. The most important variable in Algorithm 2 is the variable msgs that takes values in $(\Sigma^*)^*$ and records the transcript of Π, as it is being simulated. We consider this variable as a list and in Algorithm 2, we make sure that the last coordinate in this list always the empty string ε unless we are in the middle of communicating a long message. Adopting this convention helps us to easily detect whether or not we are in the middle of sending a long message. It also helps make our notation in the analysis a little cleaner.

In addition, we use the following notation:

- **Length of the list:** We will use $|\mathsf{msgs}|$ to denote the number of elements in msgs.
- **Accessing an element in the list:** For $1 \leq i \leq |\mathsf{msgs}|$, the notation msgs_i denotes the i^{th} element in msgs. When $i = |\mathsf{msgs}|$, we sometimes use $\mathsf{msgs}.\mathit{last}$ instead of msgs_i.[5]
- **Adding elements to the list:** When we wish to add an element $\sigma \in \Sigma^*$ to msgs, we denote this by $\mathsf{msgs}.\textsc{Add}(\sigma)$. The element σ is then added at the end of the list.
- **Removing elements in the list:** When we wish to remove the last element from msgs, we write $\mathsf{msgs}.\textsc{Rem}()$. After this operation, the list has one less element. We write $\mathsf{msgs}.\textsc{Rem}(i)$ to denote the operation of removing the last i elements in the list.

The notation $\mathsf{msgs}_{\mathrm{B}}$ will be used to denote the sublist of msgs that contains all the elements in even positions in msgs. This notation derives from the fact that the even messages in Π are messages from Bob to Alice. We similarly define $\mathsf{msgs}_{\mathrm{A}}$. Additionally, for $z > 0$, the notation $\mathsf{msgs}_{\mathrm{B},\leq z}$ denotes the elements in the first z even positions of msgs, *i.e.*, the first z positions of $\mathsf{msgs}_{\mathrm{B}}$. We similarly define $\mathsf{msgs}_{\mathrm{B},z}$, $\mathsf{msgs}_{\mathrm{B},<z}$, $\mathsf{msgs}_{\mathrm{A},z}$, $\mathsf{msgs}_{\mathrm{A},\leq z}$, and $\mathsf{msgs}_{\mathrm{A},<z}$. Finally, we use $\mathsf{DECC}(\mathsf{msgs}_{\mathrm{B}})$ to denote the list obtained by applying DECC to all the elements of $\mathsf{msgs}_{\mathrm{B}}$ that occur at coordinates that are multiples of $P+1$. We define $\mathsf{DECC}(\mathsf{msgs}_{\mathrm{B},\leq z})$, $\mathsf{DECC}(\mathsf{msgs}_{\mathrm{A}})$, $\mathsf{DECC}(\mathsf{msgs}_{\mathrm{A},\leq z})$ similarly.

Analogous notation is defined for the variables $\mathsf{D\text{-}msgs}'$ and $\mathsf{D\text{-}msgs}$.

A guide to Algorithm 2. The protocol $\hat{\Pi}$ proceeds in $\hat{R}/(P+1)$ iterations, maintaining a variable msgs that records the transcript simulated so far. Our protocol has the invariant that the last message in msgs is always ε, unless we are in the middle of sending a long message. In Line 7, we denote by $m = |\mathsf{msgs}|$, and we consider the index $\mathit{ind} \leftarrow (P+1) \cdot (\lceil m/(2(P+1)) \rceil - 1)$. The value ind captures the prefix of msgs containing chunks that have been *completely* simulated.

In Lines 8-15, one chunk of the underlying protocol Π is being executed. If $m \notin \mathsf{Long}$, then this chunk corresponds to the next chunk after msgs. If $m \in \mathsf{Long}$, then this chunk corresponds to the last chunk in msgs, and hence this is a re-execution. The reason for the re-execution is as stated in Subsection 2.4: Namely, if $m \in \mathsf{Long}$, then the parties are in the middle of transmitting a long message, and want to make sure that each block of the long message is sent with the same set of P short messages. If the P messages in the re-execution differ from the previous execution, then a flag is raised and the parties (later) act on this flag and rewind one block.

After simulating a chunk of the protocol, in Line 18 the parties exchange messages of length $4P$. If it is Bob's turn to speak (m is even), then Alice sends $\sigma = \perp^P$, and if it is

[5] In particular, if $\mathsf{msgs} = [\varepsilon]$ then $|\mathsf{msgs}| = 1$ and $|\mathsf{msgs}_1| = 0$. Namely, we consider the empty message as a message of length 0.

Alice's turn to speak then she sends her next block of her long message, also denoted by σ (if $m \notin \mathsf{Long}$ then σ is the first block of her long message). In addition to σ she also sends the following auxiliary variables: m indicating the number of messages in msgs, c indicating the length of the last message in msgs, σ which is the next block of the long message, e indicating whether we are done sending the long message or not, and $flag$ indicating whether an inconsistency was found in the last chunk.

If everything seems to be consistent (and there are no flags), then Alice appends to msgs either the message $\tilde{\sigma}$ that she received from Bob, or her own message σ, depending on whether it is Bob's turn to speak or her turn to speak. This is done in Line 20. In addition she adds ε to msgs if the party finished sending their long message, as indicated by the variable e or $\tilde{e}$, respectively. This is done in Line 22.

If things are not consistent, then Alice does the following:

1. If $m \notin \mathsf{Long}$, which corresponds to the case that we simulated a new chunk in Lines 8-15, then Alice removes her last $2P$ messages. This is done by removing the last $2P+1$ messages (which includes ε which is always appended to msgs unless we are in the middle of transmitting a long message), and then appending ε. This is done in Line 25.

2. If Alice is ahead of Bob (namely, $(\tilde{m}, \tilde{c}) \leq (m, c)$) and an inconsistency was found ($i.e.$, $\neg(flag \wedge \tilde{flag})$) then Alice distinguishes between the following cases:

   (a) If $c = 0$ and $m - 1 \notin \mathsf{Long}$, which corresponds to the case that in Line 7, it is Alice's turn to send her long message, but she hasn't started sending it yet, then Alice removes the last $2P$ messages from msgs as above (by removing $2P + 1$ messages and adding ε).

   (b) Otherwise, Alice would like to delete the last P symbols from her last long message. To do this she first checks if $c = 0$ and $m - 1 \in \mathsf{Long}$, which corresponds to the case that in Line 7 it is Bob's turn to send his long message, but he hasn't started sending it yet. In this case, Alice first removes ε from msgs, which is the last message in msgs. This is followed by Alice deleting the last P symbols from the last message in msgs.

Algorithm 2 The protocol $\hat{\Pi}$ in the proof of Claim 4.2 (Alice's side).

Input: An input $x^A \in X^A$.

Output: An element in Y^A.

$\mathsf{msgs} \leftarrow [\varepsilon]$.
for $i \in [\hat{R}/(P+1)]$ **do**
  $m \leftarrow |\mathsf{msgs}|$, $c \leftarrow |\mathsf{msgs}.last|$, $flag \leftarrow \texttt{True}$, $ind \leftarrow (P+1) \cdot (\lceil m/(2(P+1)) \rceil - 1)$.
  for $j \in [P]$ **do**
    Send $\sigma = f^A(x^A, \mathsf{DECC}(\mathsf{msgs}_{\mathrm{B},<ind+j}))$ to Bob and receive $\tilde{\sigma} \in \Sigma$.
    if $m \in \mathsf{Long}$ **then**
      If $\mathsf{msgs}_{\mathrm{B},ind+j} \neq \tilde{\sigma}$, then $flag \leftarrow \texttt{False}$.
    else
      Do $\mathsf{msgs}.last \leftarrow \sigma$ followed by $\mathsf{msgs}.\textsc{Add}(\tilde{\sigma})$ and $\mathsf{msgs}.\textsc{Add}(\varepsilon)$.
    end if
  end for
  $longmsg \leftarrow \mathsf{ECC}(f^A(x^A, \mathsf{DECC}(\mathsf{msgs}_{\mathrm{B},<ind+P+1})))$, $e \leftarrow \texttt{True}\,(c = |longmsg| - P)$.
  If $m \bmod 2 = 0$, then, we set $\sigma \leftarrow \perp^P$. Otherwise, set $\sigma \leftarrow longmsg(c : c+P]$.
  Send $M = (m, c, e, \sigma, flag)$ to Bob and receive $\tilde{M} = (\tilde{m}, \tilde{c}, \tilde{e}, \tilde{\sigma}, \tilde{flag})$. These messages are padded to contain $4P$ symbols from Σ. Our choice of P, S makes this possible as $m, c \leq 2^{4P/3}$, e and $flag$ are Boolean, and $\sigma \in \Sigma^P$.
  if $(\tilde{m}, \tilde{c}) = (m, c)$ **and** $flag \wedge \tilde{flag}$ **then**
    If $m \bmod 2 = 0$, then, $\mathsf{msgs}.last \leftarrow \mathsf{msgs}.last \| \tilde{\sigma}$. Else, $\mathsf{msgs}.last \leftarrow \mathsf{msgs}.last \| \sigma$.
    if (e **and** $m \bmod 2 = 1$) **or** ($\tilde{e}$ **and** $m \bmod 2 = 0$) **then**
      $\mathsf{msgs}.\textsc{Add}(\varepsilon)$.
    end if
  else
    If $m \notin \mathsf{Long}$, do $\mathsf{msgs}.\textsc{Rem}(2P+1)$ followed by $\mathsf{msgs}.\textsc{Add}(\varepsilon)$.
    if $(\tilde{m}, \tilde{c}) \leq (m, c)$ **then**
      if $c = 0$ **and** $m - 1 \notin \mathsf{Long}$ **then**
        Do $\mathsf{msgs}.\textsc{Rem}(2P+1)$ followed by $\mathsf{msgs}.\textsc{Add}(\varepsilon)$.
      else
        if $c = 0$ **then**
          $\mathsf{msgs}.\textsc{Rem}()$.
        end if
        $\mathsf{msgs}.last \leftarrow \mathsf{msgs}.last[1 : |\mathsf{msgs}.last| - P]$.
      end if
    end if
  end if
end for
$\mathsf{D\text{-}msgs}' \leftarrow \mathsf{msgs}$. If $|\mathsf{D\text{-}msgs}'|$ is odd or $\mathsf{D\text{-}msgs}'.last = \varepsilon$, do $\mathsf{D\text{-}msgs}'.\textsc{Rem}()$.
$\mathsf{D\text{-}msgs} \leftarrow \mathsf{D\text{-}msgs}'$. Pad $\mathsf{D\text{-}msgs}$ so that $|\mathsf{D\text{-}msgs}| \geq 2R$, by adding $\perp$ in coordinates $\notin \mathsf{Long}$ and $\mathsf{ECC}(\perp^P)$ in coordinates $\in \mathsf{Long}$. Output $g^C(x^C, \mathsf{DECC}(\mathsf{D\text{-}msgs}_{\mathrm{B},\leq R}))$.

4.1.2 Analyzing Algorithm 2 (Proof of Claim 4.2)

Having defined the protocol $\hat{\Pi}$, we now show that it satisfies the properties in item 1 to item 3 in Claim 4.2. Observe that item 1 and item 2 are easily seen to hold from the definition of $\hat{\Pi}$ and we only need to show item 3. We fix an adversary $\hat{\mathcal{A}}$ for $\hat{\Pi}$ and construct an adversary $\mathcal{A}$ for Π such that item 3 holds.

In what follows, and for the remainder of this section, we fix inputs $x^A \in X^A$ and $x^B \in X^B$ for the two parties, and construct an adversary $\mathcal{A}$ for these fixed inputs. This suffices since we assume that our adversary knows both inputs and is computationally unbounded. Observe that fixing the inputs x^A, x^B and the adversary $\hat{\mathcal{A}}$ determines the value of all variables in all iterations of $\hat{\Pi}$ when run with inputs (x^A, x^B) in the presence of $\hat{\mathcal{A}}$.

Observe that Algorithm 2 loops over $i \in [\hat{R}/(P+1)]$. For any variable var other than σ and $flag$ in Algorithm 2 and any $i \in [\hat{R}/(P+1)]$, we let $var^A[i]$ denote the value of var the first time it is set in the i^{th} iteration of Alice's execution of Algorithm 2, *e.g.*, $m^A[4]$ will denote the value of m after Line 7 in the 4^{th} iteration in Alice's execution of Algorithm 2. For a variable like msgs that is defined once for all the iterations, $\mathsf{msgs}^A[i]$ will denote the value of msgs at the beginning of the i^{th} iteration, *i.e.*, after Line 6 in the i^{th} iteration in Alice's execution of Algorithm 2. When we omit the argument i, or when $i = \hat{R}/(P+1)+1$, we mean the value of the variable at the end of the protocol. We define $var^B[i]$ and var^B analogously with Alice replaced by Bob. For the variables σ and $flag$, we let $var^A[i]$ denote the value of var after Line 17 is executed by Alice in iteration i, and $var^B[i]$ is defined similarly. Observe that, for any i and $C \in \{A, B\}$, we have $m^C[i] \notin \mathsf{Long} \implies flag^C[i] = \texttt{True}$. Thus, we can assume without loss of generality that $\tilde{m}^C[i] \notin \mathsf{Long} \implies \tilde{flag}^C[i] = \texttt{True}$.

We define $\mathcal{A}$ to satisfy

$$\mathcal{A}^A_{\leq R}(x^A, x^B) = \mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},\leq R}), \qquad \mathcal{A}^B_{\leq R}(x^A, x^B) = \mathsf{DECC}(\mathsf{D\text{-}msgs}^B_{\mathrm{A},\leq R}).$$

Together with Line 39, this definition of $\mathcal{A}$ immediately shows the property in item 3a above. It remains to show the property in item 3b. To this end, we use the following claims.

Lemma 4.3. *If* $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B) \leq \theta_2 S/100$*, it holds for* $C \in \{A, B\}$ *that* $\sum_{j>0} |\mathsf{msgs}^C_j| > 5K_0 S$*.*

We defer the proof of Lemma 4.3, and in what follows we use it to prove the following claim.

Lemma 4.4. *If* $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B) \leq \theta_2 S/100$*, it holds for* $j \in [R]$ *that,*

$$\mathsf{D\text{-}msgs}^A_{\mathrm{A},j} = \begin{cases} \mathsf{ECC}(f^A(x^A, \mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},<j}))) & , P+1 \text{ divides } j \\ f^A(x^A, \mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},<j})) & , \text{otherwise} \end{cases}.$$

Furthermore, for all $j \in [2R]$, msgs^A_j *is a prefix of* $\mathsf{D\text{-}msgs}^A_j$*. An analogous claim holds for Bob.*

Proof. We only show the claim for Alice as the claim for Bob is similar. First, consider $j \in [R]$ such that $\mathsf{D\text{-}msgs}^A_{\mathrm{A},j}$ was not set in Line 39. In this case, due to Line 38, we get that there exists an iteration $i_1 \le \hat{R}/(P+1)$ such that $|\mathsf{msgs}^A[i']| > 2j-1$ for all $i_1 < i' \le \hat{R}/(P+1)+1$. Let i_1 be the smallest such iteration. By our choice of i_1, we have

$$\mathsf{D\text{-}msgs}^A_{\mathrm{A},j} = \mathsf{msgs}^A_{\mathrm{A},j}[i_1+1] = \begin{cases} \mathsf{ECC}(f^A(x^A, \mathsf{DECC}(\mathsf{msgs}^A_{\mathrm{B},<j}[i_1+1]))) & , P+1 \text{ divides } j \\ f^A(x^A, \mathsf{DECC}(\mathsf{msgs}^A_{\mathrm{B},<j}[i_1+1])) & , \text{otherwise} \end{cases}$$
$$= \begin{cases} \mathsf{ECC}(f^A(x^A, \mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},<j}))) & , P+1 \text{ divides } j \\ f^A(x^A, \mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},<j})) & , \text{otherwise} \end{cases}.$$

On the other hand, for $j \in [R]$ such that $\mathsf{D\text{-}msgs}^A_{\mathrm{A},j}$ was set in Line 39, we have $\mathsf{D\text{-}msgs}^A_{\mathrm{A},j} = \mathsf{ECC}(\perp^P)$ or $\perp$ depending on whether j is a multiple of $(P+1)$ or not, and it is sufficient to show that $f^A(x^A, \mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},<j})) = \perp^P$ or $\perp$ depending on whether j is a multiple of $(P+1)$ or not. Using Equation 1, we get that it is sufficient to show that

$$\sum_{j'<j} |\mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},j'})| + |f^A(x^A, \mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},<j'}))| \ge S.$$

Using Theorem 3.4 and Remark 3.5, we get that it is sufficient to show that

$$\sum_{j' \le |\mathsf{D\text{-}msgs}'^A|} |\mathsf{D\text{-}msgs}'^A_{j'}| \ge 2K_0 S. \tag{3}$$

To see why this holds, observe that

$$\begin{aligned} \sum_{j' \le |\mathsf{D\text{-}msgs}'^A|} |\mathsf{D\text{-}msgs}'^A_{j'}| &= \sum_{j' \le |\mathsf{D\text{-}msgs}'^A|} |\mathsf{msgs}^A_{j'}| \\ &\ge -\mathbb{1}\left(|\mathsf{msgs}^A| \text{ is odd}\right) \cdot |longmsg^A| + \sum_{j' \le |\mathsf{msgs}^A|} |\mathsf{msgs}^A_{j'}| \\ &\ge -K_0 \cdot |f^A(x^A, \mathsf{DECC}(\mathsf{D\text{-}msgs}^A_{\mathrm{B},<ind^A+P+1}))| + \sum_{j' \le |\mathsf{msgs}^A|} |\mathsf{msgs}^A_{j'}| \\ &\qquad \text{(Theorem 3.4)} \\ &\ge 4K_0 S. \qquad \text{(Equation 1, Lemma 4.3)} \end{aligned}$$

Finally, we show the furthermore part. Let $j \in [2R]$. Observe that the claim is trivial unless $j = |\mathsf{msgs}^A| \in \mathsf{Long}$ and j is odd. Thus, it is sufficient to show that if $|\mathsf{msgs}^A| \in \mathsf{Long}$ is odd, then, we have $longmsg^A = \mathsf{ECC}(\perp^P)$. This follows from Equation 3.

□

Now, in order to prove the property in item 3b, we prove the following lemma that implies item 3b.

Lemma 4.5. *If* $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B) \le \theta_2 S/100$ *then*

$$\mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B), \mathsf{corr}^{B\to A}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B) \le 40 \cdot \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B) + 2P.$$

Proof. We only show that $\mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A,x^B) \le 40\cdot \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A,x^B)+2P$ as the other claim is symmetric. In fact, we show that, for all $r\in[R/(P+1)]$, we have

$$\mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A,x^B,r) \le 2P + 10\cdot \sum_{C\in\{A,B\}} \sum_{\substack{r'\in[\hat{R}/(P+1)]\\ ind^C[r']/(P+1)\in\{r-1,r\}}} \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A,x^B,r'),$$

where the first term is needed for at most one value of r and the result follows. Fix $r\in[R/(P+1)]$. If $\mathsf{disc}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A,x^B,r)=0$, then $\mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A,x^B,r)=0$ as well, and there is nothing to show. We therefore assume that $\mathsf{disc}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A,x^B,r)=1$ implying that there exists a value of $i'\in[P+1]$ such that $f^A(x^A,\mathcal{A}^A_{<(r-1)(P+1)+i'}(x^A,x^B)) \neq \mathcal{A}^B_{(r-1)(P+1)+i'}(x^A,x^B)$. Let i' be the smallest such value. We have the following cases:

- **When $i'\in[P]$:** In this case, by the definition of $\mathcal{A}$ and Lemma 4.4, we have that $\mathsf{D\text{-}msgs}^A_{\mathrm{A},(r-1)(P+1)+i'} \neq \mathsf{D\text{-}msgs}^B_{\mathrm{A},(r-1)(P+1)+i'}$. Let $C\in\{A,B\}$ be the lexicographically smallest such that[6] $|\mathsf{msgs}^C_{\mathrm{A},r(P+1)}| \ge |\mathsf{msgs}^{\overline{C}}_{\mathrm{A},r(P+1)}|$ and there exists $i_1\le \hat{R}/(P+1)$ such that $|\mathsf{msgs}^C[i_1]| = 2(r-1)(P+1)+1 < |\mathsf{msgs}^C[i'']|$ for all $i_1 < i'' \le \hat{R}/(P+1)+1$. Note that C is well defined as at least one such C always exists due to $\mathsf{D\text{-}msgs}^A_{\mathrm{A},(r-1)(P+1)+i'} \neq \mathsf{D\text{-}msgs}^B_{\mathrm{A},(r-1)(P+1)+i'}$. Define $a_1 = \max\left(|\mathsf{msgs}^C_{\mathrm{A},r(P+1)}|/P, 1\right)$.

  For all $l\in[a_1]$, define i''_l to the largest iteration such that $ind^C[i''_l]=(r-1)(P+1)$, $c^C[i''_l]=(l-1)P$ and party C executes Line 20 in iteration i''_l. Due to our choice of a_1, at least one such iteration always exists and therefore i''_l is well defined and we have $i''_1 < i''_2 < \cdots < i''_{a_1}$. Either $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A,x^B,i''_l)>0$ for at least $0.5a_1$ values of $l\in[a_1]$ in which case we have:

  $$10\cdot \sum_{\substack{r'\in[\hat{R}/(P+1)]\\ ind^C[r']/(P+1)\in\{r-1,r\}}} \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A,x^B,r') \ge 20a_1P \ge \mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A,x^B,r),$$

  and the lemma follows, or there exists $l_1 > 0.5a_1$ such that iteration i''_{l_1} satisfies $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A,x^B,i''_{l_1})=0$. This together with that fact that party C executes Line 20 in iteration i''_{l_1} and $c^C[i''_{l_1}] = (l_1-1)P$ implies that $\mathsf{msgs}^A_{\mathrm{A},(r-1)(P+1)+i'''}[i''_{l_1}+1] = \mathsf{msgs}^B_{\mathrm{A},(r-1)(P+1)+i'''}[i''_{l_1}+1]$ for all $i'''\in[P]$ and $c^C[i''_{l_1}] = c^{\overline{C}}[i''_{l_1}] = (l_1-1)P$.

  However, due to our choice of i''_{l_1} and i', this means that there exists at least l_1 values of $j''>i''_{l_1}$ such that $ind^{\overline{C}}[j'']=(r-1)(P+1)$, $c^{\overline{C}}[j'']\le(l_1-1)P$, and party $\overline{C}$ executes Line 28 or Line 33 in iteration j''. We get that $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A,x^B,j'')>0$ for all such j'' giving

  $$10\cdot \sum_{\substack{r'\in[\hat{R}/(P+1)]\\ ind^{\overline{C}}[r']/(P+1)\in\{r-1,r\}}} \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A,x^B,r') \ge 20a_1P \ge \mathsf{corr}^{A\to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A,x^B,r),$$

[6] We adopt the convention that, for $C\in\{A,B\}$, if $j>|\mathsf{msgs}^C_{\mathrm{A}}|$, then $|\mathsf{msgs}^C_{\mathrm{A},j}|=0$.

finishing the argument.

- **When $i' = P + 1$:** In this case, we can conclude from Theorem 3.4 that

$$\Delta(\mathsf{ECC}(f^A(x^A, \mathcal{A}^A_{<r(P+1)}(x^A, x^B))), \mathsf{D\text{-}msgs}^B_{\mathrm{A},r(P+1)}) \geq \frac{1}{3} \cdot |\mathsf{ECC}(f^A(x^A, \mathcal{A}^A_{<r(P+1)}(x^A, x^B)))|.$$

It follows by the definition of $\mathcal{A}$ and Lemma 4.4 that

$$\Delta(\mathsf{D\text{-}msgs}^A_{\mathrm{A},r(P+1)}, \mathsf{D\text{-}msgs}^B_{\mathrm{A},r(P+1)}) > \frac{1}{5} \cdot \max\left(|\mathsf{D\text{-}msgs}^A_{\mathrm{A},r(P+1)}|, |\mathsf{D\text{-}msgs}^B_{\mathrm{A},r(P+1)}|\right). \quad (4)$$

Let $C \in \{A, B\}$ be the lexicographically smallest such that $|\mathsf{msgs}^C_{\mathrm{A},r(P+1)}| \geq |\mathsf{msgs}^{\overline{C}}_{\mathrm{A},r(P+1)}|$ and there exists $i_1 \leq \hat{R}/(P+1)$ such that $|\mathsf{msgs}^C[i_1]| = 2(r-1)(P+1)+1 < |\mathsf{msgs}^C[i'']|$ for all $i_1 < i'' \leq \hat{R}/(P+1)+1$. Observe that C is well defined as at least one such C always exists due to $\mathsf{D\text{-}msgs}^A_{\mathrm{A},r(P+1)} \neq \mathsf{D\text{-}msgs}^B_{\mathrm{A},r(P+1)}$. Let $a_1 = \frac{|\mathsf{msgs}^C_{\mathrm{A},r(P+1)}|}{P}$. For all $l \in [a_1]$, define i''_l to the largest iteration such that $ind^C[i''_l] = (r-1)(P+1)$, $c^C[i''_l] = (l-1)P$, $m^C[i''_l]$ is odd, and party C executes Line 20 in iteration i''_l. Due to our choice of a_1, at least one such iteration always exists and therefore i''_l is well defined and we have $i''_1 < i''_2 < \cdots < i''_{a_1}$. Either $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i''_l) > 0$ for at least $0.1a_1$ values of $l \in [a_1]$ in which case we have:

$$10 \cdot \sum_{\substack{r' \in [\hat{R}/(P+1)] \\ ind^C[r']/(P+1) \in \{r-1, r\}}} \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, r') \geq 4a_1 P \geq \mathsf{corr}^{A \to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r),$$

and the lemma follows, or there exists at least $0.9a_1$ values of $l \in [a_1]$ such that $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i''_l) = 0$. We deal with this case in the rest of this proof. First, assume that:

$$\Delta(\mathsf{msgs}^A_{\mathrm{A},r(P+1)}, \mathsf{msgs}^B_{\mathrm{A},r(P+1)}) > \frac{1}{5} \cdot \max\left(|\mathsf{msgs}^A_{\mathrm{A},r(P+1)}|, |\mathsf{msgs}^B_{\mathrm{A},r(P+1)}|\right), \quad (5)$$

noting that the right hand side is just $\frac{1}{5} \cdot |\mathsf{msgs}^C_{\mathrm{A},r(P+1)}|$ by our choice of C. Next, note that for all $l \in [a_1]$ such that $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i''_l) = 0$, by our definition of i''_l we have,

$$\mathsf{msgs}^{\overline{C}}_{\mathrm{A},r(P+1),((l-1)P:lP]}[i''_l + 1] = \mathsf{msgs}^C_{\mathrm{A},r(P+1),((l-1)P:lP]}[i''_l + 1] = \mathsf{msgs}^C_{\mathrm{A},r(P+1),((l-1)P:lP]}.$$

Together with Equation 5, this means that for at least $0.1a_1$ of these values we have $\mathsf{msgs}^{\overline{C}}_{\mathrm{A},r(P+1),((l-1)P:lP]}[i''_l + 1] \neq \mathsf{msgs}^{\overline{C}}_{\mathrm{A},r(P+1),((l-1)P:lP]}$ implying that for at least $0.1a_1$ of these values of l, there is an iteration $j''_l > i''_l$ such that $c^{\overline{C}}[j''_l + 1] = (l-1)P$ and $ind^{\overline{C}}[j''_l]/(P+1) \in \{r-1, r\}$ and party $\overline{C}$ executes Line 33 in iteration j''_l Due to our

choice of i', this is possible only if $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, j''_l) > 0$ for all such j''_l giving

$$10 \cdot \sum_{\substack{r' \in [\hat{R}/(P+1)] \\ ind^{\overline{C}}[r']/(P+1) \in \{r-1, r\}}} \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, r') \geq 4a_1 P \geq \mathsf{corr}^{A \to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r),$$

finishing the argument in this case. Now, assume that Equation 5 does not hold. As Equation 4 holds and Equation 5 does not hold, we have that $\mathsf{D\text{-}msgs}^{C'}_{\mathrm{A},r(P+1)} \neq \mathsf{msgs}^{C'}_{\mathrm{A},r(P+1)}$ for at least one value of $C' \in \{A, B\}$. In fact, it holds for exactly one value of C' as otherwise $\mathsf{D\text{-}msgs}^{A}_{\mathrm{A},r(P+1)} = \mathsf{D\text{-}msgs}^{B}_{\mathrm{A},r(P+1)}$ contradicting Equation 4. If it holds for $C' = B$ (and therefore, not for $C' = A$) then we have $\mathsf{msgs}^{B}_{\mathrm{A},r(P+1)} = \varepsilon$ by our definition of $\mathsf{D\text{-}msgs}^{B}_{\mathrm{A},r(P+1)}$ contradicting the fact that Equation 5 does not hold. So, we can assume that $C' = A$ is the unique satisfier of $\mathsf{D\text{-}msgs}^{C'}_{\mathrm{A},r(P+1)} \neq \mathsf{msgs}^{C'}_{\mathrm{A},r(P+1)}$. By the definition of $\mathsf{D\text{-}msgs}^{A}_{\mathrm{A},r(P+1)}$ and Lemma 4.4, we get that $\mathsf{msgs}^{A}_{\mathrm{A},r(P+1)}$ is a prefix of $\mathsf{D\text{-}msgs}^{A}_{\mathrm{A},r(P+1)} = \mathsf{ECC}(\bot^P)$. Note that $|\mathsf{D\text{-}msgs}^{A}_{\mathrm{A},r(P+1)}| > |\mathsf{D\text{-}msgs}^{B}_{\mathrm{A},r(P+1)}|$ as otherwise the fact that Equation 4 holds and Equation 5 does not hold contradicts Lemma 3.3. However, this implies by Remark 3.5 that

$$\mathsf{corr}^{A \to B}_{\mathrm{L},\Pi,\mathcal{A}}(x^A, x^B, r) \leq 2P.$$

As $\mathsf{D\text{-}msgs}^{A}_{\mathrm{A},r(P+1)} \neq \mathsf{msgs}^{A}_{\mathrm{A},r(P+1)}$ for at most one value of r, the claim follows.

□

We now show Lemma 4.3. We actually prove a stronger result, namely, Lemma 4.6, that implies Lemma 4.3. Before stating Lemma 4.6, we define the following shorthands[7] for all $i \in [\hat{R}/(P+1)+1]$:

$$\begin{aligned}
\mathsf{corr}_{<i} &= \mathsf{corr}_{\leq i-1} = \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, \leq i-1), \\
\mathsf{good}_i &= \min\left(\sum_{j>0} |\mathsf{msgs}^A_j[i]|, \sum_{j>0} |\mathsf{msgs}^B_j[i]|\right), \\
\mathsf{bad}_i &= \sum_{j>0} \Delta\left(\mathsf{msgs}^A_j[i], \mathsf{msgs}^B_j[i]\right). \\
\mathsf{f\text{-}bad}_i &= \sum_{j>0} \mathbb{1}\left(\exists i' \in [2P] : \mathsf{msgs}^A_{2(j-1)(P+1)+i'}[i] \neq \mathsf{msgs}^B_{2(j-1)(P+1)+i'}[i]\right) \\
&\qquad \times \min_{C \in \{A,B\}} \sum_{i'=1}^{2(P+1)} |\mathsf{msgs}^C_{2(j-1)(P+1)+i'}[i]|.
\end{aligned}$$

We will need another definition to show Lemma 4.6. Define $\underline{m}_i = \min(m^A[i], m^B[i])$ and

[7] We assume for convenience that, for all i, j, we have $\mathsf{msgs}^A_j[i] = \varepsilon$ when $j > |\mathsf{msgs}^A[i]|$ and similarly for $\mathsf{msgs}^B_j[i]$.

$\overline{m}_i = \max(m^A[i], m^B[i])$ and:

$$\mathsf{gap}_i = P \cdot |[\underline{m}_i : \overline{m}_i) \cap \mathsf{Long}| + |[\underline{m}_i : \overline{m}_i) \cap \overline{\mathsf{Long}}|.$$

With these definitions, we are now ready to state Lemma 4.6. Observe how Lemma 4.3 follows from Lemma 4.6 by setting $i = \hat{R}/(P+1)+1$ and using the fact that $\mathsf{corr}_{<\hat{R}/(P+1)+1} = \mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B) \leq \theta_2 S/100$.

Lemma 4.6. *For all $i \in [\hat{R}/(P+1)+1]$, we have*

$$1000 \cdot \mathsf{corr}_{<i} + 2 \cdot \mathsf{good}_i - 4 \cdot \mathsf{bad}_i - 12 \cdot \mathsf{gap}_i - 20 \cdot \mathsf{f\text{-}bad}_i \geq P(i-1).$$

Proof. We show this by induction on i. For the base case, note that the claim holds for $i = 1$ as all the terms are 0. We will show that, for any $i \in [\hat{R}/(P+1)]$, we have

$$\begin{aligned} &1000 \cdot (\mathsf{corr}_{\leq i} - \mathsf{corr}_{<i}) + 2 \cdot (\mathsf{good}_{i+1} - \mathsf{good}_i) \\ &\quad - 4 \cdot (\mathsf{bad}_{i+1} - \mathsf{bad}_i) - 12 \cdot (\mathsf{gap}_{i+1} - \mathsf{gap}_i) - 20 \cdot (\mathsf{f\text{-}bad}_{i+1} - \mathsf{f\text{-}bad}_i) \geq P, \end{aligned} \tag{6}$$

and the induction step will follow. Fix $i \in [\hat{R}/(P+1)]$. We begin with some inequalities that help us bound the terms in Equation 6. First, note that, by Lemma 3.1:

$$\mathsf{bad}_{i+1} - \mathsf{bad}_i \leq \sum_{C \in \{A,B\}} \sum_{j>0} \Delta(\mathsf{msgs}_j^C[i+1], \mathsf{msgs}_j^C[i]). \tag{7}$$

Similarly, we have:

$$\begin{aligned} \mathsf{good}_i - \mathsf{good}_{i+1} &\leq \sum_{C \in \{A,B\}} \left| \sum_{j>0} |\mathsf{msgs}_j^C[i]| - \sum_{j>0} |\mathsf{msgs}_j^C[i+1]| \right| \\ &\leq \sum_{C \in \{A,B\}} \sum_{j>0} \left| |\mathsf{msgs}_j^C[i]| - |\mathsf{msgs}_j^C[i+1]| \right| \\ &\leq \sum_{C \in \{A,B\}} \sum_{j>0} \Delta(\mathsf{msgs}_j^C[i+1], \mathsf{msgs}_j^C[i]). \end{aligned} \tag{8}$$

We also have, by the definition of gap_i that:

$$\begin{aligned} \mathsf{gap}_{i+1} - \mathsf{gap}_i &\leq P \cdot \left(|[\underline{m}_{i+1} : \overline{m}_{i+1}) \cap \mathsf{Long}| - |[\underline{m}_i : \overline{m}_i) \cap \mathsf{Long}| \right) \\ &\quad + \left(|[\underline{m}_{i+1} : \overline{m}_{i+1}) \cap \overline{\mathsf{Long}}| - |[\underline{m}_i : \overline{m}_i) \cap \overline{\mathsf{Long}}| \right) \\ &\leq \left(P \cdot |[\overline{m}_i : \overline{m}_{i+1}) \cap \mathsf{Long}| + |[\overline{m}_i : \overline{m}_{i+1}) \cap \overline{\mathsf{Long}}| \right) \cdot \mathbb{1}\left(\overline{m}_i < \overline{m}_{i+1}\right) \\ &\quad + \left(P \cdot |[\underline{m}_{i+1} : \underline{m}_i) \cap \mathsf{Long}| + |[\underline{m}_{i+1} : \underline{m}_i) \cap \overline{\mathsf{Long}}| \right) \cdot \mathbb{1}\left(\underline{m}_{i+1} < \underline{m}_i\right) \\ &\leq \mathbb{1}\left(\overline{m}_i < \overline{m}_{i+1}\right) \cdot \left(2P \left\lceil \frac{\overline{m}_{i+1} - \overline{m}_i}{2P+2} \right\rceil + (\overline{m}_{i+1} - \overline{m}_i) \right) \\ &\quad + \mathbb{1}\left(\underline{m}_{i+1} < \underline{m}_i\right) \cdot \left(2P \left\lceil \frac{\underline{m}_i - \underline{m}_{i+1}}{2P+2} \right\rceil + (\underline{m}_i - \underline{m}_{i+1}) \right), \end{aligned} \tag{9}$$

where the last step uses the definition of Long. Finally, we upper bound $\mathsf{f\text{-}bad}_{i+1} - \mathsf{f\text{-}bad}_i$.

Observe that

$$\begin{aligned}
&\mathsf{f\text{-}bad}_{i+1} - \mathsf{f\text{-}bad}_i \\
&\quad\leq \sum_{C\in\{A,B\}} \sum_{j>0} \left| |\mathsf{msgs}_j^C[i]| - |\mathsf{msgs}_j^C[i+1]| \right| \\
&\qquad + \sum_{C\in\{A,B\}} \sum_{j>0} \mathbb{1}\left(\exists i' \in [2P] : \mathsf{msgs}^C_{2(j-1)(P+1)+i'}[i+1] \neq \mathsf{msgs}^C_{2(j-1)(P+1)+i'}[i]\right) \\
&\qquad\qquad \times \sum_{i'=1}^{2(P+1)} |\mathsf{msgs}^C_{2(j-1)(P+1)+i'}[i+1]| \\
&\quad\leq 6P + \sum_{C\in\{A,B\}} \sum_{j>0} \Delta(\mathsf{msgs}_j^C[i+1], \mathsf{msgs}_j^C[i]),
\end{aligned} \tag{10}$$

where the last step uses the definition of our protocol. We now consider various cases and show Equation 6 in each case.

- $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(\boldsymbol{x^A}, \boldsymbol{x^B}, \boldsymbol{i}) > \mathbf{0}$**:** In this case, we show that value of $\mathsf{corr}_{\leq i} - \mathsf{corr}_{<i} \geq 4P$ is large enough to outweigh all the other terms in Equation 6. We first upper bound $\sum_{C\in\{A,B\}} \sum_{j>0} \Delta(\mathsf{msgs}_j^C[i+1], \mathsf{msgs}_j^C[i])$. Fix $C \in \{A, B\}$ and note that, in iteration i, party C changes msgs in Line 13, Line 20, Line 25, Line 28, and Line 33. Furthermore, in each of these lines, we change at most $2P$ symbols. This gives

  $$\sum_{C\in\{A,B\}} \sum_{j>0} \Delta(\mathsf{msgs}_j^C[i+1], \mathsf{msgs}_j^C[i]) \leq 20P.$$

  From Equation 7, Equation 8, and Equation 10, we get

  $$\mathsf{good}_i - \mathsf{good}_{i+1}, \mathsf{bad}_{i+1} - \mathsf{bad}_i, \mathsf{f\text{-}bad}_{i+1} - \mathsf{f\text{-}bad}_i \leq 30P. \tag{11}$$

  Next, we show that:

  $$\mathsf{gap}_{i+1} - \mathsf{gap}_i \leq 10P. \tag{12}$$

  Observe that, to show Equation 12, it is sufficient to show that for any $C \in \{A, B\}$, m^C changes by at most $2P + 1$ in iteration i. Then, we can apply Equation 9 to get the bound on $\mathsf{gap}_{i+1} - \mathsf{gap}_i$. The reason m^C changes by at most $2P+1$ in any iteration is that either party C executes Line 25 in iteration i, which cancels the change in m^C, if any, made in Line 13, and then further decreases m^C by at most $2P + 1$ in case it executes Line 28 or Line 31, or party C does not execute Line 25, in which case party C increases m^C by at most $2P$ in the P executions of Line 13 and maybe by one more party C executes Line 22.

  Equation 6 follows from Equation 11 and Equation 12.

- $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(\boldsymbol{x^A}, \boldsymbol{x^B}, \boldsymbol{i}) = \mathbf{0}$**:** In this case, we use the definition of $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i)$ to

conclude that

$$(\tilde{m}^A[i], \tilde{c}^A[i], \tilde{e}^A[i], \tilde{\sigma}^A[i], \tilde{flag}^A[i]) = (m^B[i], c^B[i], e^B[i], \sigma^B[i], flag^B[i]),$$
$$(m^A[i], c^A[i], e^A[i], \sigma^A[i], flag^A[i]) = (\tilde{m}^B[i], \tilde{c}^B[i], \tilde{e}^B[i], \tilde{\sigma}^B[i], \tilde{flag}^B[i]). \tag{13}$$

We consider three cases:

– $(\boldsymbol{m^A[i], c^A[i]}) = (\boldsymbol{m^B[i], c^B[i]})$**:** In this case, by Equation 13, we have $(\tilde{m}^A[i], \tilde{c}^A[i]) = (m^B[i], c^B[i]) = (m^A[i], c^A[i]) = (\tilde{m}^B[i], \tilde{c}^B[i])$, and we use (m, c) to denote this common value. This also implies that $ind^A[i] = ind^B[i]$ and we use ind to denote this value. We first claim that $m^A[i+1] = m^B[i+1]$ implying by the definition of gap that

$$\mathsf{gap}_{i+1} = \mathsf{gap}_i = 0. \tag{14}$$

Indeed, due to Equation 13, either both Alice and Bob execute Line 20 but not Line 22, or they both execute Line 22, or they both execute Line 28, or they both execute Line 33. In any case, $m^A[i+1] = m^B[i+1]$ follows. We have the following subcases:

∗ $\boldsymbol{flag^A[i] \wedge flag^B[i] = \texttt{True}}$**:** Observe that Equation 13 implies that both Alice and Bob execute Line 20 in iteration i and can also execute Line 13 P times if $m \notin \mathsf{Long}$. We get:

$$\mathsf{good}_{i+1} - \mathsf{good}_i = P + 2P \cdot \mathbb{1}(m \notin \mathsf{Long}) \geq P. \tag{15}$$

Furthermore, as Alice and Bob only add symbols to msgs, and because of our assumptions that $(m^A[i], c^A[i]) = (m^B[i], c^B[i])$ and $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i) = 0$, we get that :

$$\mathsf{bad}_{i+1} = \mathsf{bad}_i. \tag{16}$$

We now analyze $\mathsf{f\text{-}bad}_i - \mathsf{f\text{-}bad}_{i+1}$. If $m \notin \mathsf{Long}$, then as we ensure that either $m^A[i]$ or $m^A[i]-1$ are always in Long, the fact that $m \notin \mathsf{Long}$ implies that $m-1 \in \mathsf{Long}$ which implies (due to the definition of Long) that $m = 2 \cdot ind + 1$. This, with the fact that both Alice and Bob execute Line 20 in iteration i implies that

$$\begin{aligned}
&\mathsf{f\text{-}bad}_i - \mathsf{f\text{-}bad}_{i+1} \\
&\quad = -\mathbb{1}\left(\exists i' \in [2P] : \mathsf{msgs}^A_{2\cdot ind+i'}[i+1] \neq \mathsf{msgs}^B_{2\cdot ind+i'}[i+1]\right) \\
&\qquad \times \min_{C \in \{A,B\}} \sum_{i'=1}^{2(P+1)} |\mathsf{msgs}^C_{2\cdot ind+i'}[i+1]| \\
&\qquad = 0,
\end{aligned}$$

as $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i) = 0$. On the other hand, if $m \in \mathsf{Long}$, we get that $flag^A[i] \wedge flag^B[i] = \texttt{True}$ implies that for all $i' \in [2P]$, we have

$\mathsf{msgs}^A_{2\cdot ind+i'}[i+1] = \mathsf{msgs}^B_{2\cdot ind+i'}[i+1]$ due to $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i) = 0$. We get that $\mathsf{f\text{-}bad}_i = \mathsf{f\text{-}bad}_{i+1}$. Thus, in either case, we have:

$$\mathsf{f\text{-}bad}_i = \mathsf{f\text{-}bad}_{i+1}. \tag{17}$$

Combining Equation 14, Equation 15, Equation 16, and Equation 17, we can conclude Equation 6.

* $\boldsymbol{flag^A[i] \wedge flag^B[i] = \texttt{False}}$**:** Observe that this is possible only if $m \in \mathsf{Long}$. If $c = 0$ and $m - 1 \notin \mathsf{Long}$, Alice and Bob both execute Line 28 in iteration i. Otherwise, they both execute Line 33 in iteration i. We get:

$$\mathsf{good}_i - \mathsf{good}_{i+1} = P + P \cdot \mathbb{1}(c = 0 \wedge m - 1 \notin \mathsf{Long}). \tag{18}$$

Additionally, as $m \in \mathsf{Long}$ and $flag^A[i] \wedge flag^B[i] = \texttt{False}$, we have using $\mathsf{corr}_{\mathrm{L},\hat{\Pi},\hat{\mathcal{A}}}(x^A, x^B, i) = 0$ that there exists $i' \in [2P]$ for which $\mathsf{msgs}^A_{2\cdot ind+i'}[i+1] \neq \mathsf{msgs}^B_{2\cdot ind+i'}[i+1]$. We get that

$$\mathsf{f\text{-}bad}_i - \mathsf{f\text{-}bad}_{i+1} = P + P \cdot \mathbb{1}(c = 0 \wedge m - 1 \notin \mathsf{Long}). \tag{19}$$

Furthermore, as Alice and Bob only remove (the same number of) symbols to msgs, and because of our assumption that $(m^A[i], c^A[i]) = (m^B[i], c^B[i])$, we get that :

$$\mathsf{bad}_{i+1} \leq \mathsf{bad}_i. \tag{20}$$

Combining Equation 14, Equation 18, Equation 19, and Equation 20, we can conclude Equation 6.

– $\boldsymbol{(m^A[i], c^A[i]) > (m^B[i], c^B[i])}$**:** In this case, by Equation 13, we have $(m^A[i], c^A[i]) > (\tilde{m}^A[i], \tilde{c}^A[i])$ and $(m^B[i], c^B[i]) < (\tilde{m}^B[i], \tilde{c}^B[i])$. Due to these inequalities, we know that both Alice and Bob execute Line 25 and this line undoes any change they made to msgs in Line 13. Thus, any changes in the variable msgs in iteration i happen after Line 25. In particular, due to the fact that $(m^B[i], c^B[i]) < (\tilde{m}^B[i], \tilde{c}^B[i])$, Bob does not execute any line after Line 25 and we have $\mathsf{msgs}^B[i+1] = \mathsf{msgs}^B[i]$. We consider various cases:

* $\boldsymbol{c^A[i] > 0}$**:** In this case, we show that the value of $\mathsf{bad}_{i+1} - \mathsf{bad}_i$ is large and negative enough to outweigh all the other terms. To begin with, observe that $\mathsf{msgs}^B[i+1] = \mathsf{msgs}^B[i]$ together with Equation 8 implies that

$$\mathsf{good}_i - \mathsf{good}_{i+1} \leq \sum_{j>0} \Delta(\mathsf{msgs}^A_j[i+1], \mathsf{msgs}^A_j[i]) \leq P, \tag{21}$$

as Alice executes Line 33 in iteration i. We again use the fact that Alice executes Line 33 in iteration i to conclude that $m^A[i] = m^A[i+1]$. This, together with $m^B[i+1] = |\mathsf{msgs}^B[i+1]| = |\mathsf{msgs}^B[i]| = m^B[i]$ and Equation 9

gives:

$$\mathsf{gap}_i = \mathsf{gap}_{i+1} \qquad \text{and} \qquad \mathsf{f\text{-}bad}_i \geq \mathsf{f\text{-}bad}_{i+1}. \tag{22}$$

Finally, we analyze $\mathsf{bad}_i - \mathsf{bad}_{i+1}$. We get:

$$\begin{aligned}
&\mathsf{bad}_{i+1} - \mathsf{bad}_i \\
&\quad = \sum_{j>0} \Delta\left(\mathsf{msgs}_j^A[i+1], \mathsf{msgs}_j^B[i+1]\right) - \Delta\left(\mathsf{msgs}_j^A[i], \mathsf{msgs}_j^B[i]\right) \\
&\quad \overset{(a)}{=} \Delta\left(\mathsf{msgs}_{m^A[i]}^A[i+1], \mathsf{msgs}_{m^A[i]}^B[i+1]\right) - \Delta\left(\mathsf{msgs}_{m^A[i]}^A[i], \mathsf{msgs}_{m^A[i]}^B[i]\right) \\
&\quad \overset{(b)}{=} -P.
\end{aligned} \tag{23}$$

In the above derivation, (a) is due to $\mathsf{msgs}^B[i+1] = \mathsf{msgs}^B[i]$ together with the fact that Alice only changes position $m^A[i]$ of $\mathsf{msgs}^A[i]$ as she only executes Line 33 and (b) is due to Lemma 3.2. From Equation 21, Equation 22 and Equation 23, we observe that Equation 6 follows.

* $\boldsymbol{c^A[i] = 0}$ **:** Observe that $c^A[i] = 0$ and $(m^A[i], c^A[i]) > (m^B[i], c^B[i])$ necessitates $m^A[i] > m^B[i]$. In this case, Alice either executes Line 28 or executes Line 31 and Line 33 after Line 25. Thus, using the fact that $\mathsf{msgs}^B[i+1] = \mathsf{msgs}^B[i]$ together with Equation 7 and Equation 8 implies that

$$\begin{aligned}
\mathsf{bad}_{i+1} - \mathsf{bad}_i, \mathsf{good}_i - \mathsf{good}_{i+1} &\leq \sum_{j>0} \Delta(\mathsf{msgs}_j^A[i+1], \mathsf{msgs}_j^A[i]) \\
&\leq P + P \cdot \mathbb{1}(m^A[i] - 1 \notin \mathsf{Long}).
\end{aligned} \tag{24}$$

We next claim that:

$$\mathsf{f\text{-}bad}_i \geq \mathsf{f\text{-}bad}_{i+1}. \tag{25}$$

If $m^A[i]-1 \in \mathsf{Long}$, this follows as Alice is only removing symbols in iteration i. On the other hand, if $m^A[i]-1 \notin \mathsf{Long}$, then, as we ensure that either $m^B[i]$ or $m^B[i]-1$ are always in Long, the fact that $m^A[i] > m^B[i]$ and $m^A[i]-1 \notin \mathsf{Long}$ implies (due to the definition of Long) that $m^A[i+1] = m^A[i] - 2P \geq m^B[i]$. This, together with $m^B[i+1] = |\mathsf{msgs}^B[i+1]| = |\mathsf{msgs}^B[i]| = m^B[i]$ gives Equation 25.

Finally, we argue about $\mathsf{gap}_{i+1} - \mathsf{gap}_i$. From the definition of gap and $m^A[i] > m^A[i+1] \geq m^B[i+1] = m^B[i]$, it follows that:

$$\begin{aligned}
\mathsf{gap}_i - \mathsf{gap}_{i+1} &= P \cdot |[m^A[i+1] : m^A[i]) \cap \mathsf{Long}| + |[m^A[i+1] : m^A[i]) \cap \overline{\mathsf{Long}}| \\
&\geq P + P \cdot \mathbb{1}(m^A[i] - 1 \notin \mathsf{Long}).
\end{aligned} \tag{26}$$

From Equation 24, Equation 25 and Equation 26, we observe that Equation 6

follows.

– $(\boldsymbol{m^A}[i], \boldsymbol{c^A}[i]) < (\boldsymbol{m^B}[i], \boldsymbol{c^B}[i])$**:** Symmetric to the case above

□

5 Our protocols

Our goal in this section is to prove the following theorem:

Theorem 5.1. *There exist constants $\theta_2 \geq 10^{-20}$, $\eta_3, \eta_4 > 1$ such that the following holds:*

Let $\Sigma, X^A, X^B, Y^A, Y^B$ be sets as in Subsection 3.3. Let $\Pi = \{f^C, g^C\}_{C\in\{A,B\}}$ be a protocol in model `STANDARD` *with $T > 2^{200K_0+10^5\theta_2}$ rounds and alphabet Σ. Furthermore, the input and output sets of Alice (resp. Bob) in Π are X^A and Y^A (resp. X^B and Y^B) respectively.*

Then, there is a protocol $\Pi' = \{f'^C, g'^C\}_{C\in\{A,B\}}$ in model `LONG` *with $R = \eta_4 \cdot T$ rounds, length of $S = \eta_3 \cdot T$ symbols, alphabet Σ, period $P = \log(S)$, and the same input and outputs sets for the two parties such that for every adversary $\mathcal{A}'$ for Π' in model* `LONG`*, for all inputs $x^A \in X^A$ and $x^B \in X^B$, and for all $C \in \{A, B\}$, we have that*

$$\mathsf{corr}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta_2 S \implies \Pi'^C_{\mathcal{A}'}(x^A, x^B) = \Pi^C(x^A, x^B).$$

Furthermore, the functions f'^C and g'^C, for $C \in \{A, B\}$ make use of the function $\mathsf{TC} = \mathsf{TC}_{1-10^{-5},|\Sigma|^{2P},S/P,\Sigma^{KP}}(\cdot)$ (for a large enough constant K so that Theorem 3.7 holds) and can be computed in time polynomial in T given oracle access to the functions f^C and g^C, where $C \in \{A, B\}$, and oracle access to the function TC.

We show that Theorem 3.8 follows from Theorem 4.1 and Theorem 5.1.

Proof of Theorem 3.8 assuming Theorem 4.1 and Theorem 5.1. Let $\theta_2 \geq 10^{-20}$, η_3, η_4 be as promised by Theorem 5.1. Let η_1 and θ_1 be as promised by Theorem 4.1 for θ_2. To show Theorem 3.8, we define $\theta = \theta_1$, $\eta = \eta_1\eta_3$, and $\eta' = \eta_3$.

Fix a protocol Π in model `STANDARD` and let Π' be a protocol in model `LONG` with S' symbols be as promised by Theorem 5.1. Let Π'' be a protocol with T'' rounds in model `STANDARD` be as promised by Theorem 4.1 when applied to Π'. We claim that Π'' satisfies Theorem 3.8. For this, we fix an adversary $\mathcal{A}''$ for Π'' in model `STANDARD`. Let $\mathcal{A}'$ be the adversary for Π' in model `LONG` promised by Theorem 4.1 and $\mathcal{A}$ be an adversary for Π promised by Theorem 5.1 for $\mathcal{A}'$. For all inputs $x^A \in X^A$ and $x^B \in X^B$, we have

$$\mathsf{corr}_{\mathrm{S},\Pi'',\mathcal{A}''}(x^A, x^B) \leq \theta T'' \implies \mathsf{corr}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta_2 S' \implies \Pi'^C_{\mathcal{A}'}(x^A, x^B) = \Pi^C(x^A, x^B).$$

However, we also have $\Pi''^C_{\mathcal{A}''}(x^A, x^B) = \Pi'^C_{\mathcal{A}'}(x^A, x^B)$ finishing the argument.

The furthermore part of Theorem 3.8 follows straightforwardly.

□

The rest of this paper is devoted to showing Theorem 5.1. Fix K to be a large enough constant such that $\mathsf{TC}_{1-10^{-5},\Sigma^{2P},n/P,\Sigma^{KP}}(\cdot)$ exists. Observe that K is well-defined due to Theorem 3.7. We define $\theta_2 = 10^{-20}$ and $\eta_3 = 10^8 K$ and $\eta_4 = 10^7$ and assume without loss of generality that R is a multiple of $P+1$ and S is a multiple of $1100KP$. Fix an alphabet Σ, input and output sets X^A, X^B, Y^A, Y^B, and protocol Π in model `STANDARD` such that Π has T rounds and alphabet Σ. Our goal is to define a protocol Π' such that Theorem 5.1 holds. We begin by giving an informal overview of Π' in Subsection 5.1 and follow it up with the actual protocols in Subsection 5.2.

5.1 Informal Overview

In order to define the protocol Π', we build on the ideas described in Section 2. Broadly, the ideas in Section 2 can be divided into two parts. First, there are the consistency checks that takes up most of Section 2 and will be covered in Subsubsection 5.1.1. Additionally, there is the synchronization mechanism that was covered in Subsection 2.3 and will be further discussed in Subsubsection 5.1.2.

5.1.1 The Rewind Mechanism

As motivated in Section 2, the protocol Π' will break the protocol Π into small chunks, and simulate the protocol Π chunk by chunk. After each chunk of Π is simulated, the transcript generated is added to a transcript π that the protocol Π' maintains.

Alongside simulating the chunks, the protocol Π' also runs a rewind mechanism to detect and fix errors in the simulation of these chunks. Namely, if the parties detect an error in one of the chunks they simulated, they start going 'backwards' over the chunks to find the source of this error. When the parties are going backwards over the chunks, they add the transcripts of these chunk to a 'backwards transcript' ψ, that the protocol maintains. This means that at any point in the protocol, the parties will be maintaining two transcripts π and ψ, where the transcript ψ is different from the empty transcript ε only if the parties are going backwards over the chunks to find a source of an error they detected.

In fact, the crux of the protocol Π' is the rewind mechanism. As discussed in Section 2, this rewind mechanism takes place through a stack of tree codes maintained by the parties.

Structure of the stack of tree codes. The stack of tree codes maintained by the parties has two kinds of tree codes: forward tree codes and backward tree codes. The forward tree codes encode suffixes of the transcript π while the backward tree codes encode the transcript ψ. The stack of the tree code begins with a forward tree code and alternates between forward and backward tree codes, *i.e.*, the second tree code on the stack will be a backward tree code, the third one will be a forward tree code and so on. This implies that when the number of tree codes in the stack is odd, then the last tree code in the stack is a forward tree code and the protocol is going forward on the transcript π, and vice versa.

In fact, in our implementation, each of the tree codes in the stack is actually the same tree code, but is used to encode a different suffix of the transcripts π and ψ maintained by the protocol. Thus, an element in the stack will be completely characterized by a parameter r denoting the root of the tree code. A value r of the root (for forward tree codes) means that the tree code will be used to encode the suffix of π starting at position r. Besides r, we also store other information about tree codes in the variables t, α, and β. We explain these variables later. We will use $\mathscr{R}$ to denote the stack of tree codes.

To finish this part of the overview, we mention that although we store forward and backward tree codes alternately in the stack, the only backward tree code that we will ever use is the last backward tree code in the stack. Nonetheless, we keep the other backward tree codes as they help the presentation in places and only affect the communication by a constant factor.

Operations done on the tree codes. We next overview the operations performed on this stack of tree codes.

- The first and the most basic operation that the parties will need to perform on the stack is to add the transcripts of the simulated (or rewound) chunks, to the tree codes in the stack. When the parties are going forward, then this operation is simply adding the transcript, σ, of the chunk just simulated to π (Line 67). On the other hand, when the parties are going backwards, then this operation involves removing the transcript, σ, of the most recent chunk from π and adding it to the backwards transcript (Line 76 and Line 77)

- Besides adding the chunk transcripts to the tree codes present in the stack, we will also need to add fresh tree codes to the stack. Recall from Subsubsection 2.2.2 that every new tree code added to the stack has a reason associated with it. This reason is, at a high level, the discrepancy that led to this tree code. We now discuss how we add new tree codes and compute their reasons.

  When the parties are going forward, the parties turn and start going backward as soon as they see that the tree code encoding they computed (Γ) is different from the tree code encoding that they received ($\tilde{\Gamma}$). Before starting a new backward tree code in Line 70, the parties store this point where they turned in the variable t (Line 69) and the values of Γ and $\tilde{\Gamma}$ as the reason in the variable α. In fact, in our implementation, the parties store only the first place where Γ and $\tilde{\Gamma}$ were different as opposed to storing all of Γ and $\tilde{\Gamma}$. This seemingly weaker idea actually suffices.

  On the other hand, when the parties see a discrepancy in their encodings while going backward, they do not turn and start a forward tree code immediately. As explained in Subsubsection 2.2.2, the parties instead record this point of discrepancy in the variable t (Line 90), store the discrepancy as their reason (Line 91) in a variable β[8], and turn

[8]When the parties are going backward, Γ and $\tilde{\Gamma}$ have only one coordinate.

after the transcript sent over the backward tree code is double of what it was when the discrepancy was found. If this happens, then Line 80 is executed and the parties add a new forward tree code (and set ψ to ε as it is no longer needed).

Observe that, we treat the reason, α, for the backward tree codes differently from the reason, β, for the backward tree codes. As the parties turn from going forward to going backward immediately after seeing the discrepancy, they carry the reason for the backward tree code when they are going backward. On the other hand, the parties, when turning from backward to forward, do *not* turn immediately after seeing a discrepancy and therefore, need to carry the reason for the forward tree code both while going backward and going forward. To simplify our implementation, we only carry the reason for turning forward on the backward tree codes (this only affects the constants). Overall, the backward tree codes may have both α and β non-trivial, while the forward tree codes always have α and β set to $\perp$.

- Finally, we discuss dropping tree codes from the stack of tree codes. We note that the parties do not need a backward tree code in the stack once they add a new forward tree code on top of it. Nonetheless, we keep the backward tree code until the parties reach a point 'beyond' the backward tree code as it only costs us a constant factor overall. More precisely, when the parties turn forwards from backward, say at point r, then we keep these two tree codes until the point where $|\pi| \leq r$. When this happens, we drop both of these tree codes from the stack (Line 88). If the parties go back all the way to $|\pi| = 0$, we drop all the tree codes from the stack and reinitialize $\mathscr{R}$ and ψ (Line 84).

  It remains to discuss what happens when the parties drop a forward tree code. As explained in Subsubsection 2.2.2, the parties drop the forward tree codes after 'doubling' them. This is implemented in Line 73, where if the parties realized that they have double *any* of the forward tree codes in stack, the pop all the tree codes starting from the forward tree code that was doubled. To check whether there is a forward tree code that has been doubled, the parties go over all odd $i \in |\mathscr{R}|$ (recall that forward tree codes are stored in odd positions in the stack) and see if $2(\mathscr{R}[i].t - \mathscr{R}[i+2].r) \leq |\pi| - \mathscr{R}[i+2].r$, *i.e.*, they see if the length of the current transcript π is at least double of where the last forward tree turned to a backward, *i.e.*, $\mathscr{R}[i].t$, measured from the current root $\mathscr{R}[i+2].r$.

  Also recall from Subsubsection 2.2.2 that the tree codes need to have more and more redundancy as the stack of the parties grows deeper and deeper. This is done in Line 50 where we pad the long message sent by the parties to length $\max(\mathcal{O}(1.1^{|\mathscr{R}|}), p/2)$. The first term inside the $\max(\cdot)$ captures the redundancy while the second term is need to ensure that the parties can resynchronize if the adversary inserts corruptions and makes them unsynchronized. Its significance will be explained in Subsubsection 5.1.2.

5.1.2 The Synchronization Mechanism

We build on the sketch of the synchronization mechanism presented in Subsection 2.3. Recall that our synchronization mechanism largely mimics the synchronization mechanism of [BK12] for the most part, but has some non-trivial adaptations required to get it to work in model `LONG`.

In the synchronization mechanism of [BK12], the parties maintain a 'state' of the protocol. In [BK12], the value of this state was just the length of the transcript simulated so far. After simulating a fresh chunk of the protocol, the parties share their state with each other. If the states are the same, then both parties have local transcripts of the same length, and they continue the protocol as normal. On the other hand, if one party has a longer transcript than the other party, then, the party that is 'ahead' will rewind chunks, one at time, so that both the parties have transcripts of the same length.

The reason the parties share the length of the transcript simulated so far with each other is that this length is a natural measure of the amount of progress the parties have made in the simulation, *i.e.*, it is true that if a party in [BK12] has a longer transcript than the other party, and this party rewinds one chunk, then the two parties will only get closer to each other. This is no longer the case in our protocol, as the party who has a longer transcript may or may not be ahead of the other party, depending on whether the parties are going forwards or backwards.

In our protocol, the proper analogue of the length of the transcript simulated is the number of times the parties added a chunk (to either a forward or a backward tree code). In fact, our protocol keeps a list, $\boldsymbol{\mathcal{S}}$, of states, and adds an element to this list every time a symbol is added to any of the tree codes (Line 96). An element of the list $\boldsymbol{\mathcal{S}}$ is define by a tuple $(\mathscr{R}, \pi, \psi, p)$, where $\mathscr{R}$, π, and ψ are as above, and p is a new variable whose role is explained later. This tuple was designed to contain all the information needed by the parties to revert to a previous 'state' of the protocol and continue the execution from there.

The variable $\mathscr{P}$. The fact that our rewind mechanism deals with a stack with multiple tree codes creates an additional complication in the synchronization mechanism. Consider a situation where Alice and Bob have the same transcript π but two different stacks of tree codes. For simplicity, let us even assume that the set of the roots of the tree codes are not the same for Alice and Bob. In this case, even though the transcripts are the same for Alice and Bob, the fact that the roots are different means that the tree code encodings are potentially different, and the parties will not be able to continue with the simulation thinking that errors have happened.

In order to get around this problem, we have the parties exchange a few parameters of their stacks with each other. These parameters are $\mathscr{R}$, the stacks of tree codes, $|\pi|$ and $|\psi|$, the lengths of the forward and backward transcripts, and variable p that we explain later. These four parameters are captured in the variable $\mathscr{P}$. Note that, in particular, $\mathscr{P}$ contains the roots of all the tree codes and the lengths of the transcript and thus, the problem in the

foregoing paragraph does not arise.

Synchronization To summarize, after simulating every chunk the parties send the values $|\boldsymbol{\mathcal{S}}|$ and $\mathscr{P}$ to each other along with the encoding on the tree codes (Line 50). If these values match, then the parties add a symbol to their (either forward or backward) transcript (see Line 52).

If the value of $|\boldsymbol{\mathcal{S}}|$ agrees with the value received but the value of $\mathscr{P}$ does not, then the parties think that they have added the same number of symbols but there was a discrepancy in one of the tree codes that they added. (Both) the parties rewind one step in this case hoping to revert to a state where the values of $\mathscr{P}$ match[9]. This is done in Line 54. We next mention a subtlety of our protocol that makes Line 54 work. This subtlety arises because the number of bits sent by the parties in Line 50 is a function of the state the parties are in, and thus may be different for different states. Consider a situation where a state where the parties communicate a lot is followed immediate by a state where the parties communicate very little. If the parties wrongly (due to corruptions) decide to execute Line 54 in the iteration with little communication, then they actually end up rewinding a lot of communication due to a small number of errors. This is problematic, and the way we get around this problem is by ensuring that the communication in adjacent states differs by a factor of at most 2 in Line 50[10].

Lastly, the value of $|\boldsymbol{\mathcal{S}}|$ is greater than the value received by the party, then the party thinks that they are ahead of the other party and would like to rewind. As in the foregoing paragraph, we would like to rewind a number of states roughly 'equivalent' to the communication in this round. As the amount of communication may be different in different iterations, there is no direct correspondence between the amount of communication in a state to the number of states. This is where the variable p comes in. The variable p for a state in $\boldsymbol{\mathcal{S}}$ stores the amount of communication done by the parties to reach that state. In Line 56, we remove a number of states so that the sum of the corresponding p values is bounded by a constant times the amount of communication in this iteration.

5.2 Our Protocols

We build our protocols based on the overview given in Subsection 5.1. As described in Subsection 5.1, we design our protocols so that the parties maintain a list of states $\boldsymbol{\mathcal{S}}$. Each element in the list $\boldsymbol{\mathcal{S}}$ is described by a tuple $(\mathscr{R}, \pi, \psi, p)$. The parameters $\mathscr{P}$ that the parties exchange when the state is $(\mathscr{R}, \pi, \psi, p)$ are $(\mathscr{R}, |\pi|, |\psi|, p)$. Here, the variable $\mathscr{R}$ denotes the stack of tree codes, and we maintain four variables (r, t, α, β) for each element in this stack. Refer to Algorithm 3 for a description of these variables.

We consider both $\boldsymbol{\mathcal{S}}$ and $\mathscr{R}$ as lists and these two variables support the following operations:

[9] There exists such a state because both the parties start with the same state.

[10] The condition $10\tilde{l} < l$ before Line 54 arises due to a technicality in out analysis

Algorithm 3 Notation

structure $\mathcal{T}$

Tree code root	r	$\in \mathbb{N}$,
Turn	t	$\in \mathbb{N}$,
Reason for current tree code	α	$\in \mathbb{N} \times \Sigma^{KP} \times \Sigma^{KP}$,
Reason for turn	β	$\in \Sigma^{KP} \times \Sigma^{KP}$.

end structure

structure $\boldsymbol{\mathcal{S}}$ **contains a list of quadruples where each quadruple has**

Tree codes	$\mathscr{R}$	$\in \mathcal{T}^*$,
Transcript-F	π	$\in \left(\Sigma^{2P}\right)^*$,
Transcript-B	ψ	$\in \left(\Sigma^{2P}\right)^*$,
Previous communication	p	$\in \mathbb{N}$.

end structure

structure $\mathscr{P}$ **is a single quadruple that has**

Tree codes	$\mathscr{R}$	$\in \mathcal{T}^*$,
Length-F	$\lvert\pi\rvert$	$\in \mathbb{N}$,
Length-B	$\lvert\psi\rvert$	$\in \mathbb{N}$,
Previous communication	p	$\in \mathbb{N}$.

end structure

- **Length of the list:** We will use $|\boldsymbol{\mathcal{S}}|$ to denote the number of elements in the list $\boldsymbol{\mathcal{S}}$. We define $|\mathscr{R}|$ similarly.
- **Accessing an element in the list:** For $1 \leq i \leq |\boldsymbol{\mathcal{S}}|$, the notation $\boldsymbol{\mathcal{S}}[i]$ will denote the i^{th} element in $\boldsymbol{\mathcal{S}}$. When $i = |\boldsymbol{\mathcal{S}}|$, we sometimes use $\boldsymbol{\mathcal{S}}.last$ instead of $\boldsymbol{\mathcal{S}}[|\boldsymbol{\mathcal{S}}|]$. The variable π in the i^{th} element of $\boldsymbol{\mathcal{S}}$ will be denoted using $\boldsymbol{\mathcal{S}}[i].\pi$. The corresponding quantities for other fields in $\boldsymbol{\mathcal{S}}[i]$ and for the list $\mathscr{R}$ are defined analogously.
- **Adding elements to the list:** When we wish to add an element $e \in \mathcal{T}^* \times \left(\Sigma^{2P}\right)^* \times \left(\Sigma^{2P}\right)^* \times \mathbb{N}$ to $\boldsymbol{\mathcal{S}}$, we denote this using $\boldsymbol{\mathcal{S}}.\textsc{Add}(e)$. The element e is then added at the end of the list. Likewise for $\mathscr{R}$.
- **Removing elements in the list:** When we wish to remove the last element from $\boldsymbol{\mathcal{S}}$, we write $\boldsymbol{\mathcal{S}}.\textsc{Rem}()$. After this operation, the list has one less element. We write $\boldsymbol{\mathcal{S}}.\textsc{Rem}(i)$ to denote the operation of removing the last i elements in the list. Likewise for $\mathscr{R}$.

The notation $\mathscr{R}_{\text{F}}$ will be used to denote the sublist of $\mathscr{R}$ that contains all the elements in odd positions in $\mathscr{R}$. This notation derives from the fact that the odd positions in $\mathscr{R}$ are occupied by forward tree codes.

Also, we use the variables $\mathscr{R}$, π, ψ, p, and ℓ freely throughout the protocols we describe. These are our global variables and can be accessed from anywhere in the protocol. The variable ℓ will be reserved for the length of the message sent by the parties in Line 50. For brevity of notation, we define $\mathsf{TC}(\cdot) = \mathsf{TC}_{1-10^{-5},|\Sigma|^{2P},S/P,\Sigma^{KP}}(\cdot)$.

We describe our interactive coding scheme in Algorithm 4, which in turn, uses Algorithm 6 and Algorithm 5. We only write Alice's side of these protocols as Bob's side is symmetric. In our description, we use $\diamond$ to denote a fixed default value of the variables α, β described above.

Algorithm 4 Our interactive coding scheme showing Theorem 5.1 (Alice's side).

Input: An input $x^A \in X^A$.
Output: An element in Y^A.

40: $\boldsymbol{\mathcal{S}} \leftarrow [([(0,0,\diamond,\diamond)],\varepsilon,\varepsilon,0)]$.
41: **for** $i \in [R/(P+1)]$ **do**
42: $\quad(\mathscr{R},\pi,\psi,p) \leftarrow \boldsymbol{\mathcal{S}}.last$.
43: $\quad\mathscr{P} \leftarrow (\mathscr{R},|\pi|,|\psi|,p)$.
44: $\quad\sigma \leftarrow \texttt{Chunk}()$.
45: $\quad$**if** $|\mathscr{R}|$ is odd **then**
46: $\quad\quad\Gamma \leftarrow \left[\mathsf{TC}((\pi\|\sigma)_{>r}) \text{ for } (r,\cdot,\cdot,\cdot) \in \mathscr{R}_{\mathrm{F}}\right]$.
47: $\quad$**else**
48: $\quad\quad\Gamma \leftarrow [\mathsf{TC}(\psi\|\sigma)]$.
49: $\quad$**end if**
50: $\quad$Send $(\mathscr{P},|\boldsymbol{\mathcal{S}}|,\Gamma)$ and receive $(\tilde{\mathscr{P}},|\tilde{\boldsymbol{\mathcal{S}}}|,\tilde{\Gamma})$ as elements of Σ^*. Observe that $\Sigma^{500KP\cdot 1.1^{|\mathscr{R}|}}$ is large enough to ensure that the tuple $(\mathscr{P},|\boldsymbol{\mathcal{S}}|,\Gamma)$ can be interpreted as an element inside it. Alice pads her message so that it has $\ell \leftarrow \max(500KP\cdot 1.1^{|\mathscr{R}|}, p/2)$ symbols from Σ. Let $\tilde{\ell}$ be the number of symbols received.
$\quad$Alice makes sure that Equation 1 is satisfied in this step as follows: If her message violates Equation 1, she replaces it with the longest string of $\perp$s so that Equation 1 is satisfied. If this happens or if Alice receives a string of $\perp$ in this line, she does not execute Line 54 and Line 56 below.
51: $\quad$**if** $|\boldsymbol{\mathcal{S}}| = |\tilde{\boldsymbol{\mathcal{S}}}|$ **and** $\mathscr{P} = \tilde{\mathscr{P}}$ **then**
52: $\quad\quad$AddSym$(\sigma,\Gamma,\tilde{\Gamma})$.
53: $\quad$**else if** $|\boldsymbol{\mathcal{S}}| = |\tilde{\boldsymbol{\mathcal{S}}}|$ **or** $10\tilde{\ell} < \ell$ **then**
54: $\quad\quad\boldsymbol{\mathcal{S}}$.Rem().
55: $\quad$**else if** $|\boldsymbol{\mathcal{S}}| > |\tilde{\boldsymbol{\mathcal{S}}}|$ **then**
56: $\quad\quad\boldsymbol{\mathcal{S}}$.Rem$(\min(\mu, |\boldsymbol{\mathcal{S}}| - |\tilde{\boldsymbol{\mathcal{S}}}| + \mathbb{1}(10\ell < \tilde{\ell})))$ where μ is the smallest integer that satisfies $\sum_{h=1}^{\mu} \boldsymbol{\mathcal{S}}[|\boldsymbol{\mathcal{S}}|+1-h].p > 10(\ell+\tilde{\ell})$ (we set $\mu = |\boldsymbol{\mathcal{S}}|+1$ if none exist).
57: $\quad$**end if**
58: **end for**
59: $(\mathscr{R},\pi,\psi,p) \leftarrow \boldsymbol{\mathcal{S}}.last$.
60: Output $g^A(x^A, \pi[1:T/P])$ interpreting $\pi[1:T/P]$ as an element of Σ^{2T}.

6 Analysis

We work with the $\Sigma, X^A, X^B, Y^A, Y^B$, and Π that we fixed in the beginning of Section 5. Recall that Π has T rounds. The furthermore part of Theorem 5.1 is easily observed from

Algorithm 5 The Protocol `Chunk`.

Alice simulates the next P rounds of the protocol Π assuming input x^A and transcript π. Formally, let π_{even} denote the even coordinates of π when it is interpreted as a string in Σ^*. Alice runs the protocol $\mathfrak{C} = \{f^C_{\mathfrak{C}}, g^C_{\mathfrak{C}}\}_{C\in\{A,B\}}$ with P rounds where, we have $f^A_{\mathfrak{C}}(x^A, \varsigma) = f^A(x^A, \pi_{even}\|\varsigma)$ for all $\varsigma \in \Sigma^{<P}$ and $g^C_{\mathfrak{C}}$ is the function that simply returns its second argument. Note that the output space of the protocol $\mathfrak{C}$ is Σ^{2P}. She sets σ to be the output of the protocol $\mathfrak{C}$.
if $|\mathscr{R}|$ is even **then**
    $\sigma \leftarrow \pi[|\pi|]$.
end if
return σ.

Algorithm 6 The Protocol $\textsc{AddSym}(\sigma, \Gamma, \tilde{\Gamma})$.

if $|\mathscr{R}|$ is odd **then**
    $\pi \leftarrow \pi\|\sigma$.
    if $\Gamma \neq \tilde{\Gamma}$ **then**
        $\mathscr{R}.last.t \leftarrow |\pi|$.
        $\mathscr{R}.\textsc{Add}(|\pi|, 0, (\mathscr{R}_{\mathrm{F}}[h].r, \Gamma_h, \tilde{\Gamma}_h), \diamond)$ where h is the smallest such that $\Gamma_h \neq \tilde{\Gamma}_h$.
    else
        $d^* \leftarrow$ smallest odd number ($|\mathscr{R}|$, if none exist) such that $2\mathscr{R}[d].t - \mathscr{R}[d+2].r \leq |\pi|$.
        $\mathscr{R}.\textsc{Rem}(|\mathscr{R}| - d^*)$.
    end if
else
    $\psi \leftarrow \psi\|\sigma$.
    $\pi \leftarrow \pi_{<|\pi|}$.
    if $|\psi| = 2(\mathscr{R}.last.r - \mathscr{R}.last.t)$ **then**
        $\mathscr{R}.last.\alpha, \mathscr{R}.last.\beta \leftarrow \diamond$.
        $\mathscr{R}.\textsc{Add}(|\pi|, 0, \diamond, \diamond)$.
        $\psi \leftarrow \varepsilon$.
    else
        if $|\pi| = 0$ **then**
            $\mathscr{R} \leftarrow [(0, 0, \diamond, \diamond)]$.
            $\psi \leftarrow \varepsilon$.
        else
            Let d^* be the largest (possibly 0) such that $\forall d' \in [d^*] : \mathscr{R}[|\mathscr{R}| - 2d' + 1].r = |\pi|$.
            Delete positions d' from $\mathscr{R}$ for all $|\mathscr{R}| - 2d^* \leq d' < |\mathscr{R}|$.
            if $\Gamma \neq \tilde{\Gamma}$ **and** $\mathscr{R}.last.t = 0$ **then**
                $\mathscr{R}.last.t \leftarrow \mathscr{R}.last.r - |\psi|$. As $|\pi| > 0$, we have $\mathscr{R}.last.r > |\psi|$ in this line.
                $\mathscr{R}.last.\beta \leftarrow (\Gamma_1, \tilde{\Gamma}_1)$. Note that $|\Gamma| = |\tilde{\Gamma}| = 1$ in this case.
            end if
        end if
    end if
end if
$\boldsymbol{\mathcal{S}}.\textsc{Add}(\mathscr{R}, \pi, \psi, \ell)$.

the description of Π'. Thus, to prove Theorem 5.1, it remains to show that:

Theorem 6.1. *For any adversary $\mathcal{A}'$ for Π', and for all inputs $x^A \in X^A$ and $x^B \in X^B$, for all $C \in \{A, B\}$, we have that:*

$$\mathsf{corr}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta_2 S \implies \Pi'^C_{\mathcal{A}'}(x^A, x^B) = \Pi^C(x^A, x^B).$$

6.1 Notations and Framework

We fix an adversary $\mathcal{A}'$ and inputs $x^A \in X^A, x^B \in X^B$ such that $\mathsf{corr}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta_2 S$ for the rest of this paper.

As the protocol Π' is deterministic, fixing the inputs and the adversary fixes the values of all the variables in all the iterations of the loop in Line 41 (for both Alice and Bob). For $i \in [R/(P+1)]$ and a variable *var* other than σ, we will use var_i^A to denote the value of the variable *var* the first time it is set in iteration i of the loop in Line 41 in Alice's execution of Algorithm 4. For a variable like $\boldsymbol{\mathcal{S}}$ that is defined once for all the iterations, the value $\boldsymbol{\mathcal{S}}_i^A$ will denote the value of $\boldsymbol{\mathcal{S}}$ at the beginning of Alice's execution of iteration i. When we omit the subscript i or when $i = R/(P+1)+1$, we mean the value of *var* at the end of Alice's execution of Algorithm 4. We define var_i^B and var^B analogously with Alice replaced by Bob. Also, the notation σ_i^A will denote the value of σ after Algorithm 5 is executed by Alice in iteration i. The notation σ_i^B is defined similarly.

Recall that the variable $\mathscr{R}$ is a list of tuples of the form (r, t, α, β). We will use $\mathscr{R}'$ to denote the same list with the last two entries omitted from each entry in the list, *i.e.*, for every entry (r, t, α, β) in $\mathscr{R}$, the list $\mathscr{R}'$ will have the entry (r, t). We define the variable $\mathscr{Q} = (\mathscr{R}', |\pi|, |\psi|, p)$. Observe that, due to Line 79, if $(\mathscr{R}, \pi, \psi, p)$ is the quadruple from Line 42 in our protocol, we may have $\alpha, \beta \neq \diamond$ only for the last element in $\mathscr{R}$. Thus, the quadruple $(\mathscr{R}, \pi, \psi, p)$ is determined by $\mathscr{Q}, \pi \| \psi, \mathscr{R}.last.\alpha, \mathscr{R}.last.\beta$

For $C \in \{A, B\}$, we define $\mathfrak{E}^C(l)$ to be the set of all iterations i such that party C executes Line l in iteration i. Also define, for $i \in [R/(P+1)]$, the values $\mathsf{corr}_i^A = \mathsf{corr}^{A\to B}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B, i)$, $\mathsf{corr}_i^B = \mathsf{corr}^{B\to A}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B, i)$, and $\mathsf{corr}_i = \mathsf{corr}_i^A + \mathsf{corr}_i^B$.

Finally, for a part of this section, we will need to consider another adversary $\mathcal{A}''$ for Π'. When we refer to the value of a variable (or the value of corr) in the execution of Π' in the presence of these adversaries (with the same inputs), we explicitly write the adversaries either in parenthesis or as a subscript. Thus, we may write $\mathscr{Q}_5^A(\mathcal{A}'')$ or $\mathsf{corr}_2^B(\mathcal{A}'')$, *etc.*

Proof of Theorem 6.1. We show Theorem 6.1 in two steps. First, we show that, at the cost of changing the constants in the theorem, we can assume that the adversary $\mathcal{A}'$ has a particular structure. More precisely,

Theorem 6.2. *There is an adversary $\mathcal{A}''$ for Π' and $num > 0$ such that the following hold:*

1. *We have $[num-1] \subseteq \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$ and for all $i \in [num]$, it holds that*

$$(\mathscr{Q}_i^A(\mathcal{A}''), |\boldsymbol{\mathcal{S}}_i^A(\mathcal{A}'')|) = (\mathscr{Q}_i^B(\mathcal{A}''), |\boldsymbol{\mathcal{S}}_i^B(\mathcal{A}'')|).$$

Furthermore, $\boldsymbol{\mathcal{S}}_i^C(\mathcal{A}'') = \boldsymbol{\mathcal{S}}_{num}^C(\mathcal{A}'')$ *for all* $num \le i \le R/(P+1)+1$ *and* $C \in \{A, B\}$.

2. *It holds that:*

$$\sum_{i<num} \ell_i^A(\mathcal{A}'') + \ell_i^B(\mathcal{A}'') \ge S/500. \qquad \sum_{i<num} \mathsf{corr}_i(\mathcal{A}'') \le 10^7\theta_2 S.$$

3. *We have:*

$$\forall C \in \{A,B\} : \Pi'^C_{\mathcal{A}''}(x^A, x^B) = \Pi^C(x^A, x^B) \implies \forall C \in \{A,B\} : \Pi'^C_{\mathcal{A}'}(x^A, x^B) = \Pi^C(x^A, x^B).$$

Fix $\mathcal{A}''$ and *num* to be the ones promised by Theorem 6.2 for the rest of this paper. We finish the proof of Theorem 6.1 by showing that:

Theorem 6.3. *For all* $C \in \{A, B\}$*, we have that* $\Pi'^C_{\mathcal{A}''}(x^A, x^B) = \Pi^C(x^A, x^B)$.

□

6.2 Proof of Theorem 6.3

We now prove Theorem 6.3. Recall that $\mathcal{A}''$ and $num > 0$ are the values promised by Theorem 6.2. As we will restrict attention to the adversary $\mathcal{A}''$, we will drop it from our notation for variables, *etc.* That is, the notation var_i^A will denote $var_i^A(\mathcal{A}'')$, $\mathfrak{E}(\cdot)$ will denote $\mathfrak{E}(\mathcal{A}'', \cdot)$, *etc.*[11]

We have from item 1 in Theorem 6.2 that $[num-1] \subseteq \mathfrak{E}^A(52) \cap \mathfrak{E}^B(52)$ and for all $i \in [num]$,

$$(\mathscr{Q}_i^A, |\boldsymbol{\mathcal{S}}_i^A|) = (\mathscr{Q}_i^B, |\boldsymbol{\mathcal{S}}_i^B|).$$

It follows from the definition of $\mathscr{Q}$, $\mathscr{R}'$, and ℓ that $(\mathscr{R}_i'^A, |\pi_i^A|, |\psi_i^A|, p_i^A, |\boldsymbol{\mathcal{S}}_i^A|, |\mathscr{R}_i^A|, \ell_i^A) = (\mathscr{R}_i'^B, |\pi_i^B|, |\psi_i^B|, p_i^B, |\boldsymbol{\mathcal{S}}_i^B|, |\mathscr{R}_i^B|, \ell_i^B)$ for all $i \in [num]$. Due to this equality, we drop the superscripts A and B from these quantities. We also drop the superscripts from $\mathfrak{E}(\cdot)$ when it is clear that the value of $\mathfrak{E}^A(\cdot)$ and $\mathfrak{E}^B(\cdot)$ are the same.

We consider the first *num* iterations of Π' when executed in the presence of $\mathcal{A}''$. Owing to the furthermore part of item 1 of Theorem 6.2, we have for $C \in \{A, B\}$ that $\pi_{num}^C = \pi^C$. Using this together with Algorithm 5 and the definition of $\Pi^C(x^A, x^B)$, we get that in order to prove Theorem 6.3, it is sufficient to show that $\pi_{num}^A[1 : T/P] = \pi_{num}^B[1 : T/P]$.

Recall that we use $\mathsf{LCP}(u, v)$ to denote the longest common prefix of two strings u, v. Thus, all we have to show is that $|\mathsf{LCP}\left(\pi_{num}^A, \pi_{num}^B\right)| \ge T/P$. This follows from the following theorem, our choice of S, and item 2 of Theorem 6.2.

[11] This should not be confused with our notation in Subsection 6.1 and Subsection 6.3, where we dropped the adversary $\mathcal{A}'$ from our notation for variables. The adversary $\mathcal{A}'$ will not appear anywhere in this section.

Theorem 6.4. *It holds that:*

$$\sum_{i<num} \ell_i \leq 16 \cdot \ell_1 \cdot |\mathsf{LCP}\left(\pi^A_{num}, \pi^B_{num}\right)| + 10^5 \cdot \sum_{i<num} \mathsf{corr}_i.$$

Proof. Note that $\ell_i = \max(500KP \cdot 1.1^{|\mathscr{R}_i|}, p_i/2)$ for $i \in [num]$, where $p_i = \ell_{i-1}$ for $i > 1$ and $p_1 = 0$. This gives:

$$\sum_{i<num} \ell_i \leq \sum_{i<num} 500KP \cdot 1.1^{|\mathscr{R}_i|} + \ell_{i-1}/2 \cdot \mathbb{1}(i > 1),$$

implying that $\sum_{i<num} \ell_i \leq \sum_{i<num} 1000KP \cdot 1.1^{|\mathscr{R}_i|}$. Thus, in order to finish the proof it is sufficient to show that $\sum_{i<num} \ell^*_i \leq 8 \cdot \ell^*_1 \cdot |\mathsf{LCP}\left(\pi^A_{num}, \pi^B_{num}\right)| + 10^5 \cdot \sum_{i<num} \mathsf{corr}_i$, where $\ell^*_i = 1000KP \cdot 1.1^{|\mathscr{R}_i|}$ for $i \in [num]$. We show this in Subsubsection 6.2.11 below. □

6.2.1 Our Framework

Define the sets $\textsc{Starts}_\textsc{F} = \mathfrak{E}(80) \cup \mathfrak{E}(84) \cup \{0\}$ and $\textsc{Starts}_\textsc{B} = \mathfrak{E}(70)$. Observe that the sets $\textsc{Starts}_\textsc{F}$ and $\textsc{Starts}_\textsc{B}$ are disjoint. Let the set:

$$\textsc{Starts} = \textsc{Starts}_\textsc{F} \cup \textsc{Starts}_\textsc{B}.$$

For $i \in \textsc{Starts}$, define the function:

$$\textsc{Stop}(i) = \begin{cases} \arg\min\{i < i' \leq num \mid i' \in \mathfrak{E}(84)\} & , i \in \mathfrak{E}(84) \cup \{0\} \\ \arg\min\{i < i' \leq num \mid |\mathscr{R}_{i'}| < |\mathscr{R}_{i+1}|\} - 1 & , i \in \mathfrak{E}(70) \cup \mathfrak{E}(80) \end{cases}.$$

If any of the $\arg\min$ is over an empty set, then we define $\textsc{Stop}(i) = num$ and say that i is 'fixed' . If $i \in \textsc{Starts}$ is not fixed, we say that i is 'direct' if $|\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{i+1}|$ is even. Otherwise, we say that i is indirect. Let $\textsc{Range}(i) = (i : \textsc{Stop}(i)]$. We make the following observations about our protocol.

Fact 6.5. *It holds that:*

1. *For all $0 \leq i < num$, we have $|\mathscr{R}_{i+1}| \geq 1$, with equality when $i \in \mathfrak{E}(84) \cup \{0\}$ and strict inequality when $i \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$.*

2. *For all $1 \leq i < num$, we have $|\mathscr{R}_{i+1}| \leq |\mathscr{R}_i| + 1$ with strict inequality unless $i \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$.*

3. *For all $i \in \textsc{Starts}$, we have $(i : \textsc{Stop}(i)) \cap \mathfrak{E}(84) = \emptyset$. Furthermore, for all $j \in \textsc{Range}(i)$, we have $|\mathscr{R}_j| \geq |\mathscr{R}_{i+1}|$.*

4. *For all $1 \leq i < num$ and $C \in \{A, B\}$, we have $\mathscr{R}^C_i[1 : \min(|\mathscr{R}_{i+1}|, |\mathscr{R}_i|)) = \mathscr{R}^C_{i+1}[1 : \min(|\mathscr{R}_{i+1}|, |\mathscr{R}_i|))$. In particular, due to item 3, for all $i \in \textsc{Starts}$, $j, j' \in \textsc{Range}(i)$, and all $C \in \{A, B\}$, we have $\mathscr{R}^C_j[1 : |\mathscr{R}_{i+1}|) = \mathscr{R}^C_{j'}[1 : |\mathscr{R}_{i+1}|)$.*

5. *For all* $1 \le i < num$ *and all* $C \in \{A, B\}$, *if* $|\mathscr{R}_i|$ *is odd, we have* $\pi_{i+1}^C = \pi_i^C \| \sigma_i^C$, *and if* $|\mathscr{R}_i|$ *is even, we have* $\pi_{i+1}^C = \pi_i^C[1 : |\pi_i|)$ *and* $\sigma_i^C = \pi_i^C[|\pi_i|]$. *If* $|\mathscr{R}_i|$ *is even and* $i \notin \textsc{Starts}$, *we have* $\psi_{i+1}^C = \psi_i^C \| \sigma_i^C$.

6. *For all* $i \in \textsc{Starts}$, *we have* $\mathscr{R}_{i+1}.last.r = |\pi_{i+1}|$.

7. *For all* $i \in \textsc{Starts}$ *that are not fixed, we have* $\textsc{Stop}(i) \in \mathfrak{E}(84) \cup \mathfrak{E}(73) \cup \mathfrak{E}(88)$.

8. *For all* $1 \le i < num$ *and all odd* $d \le \min(|\mathscr{R}_{i+1}|, |\mathscr{R}_i|)$, *we have* $\mathscr{R}_i[d].r = \mathscr{R}_{i+1}[d].r$. *In particular, due to item 3 and item 6, we have for all* $i \in \textsc{Starts}_{\mathrm{F}}$ *and* $j \in \textsc{Range}(i)$ *that* $|\pi_{i+1}| = \mathscr{R}_j[|\mathscr{R}_{i+1}|].r$.

9. *For all* $1 \le i \le i' \le num$ *such that* $|\mathscr{R}_{i''}|$ *is even for all* $i'' \in [i : i']$ *and* $C \in \{A, B\}$, *we have* $(\mathscr{R}_{i'}.last.r, \mathscr{R}_{i'}^C.last.\alpha) = (\mathscr{R}_i.last.r, \mathscr{R}_i^C.last.\alpha)$. *If* $\mathscr{R}_i.last.t > 0$, *we also have* $(\mathscr{R}_{i'}.last.t, \mathscr{R}_{i'}^C.last.\beta) = (\mathscr{R}_i.last.t, \mathscr{R}_i^C.last.\beta)$.

10. *For all* $i \in [num]$ *such that* $|\mathscr{R}_i|$ *is even, we have* $|\psi_i| + |\pi_i| = \mathscr{R}_i.last.r > 0$. *Furthermore, if* $|\mathscr{R}_i|$ *is odd, then* $|\psi_i| = 0$.

11. *For all* $1 \le i < num$ *such that* $|\mathscr{R}_i|$ *is even, we have* $|\psi_i| < 2\,(\mathscr{R}_i.last.r - \mathscr{R}_i.last.t)$. *It follows by item 10 that* $i \in \mathfrak{E}(80)$ *implies* $\mathscr{R}_i.last.t > 0$. *If* $\mathscr{R}_{i+1}.last.t > 0$, *we also have* $|\psi_i| + 1 \ge \mathscr{R}_{i+1}.last.r - \mathscr{R}_{i+1}.last.t$.

Lemma 6.6. *For all* $i \in [num]$, *if* $|\mathscr{R}_i|$ *is odd, then we have*

$$\mathscr{R}_i[1].r \le \mathscr{R}_i[3].r \le \cdots \le \mathscr{R}_i.last.r \le |\pi_i| < \min_{\text{odd } d < |\mathscr{R}_i| - 1} 2\mathscr{R}_i[d].t - \mathscr{R}_i[d+2].r.$$

On the other hand, if $|\mathscr{R}_i|$ *is even, then we have*

$$\mathscr{R}_i[1].r \le \cdots \le \mathscr{R}_i[|\mathscr{R}_i|-1].r < |\pi_i| \le \min\left(\mathscr{R}_i[|\mathscr{R}_i| - 1].t, \min_{\text{odd } d < |\mathscr{R}_i| - 1} 2\mathscr{R}_i[d].t - \mathscr{R}_i[d+2].r\right).$$

Furthermore,

- *In either case, for all odd* $d < |\mathscr{R}_i| - 1$, *we have*

$$\mathscr{R}_i[d].t > \mathscr{R}_i[d+2].r.$$

- *If* $i \in \mathfrak{E}(73)$ *and* $d_i^* < |\mathscr{R}_i|$, *we have*

$$|\pi_{i+1}| = 2\mathscr{R}_i[|\mathscr{R}_{i+1}|].t - \mathscr{R}_i[|\mathscr{R}_{i+1}| + 2].r$$

Proof. Proof by induction on i. The base case $i = 1$ is straightforward. We assume the claim holds for $i < num$ and show it for $i + 1$. We consider various cases:

- If $i \in \mathfrak{E}(67)$, then $|\pi_{i+1}| = |\pi_i| + 1$. We have:

– If $i \in \mathfrak{E}$(70), then a new entry gets added to $\mathscr{R}$ in iteration i, $|\mathscr{R}_{i+1}|$ is even, and the r field in other entries does not change. Thus, $\mathscr{R}_i[1].r \leq \mathscr{R}_i[3].r \leq \cdots \leq \mathscr{R}_i.last.r \leq |\pi_i|$ implies $\mathscr{R}_{i+1}[1].r \leq \mathscr{R}_{i+1}[3].r \leq \cdots \leq \mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].r \leq |\pi_i| < |\pi_{i+1}|$.
Furthermore, as the t entry only changes in $\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1]$ and $\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t = |\pi_{i+1}|$, we have

$$\begin{aligned}|\pi_{i+1}| &= |\pi_i| + 1 \\ &\leq \min\left(\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t, \min_{\text{odd } d<|\mathscr{R}_i|-1} 2\mathscr{R}_i[d].t - \mathscr{R}_i[d+2].r\right) \\ &= \min\left(\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t, \min_{\text{odd } d<|\mathscr{R}_{i+1}|-1} 2\mathscr{R}_{i+1}[d].t - \mathscr{R}_{i+1}[d+2].r\right).\end{aligned}$$

The furthermore part is straightforward as none of the relevant fields change.

– Otherwise, $i \in \mathfrak{E}$(73), then an even number of entries are removed from the end of $\mathscr{R}$ in iteration i. Thus, the induction hypothesis $\mathscr{R}_i[1].r \leq \mathscr{R}_i[3].r \leq \cdots \leq \mathscr{R}_i.last.r \leq |\pi_i|$ with Line 73 implies $\mathscr{R}_{i+1}[1].r \leq \mathscr{R}_{i+1}[3].r \leq \cdots \leq \mathscr{R}_{i+1}.last.r \leq |\pi_i| < |\pi_{i+1}|$.
Additionally, by definition of d^*, we have

$$|\pi_{i+1}| < \min_{\text{odd } d<|\mathscr{R}_{i+1}|-1} 2\mathscr{R}_{i+1}[d].t - \mathscr{R}_{i+1}[d+2].r.$$

The furthermore parts are straightforward.

• If $i \in \mathfrak{E}$(76), then $|\pi_{i+1}| = |\pi_i| - 1$. We have:

– If $i \in \mathfrak{E}$(80), then a new entry gets added to $\mathscr{R}$ in iteration i, $|\mathscr{R}_{i+1}|$ is odd, and the r and t field in other entries does not change. Furthermore, $\mathscr{R}_{i+1}.last.r = |\pi_{i+1}|$. Thus, $\mathscr{R}_i[1].r \leq \mathscr{R}_i[3].r \leq \cdots \leq \mathscr{R}_i[|\mathscr{R}_i| - 1].r < |\pi_i|$ implies $\mathscr{R}_{i+1}[1].r \leq \mathscr{R}_{i+1}[3].r \leq \cdots \leq \mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 2].r \leq |\pi_i| - 1 = |\pi_{i+1}| = \mathscr{R}_{i+1}.last.r$.
Furthermore, we have

$$\begin{aligned}&\min_{\text{odd } d<|\mathscr{R}_{i+1}|-1} 2\mathscr{R}_{i+1}[d].t - \mathscr{R}_{i+1}[d+2].r \\ &\quad= \min\left(2\mathscr{R}_i[|\mathscr{R}_i| - 1].t - \mathscr{R}_{i+1}.last.r, \min_{\text{odd } d<|\mathscr{R}_i|-1} 2\mathscr{R}_i[d].t - \mathscr{R}_i[d+2].r\right) \\ &\quad\geq \min\left(2|\pi_i| - |\pi_{i+1}|, |\pi_i|\right) > |\pi_{i+1}|.\end{aligned}$$

For the furthermore part, as the other relevant fields do not change, it is enough to show that $\mathscr{R}_i[|\mathscr{R}_i| - 1].t > \mathscr{R}_{i+1}.last.r = |\pi_{i+1}| = |\pi_i| - 1$ which holds due to the induction hypothesis.

– If $i \in \mathfrak{E}$(84), then $\mathscr{R}^C_{i+1} = [(0, 0, \diamond, \diamond)]$ for $C \in \{A, B\}$, and the induction step is straightforward.

– Otherwise, we have $i \in \mathfrak{E}(87)$. Using the definition of d^* and the induction hypothesis, we get $\mathscr{R}_i[1].r \leq \mathscr{R}_i[3].r \leq \cdots < \mathscr{R}_i[|\mathscr{R}_i| - 2d^* + 1].r = \cdots = \mathscr{R}_i[|\mathscr{R}_i| - 1].r = |\pi_{i+1}| = |\pi_i| - 1 < |\pi_i|$. We execute Line 88 and possibly also execute Line 90. The former deletes the entries at positions $[|\mathscr{R}_i| - 2d_i^* : |\mathscr{R}_i|)$ from $\mathscr{R}$ while the latter does not affect the r and t fields in any of the odd entries. Thus, to show that $\mathscr{R}_{i+1}[1].r \leq \mathscr{R}_{i+1}[3].r \leq \cdots \leq \mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].r < |\pi_{i+1}|$, we need to show $\mathscr{R}_i[1].r \leq \mathscr{R}_i[3].r \leq \cdots \leq \mathscr{R}_i[|\mathscr{R}_i| - 2d^* - 1].r < |\pi_{i+1}|$, which holds by definition of d^*.

  Furthermore, if $d^* = 0$, then we have

$$\begin{aligned} |\pi_{i+1}| < |\pi_i| &\leq \min\left(\mathscr{R}_i[|\mathscr{R}_i| - 1].t, \min_{\text{odd } d<|\mathscr{R}_i|-1} 2\mathscr{R}_i[d].t - \mathscr{R}_i[d+2].r\right) \\ &= \min\left(\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t, \min_{\text{odd } d<|\mathscr{R}_{i+1}|-1} 2\mathscr{R}_{i+1}[d].t - \mathscr{R}_{i+1}[d+2].r\right). \end{aligned}$$

  On the other hand, if $d^* > 0$, then we have

$$\begin{aligned} |\pi_{i+1}| &= |\pi_i| - 1 \\ &\leq \min\left(\mathscr{R}_i[|\mathscr{R}_i| - 2d^* + 1].r, \min_{\text{odd } d<|\mathscr{R}_i|-1} 2\mathscr{R}_i[d].t - \mathscr{R}_i[d+2].r\right) \\ &\leq \min\left(\mathscr{R}_i[|\mathscr{R}_i| - 2d^* - 1].t, \min_{\text{odd } d<|\mathscr{R}_{i+1}|-1} 2\mathscr{R}_i[d].t - \mathscr{R}_i[d+2].r\right) \\ &= \min\left(\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t, \min_{\text{odd } d<|\mathscr{R}_{i+1}|-1} 2\mathscr{R}_{i+1}[d].t - \mathscr{R}_{i+1}[d+2].r\right). \end{aligned}$$

  The furthermore part is straightforward as none of the relevant fields change.

□

Lemma 6.7. *For $i < i' \in$ STARTS , either* $\text{RANGE}(i) \cap \text{RANGE}(i') = \emptyset$ *or* $\text{RANGE}(i') \subseteq \text{RANGE}(i)$.

Proof. If i is fixed, the result is straightforward. So we assume that i is not fixed. We first assume $i \in \mathfrak{E}(84) \cup \{0\}$ so that $\text{STOP}(i) = \arg\min\{i < i'' \leq num \mid i'' \in \mathfrak{E}(84)\}$. If $i' \geq \text{STOP}(i)$, we are done as $\text{RANGE}(i') \cap \text{RANGE}(i) = \emptyset$. On the other hand, if $i' < \text{STOP}(i)$, then using the fact that $i' \in$ STARTS, it follows that $i' \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$. In this case, we show that $\text{RANGE}(i') \subseteq \text{RANGE}(i)$ by showing that $\text{STOP}(i) \geq \text{STOP}(i')$. To see why the latter holds, use item 1 of Fact 6.5 to get

$$|\mathscr{R}_{\text{STOP}(i)+1}| = 1 < 2 \leq |\mathscr{R}_{i'+1}|.$$

Now, assume that $i \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$ so that $\text{STOP}(i) = \arg\min\{i < i'' \leq num \mid |\mathscr{R}_{i''}| < |\mathscr{R}_{i+1}|\} - 1$. If $i' \geq \text{STOP}(i)$, we are done as $\text{RANGE}(i') \cap \text{RANGE}(i) = \emptyset$. On the other hand, if $i' < \text{STOP}(i)$, then we claim that $i' \notin \mathfrak{E}(84) \cup \{0\}$. Otherwise, by item 1 of Fact 6.5, we

have

$$|\mathscr{R}_{i'+1}| = 1 < 2 \leq |\mathscr{R}_{i+1}|,$$

contradicting $i' < \textsc{Stop}(i)$. Now, we use $i' \in \textsc{Starts}$ to get $i' \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$. As $i' < \textsc{Stop}(i)$, we get $|\mathscr{R}_{i'+1}| \geq |\mathscr{R}_{i+1}|$ and, in turn, $\textsc{Stop}(i) \geq \textsc{Stop}(i')$. It follows that $\textsc{Range}(i') \subseteq \textsc{Range}(i)$. □

Midpoints. For $i \in \textsc{Starts}$, define

$$\textsc{Mid}(i) = \max\{i' \in \textsc{Range}(i) \mid |\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|\}.$$

Observe that $\textsc{Mid}(i)$ is well defined as the maximum is taken over a non-empty (as it contains $i+1$) set. Also, for $i \in \textsc{Starts} \setminus \{0\}$, define $\textsc{Prev}(i) = \max\{i' < i \in \textsc{Starts} \mid |\mathscr{R}_{i'+1}| = |\mathscr{R}_i|\}$. This is well defined as the set over which the maximum is taken is non-empty. Indeed, if $|\mathscr{R}_i| = 1$, then 0 is in the set. Otherwise, if $|\mathscr{R}_i| > 1$, then, using the fact that $|\mathscr{R}|$ increases by at most 1 in each iteration and only increases in iterations in $\textsc{Starts}$, we can conclude that there is $i' < i \in \textsc{Starts}$ such that $|\mathscr{R}_{i'+1}| = |\mathscr{R}_i|$ and the set, therefore, is non-empty.

Lemma 6.8. *For $i \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$, we have $\textsc{Range}(i) \subseteq \textsc{Range}(\textsc{Prev}(i))$.*

Proof. Owing to Lemma 6.7, it is sufficient to show that $\textsc{Stop}(\textsc{Prev}(i)) > i$. Suppose for the sake of contradiction that $\textsc{Stop}(\textsc{Prev}(i)) \leq i$ implying that $\textsc{Prev}(i)$ is not fixed. Due to item 7 of Fact 6.5, we have that $\textsc{Stop}(\textsc{Prev}(i)) < i$. This gives $\textsc{Prev}(i) \notin \mathfrak{E}(84) \cup \{0\}$ as otherwise $\textsc{Stop}(\textsc{Prev}(i)) \in \textsc{Starts}$ and $|\mathscr{R}_{\textsc{Stop}(\textsc{Prev}(i))+1}| = |\mathscr{R}_{\textsc{Prev}(i)+1}| = |\mathscr{R}_i|$ contradicting the definition of $\textsc{Prev}(i)$.

Thus, we must have $\textsc{Prev}(i) \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$ in which case $|\mathscr{R}_{\textsc{Stop}(\textsc{Prev}(i))+1}| < |\mathscr{R}_{\textsc{Prev}(i)+1}| = |\mathscr{R}_i|$. As $|\mathscr{R}|$ increases by at most 1 in each iteration and only increases in iterations in $\textsc{Starts}$, we can conclude that there is $\textsc{Stop}(\textsc{Prev}(i)) < i'' < i \in \textsc{Starts}$ such that $|\mathscr{R}_{i''+1}| = |\mathscr{R}_i|$ contradicting the definition of $\textsc{Prev}(i)$. □

Lemma 6.9. *For all $i \in \textsc{Starts}$ that are indirect, we have:*

- $\textsc{Mid}(i) < \textsc{Stop}(i)$.
- *If $i \in \textsc{Starts}_{\mathrm{F}}$, then $\textsc{Mid}(i) \in \mathfrak{E}(70)$. If $i \in \textsc{Starts}_{\mathrm{B}}$, then $\textsc{Mid}(i) \in \mathfrak{E}(80)$.*
- $\textsc{Stop}(\textsc{Mid}(i)) = \textsc{Stop}(i)$.
- $\textsc{Prev}(\textsc{Mid}(i)) = i$.

Proof. We prove each part in turn:

- For the first part, it is sufficient to show that $|\mathscr{R}_{\textsc{Stop}(i)}| > |\mathscr{R}_{i+1}|$. If $i \in \mathfrak{E}(84) \cup \{0\}$, then, by the definition of $\textsc{Stop}(i)$, we have, $\textsc{Stop}(i) \in \mathfrak{E}(84)$. This implies that $|\mathscr{R}_{\textsc{Stop}(i)}|$ is even in turn implying $|\mathscr{R}_{\textsc{Stop}(i)}| > |\mathscr{R}_{i+1}| = 1$.

On the other hand, if $i \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$, then, by the definition of $\textsc{Stop}(i)$, we have, $|\mathscr{R}_{\textsc{Stop}(i)}| \geq |\mathscr{R}_{i+1}|$. This combined with the fact that $|\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{i+1}|$ is odd (as i is indirect) implies that $|\mathscr{R}_{\textsc{Stop}(i)}| > |\mathscr{R}_{i+1}|$.

- By the previous part, we have $\textsc{Mid}(i) < \textsc{Stop}(i)$. This combined with the definition of $\textsc{Mid}(i)$ and item 3 of Fact 6.5 implies that $|\mathscr{R}_{\textsc{Mid}(i)+1}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{\textsc{Mid}(i)}|$. Now, if $i \in \textsc{Starts}_{\mathrm{F}}$, then $|\mathscr{R}_{i+1}| = |\mathscr{R}_{\textsc{Mid}(i)}|$ is odd and $|\mathscr{R}_{\textsc{Mid}(i)+1}| > |\mathscr{R}_{\textsc{Mid}(i)}|$ is only possible when $\textsc{Mid}(i) \in \mathfrak{E}(70)$.

  Similarly, if $i \in \textsc{Starts}_{\mathrm{B}}$, then $|\mathscr{R}_{i+1}| = |\mathscr{R}_{\textsc{Mid}(i)}|$ is even and $|\mathscr{R}_{\textsc{Mid}(i)+1}| > |\mathscr{R}_{\textsc{Mid}(i)}|$ is only possible when $\textsc{Mid}(i) \in \mathfrak{E}(80)$.

- Assume for the sake of contradiction that $\textsc{Stop}(\textsc{Mid}(i)) \neq \textsc{Stop}(i)$. By Lemma 6.7, we must have $\textsc{Stop}(\textsc{Mid}(i)) < \textsc{Stop}(i)$. By the foregoing part and the definition of $\textsc{Stop}(i)$, we have that $|\mathscr{R}_{\textsc{Stop}(\textsc{Mid}(i))+1}| < |\mathscr{R}_{\textsc{Mid}(i)+1}|$. Combined with item 3 of Fact 6.5, we get

$$|\mathscr{R}_{i+1}| \leq |\mathscr{R}_{\textsc{Stop}(\textsc{Mid}(i))+1}| < |\mathscr{R}_{\textsc{Mid}(i)+1}| = |\mathscr{R}_{\textsc{Mid}(i)}| + 1 = |\mathscr{R}_{i+1}| + 1.$$

  As all the values are integers, we must have $|\mathscr{R}_{i+1}| = |\mathscr{R}_{\textsc{Stop}(\textsc{Mid}(i))+1}|$ contradicting the definition of $\textsc{Mid}(i)$.

- We argue using the definition of $\textsc{Prev}(\cdot)$:

$$\textsc{Prev}(\textsc{Mid}(i)) = \max\{i' < \textsc{Mid}(i) \in \textsc{Starts} \mid |\mathscr{R}_{i'+1}| = |\mathscr{R}_{\textsc{Mid}(i)}|\} \geq i,$$

  where the last step is because $i < \textsc{Mid}(i) \in \textsc{Starts}$ and $|\mathscr{R}_{i+1}| = |\mathscr{R}_{\textsc{Mid}(i)}|$. We next claim that $\max\{i' < \textsc{Mid}(i) \in \textsc{Starts} \mid |\mathscr{R}_{i'+1}| = |\mathscr{R}_{\textsc{Mid}(i)}|\} \leq i$. To see why, suppose for the sake of contradiction that there exists $i'' > i \in \{i' < \textsc{Mid}(i) \in \textsc{Starts} \mid |\mathscr{R}_{i'+1}| = |\mathscr{R}_{\textsc{Mid}(i)}|\}$. Observe that $i'' \notin \{0\} \cup \mathfrak{E}(84)$ as otherwise $\textsc{Mid}(i) > i'' > i$ is a contradiction to item 3 of Fact 6.5. Therefore, $i'' \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$. This implies that

$$|\mathscr{R}_{\textsc{Mid}(i)}| = |\mathscr{R}_{i''+1}| = |\mathscr{R}_{i''}| + 1 \geq |\mathscr{R}_{i+1}| + 1,$$

  a contradiction.

□

Let $i \in \textsc{Starts}$. We say that $j \in \{i\} \cup \textsc{Range}(i)$ is 'good' for i if one of the following conditions hold: (1) $j = i$, (2) $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$, (3) $j = \textsc{Stop}(i)$ and $|\mathscr{R}_j| - |\mathscr{R}_{i+1}|$ is even.

6.2.2 Some Technical Lemmas

Lemma 6.10. *For all $i \in \textsc{Starts}_{\mathrm{F}}$ that are indirect, we have $|\pi_{\textsc{Stop}(i)+1}| = |\pi_{i+1}|$.*

Proof. To start, conclude from the definition of indirect that $|\mathscr{R}_{\textsc{Stop}(i)}|$ is even. This together with item 7 of Fact 6.5 gives us that $\textsc{Stop}(i) \in \mathfrak{E}(84) \cup \mathfrak{E}(88)$.

If $\textsc{Stop}(i) \in \mathfrak{E}(84)$, then we have $|\pi_{\textsc{Stop}(i)}| = 1$ and $|\pi_{\textsc{Stop}(i)+1}| = 0$. We have using item 8 of Fact 6.5 and Lemma 6.6 that

$$|\pi_{\textsc{Stop}(i)+1}| = 0 \leq |\pi_{i+1}| = \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{i+1}|].r < |\pi_{\textsc{Stop}(i)}| = 1,$$

and the result follows as all quantities are integers. On the other hand, if $\textsc{Stop}(i) \in \mathfrak{E}(88)$, then we get from the definition of $\textsc{Stop}(\cdot)$ that $i \in \mathfrak{E}(80)$ and therefore $|\mathscr{R}_{\textsc{Stop}(i)+1}| < |\mathscr{R}_{i+1}|$. This, due to Line 87 and Line 88 means that $|\pi_{\textsc{Stop}(i)+1}| = \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{i+1}|].r$. To finish the argument, we simply invoke item 8 of Fact 6.5.

□

Lemma 6.11. *For all $i \in \textsc{Starts}_{\textsc{B}}$ and $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$, we have*

$$|\pi_{j+1}| + \min_{j' \in [i:j]} |\pi_{j'+1}| \leq 2 \cdot |\pi_{i+1}|.$$

Proof. Proof by contradiction. Suppose there exists $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ such that the result does not hold and consider the smallest such j. It must be that $|\pi_{j+1}| \neq \min_{j' \in [i:j]} |\pi_{j'+1}|$, as otherwise

$$|\pi_{j+1}| + \min_{j' \in [i:j]} |\pi_{j'+1}| = 2 \cdot \min_{j' \in [i:j]} |\pi_{j'+1}| \leq 2 \cdot |\pi_{i+1}|.$$

Thus, in particular, we have $j \neq i$ and therefore, by our choice of j, we have

$$|\pi_j| + \min_{j' \in [i:j)} |\pi_{j'+1}| < |\pi_{j+1}| + \min_{j' \in [i:j]} |\pi_{j'+1}|,$$

implying that $|\pi_j| < |\pi_{j+1}|$ and therefore that $|\mathscr{R}_j|$ is odd by item 5 of Fact 6.5. As $i \in \textsc{Starts}_{\textsc{B}}$ and $j \in \textsc{Range}(i)$, we get from item 3 of Fact 6.5 that $|\mathscr{R}_j|$ is odd implies $|\mathscr{R}_j| > |\mathscr{R}_{i+1}|$.

Let $i + 1 \leq j'' \leq j$ to be the largest such that $|\mathscr{R}_{j''}| = |\mathscr{R}_{i+1}|$. Observe that j'' is well defined as $j'' = i + 1$ is one such value. As $|\mathscr{R}_j| > |\mathscr{R}_{i+1}|$, we have $j'' < j$, and therefore, by our choice of j'', that $|\mathscr{R}_{j''+1}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{j''}|$ (we have $|\mathscr{R}_{j''+1}| > |\mathscr{R}_{i+1}|$ due to item 3 of Fact 6.5) implying that $j'' \in \mathfrak{E}(80) \subseteq \textsc{Starts}_{\textsc{F}}$ by item 2 of Fact 6.5.

Next, note that $j \leq \textsc{Stop}(j'') \implies j \in \textsc{Range}(j'')$ as otherwise, by definition of $\textsc{Stop}(\cdot)$ and item 3 of Fact 6.5, we have $|\mathscr{R}_{i+1}| \leq |\mathscr{R}_{\textsc{Stop}(j'')+1}| < |\mathscr{R}_{j''+1}| = |\mathscr{R}_{j''}| + 1 = |\mathscr{R}_{i+1}| + 1$, a contradiction to the choice of j'' as all quantities are integers. We have

$$\begin{aligned}
|\pi_{j+1}| &> 2 \cdot |\pi_{i+1}| - \min_{j' \in [i:j]} |\pi_{j'+1}| \\
&\geq 2 \cdot |\pi_{i+1}| - |\pi_{j''+1}| \\
&\geq 2 \cdot \mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t - |\pi_{j''+1}| && (\text{As } i \in \textsc{Starts}_{\textsc{B}}) \\
&\geq 2 \cdot \mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t - \mathscr{R}_j[|\mathscr{R}_{j''+1}|].r && (\text{Fact 6.5, item 8}) \\
&\geq 2 \cdot \mathscr{R}_j[|\mathscr{R}_{i+1}| - 1].t - \mathscr{R}_j[|\mathscr{R}_{j''+1}|].r && (\text{Fact 6.5, item 4}) \\
&\geq 2 \cdot \mathscr{R}_j[|\mathscr{R}_{i+1}| - 1].t - \mathscr{R}_j[|\mathscr{R}_{i+1}| + 1].r && (\text{As } j'' \in \mathfrak{E}(80))
\end{aligned}$$

$$\geq |\pi_j| + 1, \qquad \text{(Lemma 6.6)}$$

a contradiction to item 5 of Fact 6.5.

□

Lemma 6.12. *Let $i \in \textsc{Starts}$ and $i' \in \textsc{Range}(i) \cap \textsc{Starts}$ be such that $|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|$. We have:*

- *If $\textsc{Stop}(i') < \textsc{Stop}(i)$, then i' is indirect and we have $|\mathscr{R}_{\textsc{Stop}(i')+1}| = |\mathscr{R}_{i+1}|$.*
- *If $\textsc{Stop}(i') = \textsc{Stop}(i) < num$, then we have i' is indirect if and only if $\textsc{Stop}(i)$ is good for i.*

Proof. We prove each part in turn. In both the parts, we use the fact that $i' < \textsc{Stop}(i') \leq \textsc{Stop}(i)$ implies that $i' \notin \mathfrak{E}(84) \cup \{0\}$ as otherwise, we have a contradiction to item 3 of Fact 6.5.

- First, note that $\textsc{Stop}(i') < \textsc{Stop}(i)$ implies that $\textsc{Stop}(i') + 1 \in \textsc{Range}(i)$ and therefore

$$\begin{aligned}
|\mathscr{R}_{i+1}| &\leq |\mathscr{R}_{\textsc{Stop}(i')+1}| && \text{(Fact 6.5, item 3)}\\
&< |\mathscr{R}_{i'+1}| && \text{(Definition of } \textsc{Stop}(\cdot) \text{ and } i' \notin \mathfrak{E}(84) \cup \{0\})\\
&= |\mathscr{R}_{i'}| + 1 && \text{(As } i' \notin \mathfrak{E}(84) \cup \{0\})\\
&= |\mathscr{R}_{i+1}| + 1. && (|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|)
\end{aligned}$$

  As all quantities are integers, we get that $|\mathscr{R}_{\textsc{Stop}(i')+1}| = |\mathscr{R}_{i+1}|$. It remains to show that i' is indirect. For this, we need to show that $|\mathscr{R}_{\textsc{Stop}(i')}| - |\mathscr{R}_{i'+1}|$ is odd. As $\textsc{Stop}(i') < \textsc{Stop}(i)$, we have that $\textsc{Stop}(i') \notin \mathfrak{E}(84)$ and therefore, by item 7 of Fact 6.5 that $\textsc{Stop}(i') \in \mathfrak{E}(73) \cup \mathfrak{E}(88)$. This means that $|\mathscr{R}_{\textsc{Stop}(i')}| - |\mathscr{R}_{\textsc{Stop}(i')+1}|$ is even and it is sufficient to show that $|\mathscr{R}_{\textsc{Stop}(i')+1}| - |\mathscr{R}_{i'+1}|$ is odd. The latter is because:

$$|\mathscr{R}_{\textsc{Stop}(i')+1}| - |\mathscr{R}_{i'+1}| = |\mathscr{R}_{i+1}| - |\mathscr{R}_{i'+1}| = |\mathscr{R}_{i'}| - |\mathscr{R}_{i'+1}| = -1,$$

  as $i' \notin \mathfrak{E}(84) \cup \{0\}$.

- As $\textsc{Stop}(i) = \textsc{Stop}(i') < num$, we have that i' is indirect if and only if $|\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{i'+1}|$ is odd. As $i' \notin \mathfrak{E}(84) \cup \{0\}$ and $|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|$, this happens if and only if $|\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{i+1}|$ is even which is if and only if $\textsc{Stop}(i)$ is good for i.

□

Lemma 6.13. *Let $i \in \textsc{Starts}_{\textsc{B}}$ and $j \in \textsc{Range}(i) \setminus \{num\}$ be good for i. We have*

- $|\pi_{j+1}| \leq \min_{j' \in [i:j)} |\pi_{j'+1}|$. *The inequality is strict if $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$.*
- $|\psi_j| < 2 \cdot (|\pi_{i+1}| - |\pi_{j+1}|)$.

Proof. Proof by induction. For the base case $j = i+1$, we have by item 5 of Fact 6.5 that $|\pi_{i+1}| - |\pi_{j+1}| = 1$ and $|\psi_j| = 0$ and the claim follows. We show it for $j > i+1$ assuming that it holds for all values $< j$. Let $i+1 \leq j' < j$ be the largest such that j' is good for i. This is well defined as $j' = i+1$ is one such value. Note that $|\mathscr{R}_{j'}|$ and $|\mathscr{R}_j|$ are even by definition of good. If $j' = j-1$, then we argue using item 5 of Fact 6.5:

$$|\pi_{j+1}| < |\pi_{j'+1}| \leq \min\left(|\pi_{j'+1}|, \min_{j'' \in [i:j')} |\pi_{j''+1}|\right) = \min_{j'' \in [i:j)} |\pi_{j''+1}|,$$

and

$$|\psi_j| \leq |\psi_{j'}| + 1 < 2 \cdot (|\pi_{i+1}| - |\pi_j|) + 1 < 2 \cdot (|\pi_{i+1}| - |\pi_{j+1}|)\,.$$

The remainder of this proof deals with the case $j' < j-1$. In this case, by our choice of j' we have that $j'+1$ is not good for i implying that $|\mathscr{R}_{j'+1}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{j'}|$ (we have $|\mathscr{R}_{j'+1}| > |\mathscr{R}_{i+1}|$ due to item 3 of Fact 6.5) implying that $j' \in \mathfrak{E}(80) \subseteq \textsc{Starts}_{\mathrm{F}}$ by item 2 of Fact 6.5.

As $j' < j \leq \textsc{Stop}(i)$, we have by Lemma 6.7 that $\textsc{Stop}(j') \leq \textsc{Stop}(i)$. We consider two cases:

- **When** $\textsc{Stop}(j') < \textsc{Stop}(i)$**:** In this case, we first claim that $j = \textsc{Stop}(j') + 1$. Indeed, $j \leq \textsc{Stop}(j') + 1$ as otherwise we get $|\mathscr{R}_{\textsc{Stop}(j')+1}| = |\mathscr{R}_{i+1}|$ from Lemma 6.12 implying that $\textsc{Stop}(j') + 1 < j$ is good for i contradicting the choice of j'. Also $j \geq \textsc{Stop}(j') + 1$, as either $j = \textsc{Stop}(i) > \textsc{Stop}(j')$ or by the definition of good, we have $|\mathscr{R}_j| = |\mathscr{R}_{i+1}| < |\mathscr{R}_{j'+1}|$ implying that $j \geq \textsc{Stop}(j') + 1$ by the definition of $\textsc{Stop}(\cdot)$.

  Next, we use Lemma 6.12 to conclude that j' is indirect, which with Lemma 6.10 means:

  $$|\pi_{j+1}| < |\pi_{\textsc{Stop}(j')+1}| = |\pi_{j'+1}| \leq \min\left(|\pi_{j'+1}|, \min_{j'' \in [i:j')} |\pi_{j''+1}|\right) = \min_{j'' \in [i:j']} |\pi_{j''+1}|.$$

  Due to item 8 of Fact 6.5 and Lemma 6.6, we also have

  $$|\pi_{j+1}| < |\pi_{\textsc{Stop}(j')+1}| = |\pi_{j'+1}| \leq \min_{j'' \in (j':\textsc{Stop}(j')]} |\pi_{j''}|.$$

  We combine these two equations to conclude that $|\pi_{j+1}| < |\pi_{j'+1}| = \min_{j'' \in [i:j)} |\pi_{j''+1}|$, as desired. For the second part, let $j' < j_1 \leq j$ be the largest such that $|\mathscr{R}_{j_1}|$ is odd. This is well defined as $|\mathscr{R}_{j'+1}|$ is odd. By our choice of j_1, we have that $|\mathscr{R}_{j''}|$ is even for all $j_1 < j'' \leq j$ implying that $(j_1 : j) \cap \textsc{Starts} = \emptyset$. Furthermore, as $|\mathscr{R}_{j_1}|$ is odd, we have that $|\psi_{j_1+1}| = 0$.

  Due to item 5 of Fact 6.5, we have that $|\psi_j| - |\psi_{j_1+1}| = |\pi_{j_1+1}| - |\pi_j|$. Combining, we get

  $$|\psi_j| = |\pi_{j_1+1}| - |\pi_j|$$

$$
\begin{aligned}
&\leq 2 \cdot |\pi_{i+1}| - \min_{j'' \in [i:j_1]} |\pi_{j''+1}| - |\pi_j| && \text{(Lemma 6.11)} \\
&\leq 2 \cdot |\pi_{i+1}| - |\pi_{j'+1}| - |\pi_j| && \text{(As } |\pi_{j'+1}| = \min_{j'' \in [i:j)} |\pi_{j''+1}|\text{)} \\
&\leq 2 \cdot (|\pi_{i+1}| - |\pi_j|) && \text{(Lemma 6.10 and } j = \textsc{Stop}(j') + 1\text{)} \\
&< 2 \cdot (|\pi_{i+1}| - |\pi_{j+1}|)\,. && \text{(Fact 6.5, item 5)}
\end{aligned}
$$

- **When** $\textsc{Stop}(j') = \textsc{Stop}(i)$**:** As $j' < j \leq \textsc{Stop}(i) = \textsc{Stop}(j')$, we have that $j \in \textsc{Range}(j')$ and therefore, using item 3 of Fact 6.5 and the fact that j is good for i, we have that $|\mathscr{R}_j| \geq |\mathscr{R}_{j'+1}| > |\mathscr{R}_{i+1}|$ and $j = \textsc{Stop}(i)$. Thus, we don't have to show a strict inequality in the first part of this lemma.

  Using the fact that $j = \textsc{Stop}(i)$ is good for i, we have by Lemma 6.12 that j' is indirect, which with Lemma 6.10 means:

  $$|\pi_{j+1}| = |\pi_{j'+1}| \leq \min\left(|\pi_{j'+1}|, \min_{j'' \in [i:j')} |\pi_{j''+1}|\right) = \min_{j'' \in [i:j']} |\pi_{j''+1}|.$$

  Due to item 8 of Fact 6.5 and Lemma 6.6, we also have

  $$|\pi_{j+1}| = |\pi_{j'+1}| \leq \min_{j'' \in (j':\textsc{Stop}(j'))} |\pi_{j''}|.$$

  We combine these two equations to conclude that $|\pi_{j+1}| = |\pi_{j'+1}| = \min_{j'' \in [i:j)} |\pi_{j''+1}|$, as desired. For the second part, let $j' < j_1 \leq j$ be the largest such that $|\mathscr{R}_{j_1}|$ is odd. This is well defined as $|\mathscr{R}_{j'+1}|$ is odd. By our choice of j_1, we have that $|\mathscr{R}_{j''}|$ is even for all $j_1 < j'' \leq j$ implying that $(j_1 : j) \cap \textsc{Starts} = \emptyset$. Furthermore, as $|\mathscr{R}_{j_1}|$ is odd, we have that $|\psi_{j_1+1}| = 0$.

  Due to item 5 of Fact 6.5, we have that $|\psi_j| - |\psi_{j_1+1}| = |\pi_{j_1+1}| - |\pi_j|$. Combining, we get

  $$
  \begin{aligned}
  |\psi_j| &= |\pi_{j_1+1}| - |\pi_j| \\
  &\leq 2 \cdot |\pi_{i+1}| - \min_{j'' \in [i:j_1]} |\pi_{j''+1}| - |\pi_j| && \text{(Lemma 6.11)} \\
  &\leq 2 \cdot |\pi_{i+1}| - |\pi_{j'+1}| - |\pi_j| && \text{(As } |\pi_{j'+1}| = \min_{j'' \in [i:j)} |\pi_{j''+1}|\text{)} \\
  &\leq 2 \cdot |\pi_{i+1}| - |\pi_{j'+1}| - |\pi_{j+1}| - 1 && \text{(Fact 6.5, item 5)} \\
  &< 2 \cdot (|\pi_{i+1}| - |\pi_{j+1}|)\,. && \text{(As } |\pi_{j+1}| = |\pi_{j'+1}|\text{)}
  \end{aligned}
  $$

□

Corollary 6.14. *Let $i \in \textsc{Starts}_B$ and $j \in \textsc{Range}(i) \setminus \{num\}$. If $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$, we have for all $j' \in (i : j]$ that $|\pi_j| \leq |\pi_{j'}|$ and $\pi_j^C = \pi_{j'}^C[1 : |\pi_j|]$ for all $C \in \{A, B\}$.*

Proof. We only show that $|\pi_j| \leq |\pi_{j'}|$ as the other part follows because the parties only add/remove one symbol from π in every iteration. As $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ implies j is good for i,

we get using item 5 of Fact 6.5 that:

$$|\pi_j| \leq |\pi_{j+1}| + 1 \leq \min_{j' \in [i:j)} |\pi_{j'+1}| = \min_{j' \in (i:j]} |\pi_{j'}|.$$

□

Lemma 6.15. *Let $i \in \textsc{Starts}_{\mathrm{B}}$ and $i' \in (i : \textsc{Stop}(i)) \cap \textsc{Starts}_{\mathrm{F}}$ be such that $|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|$. We have for all $j \in [i : \textsc{Stop}(i')] \setminus \{num\}$ that:*

$$|\pi_{i'+1}| \leq |\pi_{j+1}|.$$

Proof. If $j \in [i : i']$, this follows using Lemma 6.13. We next show this for $j \in [i : \textsc{Stop}(i')] \setminus \{num\}$. For all such j, we have by item 8 of Fact 6.5 that $|\pi_{i'+1}| = \mathscr{R}_j[|\mathscr{R}_{i'+1}|].r$. If $|\mathscr{R}_j|$ is odd, we get using Lemma 6.6 and item 5 of Fact 6.5 that:

$$|\pi_{j+1}| = |\pi_j| + 1 \geq \mathscr{R}_j[|\mathscr{R}_{i'+1}|].r + 1 = |\pi_{i'+1}| + 1.$$

On the other hand, if $|\mathscr{R}_j|$ is even, we get using Lemma 6.6 and item 5 of Fact 6.5 that:

$$|\pi_{j+1}| = |\pi_j| - 1 > \mathscr{R}_j[|\mathscr{R}_{i'+1}|].r - 1 > |\pi_{i'+1}| - 1,$$

and the result follows as all quantities are integers. □

Lemma 6.16. *For all $i \in \textsc{Starts}_{\mathrm{B}}$ that are indirect, we have:*

$$0 \leq |\pi_{\textsc{Stop}(i)+1}| - |\pi_{i+1}| \leq |\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|.$$

Furthermore, if $|\mathscr{R}_{\textsc{Stop}(i)+1}| + 1 = |\mathscr{R}_{i+1}|$, then the second inequality is an equality.

Proof. To start, conclude from the definition of indirect that $|\mathscr{R}_{\textsc{Stop}(i)}|$ is odd. We show that $\textsc{Stop}(i) \in \mathfrak{E}(73)$ and $d^*_{\textsc{Stop}(i)} < |\mathscr{R}_{\textsc{Stop}(i)}|$ and apply the "furthermore" part of Lemma 6.6. Indeed, by item 7 of Fact 6.5, we get $\textsc{Stop}(i) \in \mathfrak{E}(84) \cup \mathfrak{E}(73) \cup \mathfrak{E}(88)$ which together with the fact that $|\mathscr{R}_{\textsc{Stop}(i)}|$ is odd gives $\textsc{Stop}(i) \in \mathfrak{E}(73)$. Also, $d^*_{\textsc{Stop}(i)} \leq |\mathscr{R}_{\textsc{Stop}(i)}| - 2 \implies |\mathscr{R}_{\textsc{Stop}(i)+1}| \leq |\mathscr{R}_{\textsc{Stop}(i)}| - 2$ as otherwise, we have by Line 73 that

$$\begin{aligned} |\mathscr{R}_{\textsc{Stop}(i)}| &= |\mathscr{R}_{\textsc{Stop}(i)+1}| \\ &< |\mathscr{R}_{i+1}| && \text{(Definition of } \textsc{Stop}(\cdot)) \\ &\leq |\mathscr{R}_{\textsc{Stop}(i)}|, && \text{(Fact 6.5, item 3)} \end{aligned}$$

a contradiction. From the "furthermore" part of Lemma 6.6, we get that

$$|\pi_{\textsc{Stop}(i)+1}| = 2\mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{\textsc{Stop}(i)+1}|].t - \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{\textsc{Stop}(i)+1}| + 2].r.$$

Assuming that $|\mathscr{R}_{\textsc{Stop}(i)+1}| + 1 = |\mathscr{R}_{i+1}|$, we derive

$$\begin{aligned} |\pi_{\textsc{Stop}(i)+1}| &= 2\mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{\textsc{Stop}(i)+1}|].t - \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{\textsc{Stop}(i)+1}| + 2].r \\ &= 2\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t - \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{i+1}| + 1].r && \text{(Fact 6.5, item 4)} \end{aligned}$$

$$
\begin{aligned}
&= 2\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t - \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{\textsc{Mid}(i)+1}|].r && \text{(Lemma 6.9)}\\
&= 2\mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t - |\pi_{\textsc{Mid}(i)+1}| && \text{(Lemma 6.9 and Fact 6.5, item 8)}\\
&= 2|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|, && \text{(Line 69)}
\end{aligned}
$$

showing the "furthermore" part of the lemma. Moreover using Lemma 6.13, we can continue as $|\pi_{\textsc{Stop}(i)+1}| = 2|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}| \geq |\pi_{i+1}|$ showing the first inequality in this case. If $|\mathscr{R}_{\textsc{Stop}(i)+1}| + 1 \neq |\mathscr{R}_{i+1}|$, the fact that $|\mathscr{R}_{\textsc{Stop}(i)+1}| < |\mathscr{R}_{i+1}|$ (definition of $\textsc{Stop}(\cdot)$) and the fact that $|\mathscr{R}_{\textsc{Stop}(i)+1}|$ is odd (as $\textsc{Stop}(i) \in \mathfrak{E}(73)$) gives us that $|\mathscr{R}_{\textsc{Stop}(i)+1}| + 2 < |\mathscr{R}_{i+1}|$. In this case, we have by item 4 of Fact 6.5 that:

$$
\begin{aligned}
|\pi_{\textsc{Stop}(i)+1}| &= 2\mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{\textsc{Stop}(i)+1}|].t - \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{\textsc{Stop}(i)+1}| + 2].r\\
&= 2\mathscr{R}_{i+1}[|\mathscr{R}_{\textsc{Stop}(i)+1}|].t - \mathscr{R}_{i+1}[|\mathscr{R}_{\textsc{Stop}(i)+1}| + 2].r\\
&\geq |\pi_{i+1}|. && \text{(Lemma 6.6)}
\end{aligned}
$$

For the second inequality, we proceed via contradiction. If the inequality is not true, then we have.

$$
\begin{aligned}
|\pi_{\textsc{Stop}(i)}| &= |\pi_{\textsc{Stop}(i)+1}| - 1 && \text{(Fact 6.5, item 5)}\\
&\geq 2 \cdot |\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\\
&\geq 2 \cdot \mathscr{R}_{i+1}[|\mathscr{R}_{i+1}| - 1].t - |\pi_{\textsc{Mid}(i)+1}| && \text{(As } i \in \textsc{Starts}_{\textsc{B}}\text{)}\\
&\geq 2 \cdot \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{i+1}| - 1].t - |\pi_{\textsc{Mid}(i)+1}| && \text{(Fact 6.5, item 4)}\\
&\geq 2 \cdot \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{i+1}| - 1].t - \mathscr{R}_{\textsc{Mid}(i)+1}[|\mathscr{R}_{i+1}| + 1].r\\
& && \text{(Definition of } \textsc{Mid}(i) \text{ and Lemma 6.9)}\\
&\geq 2 \cdot \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{i+1}| - 1].t - \mathscr{R}_{\textsc{Stop}(i)}[|\mathscr{R}_{i+1}| + 1].r\\
& && \text{(Lemma 6.9 and Fact 6.5, item 8)}
\end{aligned}
$$

However, as $|\mathscr{R}_{\textsc{Stop}(i)}| > |\mathscr{R}_{i+1}|$ due to the fact that i is indirect and item 3 of Fact 6.5, this contradicts Lemma 6.6. □

6.2.3 Analyzing One $i \in \textsc{Starts}$

The goal in this section is to state our results about a given $i \in \textsc{Starts}$. We defer the proofs of these results to Subsubsection 6.2.10. We first state the results when $i \in \textsc{Starts}_{\textsc{F}}$, *i.e.*, when a forward tree code is pushed at iteration i.

Analyzing forward tree codes. For $1 \leq j < num$ and $l \in [|\pi_{j+1}|]$, define

$$\mathsf{latest}(j, l) = \arg\max\{j' \leq j \mid |\mathscr{R}_{j'}| \text{ is odd} \wedge |\pi_{j'+1}| = l\}.$$

We show that $\mathsf{latest}(\cdot)$ is always well defined as the arg max is always over a non-empty set. This is because $|\pi|$ increases by at most one in any iteration, and only increases when $|\mathscr{R}|$ is

odd (Fact 6.5, item 5). Next, for $1 \le j' \le j < num$ and $d > 0$, define

$$\mathsf{E}^{\mathrm{F}}_d(j,j') = \begin{cases} \mathsf{corr}_{j'} & ,|\mathscr{R}_{j'}| \text{ is even} \\ \mathsf{corr}_{j'} \cdot \mathbb{1}(\Gamma^A_{j',\ge d} \neq \Gamma^B_{j',\ge d}) & ,\exists l \in [|\pi_{j+1}|] \text{ such that } j' = \mathsf{latest}(j,l)\,. \\ 2 \cdot \mathsf{corr}_{j'} & ,\text{otherwise} \end{cases}$$

The function $\mathsf{E}(\cdot)$ captures the amount of corruptions inserted in iteration j' (up to constant factors). Next, for $i \in \textsc{Starts}_{\mathrm{F}}$ and $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$, define $\mathsf{depth}(i) = (|\mathscr{R}_{i+1}| + 1)/2$ and:

$$\begin{aligned} \mathsf{G}_i(j) &= |\mathsf{LCP}(\pi^A_{j+1}(|\pi_{i+1}| : |\pi_{j+1}|], \pi^B_{j+1}(|\pi_{i+1}| : |\pi_{j+1}|])|. \\ \mathsf{B}_i(j) &= |\pi_{j+1}| - |\pi_{i+1}| - \mathsf{G}_i(j). \\ \mathsf{D}_i(j) &= |\{|\pi_{i+1}| < l \le |\pi_{j+1}| \mid \Gamma^A_{\mathsf{latest}(j,l),\ge \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\ge \mathsf{depth}(i)}\}|. \\ \mathsf{spare}_i(j) &= \mathbb{1}\left(\mathsf{B}_i(j) > 0 \wedge (j \notin \mathfrak{E}(70) \vee \mathsf{D}_i(j) = \mathsf{D}_i(j-1))\right). \end{aligned}$$

Lastly, for $d > 0$, define:

$$\mathsf{E}^{\mathrm{F}}_{i,d}(j) = \sum_{j' \in (i:j]} \mathsf{E}^{\mathrm{F}}_d(j,j').$$

With these definitions, we are now ready to state our result for forward tree codes.

Lemma 6.17. *For all $i \in \textsc{Starts}_{\mathrm{F}}$ and all $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ that are good for i, we have:*

$$\begin{aligned} \sum_{i'=i+1}^{j} \ell^*_{i'} \le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) &+ \ell^*_{i+1} \cdot (\mathsf{G}_i(j) + 150\mathsf{B}_i(j) - 2500 \cdot \mathsf{D}_i(j)) \\ &+ \ell^*_{i+1} \cdot \mathbb{1}(j = \textsc{Stop}(i) \wedge |\mathscr{R}_j| \neq |\mathscr{R}_{i+1}|) \cdot (\mathsf{G}_i(j) + \mathsf{B}_i(j)) \\ &- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j). \end{aligned}$$

We now state our results when $i \in \textsc{Starts}_{\mathrm{B}}$, *i.e.*, when a backward tree code is pushed at iteration i.

Analyzing Backward Tree Codes. For $1 \le j < num$ such that $|\mathscr{R}_j|$ is even, define

$$\mathsf{turn}(j) = \mathbb{1}\left(\psi^A_j \| \sigma^A_j \neq \psi^B_j \| \sigma^B_j\right).$$

$$\mathsf{F}(j) = \frac{20}{1 - 10^{-5}} \cdot \Delta\left(\overline{\mathsf{TC}}(\psi^A_j \| \sigma^A_j), \overline{\mathsf{TC}}(\psi^B_j \| \sigma^B_j)\right) + 20 \cdot \left(|\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)| - |\psi_j|\right) + 80.$$

Also, define for $\eta \ge 0$, the function $\mathsf{tax}_0(\eta, j)$ as in Algorithm 7.

For $1 \le j < num$ such that $|\mathscr{R}_j|$ is odd, we define all of $\mathsf{turn}(j)$, $\mathsf{F}(j)$ and $\mathsf{tax}_0(\cdot, j)$ to be 0. Next, we define for $i \in \textsc{Starts}_{\mathrm{B}}$ and all $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ such that

Algorithm 7 The definition of $\mathsf{tax}_0(\eta, j)$.

if $\pi_j^A \| \psi_j^A = \pi_j^B \| \psi_j^B$ **then**
  $\mathsf{tax}_0(\eta, j) \leftarrow \eta \cdot (|\psi_j| + 1)$.
else if $\mathsf{turn}(j) = 1$ **then**
  $\mathsf{tax}_0(\eta, j) \leftarrow 3 \cdot (|\psi_j| + 1)$.
  if $\mathscr{R}_{j+1}.last.t > 0$ **then**
    $\mathsf{tax}_0(\eta, j) \leftarrow \mathsf{tax}_0(\eta, j) + \eta \cdot (2 \cdot (\mathscr{R}_{j+1}.last.r - \mathscr{R}_{j+1}.last.t) - |\psi_j| - 1)$.
  else if $j \notin \mathfrak{E}(80) \cup \mathfrak{E}(84)$ **then**
    $\mathsf{tax}_0(\eta, j) \leftarrow \mathsf{tax}_0(\eta, j) + \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j) + |\psi_j| + 1\right)$.
  end if
else if $\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) > 0$ **then**
  $\mathsf{tax}_0(\eta, j) \leftarrow \eta \cdot (\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) - |\pi_{j+1}|)$.
end if

$|\pi_{j+1}| \le |\pi_{i+1}|$, the functions[12]:

$$\mathsf{tax}_{1,i}(j) = 100 \max\left(0, 9|\mathsf{LCP}(\pi_{i+1}^A(|\pi_{j+1}| : |\pi_{i+1}|], \pi_{i+1}^B(|\pi_{j+1}| : |\pi_{i+1}|])| - 8\left(|\pi_{i+1}| - |\pi_{j+1}|\right)\right).$$

$$\mathsf{E}_i^{\mathrm{B}}(j) = \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} + \sum_{i'=i+1}^{j} \mathsf{corr}_{i'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{i'}| \text{ is odd}\right)).$$

Finally, for $\eta, \eta' \ge 0$, define:

$$\mathsf{extra}_i(\eta, \eta', j) = \ell_{i+1}^* \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30} - \mathsf{tax}_0(\eta, j), 35\left(|\pi_{i+1}| - |\pi_{j+1}|\right) - \mathsf{tax}_0(\eta', j)\right).$$

For brevity sake, we adopt the convention that $\mathsf{extra}_i(j) = \mathsf{extra}_i(225, 10, j)$. With these definitions, we are now ready to state our result for backward tree codes.

Lemma 6.18. *For all $i \in \textsc{Starts}_{\mathrm{B}}$ and all $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ that are good for i, we have:*

$$\sum_{i'=i+1}^{j} \ell_{i'}^* \le 10^4 \cdot \mathsf{E}_i^{\mathrm{B}}(j) + \mathsf{extra}_i(j) + 3 \cdot \ell_{i+1}^* \cdot \mathbb{1}(j \ne i) \cdot (|\psi_j| + 1) - 2 \cdot \ell_{i+1}^* \cdot (|\pi_{i+1}| - |\pi_{j+1}|)$$
$$- \ell_{i+1}^* \cdot \mathbb{1}\left(j \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(j).$$

Analyzing Indirect Tree Codes. Finally, if $i \in \textsc{Starts}$ is indirect, we shall also have the following additional results.

Lemma 6.19. *For all $i \in \textsc{Starts}_{\mathrm{F}}$ that are indirect, we have*

$$\sum_{i'=i+1}^{\textsc{Stop}(i)} \ell_{i'}^* \le 10^4 \cdot \mathsf{E}_{i,\mathsf{depth}(i)}^{\mathrm{F}}(\textsc{Mid}(i)) + 10^4 \cdot \mathsf{E}_{\textsc{Mid}(i)}^{\mathrm{B}}(\textsc{Stop}(i))$$

[12] In particular, by Lemma 6.13, these functions are well defined for all j that are good for i. Similarly, by Corollary 6.14, these are also defined for all j such that $j + 1 \in \textsc{Range}(i) \setminus \{num\}$ and $|\mathscr{R}_{j+1}| = |\mathscr{R}_{i+1}|$.

$$+ \frac{3}{1.1} \cdot \ell^*_{i+1} \cdot \big(|\psi_{\textsc{Stop}(i)}| + 1\big) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)).$$

Lemma 6.20. *For all $i \in \textsc{Starts}_{\mathrm{B}}$ that are indirect, we have:*

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(i)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Mid}(i)) + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i),\mathsf{depth}(\textsc{Mid}(i))}(\textsc{Stop}(i)) \\ &+ \ell^*_{\textsc{Mid}(i)+1} \cdot \big(150 \cdot \mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\big) \\ &+ 44 \cdot \ell^*_{i+1} \cdot \big(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\big) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\textsc{Mid}(i)) \\ &- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(i)}(\textsc{Stop}(i)).\end{aligned}$$

6.2.4 Lemmas Concerning $\mathsf{latest}(\cdot)$ and $\mathsf{D}(\cdot)$

Lemma 6.21. *Let $1 \leq j < num$ and $l \in [|\pi_{j+1}|]$. For all $j' \in [\mathsf{latest}(j,l) : j]$, it holds that $|\pi_{j'+1}| \geq l$.*

Proof. Suppose not and let $j' \in [\mathsf{latest}(j,l) : j]$ be such that $|\pi_{j'+1}| < l \leq |\pi_{j+1}|$. As $|\pi|$ increases by at most one in every iteration and increases only when $|\mathscr{R}|$ is odd (item 5 of Fact 6.5), we have a $j'' \in (j' : j] \subseteq (\mathsf{latest}(j,l) : j]$ such that $|\mathscr{R}_{j''}|$ is odd and $|\pi_{j''+1}| = l$. This is a contradiction to the definition of $\mathsf{latest}(j,l)$. □

Corollary 6.22. *For all $1 \leq j < num$, $l \in [|\pi_{j+1}|]$, and $C \in \{A, B\}$, it holds that $\pi^C_{\mathsf{latest}(j,l)+1} = \pi^C_{j+1}[1 : l]$.*

Lemma 6.23. *For all $1 \leq j < num$ and $l \in [|\pi_{j+1}|]$, we either have $\mathsf{latest}(j,l) = j \in \mathfrak{E}(70)$ or we have for all $C \in \{A, B\}$ that $\Gamma^C_{\mathsf{latest}(j,l)} = \tilde{\Gamma}^C_{\mathsf{latest}(j,l)}$.*

Proof. If $\mathsf{latest}(j,l) = j \in \mathfrak{E}(70)$, then there is nothing to show, so we assume that this is not the case. Suppose for the sake of contradiction that there exists $C \in \{A, B\}$ such that $\Gamma^C_{\mathsf{latest}(j,l)} \neq \tilde{\Gamma}^C_{\mathsf{latest}(j,l)}$. Consider iteration $\mathsf{latest}(j,l)$ in the execution of party C. As $|\mathscr{R}_{\mathsf{latest}(j,l)}|$ is odd, party C executes Line 70 in iteration $\mathsf{latest}(j,l)$. Due to our assumption above, this means that $\mathsf{latest}(j,l) < j \implies \mathsf{latest}(j,l) + 1 \in (\mathsf{latest}(j,l) : j]$. However, as party C executes Line 70 in iteration $\mathsf{latest}(j,l)$, we have that $|\mathscr{R}_{\mathsf{latest}(j,l)+1}|$ is even implying that $|\pi_{\mathsf{latest}(j,l)+2}| = |\pi_{\mathsf{latest}(j,l)+1}| - 1 = l - 1$ contradicting Lemma 6.21. □

Lemma 6.24. *For $i \in \textsc{Starts}_{\mathrm{F}}$ and $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$, we have*

$$\big(1 - 10^{-5}\big) \cdot \mathsf{B}_i(j) \leq \mathsf{D}_i(j) \leq \mathsf{B}_i(j).$$

Proof. We first show that $\mathsf{latest}(j,l) \in \textsc{Range}(i)$ for all $|\pi_{i+1}| < l \leq |\pi_{j+1}|$. To show this, it is sufficient to show that $\mathsf{latest}(j,l) > i$. This is because, otherwise, we have a contradiction to Lemma 6.21. For the first part, note that:

$$\mathsf{D}_i(j) = |\{|\pi_{i+1}| < l \leq |\pi_{j+1}| \mid \Gamma^A_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)}\}|$$

$$
\begin{aligned}
&\geq |\{|\pi_{i+1}| < l \leq |\pi_{j+1}| \mid \Gamma^A_{\mathsf{latest}(j,l),\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\mathsf{depth}(i)}\}| \\
&\geq \left|\left\{|\pi_{i+1}| < l \leq |\pi_{j+1}| \mid \mathsf{TC}\left(\pi^A_{\mathsf{latest}(j,l)+1,>|\pi_{i+1}|}\right) \neq \mathsf{TC}\left(\pi^B_{\mathsf{latest}(j,l)+1,>|\pi_{i+1}|}\right)\right\}\right| \\
&\qquad\qquad \text{(Fact 6.5, item 8 on } \mathsf{latest}(j,l)) \\
&\geq \left|\left\{|\pi_{i+1}| < l \leq |\pi_{j+1}| \mid \mathsf{TC}\left(\pi^A_{j+1}(|\pi_{i+1}| : l]\right) \neq \mathsf{TC}\left(\pi^B_{j+1}(|\pi_{i+1}| : l]\right)\right\}\right| \\
&\qquad\qquad \text{(Corollary 6.22)} \\
&\geq \Delta(\overline{\mathsf{TC}}(\pi^A_{j+1}(|\pi_{i+1}| : |\pi_{j+1}|]), \overline{\mathsf{TC}}(\pi^B_{j+1}(|\pi_{i+1}| : |\pi_{j+1}|])) \\
&\geq (1 - 10^{-5}) \cdot \left(|\pi_{j+1}| - |\pi_{i+1}| - |\mathsf{LCP}(\pi^A_{j+1}(|\pi_{i+1}| : |\pi_{j+1}|], \pi^B_{j+1}(|\pi_{i+1}| : |\pi_{j+1}|])|\right) \\
&\qquad\qquad \text{(Definition 3.6)} \\
&\geq (1 - 10^{-5}) \cdot \mathsf{B}_i(j).
\end{aligned}
$$

For the second part, note that:

$$
\begin{aligned}
\mathsf{D}_i(j) &= |\{|\pi_{i+1}| < l \leq |\pi_{j+1}| \mid \Gamma^A_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)}\}| \\
&= |\{|\pi_{i+1}| < l \leq |\pi_{i+1}| + \mathsf{G}_i(j) \mid \Gamma^A_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)}\}| \\
&\quad + |\{|\pi_{i+1}| + \mathsf{G}_i(j) < l \leq |\pi_{j+1}| \mid \Gamma^A_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)}\}| \\
&\leq |\{|\pi_{i+1}| < l \leq |\pi_{i+1}| + \mathsf{G}_i(j) \mid \Gamma^A_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)}\}| \\
&\quad + |\pi_{j+1}| - |\pi_{i+1}| - \mathsf{G}_i(j) \\
&\leq |\{|\pi_{i+1}| < l \leq |\pi_{i+1}| + \mathsf{G}_i(j) \mid \Gamma^A_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)}\}| + \mathsf{B}_i(j).
\end{aligned}
$$

With this, to finish the proof, it is sufficient to show that $\Gamma^A_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)} = \Gamma^B_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)}$ for all $|\pi_{i+1}| < l \leq |\pi_{i+1}| + \mathsf{G}_i(j)$. To show this, fix $|\pi_{i+1}| < l \leq |\pi_{i+1}| + \mathsf{G}_i(j)$ and note that by the definition of $\mathsf{G}_i(j)$ we have

$$
\begin{aligned}
&\pi^A_{j+1}(|\pi_{i+1}| : l] = \pi^B_{j+1}(|\pi_{i+1}| : l] \\
&\quad\implies \pi^A_{\mathsf{latest}(j,l)+1,>|\pi_{i+1}|} = \pi^B_{\mathsf{latest}(j,l)+1,>|\pi_{i+1}|} \qquad \text{(Corollary 6.22)} \\
&\quad\implies \pi^A_{\mathsf{latest}(j,l)+1,>\mathscr{R}_{\mathsf{latest}(j,l)}[2\cdot\mathsf{depth}(i)-1].r} = \pi^B_{\mathsf{latest}(j,l)+1,>\mathscr{R}_{\mathsf{latest}(j,l)}[2\cdot\mathsf{depth}(i)-1].r}. \\
&\qquad\qquad \text{(Fact 6.5, item 8 on } \mathsf{latest}(j,l))
\end{aligned}
$$

This implies by Lemma 6.6 that for all $d \geq \mathsf{depth}(i)$, we have

$$
\begin{aligned}
&\pi^A_{\mathsf{latest}(j,l)+1,>\mathscr{R}_{\mathsf{latest}(j,l)}[2d-1].r} = \pi^B_{\mathsf{latest}(j,l)+1,>\mathscr{R}_{\mathsf{latest}(j,l)}[2d-1].r} \\
&\quad\implies \mathsf{TC}\left(\pi^A_{\mathsf{latest}(j,l)+1,>\mathscr{R}_{\mathsf{latest}(j,l)}[2d-1].r}\right) = \mathsf{TC}\left(\pi^B_{\mathsf{latest}(j,l)+1,>\mathscr{R}_{\mathsf{latest}(j,l)}[2d-1].r}\right) \\
&\quad\implies \Gamma^A_{\mathsf{latest}(j,l),d} = \Gamma^B_{\mathsf{latest}(j,l),d},
\end{aligned}
$$

and $\Gamma^A_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)} = \Gamma^B_{\mathsf{latest}(j,l),\geq\mathsf{depth}(i)}$ follows.

□

Lemma 6.25. *For $i \in \textsc{Starts}_{\mathrm{F}}$ and $j \in \textsc{Range}(i) \setminus \{num\}$ such that $|\mathscr{R}_j|$ is odd, we have*

$$4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j-1)$$

$$\leq 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j).$$

Proof. As $|\mathscr{R}_j|$ is odd, we have by item 5 of Fact 6.5 that $|\pi_{j+1}| = |\pi_j| + 1$ and $\mathsf{latest}(j,l) = \mathsf{latest}(j-1,l)$ for all $l \in [|\pi_j|]$ and $\mathsf{latest}(j,|\pi_{j+1}|) = j$. The former implies that $\mathsf{E}^{\mathrm{F}}_{\mathsf{depth}(i)}(j,j') = \mathsf{E}^{\mathrm{F}}_{\mathsf{depth}(i)}(j-1,j')$ for all $j' \in (i:j)$. We get from the definition of $\mathsf{E}(\cdot)$ that:

$$\begin{aligned}
\mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) &= \sum_{j' \in (i:j)} \mathsf{E}^{\mathrm{F}}_{\mathsf{depth}(i)}(j-1,j') \\
&= \sum_{j' \in (i:j)} \mathsf{E}^{\mathrm{F}}_{\mathsf{depth}(i)}(j,j') \\
&= \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \mathsf{E}^{\mathrm{F}}_{\mathsf{depth}(i)}(j,j) \\
&= \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \mathsf{corr}_j \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}),
\end{aligned} \tag{27}$$

as $\mathsf{latest}(j,|\pi_{j+1}|) = j$. Again, using the fact that $|\pi_{j+1}| = |\pi_j| + 1$ and $\mathsf{latest}(j,l) = \mathsf{latest}(j-1,l)$ for all $l \in [|\pi_j|]$ and $\mathsf{latest}(j,|\pi_{j+1}|) = j$, we get from the definition of $\mathsf{D}(\cdot)$ that:

$$\begin{aligned}
\mathsf{D}_i(j-1) &= |\{|\pi_{i+1}| < l \leq |\pi_j| \mid \Gamma^A_{\mathsf{latest}(j-1,l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j-1,l),\geq \mathsf{depth}(i)}\}| \\
&= |\{|\pi_{i+1}| < l \leq |\pi_j| \mid \Gamma^A_{\mathsf{latest}(j,l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\geq \mathsf{depth}(i)}\}| \\
&= |\{|\pi_{i+1}| < l \leq |\pi_{j+1}| \mid \Gamma^A_{\mathsf{latest}(j,l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,l),\geq \mathsf{depth}(i)}\}| \\
&\qquad - \mathbb{1}\left(\Gamma^A_{\mathsf{latest}(j,|\pi_{j+1}|),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,|\pi_{j+1}|),\geq \mathsf{depth}(i)}\right) \\
&= \mathsf{D}_i(j) - \mathbb{1}\left(\Gamma^A_{\mathsf{latest}(j,|\pi_{j+1}|),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(j,|\pi_{j+1}|),\geq \mathsf{depth}(i)}\right) \\
&= \mathsf{D}_i(j) - \mathbb{1}\left(\Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}\right),
\end{aligned} \tag{28}$$

as $\mathsf{latest}(j,|\pi_{j+1}|) = j$. Combining the two equations above, we get:

$$\begin{aligned}
&2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) \\
&\quad \leq 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) \\
&\qquad - 2 \cdot \mathsf{corr}_j \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) + \ell^*_{i+1} \cdot \mathbb{1}\left(\Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}\right) \\
&\quad \leq 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) \\
&\qquad - 2 \cdot \mathsf{corr}_j \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) \\
&\qquad + \ell^*_{i+1} \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) \\
&\qquad + \ell^*_{i+1} \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)} \wedge \Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)}) \\
&\quad \leq 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) \\
&\qquad - 2 \cdot \mathsf{corr}_j \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) \\
&\qquad + \ell^*_{j} \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)})
\end{aligned}$$

$$
\begin{aligned}
&\quad + \ell^*_{i+1} \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)} \wedge \Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)}) \\
&\qquad\qquad \text{(Fact 6.5, item 3 and definition of } \ell^*) \\
&\leq 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) \\
&\quad - \left(2 \cdot \mathsf{corr}_j - \ell^*_j\right) \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) \\
&\quad + \ell^*_{i+1} \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)} \wedge \Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)}) \\
&\leq 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) \\
&\quad - \left(2 \cdot \mathsf{corr}_j - \ell^*_j\right) \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) \\
&\quad + \ell^*_{i+1} \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)} \wedge j \in \mathfrak{E}(70)) \qquad \text{(Definition of Line 70)} \\
&\leq 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) \\
&\quad - \left(2 \cdot \mathsf{corr}_j - \ell^*_j\right) \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) \\
&\quad + \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{D}_i(j) > \mathsf{D}_i(j-1) \wedge j \in \mathfrak{E}(70)) \qquad \text{(Equation 28)}
\end{aligned}
$$

To continue, we claim that $\left(2 \cdot \mathsf{corr}_j - \ell^*_j\right) \cdot \mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) \geq 0$. Indeed, either $\mathbb{1}(\Gamma^A_{j,\geq \mathsf{depth}(i)} = \tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}) = 0$ in which case, there is nothing to show, or $\tilde{\Gamma}^A_{j,\geq \mathsf{depth}(i)} \neq \Gamma^B_{j,\geq \mathsf{depth}(i)}$ implying that $2 \cdot \mathsf{corr}_j \geq \ell^*_j$. This gives:

$$
\begin{aligned}
&2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) \\
&\quad \leq 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) + \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{D}_i(j) > \mathsf{D}_i(j-1) \wedge j \in \mathfrak{E}(70)).
\end{aligned} \tag{29}
$$

We next show:

Claim 6.26. $\mathbb{1}(\mathsf{B}_i(j-1) > 0) + \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) \geq \mathbb{1}(\mathsf{B}_i(j) > 0)$.

Proof. We show that $\mathsf{B}_i(j) > 0$ implies that either $\mathsf{B}_i(j-1) > 0$ or $\mathsf{D}_i(j) > \mathsf{D}_i(j-1)$ and the claim follows. To this end, suppose that $\mathsf{B}_i(j) > 0$. If $\mathsf{B}_i(j-1) > 0$, we are done, so assume that $\mathsf{B}_i(j-1) = 0$. By Lemma 6.24, we get that $\mathsf{D}_i(j) > 0 = \mathsf{D}_i(j-1)$, as desired. □

Finally, observe that:

$$
\begin{aligned}
&4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j-1) \\
&\quad \leq 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) - \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{B}_i(j-1) > 0) \\
&\qquad\qquad \text{(Definition of } \mathsf{spare}(\cdot) \text{ as } |\mathscr{R}_j| \text{ is odd)} \\
&\quad \leq 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) - \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{B}_i(j) > 0) \\
&\qquad + \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) \qquad \text{(Claim 6.26)} \\
&\quad \leq 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j) \\
&\qquad - \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{B}_i(j) > 0 \wedge j \in \mathfrak{E}(70) \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) \\
&\qquad + \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)). \\
&\qquad\qquad \text{(Definition of } \mathsf{spare}(\cdot) \text{ and } \mathsf{D}_i(j) \geq \mathsf{D}_i(j-1))
\end{aligned}
$$

Noting that $\mathsf{D}_i(j) > \mathsf{D}_i(j-1)$ implies $\mathsf{D}_i(j) > 0$ which in turn implies $\mathsf{B}_i(j) > 0$ by Lemma 6.24, we continue as,

$$
\begin{aligned}
&4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j-1) \\
&\quad \le 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) - \ell^*_{i+1} \cdot \mathsf{D}_i(j-1) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j) \\
&\qquad\quad - \ell^*_{i+1} \cdot \mathbb{1}(j \in \mathfrak{E}(70) \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) \\
&\qquad\quad + \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) \\
&\quad \le 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j-1) + 2 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j) \\
&\qquad\quad + \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) && \text{(Equation 29)} \\
&\quad \le 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j) \\
&\qquad\quad - 2 \cdot \mathsf{corr}_j \cdot \mathbb{1}(\Gamma^A_{j,\ge \mathsf{depth}(i)} \neq \Gamma^B_{j,\ge \mathsf{depth}(i)}) \\
&\qquad\quad + \ell^*_{i+1} \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) && \text{(Equation 27)} \\
&\quad \le 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j) \\
&\qquad\quad - 2 \cdot \mathsf{corr}_j \cdot \mathbb{1}(\Gamma^A_{j,\ge \mathsf{depth}(i)} \neq \Gamma^B_{j,\ge \mathsf{depth}(i)}) \\
&\qquad\quad + \ell^*_{j} \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) \\
&\qquad\qquad && \text{(Fact 6.5, item 3 and definition of } \ell^*) \\
&\quad \le 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j) \\
&\qquad\quad - 2 \cdot \mathsf{corr}_j \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \Gamma^A_{j,\ge \mathsf{depth}(i)} \neq \Gamma^B_{j,\ge \mathsf{depth}(i)}) \\
&\qquad\quad + \ell^*_{j} \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \mathsf{D}_i(j) > \mathsf{D}_i(j-1)) \\
&\quad \le 4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) - \ell^*_{i+1} \cdot \mathsf{D}_i(j) - \ell^*_{i+1} \cdot \mathsf{spare}_i(j) \\
&\qquad\quad - \left(2 \cdot \mathsf{corr}_j - \ell^*_j\right) \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \Gamma^A_{j,\ge \mathsf{depth}(i)} \neq \Gamma^B_{j,\ge \mathsf{depth}(i)}). && \text{(Equation 28)}
\end{aligned}
$$

To finish all, we need to show is that $\left(2 \cdot \mathsf{corr}_j - \ell^*_j\right) \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \Gamma^A_{j,\ge \mathsf{depth}(i)} \neq \Gamma^B_{j,\ge \mathsf{depth}(i)}) \ge 0$. If $\mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \Gamma^A_{j,\ge \mathsf{depth}(i)} \neq \Gamma^B_{j,\ge \mathsf{depth}(i)}) = 0$, there is nothing to show, so we assume that $\mathsf{B}_i(j-1) = 0$ and $\Gamma^A_{j,\ge \mathsf{depth}(i)} \neq \Gamma^B_{j,\ge \mathsf{depth}(i)}$. By definition of Γ, we get that there is an $h \ge \mathsf{depth}(i)$ such that

$$
\begin{aligned}
\Gamma^A_{j,h} \neq \Gamma^B_{j,h} &\implies \mathsf{TC}(\pi^A_{j+1,>\mathscr{R}_j[2h-1].r}) \neq \mathsf{TC}(\pi^B_{j+1,>\mathscr{R}_j[2h-1].r}) && \text{(As } |\mathscr{R}_j| \text{ is odd)} \\
&\implies \pi^A_{j+1,>\mathscr{R}_j[2h-1].r} \neq \pi^B_{j+1,>\mathscr{R}_j[2h-1].r} \\
&\implies \pi^A_{j+1,>\mathscr{R}_j[2\mathsf{depth}(i)-1].r} \neq \pi^B_{j+1,>\mathscr{R}_j[2\mathsf{depth}(i)-1].r} && \text{(Lemma 6.6 as } h \ge \mathsf{depth}(i)) \\
&\implies \pi^A_{j+1,>\mathscr{R}_j[|\mathscr{R}_{i+1}|].r} \neq \pi^B_{j+1,>\mathscr{R}_j[|\mathscr{R}_{i+1}|].r} && \text{(Definition of } \mathsf{depth}(i)) \\
&\implies \pi^A_{j+1,>|\pi_{i+1}|} \neq \pi^B_{j+1,>|\pi_{i+1}|} && \text{(Fact 6.5, item 8)} \\
&\implies \pi^A_{j,>|\pi_{i+1}|} \neq \pi^B_{j,>|\pi_{i+1}|} \vee \sigma^A_j \neq \sigma^B_j && \text{(Fact 6.5, item 5)} \\
&\implies \sigma^A_j \neq \sigma^B_j. && \text{(As } \mathsf{B}_i(j-1) = 0)
\end{aligned}
$$

From $\sigma^A_j \neq \sigma^B_j$, it follows that $2 \cdot \mathsf{corr}_j - \ell^*_j \ge 0$ implying $\left(2 \cdot \mathsf{corr}_j - \ell^*_j\right) \cdot \mathbb{1}(\mathsf{B}_i(j-1) = 0 \wedge \Gamma^A_{j,\ge \mathsf{depth}(i)} \neq \Gamma^B_{j,\ge \mathsf{depth}(i)}) \ge 0$ and finishing the proof.

□

Lemma 6.27. *For $i, i' \in \textsc{Starts}_{\mathrm{F}}$ such that i' is direct, $\textsc{Range}(i') \subseteq \textsc{Range}(i)$, and $\mathsf{depth}(i') = \mathsf{depth}(i) + 1$, we have*

$$\mathsf{D}_i(\textsc{Stop}(i')) - \mathsf{D}_i(i') - \mathsf{D}_{i'}(\textsc{Stop}(i')) \leq \frac{2}{\ell^*_{i'+1}} \left(\mathsf{E}^{\mathrm{F}}_{i',\mathsf{depth}(i)}(\textsc{Stop}(i')) - \mathsf{E}^{\mathrm{F}}_{i',\mathsf{depth}(i')}(\textsc{Stop}(i'))\right).$$

Proof. We first show that $\mathsf{latest}(i', l) = \mathsf{latest}(\textsc{Stop}(i'), l)$ for all $|\pi_{i+1}| < l \leq |\pi_{i'+1}|$. Suppose not. Then, for $|\pi_{i+1}| < l \leq |\pi_{i'+1}|$, we have by the definition of $\mathsf{latest}(\cdot)$ that there exists $j' \in \textsc{Range}(i')$ such that $|\mathscr{R}_{j'}|$ is odd and $|\pi_{j'+1}| = l$. By item 5 of Fact 6.5, we conclude that $|\pi_{j'}| = l - 1 < |\pi_{i'+1}|$. Next, using item 8 of Fact 6.5 on j', we get that $|\pi_{j'}| < \mathscr{R}_{j'}[|\mathscr{R}_{i'+1}|].r$, a contradiction to Lemma 6.6.

We use the definition $\mathsf{D}(\cdot)$ to derive:

$$\begin{aligned}
&\mathsf{D}_i(\textsc{Stop}(i')) - \mathsf{D}_i(i') - \mathsf{D}_{i'}(\textsc{Stop}(i')) \\
&\quad = |\{|\pi_{i+1}| < l \leq |\pi_{\textsc{Stop}(i')+1}| \mid \Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)}\}| \\
&\qquad - |\{|\pi_{i+1}| < l \leq |\pi_{i'+1}| \mid \Gamma^A_{\mathsf{latest}(i',l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(i',l),\geq\mathsf{depth}(i)}\}| \\
&\qquad - |\{|\pi_{i'+1}| < l \leq |\pi_{\textsc{Stop}(i')+1}| \mid \Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i')}\}| \\
&\quad = |\{|\pi_{i+1}| < l \leq |\pi_{\textsc{Stop}(i')+1}| \mid \Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)}\}| \\
&\qquad - |\{|\pi_{i+1}| < l \leq |\pi_{i'+1}| \mid \Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)}\}| \\
&\qquad - |\{|\pi_{i'+1}| < l \leq |\pi_{\textsc{Stop}(i')+1}| \mid \Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i')}\}| \\
&\quad = |\{|\pi_{i'+1}| < l \leq |\pi_{\textsc{Stop}(i')+1}| \mid \Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)}\}| \\
&\qquad - |\{|\pi_{i'+1}| < l \leq |\pi_{\textsc{Stop}(i')+1}| \mid \Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i')}\}| \\
&\quad = \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Stop}(i')+1}|} \mathbb{1}\left(\Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i)}\right) \\
&\qquad - \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Stop}(i')+1}|} \mathbb{1}\left(\Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq\mathsf{depth}(i')}\right),
\end{aligned} \tag{30}$$

Next, we claim that $\mathsf{latest}(\textsc{Stop}(i'), l) \in \textsc{Range}(i')$ for all $|\pi_{i'+1}| < l \leq |\pi_{\textsc{Stop}(i')+1}|$. To show this, it is sufficient to show that $\mathsf{latest}(\textsc{Stop}(i'), l) > i'$. This is because, otherwise, we have a contradiction to Lemma 6.21. Since $\mathsf{latest}(\textsc{Stop}(i'), l) \in \textsc{Range}(i')$, we have from item 3 of Fact 6.5 that $\ell^*_{\mathsf{latest}(\textsc{Stop}(i'),l)} \geq \ell^*_{i'+1}$. Using these two claims, we get:

$$\begin{aligned}
&\frac{2}{\ell^*_{i'+1}} \left(\mathsf{E}^{\mathrm{F}}_{i',\mathsf{depth}(i)}(\textsc{Stop}(i')) - \mathsf{E}^{\mathrm{F}}_{i',\mathsf{depth}(i')}(\textsc{Stop}(i'))\right) \\
&\quad = \frac{2}{\ell^*_{i'+1}} \cdot \sum_{j' \in (i':\textsc{Stop}(i')]} \left(\mathsf{E}^{\mathrm{F}}_{\mathsf{depth}(i)}(\textsc{Stop}(i'), j') - \mathsf{E}^{\mathrm{F}}_{\mathsf{depth}(i')}(\textsc{Stop}(i'), j')\right)
\end{aligned}$$

$$\geq \frac{2}{\ell^*_{i'+1}} \cdot \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Stop}(i')+1}|} \mathsf{corr}_{\mathsf{latest}(\textsc{Stop}(i'),l)} \cdot \Big(\mathbb{1}(\Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)}) - \mathbb{1}(\Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')}) \Big)$$

$$\geq \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Stop}(i')+1}|} \frac{2 \cdot \mathsf{corr}_{\mathsf{latest}(\textsc{Stop}(i'),l)}}{\ell^*_{\mathsf{latest}(\textsc{Stop}(i'),l)}} \cdot \Big(\mathbb{1}(\Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)}) - \mathbb{1}(\Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')}) \Big).$$

To continue, we use item 7 of Fact 6.5 to get that $\textsc{Stop}(i') \notin \mathfrak{E}(70)$. This with Lemma 6.23 gives:

$$\frac{2}{\ell^*_{i'+1}} \left(\mathsf{E}^{\mathrm{F}}_{i',\mathsf{depth}(i)}(\textsc{Stop}(i')) - \mathsf{E}^{\mathrm{F}}_{i',\mathsf{depth}(i')}(\textsc{Stop}(i'))\right)$$

$$\geq \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Stop}(i')+1}|} \frac{2 \cdot \mathsf{corr}_{\mathsf{latest}(\textsc{Stop}(i'),l)}}{\ell^*_{\mathsf{latest}(\textsc{Stop}(i'),l)}} \cdot \Big(\mathbb{1}(\tilde{\Gamma}^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)}) - \mathbb{1}(\tilde{\Gamma}^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')}) \Big).$$

Note that $\mathbb{1}(\tilde{\Gamma}^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)}) \geq \mathbb{1}(\tilde{\Gamma}^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')})$ and the inequality is strict only if $2 \cdot \mathsf{corr}_{\mathsf{latest}(\textsc{Stop}(i'),l)} \geq \ell^*_{\mathsf{latest}(\textsc{Stop}(i'),l)}$. Thus, we get:

$$\frac{2}{\ell^*_{i'+1}} \left(\mathsf{E}^{\mathrm{F}}_{i',\mathsf{depth}(i)}(\textsc{Stop}(i')) - \mathsf{E}^{\mathrm{F}}_{i',\mathsf{depth}(i')}(\textsc{Stop}(i'))\right)$$

$$\geq \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Stop}(i')+1}|} \Big(\mathbb{1}(\tilde{\Gamma}^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)}) - \mathbb{1}(\tilde{\Gamma}^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')}) \Big)$$

$$\geq \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Stop}(i')+1}|} \Big(\mathbb{1}(\Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i)}) - \mathbb{1}(\Gamma^A_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')} \neq \Gamma^B_{\mathsf{latest}(\textsc{Stop}(i'),l),\geq \mathsf{depth}(i')}) \Big)$$

(Lemma 6.23)

$$= \mathsf{D}_i(\textsc{Stop}(i')) - \mathsf{D}_i(i') - \mathsf{D}_{i'}(\textsc{Stop}(i')).$$ (Equation 30)

□

6.2.5 Lemmas Concerning $\mathsf{E}(\cdot)$

Lemma 6.28. *Let $i \in \textsc{Starts}_{\mathrm{F}}$. For $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$, we have for all $d > 0$:*

$$\mathsf{E}^{\mathrm{F}}_{i,d}(j) \leq 2 \cdot \sum_{j'=i+1}^{j} \mathsf{corr}_{j'}.$$

Proof. Using the definition of $\mathsf{E}(\cdot)$, we get:

$$\mathsf{E}^{\mathrm{F}}_{i,d}(j) = \sum_{j' \in (i:j]} \mathsf{E}^{\mathrm{F}}_{d}(j,j') \leq 2 \cdot \sum_{j' \in (i:j]} \mathsf{corr}_{j'}.$$

□

Lemma 6.29. *Let $i \in \textsc{Starts}_{\mathrm{F}}$ and $i' \in (i : \textsc{Stop}(i)) \cap \textsc{Starts}_{\mathrm{B}}$. For $j \in \{i'\} \cup \textsc{Range}(i') \setminus \{num\}$ such that $|\pi_{j+1}| \leq |\pi_{i'+1}|$, we have for all $d > 0$:*

$$\mathsf{E}^{\mathrm{F}}_{i,d}(i') + \mathsf{E}^{\mathrm{B}}_{i'}(j) \leq 3 \cdot \sum_{j'=i+1}^{j} \mathsf{corr}_{j'}.$$

Proof. Use the definition of $\mathsf{E}(\cdot)$ to get:

$$\begin{aligned}\mathsf{E}^{\mathrm{B}}_{i'}(j) &= \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i'+1}|} \mathsf{corr}_{\mathsf{latest}(i',l)} + \sum_{j'=i'+1}^{j} \mathsf{corr}_{j'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{j'}| \text{ is odd}\right)) \\ &\leq \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i'+1}|} \mathsf{corr}_{\mathsf{latest}(i',l)} + 2 \cdot \sum_{j'=i'+1}^{j} \mathsf{corr}_{j'}.\end{aligned}$$

We claim that $\mathsf{latest}(i',l) > i$ for all $l \in (|\pi_{j+1}| : |\pi_{i'+1}|]$. Indeed, if not, then using Lemma 6.21, we get that $|\pi_{i+1}| \geq l > |\pi_{j+1}|$. As $j \in \{i'\} \cup \textsc{Range}(i') \subseteq \textsc{Range}(i)$ by Lemma 6.7, we get $|\pi_{j+1}| < \mathscr{R}_j[|\mathscr{R}_{i+1}|].r$ using item 8 of Fact 6.5. This contradicts Lemma 6.6.

Additionally, observing that $\mathsf{latest}(i',l) > i$ is distinct for all $l \in (|\pi_{j+1}| : |\pi_{i'+1}|]$, we get:

$$\mathsf{E}^{\mathrm{B}}_{i'}(j) \leq \sum_{j'=i+1}^{i'} \mathsf{corr}_{j'} + 2 \cdot \sum_{j'=i'+1}^{j} \mathsf{corr}_{j'},$$

which with Lemma 6.28 gives:

$$\mathsf{E}^{\mathrm{F}}_{i,d}(i') + \mathsf{E}^{\mathrm{B}}_{i'}(j) \leq 3 \cdot \sum_{j'=i+1}^{i'} \mathsf{corr}_{j'} + 2 \cdot \sum_{j'=i'+1}^{j} \mathsf{corr}_{j'} \leq 3 \cdot \sum_{j'=i+1}^{j} \mathsf{corr}_{j'}.$$

□

Lemma 6.30. *Let $i \in \textsc{Starts}_{\mathrm{F}}$ and $i' \in (i : \textsc{Stop}(i)) \cap \textsc{Starts}_{\mathrm{B}}$ be such that i' is indirect*

and $|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|$. *We have for all* $d > 0$*:*

$$\mathsf{E}^{\mathrm{F}}_{i,d}(i') + \mathsf{E}^{\mathrm{B}}_{i'}(\textsc{Mid}(i')) + \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i'),d}(\textsc{Stop}(i')) \le \mathsf{E}^{\mathrm{F}}_{i,d}(\textsc{Stop}(i')).$$

Proof. To start, we need the following claim:

Claim 6.31. *For all* $l \in [|\pi_{\textsc{Mid}(i')+1}|]$*, we have* $\mathsf{latest}(i', l) = \mathsf{latest}(\textsc{Stop}(i'), l)$*. It follows that* $\mathsf{latest}(\textsc{Stop}(i'), l) \le i'$*.*

Proof. Proof by contradiction. Suppose that, for some $l \le |\pi_{\textsc{Mid}(i')+1}|$, we have $\mathsf{latest}(i', l) \neq \mathsf{latest}(\textsc{Stop}(i'), l)$. Then, by the definition of $\mathsf{latest}(\cdot)$, there exists $j' \in \textsc{Range}(i')$ such that $|\mathscr{R}_{j'}|$ is odd and $|\pi_{j'+1}| = l$. By item 5 of Fact 6.5, we conclude that $|\pi_{j'}| = l-1 < |\pi_{\textsc{Mid}(i')+1}|$. Now, either $j' \le \textsc{Mid}(i')$, in which case, by Lemma 6.13, we have $|\pi_{j'}| < |\pi_{\textsc{Mid}(i')+1}| \le |\pi_{j'}|$, a contradiction ($\textsc{Mid}(i')$ is good for i' by definition), or we have $\textsc{Mid}(i') < j' \le \textsc{Stop}(i') \implies j' \in \textsc{Range}(\textsc{Mid}(i'))$ by Lemma 6.9. When this happens, we use item 8 of Fact 6.5 on $\textsc{Mid}(i')$ and j' to get that $|\pi_{j'}| < \mathscr{R}_{j'}[|\mathscr{R}_{\textsc{Mid}(i')+1}|].r$, a contradiction to Lemma 6.6. □

Now, using the fact that $\mathsf{latest}(i', l) = \mathsf{latest}(\textsc{Stop}(i'), l)$ for all $l \le |\pi_{\textsc{Mid}(i')+1}|$, we have for $j' \in (i : i']$ that:

$$\begin{aligned}
\mathsf{E}^{\mathrm{F}}_{d}(i', j') &= \begin{cases} \mathsf{corr}_{j'} & ,|\mathscr{R}_{j'}| \text{ is even} \\ \mathsf{corr}_{j'} \cdot \mathbb{1}(\Gamma^{A}_{j',\ge d} \neq \Gamma^{B}_{j',\ge d}) & ,\exists l \in [|\pi_{i'+1}|] \text{ such that } j' = \mathsf{latest}(i', l) \\ 2 \cdot \mathsf{corr}_{j'} & ,\text{otherwise} \end{cases} \\
&= \begin{cases} \mathsf{corr}_{j'} & ,|\mathscr{R}_{j'}| \text{ is even} \\ \mathsf{corr}_{j'} \cdot \mathbb{1}(\Gamma^{A}_{j',\ge d} \neq \Gamma^{B}_{j',\ge d}) & ,\exists l \in [|\pi_{\textsc{Mid}(i')+1}|] \text{ such that } j' = \mathsf{latest}(i', l) \\ \mathsf{corr}_{j'} \cdot \mathbb{1}(\Gamma^{A}_{j',\ge d} \neq \Gamma^{B}_{j',\ge d}) & ,\exists l \in (|\pi_{\textsc{Mid}(i')+1}| : |\pi_{i'+1}|] \text{ such that } j' = \mathsf{latest}(i', l) \\ 2 \cdot \mathsf{corr}_{j'} & ,\text{otherwise} \end{cases} \\
&= \begin{cases} \mathsf{corr}_{j'} & ,|\mathscr{R}_{j'}| \text{ is even} \\ \mathsf{corr}_{j'} \cdot \mathbb{1}(\Gamma^{A}_{j',\ge d} \neq \Gamma^{B}_{j',\ge d}) & ,\exists l \in [|\pi_{\textsc{Mid}(i')+1}|] \text{ such that } j' = \mathsf{latest}(\textsc{Stop}(i'), l) \\ \mathsf{corr}_{j'} \cdot \mathbb{1}(\Gamma^{A}_{j',\ge d} \neq \Gamma^{B}_{j',\ge d}) & ,\exists l \in (|\pi_{\textsc{Mid}(i')+1}| : |\pi_{i'+1}|] \text{ such that } j' = \mathsf{latest}(i', l) \\ 2 \cdot \mathsf{corr}_{j'} & ,\text{otherwise} \end{cases} \\
&\le \begin{cases} \mathsf{corr}_{j'} & ,|\mathscr{R}_{j'}| \text{ is even} \\ \mathsf{corr}_{j'} \cdot \mathbb{1}(\Gamma^{A}_{j',\ge d} \neq \Gamma^{B}_{j',\ge d}) & ,\exists l \in [|\pi_{\textsc{Mid}(i')+1}|] \text{ such that } j' = \mathsf{latest}(\textsc{Stop}(i'), l) \\ \mathsf{corr}_{j'} & ,\exists l \in (|\pi_{\textsc{Mid}(i')+1}| : |\pi_{i'+1}|] \text{ such that } j' = \mathsf{latest}(i', l) \\ 2 \cdot \mathsf{corr}_{j'} & ,\text{otherwise} \end{cases}.
\end{aligned}$$

To continue, we claim that

Claim 6.32. *For all* $l \in (|\pi_{\textsc{Mid}(i')+1}| : |\pi_{\textsc{Stop}(i')+1}|]$*, it holds that* $\mathsf{latest}(\textsc{Stop}(i'), l) \in \textsc{Range}(\textsc{Mid}(i'))$*.*

Proof. Due to Lemma 6.9, it is sufficient to show that $\mathsf{latest}(\textsc{Stop}(i'), l) > \textsc{Mid}(i')$. This is because, otherwise, we have a contradiction to Lemma 6.21. □

Using this claim, we can continue as (for $j' \in (i : i']$):

$$\mathsf{E}^{\mathrm{F}}_d(i', j') \leq \begin{cases} \mathsf{corr}_{j'} & , |\mathscr{R}_{j'}| \text{ is even} \\ \mathsf{corr}_{j'} \cdot \mathbb{1}(\Gamma^A_{j',\geq d} \neq \Gamma^B_{j',\geq d}) & , \exists l \in [|\pi_{\textsc{Stop}(i')+1}|] \text{ such that } j' = \mathsf{latest}(\textsc{Stop}(i'), l) \\ \mathsf{corr}_{j'} & , \exists l \in (|\pi_{\textsc{Mid}(i')+1}| : |\pi_{i'+1}|] \text{ such that } j' = \mathsf{latest}(i', l) \\ 2 \cdot \mathsf{corr}_{j'} & , \text{otherwise} \end{cases}$$
$$= \mathsf{E}^{\mathrm{F}}_d(\textsc{Stop}(i'), j') - \mathsf{corr}_{j'} \cdot \mathbb{1}\left(\exists l \in (|\pi_{\textsc{Mid}(i')+1}| : |\pi_{i'+1}|] : j' = \mathsf{latest}(i', l)\right).$$

Summing over all $j' \in (i : i']$, we derive:

$$\begin{aligned} \mathsf{E}^{\mathrm{F}}_{i,d}(i') &= \sum_{j' \in (i:i']} \mathsf{E}^{\mathrm{F}}_d(i', j') \\ &\leq \sum_{j' \in (i:i']} \mathsf{E}^{\mathrm{F}}_d(\textsc{Stop}(i'), j') - \mathsf{corr}_{j'} \cdot \mathbb{1}\left(\exists l \in (|\pi_{\textsc{Mid}(i')+1}| : |\pi_{i'+1}|] : j' = \mathsf{latest}(i', l)\right) \\ &= \sum_{j' \in (i:i']} \mathsf{E}^{\mathrm{F}}_d(\textsc{Stop}(i'), j') - \sum_{l=|\pi_{\textsc{Mid}(i')+1}|+1}^{|\pi_{i'+1}|} \mathsf{corr}_{\mathsf{latest}(i',l)}, \end{aligned}$$

where the last step uses the following claim:

Claim 6.33. *For all $l \in (|\pi_{\textsc{Mid}(i')+1}| : |\pi_{i'+1}|]$, we have $\mathsf{latest}(i', l) \in (i : i']$.*

Proof. To start, note that $\textsc{Mid}(i') + 1 \in \textsc{Range}(\textsc{Mid}(i)) \subseteq \textsc{Range}(i') \subseteq \textsc{Range}(i)$ by Lemma 6.9 and Lemma 6.7, implying by item 8 of Fact 6.5 and Lemma 6.6 that $|\pi_{i+1}| = \mathscr{R}_{\textsc{Mid}(i')+1}[|\mathscr{R}_{i+1}|].r \leq \mathscr{R}_{\textsc{Mid}(i')+1}[|\mathscr{R}_{\textsc{Mid}(i')+1}|].r = |\pi_{\textsc{Mid}(i')+1}|$.

We will actually show that the claim holds for all $l \in (|\pi_{i+1}| : |\pi_{i'+1}|]$. It is sufficient to show that $\mathsf{latest}(i', l) > i$. This is because, otherwise, we have a contradiction to Lemma 6.21. □

Using the definition of $\mathsf{E}^{\mathrm{F}}(\cdot)$ and $\mathsf{E}^{\mathrm{B}}(\cdot)$, we continue as:

$$\begin{aligned} &\mathsf{E}^{\mathrm{F}}_{i,d}(i') + \mathsf{E}^{\mathrm{B}}_{i'}(\textsc{Mid}(i')) + \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i'),d}(\textsc{Stop}(i')) \\ &\quad\leq \sum_{j' \in (i:i']} \mathsf{E}^{\mathrm{F}}_d(\textsc{Stop}(i'), j') + \sum_{j'=i'+1}^{\textsc{Mid}(i')} \mathsf{corr}_{j'} \cdot (1 + \mathbb{1}(|\mathscr{R}_{j'}| \text{ is odd})) \\ &\qquad + \sum_{j'=\textsc{Mid}(i')+1}^{\textsc{Stop}(i')} \mathsf{E}^{\mathrm{F}}_d(\textsc{Stop}(i'), j'). \end{aligned}$$

Finally, due to Claim 6.31 and Claim 6.32, we have that for all $j' \in (i' : \textsc{Mid}(i')]$ there does

not exists any $l \in [|\pi_{\textsc{Stop}(i')+1}|]$ such that $j' = \mathsf{latest}(\textsc{Stop}(i'), l)$. This gives:

$$\begin{aligned}
&\mathsf{E}^{\mathrm{F}}_{i,d}(i') + \mathsf{E}^{\mathrm{B}}_{i'}(\textsc{Mid}(i')) + \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i'),d}(\textsc{Stop}(i')) \\
&\quad\leq \sum_{j' \in (i:i']} \mathsf{E}^{\mathrm{F}}_{d}(\textsc{Stop}(i'), j') + \sum_{j'=i'+1}^{\textsc{Mid}(i')} \mathsf{E}^{\mathrm{F}}_{d}(\textsc{Stop}(i'), j') + \sum_{j'=\textsc{Mid}(i')+1}^{\textsc{Stop}(i')} \mathsf{E}^{\mathrm{F}}_{d}(\textsc{Stop}(i'), j') \\
&\quad\leq \sum_{j'=i+1}^{\textsc{Stop}(i')} \mathsf{E}^{\mathrm{F}}_{d}(\textsc{Stop}(i'), j') \\
&\quad\leq \mathsf{E}^{\mathrm{F}}_{i,d}(\textsc{Stop}(i')).
\end{aligned}$$

□

Lemma 6.34. *Let $i \in \textsc{Starts}_{\mathrm{B}}$ and $i' \in (i : \textsc{Stop}(i)) \cap \textsc{Starts}_{\mathrm{F}}$ be such that i' is indirect and $|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|$. We have for all $d > 0$:*

$$\mathsf{E}^{\mathrm{B}}_{i}(i') + \mathsf{E}^{\mathrm{F}}_{i',d}(\textsc{Mid}(i')) + \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i')}(\textsc{Stop}(i')) \leq \mathsf{E}^{\mathrm{B}}_{i}(\textsc{Stop}(i')).$$

Proof. By definition, we have for all $j' \in (i' : \textsc{Mid}(i')]$ and $d > 0$:

$$\mathsf{E}^{\mathrm{F}}_{d}(\textsc{Mid}(i'), j') \leq \begin{cases} \mathsf{corr}_{j'} & , |\mathscr{R}_{j'}| \text{ is even} \\ \mathsf{corr}_{j'} & , \exists l \in [|\pi_{\textsc{Mid}(i')+1}|] \text{ such that } j' = \mathsf{latest}(\textsc{Mid}(i'), l) \\ 2 \cdot \mathsf{corr}_{j'} & , \text{otherwise} \end{cases}.$$

We also have the following claim:

Claim 6.35. *For all $l \in (|\pi_{i'+1}| : |\pi_{\textsc{Mid}(i')+1}|]$, we have $\mathsf{latest}(\textsc{Mid}(i'), l) \in (i' : \textsc{Mid}(i')]$.*

Proof. It is sufficient to show that $\mathsf{latest}(\textsc{Mid}(i'), l) > i'$. This is because, otherwise, we have a contradiction to Lemma 6.21. □

Using this claim, we derive, for all $d > 0$:

$$\begin{aligned}
\mathsf{E}^{\mathrm{F}}_{i',d}(\textsc{Mid}(i')) &= \sum_{j' \in (i':\textsc{Mid}(i')]} \mathsf{E}^{\mathrm{F}}_{d}(\textsc{Mid}(i'), j') \\
&\leq \sum_{j'=i'+1}^{\textsc{Mid}(i')} \mathsf{corr}_{j'} \cdot (1 + \mathbb{1}(|\mathscr{R}_{j'}| \text{ is odd})) - \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Mid}(i')+1}|} \mathsf{corr}_{\mathsf{latest}(\textsc{Mid}(i'),l)}.
\end{aligned}$$

Using the definition of $\mathsf{E}^{\mathrm{B}}(\cdot)$, we continue as:

$$\begin{aligned}
&\mathsf{E}^{\mathrm{B}}_{i}(i') + \mathsf{E}^{\mathrm{F}}_{i',d}(\textsc{Mid}(i')) + \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i')}(\textsc{Stop}(i')) \\
&\quad\leq \sum_{j'=i'+1}^{\textsc{Mid}(i')} \mathsf{corr}_{j'} \cdot (1 + \mathbb{1}(|\mathscr{R}_{j'}| \text{ is odd})) - \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Mid}(i')+1}|} \mathsf{corr}_{\mathsf{latest}(\textsc{Mid}(i'),l)}
\end{aligned}$$

$$
\begin{aligned}
&+ \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} + \sum_{j'=i+1}^{i'} \mathsf{corr}_{j'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{j'}| \text{ is odd}\right)) \\
&+ \sum_{l=|\pi_{\textsc{Stop}(i')+1}|+1}^{|\pi_{\textsc{Mid}(i')+1}|} \mathsf{corr}_{\mathsf{latest}(\textsc{Mid}(i'),l)} + \sum_{j'=\textsc{Mid}(i')+1}^{\textsc{Stop}(i')} \mathsf{corr}_{j'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{j'}| \text{ is odd}\right)) \\
\leq \sum_{j'=i'+1}^{\textsc{Mid}(i')} &\mathsf{corr}_{j'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{j'}| \text{ is odd}\right)) - \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Mid}(i')+1}|} \mathsf{corr}_{\mathsf{latest}(\textsc{Mid}(i'),l)} \\
&+ \sum_{l=|\pi_{\textsc{Stop}(i')+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} + \sum_{j'=i+1}^{i'} \mathsf{corr}_{j'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{j'}| \text{ is odd}\right)) \\
&+ \sum_{l=|\pi_{i'+1}|+1}^{|\pi_{\textsc{Mid}(i')+1}|} \mathsf{corr}_{\mathsf{latest}(\textsc{Mid}(i'),l)} + \sum_{j'=\textsc{Mid}(i')+1}^{\textsc{Stop}(i')} \mathsf{corr}_{j'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{j'}| \text{ is odd}\right)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Lemma 6.10)} \\
\leq \sum_{j'=i+1}^{\textsc{Stop}(i')} &\mathsf{corr}_{j'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{j'}| \text{ is odd}\right)) + \sum_{l=|\pi_{\textsc{Stop}(i')+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} \\
&\leq \mathsf{E}_i^{\mathrm{B}}(\textsc{Stop}(i')).
\end{aligned}
$$

□

Lemma 6.36. *Let $i \in \textsc{Starts}_{\mathrm{B}}$ and $j \in \textsc{Range}(i) \setminus \{num\}$ be such that $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ and $\sigma_j^A \neq \sigma_j^B$. It holds that*[13] $2.2 \cdot \mathsf{corr}_{\mathsf{latest}(i,|\pi_j|)} \geq \ell^*_{i+1}$ *and*

$$
5000 \cdot \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} + \frac{\ell^*_{i+1}}{30} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|\right) \geq 500 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{j+1}|\right) \quad (31)
$$

Proof. Conclude from the definition of $\textsc{Prev}(\cdot)$ that $\textsc{Prev}(i) \in \textsc{Starts}$ and $|\mathscr{R}_{\textsc{Prev}(i)+1}| = |\mathscr{R}_i| = |\mathscr{R}_{i+1}| - 1$ is odd. This means that $\textsc{Prev}(i) \in \textsc{Starts}_{\mathrm{F}}$. We start by showing the following claims:

Claim 6.37. $|\pi_{\textsc{Prev}(i)+1}| \leq |\pi_{j+1}| < |\pi_{i+1}|$.

Proof. By Lemma 6.8, we have $\textsc{Range}(i) \subseteq \textsc{Range}(\textsc{Prev}(i))$ implying that $j \in \textsc{Range}(\textsc{Prev}(i))$. Thus, we have from item 8 of Fact 6.5 that $|\pi_{\textsc{Prev}(i)+1}| = \mathscr{R}_j[|\mathscr{R}_{\textsc{Prev}(i)+1}|].r$. Using Lemma 6.6 and item 8 of Fact 6.5, we conclude that $|\pi_{\textsc{Prev}(i)+1}| \leq |\pi_{j+1}|$. For the second inequality, we simply use Lemma 6.13. □

Claim 6.38. *For all $l \in (|\pi_{j+1}| : |\pi_{i+1}|]$, we have that $\mathsf{latest}(i,l) \in \textsc{Range}(\textsc{Prev}(i))$.*

[13] Due to Corollary 6.14, we have that $|\pi_j| \leq |\pi_{i+1}|$ and therefore, $\mathsf{latest}(i,l)$ is well defined for $l \in [|\pi_j| : |\pi_{i+1}|] = (|\pi_{j+1}| : |\pi_{i+1}|]$ as $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ is even.

Proof. By definition of $\mathsf{latest}(\cdot)$, we have that $\mathsf{latest}(i,l) \leq i < \textsc{Stop}(i) \leq \textsc{Stop}(\textsc{Prev}(i))$ as $\textsc{Range}(i) \subseteq \textsc{Range}(\textsc{Prev}(i))$ by Lemma 6.8. It is thus, sufficient to show that $\mathsf{latest}(i,l) > \textsc{Prev}(i)$. This is because, otherwise, Lemma 6.21 says $|\pi_{\textsc{Prev}(i)+1}| \geq l > |\pi_{j+1}|$, a contradiction to Claim 6.37. □

Observe that:

$$\begin{aligned} \sigma_j^A \neq \sigma_j^B &\implies \pi_j^A[|\pi_j|] \neq \pi_j^B[|\pi_j|] && \text{(Fact 6.5, item 5)} \\ &\implies \pi_{i+1}^A[|\pi_j|] \neq \pi_{i+1}^B[|\pi_j|]. && \text{(Corollary 6.14)} \end{aligned}$$

By Corollary 6.22, this means that, for $l \in (|\pi_{j+1}| : |\pi_{i+1}|] = [|\pi_j| : |\pi_{i+1}|]$, we have

$$\pi^A_{\mathsf{latest}(i,l)+1}[|\pi_j|] \neq \pi^B_{\mathsf{latest}(i,l)+1}[|\pi_j|]. \tag{32}$$

In particular, putting $l = |\pi_j|$ and using the fact that $|\pi_j| = |\pi_{\mathsf{latest}(i,|\pi_j|)+1}|$, we get that:

$$\pi^A_{\mathsf{latest}(i,|\pi_j|)+1}[|\pi_{\mathsf{latest}(i,|\pi_j|)+1}|] \neq \pi^B_{\mathsf{latest}(i,|\pi_j|)+1}[|\pi_{\mathsf{latest}(i,|\pi_j|)+1}|]$$

As $|\mathscr{R}_{\mathsf{latest}(i,|\pi_j|)}|$ is odd by definition, we have by item 5 of Fact 6.5 that, for $C \in \{A,B\}$, it holds that $\pi^C_{\mathsf{latest}(i,|\pi_j|)+1}[|\pi_{\mathsf{latest}(i,|\pi_j|)+1}|] = \sigma^C_{\mathsf{latest}(i,|\pi_j|)}$. This allows us to continue as:

$$\sigma_j^A \neq \sigma_j^B \implies \sigma^A_{\mathsf{latest}(i,|\pi_j|)} \neq \sigma^B_{\mathsf{latest}(i,|\pi_j|)}.$$

Again using the fact that $|\mathscr{R}_{\mathsf{latest}(i,|\pi_j|)}|$ is odd, we get by Algorithm 5 that $2 \cdot \mathsf{corr}_{\mathsf{latest}(i,|\pi_j|)} \geq \ell^*_{\mathsf{latest}(i,|\pi_j|)}$. As $\textsc{Prev}(i) \in \textsc{Starts}$ and $\mathsf{latest}(i,|\pi_j|) \in \textsc{Range}(\textsc{Prev}(i))$, we have by item 3 of Fact 6.5 that $|\mathscr{R}_{\mathsf{latest}(i,|\pi_j|)}| \geq |\mathscr{R}_{\textsc{Prev}(i)+1}| = |\mathscr{R}_i| = |\mathscr{R}_{i+1}| - 1$. Using the definition of ℓ^*, this means that $2.2 \cdot \mathsf{corr}_{\mathsf{latest}(i,|\pi_j|)} \geq 1.1\ell^*_{\mathsf{latest}(i,|\pi_j|)} \geq \ell^*_{i+1}$, as desired.

It remains to show Equation 31. If $|\pi_{j+1}| + 1 = |\pi_{i+1}|$, Equation 31 follows because $|\pi_{i+1}| \geq |\pi_{\textsc{Prev}(i)+1}|$ (Claim 6.37) and

$$500 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) = 500 \cdot \ell^*_{i+1} \leq 5000 \cdot \mathsf{corr}_{\mathsf{latest}(i,|\pi_j|)}.$$

Due to Claim 6.37, we can henceforth assume that $|\pi_{i+1}| - |\pi_{j+1}| > 1$. Consider an $l \in (|\pi_{j+1}| : |\pi_{i+1}|)$. We have from Equation 32 that:

$$\begin{aligned} &\pi^A_{\mathsf{latest}(i,l)+1}[|\pi_j|] \neq \pi^B_{\mathsf{latest}(i,l)+1}[|\pi_j|] \\ &\quad\implies \pi^A_{\mathsf{latest}(i,l)+1}[|\pi_j| : l] \neq \pi^B_{\mathsf{latest}(i,l)+1}[|\pi_j| : l] \\ &\quad\implies \pi^A_{\mathsf{latest}(i,l)+1}(|\pi_{\textsc{Prev}(i)+1}| : l] \neq \pi^B_{\mathsf{latest}(i,l)+1}(|\pi_{\textsc{Prev}(i)+1}| : l]. && \text{(Claim 6.37)} \end{aligned}$$

We also have, by Lemma 6.23 that $\Gamma^C_{\mathsf{latest}(i,l)} = \tilde{\Gamma}^C_{\mathsf{latest}(i,l)}$ for all $C \in \{A,B\}$. This means that, for all $l \in (|\pi_{j+1}| : |\pi_{i+1}|)$, either $\Gamma^A_{\mathsf{latest}(i,l)} \neq \tilde{\Gamma}^B_{\mathsf{latest}(i,l)}$ or we have

$$\begin{aligned} &\Gamma^A_{\mathsf{latest}(i,l)} = \Gamma^B_{\mathsf{latest}(i,l)} \\ &\quad\implies \Gamma^A_{\mathsf{latest}(i,l),\mathsf{depth}(\textsc{Prev}(i))} = \Gamma^B_{\mathsf{latest}(i,l),\mathsf{depth}(\textsc{Prev}(i))} \end{aligned}$$

$$\implies \mathsf{TC}(\pi^A_{\mathsf{latest}(i,l)+1,>\mathscr{R}_{\mathsf{latest}(i,l)}[|\mathscr{R}_{\textsc{Prev}(i)+1}|].r}) = \mathsf{TC}(\pi^B_{\mathsf{latest}(i,l)+1,>\mathscr{R}_{\mathsf{latest}(i,l)}[|\mathscr{R}_{\textsc{Prev}(i)+1}|].r}).$$
(Definition of Γ and $|\mathscr{R}_{\mathsf{latest}(i,l)}|$ is odd)

Due to Claim 6.38, we have $\mathsf{latest}(i,l) \in \textsc{Range}(\textsc{Prev}(i))$ which together with $\textsc{Prev}(i) \in \textsc{Starts}_{\mathrm{F}}$ and item 8 of Fact 6.5 gives us that

$$\mathsf{TC}(\pi^A_{\mathsf{latest}(i,l)+1,>|\pi_{\textsc{Prev}(i)+1}|}) = \mathsf{TC}(\pi^B_{\mathsf{latest}(i,l)+1,>|\pi_{\textsc{Prev}(i)+1}|})$$
$$\implies \mathsf{TC}(\pi^A_{i+1}(|\pi_{\textsc{Prev}(i)+1}| : l]) = \mathsf{TC}(\pi^B_{i+1}(|\pi_{\textsc{Prev}(i)+1}| : l]). \qquad \text{(Corollary 6.22)}$$

Overall, we get that for all $l \in (|\pi_{j+1}| : |\pi_{i+1}|)$, either $\Gamma^A_{\mathsf{latest}(i,l)} \neq \tilde{\Gamma}^B_{\mathsf{latest}(i,l)}$ or $\mathsf{TC}(\pi^A_{i+1}(|\pi_{\textsc{Prev}(i)+1}| : l]) = \mathsf{TC}(\pi^B_{i+1}(|\pi_{\textsc{Prev}(i)+1}| : l])$. The number of $l \in (|\pi_{j+1}| : |\pi_{i+1}|)$ is $|\pi_{i+1}| - |\pi_{j+1}| - 1 \geq \frac{|\pi_{i+1}|-|\pi_{j+1}|}{2}$. Thus, either there are at least $\frac{|\pi_{i+1}|-|\pi_{j+1}|}{4}$ values of $l \in (|\pi_{j+1}| : |\pi_{i+1}|)$ such that $\Gamma^A_{\mathsf{latest}(i,l)} \neq \tilde{\Gamma}^B_{\mathsf{latest}(i,l)}$ or there are at least $\frac{|\pi_{i+1}|-|\pi_{j+1}|}{4}$ values of $l \in (|\pi_{j+1}| : |\pi_{i+1}|)$ such that $\mathsf{TC}(\pi^A_{i+1}(|\pi_{\textsc{Prev}(i)+1}| : l]) = \mathsf{TC}(\pi^B_{i+1}(|\pi_{\textsc{Prev}(i)+1}| : l])$.

In the former case, we have at least $\frac{|\pi_{i+1}|-|\pi_{j+1}|}{4}$ values of l such that $2 \cdot \mathsf{corr}_{\mathsf{latest}(i,l)} \geq \ell^*_{\mathsf{latest}(i,l)}$. As $\textsc{Prev}(i) \in \textsc{Starts}$ and $\mathsf{latest}(i,l) \in \textsc{Range}(\textsc{Prev}(i))$ by Claim 6.38, we have by item 3 of Fact 6.5 that $|\mathscr{R}_{\mathsf{latest}(i,l)}| \geq |\mathscr{R}_{\textsc{Prev}(i)+1}| = |\mathscr{R}_i| = |\mathscr{R}_{i+1}| - 1$. Using the definition of ℓ^*, this means that $2.2 \cdot \mathsf{corr}_{\mathsf{latest}(i,l)} \geq 1.1\ell^*_{\mathsf{latest}(i,l)} \geq \ell^*_{i+1}$ for at least $\frac{|\pi_{i+1}|-|\pi_{j+1}|}{4}$ values of $l \in (|\pi_{j+1}| : |\pi_{i+1}|)$ implying

$$5000 \cdot \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} \geq 500 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|)\,,$$

and Equation 31 follows.

In the latter case, recall the definition of $\overline{\mathsf{TC}}$ from Definition 3.6 and define $\tau^C = \overline{\mathsf{TC}}\left(\pi^C_{i+1,>|\pi_{\textsc{Prev}(i)+1}|}\right)$. Note that $|\tau^A| = |\tau^B| = |\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|$. We have from Definition 3.6 that

$$\Delta(\tau^A, \tau^B) \geq \left(1 - 10^{-5}\right) \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}| - |\mathsf{LCP}(\pi^A_{i+1,>|\pi_{\textsc{Prev}(i)+1}|}, \pi^B_{i+1,>|\pi_{\textsc{Prev}(i)+1}|})|\right).$$

Define $z = |\mathsf{LCP}(\pi^A_{i+1,>|\pi_{\textsc{Prev}(i)+1}|}, \pi^B_{i+1,>|\pi_{\textsc{Prev}(i)+1}|})|$. As the function $\overline{\mathsf{TC}}(\cdot)$ is online, we have

$$\Delta(\tau^A, \tau^B) \geq \left(1 - 10^{-5}\right) \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}| - z\right)$$
$$\implies \Delta(\tau^A_{>z}, \tau^B_{>z}) \geq \left(1 - 10^{-5}\right) \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}| - z\right).$$

Using the definition of $\Delta(\cdot)$, we get :

$$\sum_{z'=z+1}^{|\pi_{i+1}|-|\pi_{\textsc{Prev}(i)+1}|} \mathbb{1}\left(\tau^A[z'] \neq \tau^B[z']\right) \geq \left(1 - 10^{-5}\right) \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}| - z\right)$$
$$\implies \sum_{z'=z+1}^{|\pi_{i+1}|-|\pi_{\textsc{Prev}(i)+1}|} \mathbb{1}\left(\tau^A[z'] = \tau^B[z']\right) \leq 10^{-5} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}| - z\right)$$

$$\implies \sum_{z'=z+1}^{|\pi_{i+1}|-|\pi_{\text{PREV}(i)+1}|} \mathbb{1}\left(\tau^A[z'] = \tau^B[z']\right) \leq 10^{-5} \cdot \left(|\pi_{i+1}| - |\pi_{\text{PREV}(i)+1}|\right).$$

Recall that $\pi^A_{i+1}[|\pi_j|] \neq \pi^B_{i+1}[|\pi_j|]$ and $|\pi_j| > |\pi_{\text{PREV}(i)+1}|$ (Claim 6.37). This means that $z \leq |\pi_{j+1}| - |\pi_{\text{PREV}(i)+1}|$ and we get

$$\sum_{z'=|\pi_{j+1}|-|\pi_{\text{PREV}(i)+1}|+1}^{|\pi_{i+1}|-|\pi_{\text{PREV}(i)+1}|} \mathbb{1}\left(\tau^A[z'] = \tau^B[z']\right) \leq 10^{-5} \cdot \left(|\pi_{i+1}| - |\pi_{\text{PREV}(i)+1}|\right)$$

$$\implies \sum_{z'=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathbb{1}\left(\mathsf{TC}\left(\pi^A_{i+1}(|\pi_{\text{PREV}(i)+1}| : z']\right) = \mathsf{TC}\left(\pi^B_{i+1}(|\pi_{\text{PREV}(i)+1}| : z']\right)\right)$$

$$\leq 10^{-5} \cdot \left(|\pi_{i+1}| - |\pi_{\text{PREV}(i)+1}|\right).$$

As there are at least $\frac{|\pi_{i+1}|-|\pi_{j+1}|}{4}$ values of $l \in (|\pi_{j+1}| : |\pi_{i+1}|)$ such that $\mathsf{TC}(\pi^A_{i+1}(|\pi_{\text{PREV}(i)+1}| : l]) = \mathsf{TC}(\pi^B_{i+1}(|\pi_{\text{PREV}(i)+1}| : l])$, we conclude that

$$\frac{|\pi_{i+1}| - |\pi_{j+1}|}{4} \leq 10^{-5} \cdot \left(|\pi_{i+1}| - |\pi_{\text{PREV}(i)+1}|\right).$$

This means that

$$\frac{\ell^*_{i+1}}{30} \cdot \left(|\pi_{i+1}| - |\pi_{\text{PREV}(i)+1}|\right) \geq 500 \cdot \left(|\pi_{i+1}| - |\pi_{j+1}|\right) \cdot \ell^*_{i+1},$$

and Equation 31 follows.

□

Lemma 6.39. *Consider $i \in \text{STARTS}_\text{B}$ and $j' < j \in \{i\} \cup \text{RANGE}(i) \setminus \{num\}$ such that $|\mathscr{R}_{j''}| = |\mathscr{R}_{i+1}|$ for all $j'' \in (j' : j]$. We have:*

$$\mathsf{E}^\text{B}_i(j') + \sum_{i'=j'+1}^{j} \mathsf{corr}_{i'} \leq \mathsf{E}^\text{B}_i(j') + \sum_{i'=j'+1}^{j} \mathsf{corr}_{i'} + \sum_{l=|\pi_{j+1}|+1}^{|\pi_{j'+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} \leq \mathsf{E}^\text{B}_i(j).$$

Proof. We have:

$$\mathsf{E}^\text{B}_i(j) - \mathsf{E}^\text{B}_i(j') \geq \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} + \sum_{i'=i+1}^{j} \mathsf{corr}_{i'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{i'}| \text{ is odd}\right))$$

$$- \sum_{l=|\pi_{j'+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} - \sum_{i'=i+1}^{j'} \mathsf{corr}_{i'} \cdot (1 + \mathbb{1}\left(|\mathscr{R}_{i'}| \text{ is odd}\right)).$$

As $|\mathscr{R}_{j''}|$ is even for all $j'' \in (j' : j]$, we have by item 5 of Fact 6.5 that $|\pi_{j+1}| \leq |\pi_{j'+1}|$

implying:

$$\begin{aligned}\mathsf{E}^{\mathrm{B}}_i(j) - \mathsf{E}^{\mathrm{B}}_i(j') &\geq \sum_{l=|\pi_{j+1}|+1}^{|\pi_{j'+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} + \sum_{i'=j'+1}^{j} \mathsf{corr}_{i'} \cdot \left(1 + \mathbb{1}\left(|\mathscr{R}_{i'}| \text{ is odd}\right)\right) \\ &\geq \sum_{l=|\pi_{j+1}|+1}^{|\pi_{j'+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} + \sum_{i'=j'+1}^{j} \mathsf{corr}_{i'}.\end{aligned}$$

□

6.2.6 Lemmas Concerning $\mathsf{F}(\cdot)$

Lemma 6.40. *Consider $1 \leq j < num$ such that $|\mathscr{R}_j|$ is even. We have $100 \leq \mathsf{F}(j) \leq 100 + 0.2 \cdot \left(|\psi_j| + 1 - |\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)|\right)$.*

Proof. The first inequality follows using a simple application of Definition 3.6. For the second one, note that the function $\overline{\mathsf{TC}}$ is online and therefore:

$$\begin{aligned}\mathsf{F}(j) &= \frac{20}{1-10^{-5}} \cdot \Delta\left(\overline{\mathsf{TC}}(\psi^A_j \| \sigma^A_j), \overline{\mathsf{TC}}(\psi^B_j \| \sigma^B_j)\right) + 20 \cdot \left(|\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)| - |\psi_j|\right) + 80 \\ &\leq 100 + \frac{20}{1-10^{-5}} \cdot \left(|\psi_j| + 1 - |\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)|\right) \\ &\qquad + 20 \cdot \left(|\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)| - |\psi_j| - 1\right) \\ &\leq 100 + 0.2 \cdot \left(|\psi_j| + 1 - |\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)|\right).\end{aligned}$$

□

6.2.7 Lemmas Concerning $\mathsf{tax}_0(\cdot)$ and $\mathsf{tax}_1(\cdot)$

Lemma 6.41. *Let $i \in \textsc{Starts}_{\mathrm{B}}$ and $j, j' \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ be such that $|\pi_{j+1}| \leq |\pi_{j'+1}| \leq |\pi_{i+1}|$. It holds that*

$$\mathsf{tax}_{1,i}(j) - \mathsf{tax}_{1,i}(j') \leq 100 \cdot \left(|\pi_{j'+1}| - |\pi_{j+1}|\right).$$

Proof. We first claim that:

$$\begin{aligned}&|\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|])| \\ &\qquad - |\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j'+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j'+1}| : |\pi_{i+1}|])| \leq |\pi_{j'+1}| - |\pi_{j+1}|.\end{aligned} \tag{33}$$

Indeed, either $|\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|])| \leq |\pi_{j'+1}| - |\pi_{j+1}|$ in which case there is nothing to show or $|\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|])| > |\pi_{j'+1}| - |\pi_{j+1}|$, in which case Equation 33 follows by the definition of $\mathsf{LCP}(\cdot)$.

We now show the lemma. If $\mathsf{tax}_{1,i}(j) = 0$, there is nothing to show. So we assume that $\mathsf{tax}_{1,i}(j) > 0$ and derive

$\mathsf{tax}_{1,i}(j) - \mathsf{tax}_{1,i}(j')$

$$
\begin{aligned}
&\leq 900 \cdot |\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|])| - 800 \cdot (|\pi_{i+1}| - |\pi_{j+1}|) \\
&\qquad - 900 \cdot |\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j'+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j'+1}| : |\pi_{i+1}|])| + 800 \cdot (|\pi_{i+1}| - |\pi_{j'+1}|) \\
&\leq 900 \cdot |\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|])| \\
&\qquad - 900 \cdot |\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j'+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j'+1}| : |\pi_{i+1}|])| + 800 \cdot (|\pi_{j+1}| - |\pi_{j'+1}|) \\
&\leq 900 \cdot (|\pi_{j'+1}| - |\pi_{j+1}|) + 800 \cdot (|\pi_{j+1}| - |\pi_{j'+1}|) && \text{(Equation 33)} \\
&\leq 100 \cdot (|\pi_{j'+1}| - |\pi_{j+1}|)\,.
\end{aligned}
$$

□

Lemma 6.42. *For all $0 \leq \eta' \leq \eta$ and all $1 \leq j < num$, it holds that $\mathsf{tax}_0(\eta', j) \leq \mathsf{tax}_0(\eta, j)$. Moreover, if $|\mathscr{R}_j|$ is even and $\mathsf{turn}(j) = 1$, then $\mathsf{tax}_0(\eta, j) \geq \min(3, \eta/2) \cdot (|\psi_j| + 1)$.*

Proof. If $|\mathscr{R}_j|$ is odd, there is nothing to show so we assume that $|\mathscr{R}_j|$ is even. To show the lemma (including the "moreover" part), observe that it is sufficient to show that all terms multiplied to η in Algorithm 7 are non-negative. We do this term by term. The terms $|\psi_j|+1$ and $\frac{1}{10} \cdot \mathsf{F}(j) + |\psi_j| + 1$ are clearly non-negative due to Lemma 6.40.

Next, we show that the term $2 \cdot (\mathscr{R}_{j+1}.last.r - \mathscr{R}_{j+1}.last.t) - |\psi_j| - 1$ is non-negative assuming $\mathscr{R}_{j+1}.last.t > 0$. As $\mathscr{R}_{j+1}.last.t > 0$ and $|\mathscr{R}_j|$ is even, we must have that $|\mathscr{R}_{j+1}|$ is even. If $\mathscr{R}_j.last.t > 0$, we have by item 9 and item 11 of Fact 6.5 that

$$2 \cdot (\mathscr{R}_{j+1}.last.r - \mathscr{R}_{j+1}.last.t) - |\psi_j| - 1 = 2 \cdot (\mathscr{R}_j.last.r - \mathscr{R}_j.last.t) - |\psi_j| - 1 \geq 0.$$

On the other hand, if $\mathscr{R}_j.last.t = 0$, we must have $j \in \mathfrak{E}(90)$ implying that

$$2 \cdot (\mathscr{R}_{j+1}.last.r - \mathscr{R}_{j+1}.last.t) - |\psi_j| - 1 = |\psi_j| + 1 \geq 0.$$

Finally, we show that $\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) - |\pi_{j+1}| \geq 0$ assuming $\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) > 0$. If $|\pi_{j+1}| = 0$, then there is nothing to show, so we assume that $|\pi_{j+1}| > 0 \implies j \notin \mathfrak{E}(84)$. Either $j \in \mathfrak{E}(80)$, in which case we get:

$$
\begin{aligned}
\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) - |\pi_{j+1}| &= \mathscr{R}_j.last.t - |\pi_{j+1}| \\
&= |\psi_j| + 1 + \mathscr{R}_j.last.t - \mathscr{R}_j.last.r \\
&\qquad \text{(Fact 6.5, item 5 and item 10)} \\
&= \frac{1}{2} \cdot (|\psi_j| + 1) \qquad \text{(As } j \in \mathfrak{E}(80)\text{)} \\
&\geq 0,
\end{aligned}
$$

or $j \in \mathfrak{E}(87)$ implying that $|\mathscr{R}_{j+1}|$ is even and $\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) = \mathscr{R}_{j+1}.last.t$. Due to our assumption that $\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) > 0$, we get:

$$
\begin{aligned}
\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) - |\pi_{j+1}| &= \mathscr{R}_{j+1}.last.t - |\pi_{j+1}| \\
&\geq \mathscr{R}_{j+1}.last.r - |\psi_j| - 1 - |\pi_{j+1}| \quad \text{(Fact 6.5, item 11)} \\
&= \mathscr{R}_{j+1}.last.r - |\psi_j| - |\pi_j| \qquad \text{(Fact 6.5, item 5)}
\end{aligned}
$$

$$
\begin{aligned}
&= \mathscr{R}_j.last.r - |\psi_j| - |\pi_j| && \text{(Fact 6.5, item 9)}\\
&= 0. && \text{(Fact 6.5, item 10)}
\end{aligned}
$$

□

Corollary 6.43. *For all $\eta \geq 0$ and all $1 \leq j < num$, it holds that $0 \leq \mathsf{tax}_0(\eta, j)$.*

Proof. Apply the foregoing lemma on 0 and η noting that $\mathsf{tax}_0(0, j) \geq 0$. □

Lemma 6.44. *Consider $\eta \geq 0$ and $1 \leq j < num$ such that $j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)$. We have $\mathsf{tax}_0(\eta, j) \geq \min(3, \eta/2) \cdot (|\psi_j| + 1)$.*

Proof. We consider the definition of $\mathsf{tax}_0(\eta, j)$. Note that as $j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)$, we have that $|\mathscr{R}_j|$ is even. If $\pi_j^A \| \psi_j^A = \pi_j^B \| \psi_j^B$, then the lemma clearly holds. Additionally, if $\mathsf{turn}(j) = 1$, then the lemma holds due to Lemma 6.42. Therefore, for the rest of the proof, we can assume that

$$
\pi_j^A \| \psi_j^A \neq \pi_j^B \| \psi_j^B \qquad \text{and} \qquad \mathsf{turn}(j) = 0 \implies \psi_j^A \| \sigma_j^A = \psi_j^B \| \sigma_j^B.
$$

Under these assumptions, we claim that $j \in \mathfrak{E}(84)$ is not possible. Indeed, if $j \in \mathfrak{E}(84)$, then $|\pi_j| = 1 \implies \pi_j^C = \sigma_j^C$ for $C \in \{A, B\}$ contradicting the foregoing equation. Thus, we get that $j \in \mathfrak{E}(80)$ which means that $\mathscr{R}_j.last.t > 0$ by item 11 of Fact 6.5. Combining with the foregoing equation, we get

$$
\begin{aligned}
\mathsf{tax}_0(\eta, j) &\geq \eta \cdot (\mathscr{R}_j.last.t - |\pi_{j+1}|)\\
&\geq \eta \cdot (\mathscr{R}_j.last.t - \mathscr{R}_j.last.r + |\psi_j| + 1) && \text{(Fact 6.5, item 5 and item 10)}\\
&\geq \frac{\eta}{2} \cdot (|\psi_j| + 1)\,. && \text{(As } j \in \mathfrak{E}(80)\text{)}
\end{aligned}
$$

□

Lemma 6.45. *Consider $1 \leq j' \leq j < num$ such that $|\mathscr{R}_{j''}| = |\mathscr{R}_j|$ is even for all $j'' \in (j' : j]$ and $\mathsf{turn}(j'') = \mathsf{turn}(j)$ for all $j'' \in [j' : j]$. For all $0 \leq z < 1$ and all $\eta \geq \frac{3}{1-z}$, we have*

$$
5\eta \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} \geq z\eta\ell_j^* \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0) + \ell_j^* \left(\mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j')\right).
$$

Proof. Proof by induction on j. If $j = j'$, then there is nothing to show. We show the result for $j > j'$ by assuming it for $j - 1$. From our induction hypothesis, we have:

$$
\begin{aligned}
5\eta \cdot \sum_{j''=j'+1}^{j-1} \mathsf{corr}_{j''} &\geq z\eta\ell_{j-1}^* \cdot \sum_{j''=j'+1}^{j-1} \mathbb{1}(\mathsf{turn}(j-1) = 1 \vee \mathscr{R}_{j''}.last.t > 0)\\
&\quad + \ell_{j-1}^* \left(\mathsf{tax}_0(\eta, j-1) - \mathsf{tax}_0(\eta, j')\right)\\
&\geq z\eta\ell_{j-1}^* \cdot \sum_{j''=j'+1}^{j-1} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0)
\end{aligned}
$$

$$
\begin{aligned}
&\quad + \ell^*_{j-1}\left(\mathsf{tax}_0(\eta, j-1) - \mathsf{tax}_0(\eta, j')\right) \qquad (\text{As } \mathsf{turn}(j-1) = \mathsf{turn}(j)) \\
&\geq z\eta\ell^*_j \cdot \sum_{j''=j'+1}^{j-1} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0) \\
&\quad + \ell^*_j\left(\mathsf{tax}_0(\eta, j-1) - \mathsf{tax}_0(\eta, j')\right),
\end{aligned}
$$

as either $j-1 = j'$ in which case, the right hand sides are $= 0$ or $\ell^*_{j-1} = \ell^*_j$ under the assumption of the lemma. Owing to this, it is sufficient to show that:

$$
5\eta \cdot \mathsf{corr}_j \geq z\eta\ell^*_j \cdot \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_j.last.t > 0) + \ell^*_j\left(\mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1)\right). \tag{34}
$$

To show this, assume first that $\pi^A_j \| \psi^A_j = \pi^B_j \| \psi^B_j$. Under this assumption, we claim that $\mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1) = \eta$. Indeed, either $j-1 \in \textsc{Starts}$ in which case the fact that $|\mathscr{R}_j|$ is even means that $j-1 \in \textsc{Starts}_{\mathrm{B}} \implies |\mathscr{R}_{j-1}|$ is odd and we have

$$
\begin{aligned}
\mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1) &= \eta \cdot (|\psi_j| + 1) - 0 && (\text{As } |\mathscr{R}_{j-1}| \text{ is odd}) \\
&= \eta, && (\text{As } j-1 \in \textsc{Starts}_{\mathrm{B}})
\end{aligned}
$$

or $j-1 \notin \textsc{Starts}$ in which case, by item 5 of Fact 6.5, we get that $\pi^A_{j-1} \| \psi^A_{j-1} = \pi^B_{j-1} \| \psi^B_{j-1}$ and Algorithm 7 shows $\mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1) = \eta$. Consequently, we have

$$
z\eta\ell^*_j \cdot \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_j.last.t > 0) + \ell^*_j\left(\mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1)\right) \leq \eta\ell^*_j + \eta\ell^*_j \leq 2\eta \cdot \ell^*_j.
$$

This means that it is sufficient to show that $\ell^*_j \leq 2 \cdot \mathsf{corr}_j$. As Theorem 6.2 promises that $j \in \mathfrak{E}(52)$, it is enough to show that $\mathscr{R}^A_j.last.\alpha \neq \mathscr{R}^B_j.last.\alpha$. To this end, define $j_1 \leq j$ be the largest such that $|\mathscr{R}_{j_1}|$ is odd. This is well defined as $j_1 = 1$ is one such value. As $|\mathscr{R}_j|$ is even, we have by our choice of j_1 that $j_1 + 1 \leq j$ and $|\mathscr{R}_{j''}|$ is even for all $j'' \in (j_1 : j]$. It follows that $j_1 \in \mathfrak{E}(70)$ and (using item 9 of Fact 6.5) that, in order to show $\mathscr{R}^A_j.last.\alpha \neq \mathscr{R}^B_j.last.\alpha$, it is sufficient to show $\mathscr{R}^A_{j_1+1}.last.\alpha \neq \mathscr{R}^B_{j_1+1}.last.\alpha$.

We now focus on showing $\mathscr{R}^A_{j_1+1}.last.\alpha \neq \mathscr{R}^B_{j_1+1}.last.\alpha$. Suppose not, then we have using $j_1 \in \mathfrak{E}(70)$ that $(\mathscr{R}_{\mathrm{F},j_1}[h^A_{j_1}].r, \Gamma^A_{j_1,h^A_{j_1}}, \tilde{\Gamma}^A_{j_1,h^A_{j_1}}) = (\mathscr{R}_{\mathrm{F},j_1}[h^B_{j_1}].r, \tilde{\Gamma}^B_{j_1,h^B_{j_1}}, \Gamma^B_{j_1,h^B_{j_1}})$ and $\Gamma^A_{j_1,h^A_{j_1}} \neq \tilde{\Gamma}^A_{j_1,h^A_{j_1}}$. Using h^* to denote the common value of $\mathscr{R}_{\mathrm{F},j_1}[h^A_{j_1}].r$ and $\mathscr{R}_{\mathrm{F},j_1}[h^B_{j_1}].r$ and using the definition of Γ, we get,

$$
\begin{aligned}
&(\mathscr{R}_{\mathrm{F},j_1}[h^A_{j_1}].r, \Gamma^A_{j_1,h^A_{j_1}}, \tilde{\Gamma}^A_{j_1,h^A_{j_1}}) = (\mathscr{R}_{\mathrm{F},j_1}[h^B_{j_1}].r, \tilde{\Gamma}^B_{j_1,h^B_{j_1}}, \Gamma^B_{j_1,h^B_{j_1}}) \\
&\quad \implies \Gamma^A_{j_1,h^A_{j_1}} \neq \Gamma^B_{j_1,h^B_{j_1}} && (\text{As } \Gamma^A_{j_1,h^A_{j_1}} \neq \tilde{\Gamma}^A_{j_1,h^A_{j_1}}) \\
&\quad \implies \mathsf{TC}(\pi^A_{j_1+1,>h^*}) \neq \mathsf{TC}(\pi^B_{j_1+1,>h^*}) && (\text{As } j_1 \in \mathfrak{E}(70)) \\
&\quad \implies \pi^A_{j_1+1} \neq \pi^B_{j_1+1}.
\end{aligned}
$$

However, due to item 5 of Fact 6.5 (we have $(j_1 : j) \notin \textsc{Starts}$ as $|\mathscr{R}_{j''}|$ is even for all $j'' \in (j_1 : j]$), this means that $\pi^A_j \| \psi^A_j \neq \pi^B_j \| \psi^B_j$, a contradiction to our assumption. For the rest of the proof, we assume that $\pi^A_j \| \psi^A_j \neq \pi^B_j \| \psi^B_j$. We consider various cases and show

Equation 34 in each case.

- **When $\mathsf{turn}(j) = 1$:** As we assume that $\mathsf{turn}(j'') = \mathsf{turn}(j)$ for all $j'' \in [j' : j]$, we have that $\mathsf{turn}(j-1) = 1$ as well. In particular, this means that $|\mathscr{R}_{j-1}|$ is even. As $|\mathscr{R}_j|$ is also even, we have $j - 1 \notin \textsc{Starts}$ and using item 5 of Fact 6.5, we get that $\pi^A_{j-1} \| \psi^A_{j-1} \neq \pi^B_{j-1} \| \psi^B_{j-1}$. We have two subcases:

  - **When $\mathscr{R}_j.last.t = 0$:** As $j - 1 \notin \textsc{Starts}$, we have $j - 1 \notin \mathfrak{E}(80) \cup \mathfrak{E}(84)$ which, combined with $\pi^A_{j-1} \| \psi^A_{j-1} \neq \pi^B_{j-1} \| \psi^B_{j-1}$ gives:

$$\mathsf{tax}_0(\eta, j-1) = 3 \cdot (|\psi_{j-1}| + 1) + \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j-1) + |\psi_{j-1}| + 1 \right). \tag{35}$$

    We claim that:

    Claim 6.46. $\mathsf{tax}_0(\eta, j) \leq 3 \cdot (|\psi_j| + 1) + \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j) + |\psi_j| + 1 \right) - 10\eta \cdot \mathbb{1}\left(\mathscr{R}_{j+1}.last.t > 0 \vee j \in \mathfrak{E}(80) \cup \mathfrak{E}(84) \right)$.

    Proof. If $\mathscr{R}_{j+1}.last.t > 0$, then we have

$$\begin{aligned}
\mathsf{tax}_0(\eta, j) &= 3 \cdot (|\psi_j| + 1) + \eta \cdot (2 \cdot (\mathscr{R}_{j+1}.last.r - \mathscr{R}_{j+1}.last.t) - |\psi_j| - 1) \\
&\leq 3 \cdot (|\psi_j| + 1) + \eta \cdot (|\psi_j| + 1) && \text{(Fact 6.5, item 11)} \\
&\leq 3 \cdot (|\psi_j| + 1) + \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j) + |\psi_j| + 1 \right) - 10\eta. && \text{(Lemma 6.40)}
\end{aligned}$$

    If $\mathscr{R}_{j+1}.last.t = 0$ and $j \notin \mathfrak{E}(80) \cup \mathfrak{E}(84)$, then we have

$$\mathsf{tax}_0(\eta, j) = 3 \cdot (|\psi_j| + 1) + \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j) + |\psi_j| + 1 \right).$$

    Finally, if $\mathscr{R}_{j+1}.last.t = 0$ and $j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)$, then we have

$$\begin{aligned}
\mathsf{tax}_0(\eta, j) &= 3 \cdot (|\psi_j| + 1) \\
&\leq 3 \cdot (|\psi_j| + 1) + \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j) + |\psi_j| + 1 \right) - 10\eta. && \text{(Lemma 6.40)}
\end{aligned}$$

    □

    Claim 6.47. $\mathsf{F}(j) - \mathsf{F}(j-1) = \frac{20}{1-10^{-5}} \cdot \mathbb{1}\left(\mathsf{TC}(\psi^A_j \| \sigma^A_j) \neq \mathsf{TC}(\psi^B_j \| \sigma^B_j) \right) - 20$.

    Proof. As $|\mathscr{R}_{j-1}|$ and $|\mathscr{R}_j|$ are both even, we have by definition that:

$$\begin{aligned}
&\mathsf{F}(j) - \mathsf{F}(j-1) \\
&\quad = \frac{20}{1 - 10^{-5}} \cdot \Delta\left(\overline{\mathsf{TC}}(\psi^A_j \| \sigma^A_j), \overline{\mathsf{TC}}(\psi^B_j \| \sigma^B_j) \right) \\
&\qquad + 20 \cdot \left(|\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)| - |\psi_j| \right) \\
&\qquad - \frac{20}{1 - 10^{-5}} \cdot \Delta\left(\overline{\mathsf{TC}}(\psi^A_{j-1} \| \sigma^A_{j-1}), \overline{\mathsf{TC}}(\psi^B_{j-1} \| \sigma^B_{j-1}) \right)
\end{aligned}$$

$$
\begin{aligned}
&\quad - 20 \cdot \left(|\mathsf{LCP}(\psi^A_{j-1}\|\sigma^A_{j-1}, \psi^B_{j-1}\|\sigma^B_{j-1})| - |\psi_{j-1}|\right) \\
&= \frac{20}{1-10^{-5}} \cdot \mathbb{1}\left(\mathsf{TC}(\psi^A_j\|\sigma^A_j) \neq \mathsf{TC}(\psi^B_j\|\sigma^B_j)\right) - 20 \\
&\quad + 20 \cdot |\mathsf{LCP}(\psi^A_j\|\sigma^A_j, \psi^B_j\|\sigma^B_j)| - 20 \cdot |\mathsf{LCP}(\psi^A_{j-1}\|\sigma^A_{j-1}, \psi^B_{j-1}\|\sigma^B_{j-1})| \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Fact 6.5, item 5)} \\
&= \frac{20}{1-10^{-5}} \cdot \mathbb{1}\left(\mathsf{TC}(\psi^A_j\|\sigma^A_j) \neq \mathsf{TC}(\psi^B_j\|\sigma^B_j)\right) - 20. \qquad \text{(As } \mathsf{turn}(j) = 1\text{)}
\end{aligned}
$$

□

Using Equation 35 and Claim 6.46, we have

$$
\begin{aligned}
&z\eta \cdot \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_j.last.t > 0) + \mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1) \\
&\quad \leq z\eta - 3 \cdot (|\psi_{j-1}| + 1) - \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j-1) + |\psi_{j-1}| + 1\right) \\
&\qquad + 3 \cdot (|\psi_j| + 1) + \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j) + |\psi_j| + 1\right) \\
&\qquad - 10\eta \cdot \mathbb{1}(\mathscr{R}_{j+1}.last.t > 0 \vee j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)) \\
&\quad \leq 3 + \eta + z\eta - \frac{\eta}{10} \cdot (\mathsf{F}(j) - \mathsf{F}(j-1)) \\
&\qquad - 10\eta \cdot \mathbb{1}(\mathscr{R}_{j+1}.last.t > 0 \vee j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)) \qquad \text{(Fact 6.5, item 5)} \\
&\quad \leq 2\eta + \frac{\eta}{10}(\mathsf{F}(j) - \mathsf{F}(j-1)) - 10\eta \cdot \mathbb{1}(\mathscr{R}_{j+1}.last.t > 0 \vee j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(As } \eta \geq \tfrac{3}{1-z}\text{)} \\
&\quad \leq 2\eta + \frac{\eta}{10} \cdot \left(25 \cdot \mathbb{1}\left(\mathsf{TC}(\psi^A_j\|\sigma^A_j) \neq \mathsf{TC}(\psi^B_j\|\sigma^B_j)\right) - 20\right) \\
&\qquad - 10\eta \cdot \mathbb{1}(\mathscr{R}_{j+1}.last.t > 0 \vee j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)) \qquad \text{(Claim 6.47)} \\
&\quad \leq 2.5\eta \cdot \mathbb{1}\left(\mathsf{TC}(\psi^A_j\|\sigma^A_j) \neq \mathsf{TC}(\psi^B_j\|\sigma^B_j)\right) \\
&\qquad - 10\eta \cdot \mathbb{1}(\mathscr{R}_{j+1}.last.t > 0 \vee j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)) \\
&\quad \leq 2.5\eta \cdot \mathbb{1}\left(\Gamma^A_j \neq \Gamma^B_j\right) - 10\eta \cdot \mathbb{1}(\mathscr{R}_{j+1}.last.t > 0 \vee j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)). \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(As } |\mathscr{R}_j| \text{ is even)}
\end{aligned}
$$

Now, if $\mathscr{R}_{j+1}.last.t > 0$ or $j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)$ then $z\eta \cdot \mathbb{1}(\mathsf{turn}(j) \vee \mathscr{R}_j.last.t > 0) + \mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1) \leq 0$ and Equation 34 follows. Similarly, if $\Gamma^A_j = \Gamma^B_j$, then Equation 34 follows. It remains to argue the case, when neither of these hold.

In this case, as $j \notin \mathfrak{E}(80) \cup \mathfrak{E}(84)$, we must have $j \in \mathfrak{E}(87)$. Furthermore, as we have $\mathscr{R}_j.last.t = 0$ and $\mathscr{R}_{j+1}.last.t = 0$, we must have $j \notin \mathfrak{E}(90)$ implying that $\Gamma^A_j = \tilde{\Gamma}^A_j$. However, as we have $\Gamma^A_j \neq \Gamma^B_j$, this gives $\Gamma^B_j \neq \tilde{\Gamma}^A_j$ implying that $\ell^*_j \leq 2 \cdot \mathsf{corr}_j$ and we can continue as:

$$
z\eta \cdot \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_j.last.t > 0) + \mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1) \leq 2.5\eta \leq 5\eta \cdot \frac{\mathsf{corr}_j}{\ell^*_j},
$$

and Equation 34 follows.

  - **When $\mathscr{R}_j$.*last*.*t* > 0:** In this case, as we have $\mathsf{turn}(j-1) = 1$ and $\pi^A_{j-1} \| \psi^A_{j-1} \neq \pi^B_{j-1} \| \psi^B_{j-1}$, we get

$$\mathsf{tax}_0(\eta, j-1) = 3 \cdot (|\psi_{j-1}| + 1) + \eta \cdot (2 \cdot (\mathscr{R}_j.last.r - \mathscr{R}_j.last.t) - |\psi_{j-1}| - 1) \,. \quad (36)$$

    We claim that:

    Claim 6.48. *It holds that:*

$$\mathsf{tax}_0(\eta, j) \leq 3 \cdot (|\psi_j| + 1) + \eta \cdot (2 \cdot (\mathscr{R}_j.last.r - \mathscr{R}_j.last.t) - |\psi_j| - 1) \,.$$

    Proof. If $\mathscr{R}_{j+1}.last.t > 0$, then we must have $j \notin \mathfrak{E}(80) \cup \mathfrak{E}(84)$ implying that $|\mathscr{R}_{j+1}|$ is even and

$$\begin{aligned} \mathsf{tax}_0(\eta, j) &= 3 \cdot (|\psi_j| + 1) + \eta \cdot (2 \cdot (\mathscr{R}_{j+1}.last.r - \mathscr{R}_{j+1}.last.t) - |\psi_j| - 1) \\ &= 3 \cdot (|\psi_j| + 1) + \eta \cdot (2 \cdot (\mathscr{R}_j.last.r - \mathscr{R}_j.last.t) - |\psi_j| - 1) \,. \\ &\qquad\qquad\qquad\qquad \text{(Fact 6.5, item 9)} \end{aligned}$$

    Otherwise, if $\mathscr{R}_{j+1}.last.t = 0$, then we must have $|\mathscr{R}_{j+1}|$ is odd implying $j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)$ as otherwise, we have a contradiction to item 9 of Fact 6.5. We get:

$$\begin{aligned} \mathsf{tax}_0(\eta, j) &= 3 \cdot (|\psi_j| + 1) \\ &\leq 3 \cdot (|\psi_j| + 1) + \eta \cdot (2 \cdot (\mathscr{R}_j.last.r - \mathscr{R}_j.last.t) - |\psi_j| - 1) \,. \\ &\qquad\qquad\qquad\qquad \text{(Fact 6.5, item 11)} \end{aligned}$$

    □

    Using Equation 36 and Claim 6.48, we have

$$\begin{aligned} &z\eta \cdot \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_j.last.t > 0) + \mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1) \\ &\quad \leq z\eta - 3 \cdot (|\psi_{j-1}| + 1) - \eta \cdot (2 \cdot (\mathscr{R}_j.last.r - \mathscr{R}_j.last.t) - |\psi_{j-1}| - 1) \\ &\qquad + 3 \cdot (|\psi_j| + 1) + \eta \cdot (2 \cdot (\mathscr{R}_j.last.r - \mathscr{R}_j.last.t) - |\psi_j| - 1) \\ &\quad \leq 3 + z\eta - \eta \qquad \text{(Fact 6.5, item 5)} \\ &\quad \leq 0, \qquad \left(\text{As } \eta \geq \tfrac{3}{1-z}\right) \end{aligned}$$

    and Equation 34 follows.

- **When $\mathsf{turn}(j) = 0$:** As we assume that $\mathsf{turn}(j'') = \mathsf{turn}(j)$ for all $j'' \in [j' : j]$, we have that $\mathsf{turn}(j-1) = 0$ as well. We have two subcases:

  - **When $\mathscr{R}_j$.*last*.*t* $= 0$:** In this case, we claim that $\mathsf{tax}_0(\eta, j-1) = 0$. Indeed, either $j - 1 \in \textsc{Starts}$ in which case the fact that $|\mathscr{R}_j|$ is even means that $j - 1 \in \textsc{Starts}_\text{B} \implies |\mathscr{R}_{j-1}|$ is odd and we have $\mathsf{tax}_0(\eta, j-1) = 0$, or $j - 1 \notin \textsc{Starts}$

in which case, we have that $|\mathscr{R}_{j-1}|$ is even and (by item 5 of Fact 6.5) that $\pi^A_{j-1}\|\psi^A_{j-1} \neq \pi^B_{j-1}\|\psi^B_{j-1}$. In this case, we must have $\mathscr{R}_{j-1}.last.t = 0$ as otherwise $\mathscr{R}_j.last.t = 0$ contradicts item 9 of Fact 6.5. However, if $\pi^A_{j-1}\|\psi^A_{j-1} \neq \pi^B_{j-1}\|\psi^B_{j-1}$ and $\mathsf{turn}(j-1) = 0$ and $\mathscr{R}_{j-1}.last.t = \mathscr{R}_j.last.t = 0$, we have $\mathsf{tax}_0(\eta, j-1) = 0$, as desired. We claim that:

Claim 6.49. $\mathsf{tax}_0(\eta, j) = 0$.

Proof. If $\mathscr{R}_{j+1}.last.t = 0$, then the claim is straightforward. Otherwise, the fact that $\mathscr{R}_j.last.t = 0$ and $\mathscr{R}_{j+1}.last.t > 0$ implies that $j \in \mathfrak{E}(90)$ implying that

$$\begin{aligned}\mathsf{tax}_0(\eta, j) &= \eta \cdot (\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) - |\pi_{j+1}|) \\ &= \eta \cdot (\mathscr{R}_{j+1}.last.t - |\pi_{j+1}|) && \text{(As } \mathscr{R}_j.last.t = 0\text{)} \\ &= 0. && \text{(As } j \in \mathfrak{E}(90) \text{ and Fact 6.5, item 10 and item 5)}\end{aligned}$$

□

Using Claim 6.49 and the fact that $\mathsf{tax}_0(\eta, j-1) = 0$, Equation 34 follows straightforwardly.

– **When $\mathscr{R}_j.last.t > 0$:** As $\mathscr{R}_j.last.t > 0$, we have $j - 1 \notin$ STARTS and therefore $|\mathscr{R}_{j-1}|$ is even. Using item 5 of Fact 6.5, this means that $\pi^A_{j-1}\|\psi^A_{j-1} \neq \pi^B_{j-1}\|\psi^B_{j-1}$. We claim that:

$$\mathscr{R}_j.last.t = \max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) = \max(\mathscr{R}_{j-1}.last.t, \mathscr{R}_j.last.t). \tag{37}$$

Indeed, if the first equality is not true, then we have $\mathscr{R}_{j+1}.last.t > \mathscr{R}_j.last.t > 0$ implying that $j \notin \mathfrak{E}(80) \cup \mathfrak{E}(84)$ which means that $|\mathscr{R}_{j+1}|$ is even. However, if $|\mathscr{R}_{j+1}|$ and $|\mathscr{R}_j|$ are both even, then $\mathscr{R}_{j+1}.last.t > \mathscr{R}_j.last.t > 0$ is a contradiction to item 9 of Fact 6.5.

Similarly, if the second equality is not true, then we have $\mathscr{R}_{j-1}.last.t > \mathscr{R}_j.last.t > 0$. As we have that $|\mathscr{R}_j|$ and $|\mathscr{R}_{j-1}|$ are both even, then $\mathscr{R}_{j-1}.last.t > \mathscr{R}_j.last.t > 0$ is a contradiction to item 9 of Fact 6.5.

Together with $\pi^A_j\|\psi^A_j \neq \pi^B_j\|\psi^B_j$ and $\pi^A_{j-1}\|\psi^A_{j-1} \neq \pi^B_{j-1}\|\psi^B_{j-1}$ and $\mathsf{turn}(j-1) = \mathsf{turn}(j) = 0$, Equation 37 allows us to conclude:

$$\begin{aligned}\mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1) &= \eta \cdot (\mathscr{R}_j.last.t - |\pi_{j+1}|) - \eta \cdot (\mathscr{R}_j.last.t - |\pi_j|) \\ &= \eta \cdot (|\pi_j| - |\pi_{j+1}|) \\ &= \eta. && \text{(Fact 6.5, item 5)}\end{aligned}$$

Thus, we have that:

$$z\eta\ell^*_j \cdot \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_j.last.t > 0) + \ell^*_j\left(\mathsf{tax}_0(\eta, j) - \mathsf{tax}_0(\eta, j-1)\right) \leq 2\eta\ell^*_j.$$

This means that, in order to show Equation 34, it is enough to show that

$\ell_j^* \leq 2 \cdot \mathsf{corr}_j$. As Theorem 6.2 promises that $j \in \mathfrak{E}(52)$, it is enough to show that $\mathscr{R}_j^A.last.\beta \neq \mathscr{R}_j^B.last.\beta$. To this end, define $j_1 \leq j$ be the largest such that $\mathscr{R}_{j_1}.last.t = 0$. This is well defined as $j_1 = 1$ is one such value. As $\mathscr{R}_j.last.t > 0$, we have by our choice of j_1 that $j_1 + 1 \leq j$ and $\mathscr{R}_{j''}.last.t > 0$ for all $j'' \in (j_1 : j]$. It follows that $j_1 \in \mathfrak{E}(90)$. We claim that:

Claim 6.50. *We have $|\mathscr{R}_{j''}|$ is even for all $j'' \in [j_1 : j]$.*

Proof. Suppose for the sake of contradiction that there exists $j_2 \in [j_1 : j]$ such that $|\mathscr{R}_{j_2}|$ is odd and let j_2 denote the smallest such value. As $|\mathscr{R}_{j_1}|$ is even, we must have that $|\mathscr{R}_{j_2-1}|$ is even implying that $j_2 - 1 \in [j_1 : j) \cap \textsc{Starts}$. However, this means that $\mathscr{R}_{j_2}.last.t = 0$, a contradiction to the fact that $\mathscr{R}_{j''}.last.t > 0$ for all $j'' \in (j_1 : j]$. □

Using Claim 6.50 and item 9 of Fact 6.5, in order to show $\mathscr{R}_j^A.last.\beta \neq \mathscr{R}_j^B.last.\beta$, it is sufficient to show $\mathscr{R}_{j_1+1}^A.last.\beta \neq \mathscr{R}_{j_1+1}^B.last.\beta$.

We now focus on showing $\mathscr{R}_{j_1+1}^A.last.\beta \neq \mathscr{R}_{j_1+1}^B.last.\beta$. Suppose not, then we have using $j_1 \in \mathfrak{E}(90)$ that $(\Gamma_{j_1}^A, \tilde{\Gamma}_{j_1}^A) = (\tilde{\Gamma}_{j_1}^B, \Gamma_{j_1}^B)$ and $\Gamma_{j_1}^A \neq \tilde{\Gamma}_{j_1}^A$. Using the definition of Γ, we get,

$$\begin{aligned}
(\Gamma_{j_1}^A, \tilde{\Gamma}_{j_1}^A) = (\tilde{\Gamma}_{j_1}^B, \Gamma_{j_1}^B) &\implies \Gamma_{j_1}^A \neq \Gamma_{j_1}^B && (\text{As } \Gamma_{j_1}^A \neq \tilde{\Gamma}_{j_1}^A) \\
&\implies \mathsf{TC}(\psi_{j_1}^A \| \sigma_{j_1}^A) \neq \mathsf{TC}(\psi_{j_1}^B \| \sigma_{j_1}^B) && (\text{As } j_1 \in \mathfrak{E}(90)) \\
&\implies \psi_{j_1}^A \| \sigma_{j_1}^A \neq \psi_{j_1}^B \| \sigma_{j_1}^B.
\end{aligned}$$

However, due to item 5 of Fact 6.5 (we have $[j_1 : j) \notin \textsc{Starts}$ due to Claim 6.50), this means that $\psi_j^A \| \sigma_j^A \neq \psi_j^B \| \sigma_j^B$, a contradiction to the fact that $\mathsf{turn}(j) = 0$.

□

Lemma 6.51. *Let $i \in \textsc{Starts}_{\mathrm{B}}$ and $j \in \textsc{Range}(i) \setminus \{num\}$ be good for i. For all $\eta > 0$, we have:*

$$\mathsf{tax}_0(\eta, j) \leq (1.02\eta + 3) \cdot (|\psi_j| + 1) + 10\eta \leq (2.04\eta + 6) \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + 10\eta.$$

Proof. We only show the first inequality as the second follows from Lemma 6.13. As we assume that $j \neq i$ is good for i, we have by the definition of good that $|\mathscr{R}_j|$ is even. We consider the definition of $\mathsf{tax}_0(\eta, j)$. If $\pi_j^A \| \psi_j^A = \pi_j^B \| \psi_j^B$, then we have $\mathsf{tax}_0(\eta, j) = \eta \cdot (|\psi_j| + 1)$ and there is nothing to show. Therefore, we assume henceforth that $\pi_j^A \| \psi_j^A \neq \pi_j^B \| \psi_j^B$.

If $\mathsf{turn}(j) = 1$ and $\mathscr{R}_{j+1}.last.t > 0$, then we have:

$$\begin{aligned}
\mathsf{tax}_0(\eta, j) &= 3 \cdot (|\psi_j| + 1) + \eta \cdot (2 \cdot (\mathscr{R}_{j+1}.last.r - \mathscr{R}_{j+1}.last.t) - |\psi_j| - 1) \\
&\leq (\eta + 3) \cdot (|\psi_j| + 1), && (\text{Fact 6.5, item 11})
\end{aligned}$$

and the lemma follows. If $\mathsf{turn}(j) = 1$, $\mathscr{R}_{j+1}.last.t = 0$, and $j \notin \mathfrak{E}(80) \cup \mathfrak{E}(84)$, then we have:

$$\begin{aligned}\mathsf{tax}_0(\eta, j) &= 3 \cdot (|\psi_j| + 1) + \eta \cdot \left(\frac{1}{10} \cdot \mathsf{F}(j) + |\psi_j| + 1\right) \\ &\leq 3 \cdot (|\psi_j| + 1) + \eta \cdot (10 + 1.02 \cdot (|\psi_j| + 1)) && \text{(Lemma 6.40)} \\ &\leq (1.02\eta + 3) \cdot (|\psi_j| + 1) + 10\eta,\end{aligned}$$

and the lemma follows. If $\mathsf{turn}(j) = 1$, $\mathscr{R}_{j+1}.last.t = 0$, and $j \in \mathfrak{E}(80) \cup \mathfrak{E}(84)$, then we have $\mathsf{tax}_0(\eta, j) = 3 \cdot (|\psi_j| + 1)$ and there is nothing to show. This completes the proof when $\mathsf{turn}(j) = 1$ and we assume henceforth that $\mathsf{turn}(j) = 0$. If $\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) = \mathscr{R}_j.last.t > 0$, then we have

$$\begin{aligned}\mathsf{tax}_0(\eta, j) &= \eta \cdot (\mathscr{R}_j.last.t - |\pi_{j+1}|) \\ &= \eta \cdot (\mathscr{R}_j.last.t - |\pi_j| + 1) && \text{(Fact 6.5, item 5)} \\ &= \eta \cdot (\mathscr{R}_j.last.t - \mathscr{R}_j.last.r + |\psi_j| + 1) && \text{(Fact 6.5, item 10)} \\ &\leq \frac{\eta}{2} \cdot (|\psi_j| + 1)\,, && \text{(Fact 6.5, item 11)}\end{aligned}$$

and the lemma follows. If $\mathscr{R}_{j+1}.last.t > \mathscr{R}_j.last.t$, then we must have $j \in \mathfrak{E}(90) \implies |\mathscr{R}_{j+1}|$ is even and we get

$$\begin{aligned}\mathsf{tax}_0(\eta, j) &= \eta \cdot (\mathscr{R}_{j+1}.last.t - |\pi_{j+1}|) \\ &= \eta \cdot (\mathscr{R}_{j+1}.last.r - |\psi_{j+1}| - |\pi_{j+1}|) && \text{(As } j \in \mathfrak{E}(90)\text{)} \\ &= 0, && \text{(Fact 6.5, item 10)}\end{aligned}$$

and the lemma follows. Finally, if $\max(\mathscr{R}_j.last.t, \mathscr{R}_{j+1}.last.t) = 0$, then $\mathsf{tax}_0(\eta, j) = 0$ and the lemma follows straightforwardly.

□

Lemma 6.52. *Consider $i \in \textsc{Starts}_{\mathrm{B}}$ and $j' < j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ such that $|\mathscr{R}_{j''}| = |\mathscr{R}_{i+1}|$ for all $j'' \in (j' : j]$. Suppose that $j \in \mathfrak{E}(80)$. The following hold:*

- *If $\mathscr{R}_{j'+1}.last.t > 0$, then, for all $\eta \geq 6$, we have*

$$15 \cdot \sum_{i'=j'+1}^{j} \mathsf{corr}_{i'} \geq 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - \ell^*_{i+1} \cdot \mathsf{tax}_0(\eta, j').$$

- *If $\mathsf{tax}_{1,i}(j) > 0$ and $\mathsf{turn}(j) = 1$ and $\mathsf{turn}(j') = 0$, we have*

$$60 \cdot \sum_{i'=j'+1}^{j} \mathsf{corr}_{i'} \geq 15 \cdot \ell^*_{i+1} + 2 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) + \ell^*_{i+1} \cdot (|\pi_{j'+1}| - |\pi_{j+1}|)\,.$$

Proof. We prove each part in turn:

- First, observe that due to Lemma 6.42, we can assume $\eta = 6$ without loss of generality. As $\mathscr{R}_{j'+1}.last.t > 0$ and $|\mathscr{R}_{j'+1}|$ is even, we have that $|\mathscr{R}_{j'}|$ is even as well. We consider the definition of $\mathsf{tax}_0(\cdot)$. If $\pi^A_{j'}\|\psi^A_{j'} = \pi^B_{j'}\|\psi^B_{j'}$, then the right hand side is at most 0 and the lemma clearly holds. Similarly, if $\mathsf{turn}(j) = 1$, then the lemma holds due to Lemma 6.42. Therefore, for the rest of the proof, we can assume that

$$\pi^A_{j'}\|\psi^A_{j'} \neq \pi^B_{j'}\|\psi^B_{j'} \qquad \text{and} \qquad \mathsf{turn}(j') = 0.$$

Under these assumptions and due to the fact that $\mathscr{R}_{j'+1}.last.t > 0$, we have

$$\begin{aligned}
\ell^*_{i+1} \cdot \mathsf{tax}_0(6, j') &\geq 6 \cdot \ell^*_{i+1} \cdot (\mathscr{R}_{j'+1}.last.t - |\pi_{j'+1}|) \\
&\geq 6 \cdot \ell^*_{i+1} \cdot (\mathscr{R}_{j'+1}.last.t - |\pi_{j+1}|) - 6 \cdot \ell^*_{i+1} \cdot (|\pi_{j'+1}| - |\pi_{j+1}|) \\
&\geq 6 \cdot \ell^*_{i+1} \cdot (\mathscr{R}_{j}.last.t - |\pi_{j+1}|) - 6 \cdot \ell^*_{i+1} \cdot (|\pi_{j'+1}| - |\pi_{j+1}|) \\
&\qquad \text{(Fact 6.5, item 9)} \\
&\geq 6 \cdot \ell^*_{i+1} \cdot (\mathscr{R}_{j}.last.t - |\pi_{j}| + 1) - 6 \cdot \ell^*_{i+1} \cdot (j - j') \\
&\qquad \text{(Fact 6.5, item 5 and } |\mathscr{R}_{j''}| \text{ is even for all } j'' \in (j' : j]) \\
&\geq 6 \cdot \ell^*_{i+1} \cdot (\mathscr{R}_{j}.last.t - \mathscr{R}_{j}.last.r + |\psi_j| + 1) - 6 \cdot \ell^*_{i+1} \cdot (j - j') \\
&\qquad \text{(Fact 6.5, item 10 and } |\mathscr{R}_j| \text{ is even)} \\
&\geq 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 6 \cdot \ell^*_{i+1} \cdot (j - j') \qquad \text{(As } j \in \mathfrak{E}(80)) \\
&\geq 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 6 \cdot \sum_{i'=j'+1}^{j} \ell^*_{i'}. \\
&\qquad \text{(As } |\mathscr{R}_{j''}| = |\mathscr{R}_{i+1}| \text{ for all } j'' \in (j' : j])
\end{aligned}$$

Thus, it is sufficient to show that $\ell^*_{i'} \leq 2 \cdot \mathsf{corr}_{i'}$ for all $i' \in (j' : j]$. As Theorem 6.2 promises that $i' \in \mathfrak{E}(52)$, it is enough to show that $\mathscr{R}^A_{i'}.last.\beta \neq \mathscr{R}^B_{i'}.last.\beta$. Next, using item 9 of Fact 6.5, it is enough to show that $\mathscr{R}^A_{j'+1}.last.\beta \neq \mathscr{R}^B_{j'+1}.last.\beta$. To this end, define $j_1 \leq j' + 1$ be the largest such that $\mathscr{R}_{j_1}.last.t = 0$. This is well defined as $j_1 = 1$ is one such value. As $\mathscr{R}_{j'+1}.last.t > 0$, we have by our choice of j_1 that $j_1 \leq j'$ and $\mathscr{R}_{j''}.last.t > 0$ for all $j'' \in (j_1 : j' + 1]$. It follows that $j_1 \in \mathfrak{E}(90)$. We claim that:

Claim 6.53. *We have $|\mathscr{R}_{j''}|$ is even for all $j'' \in [j_1 : j' + 1]$.*

Proof. Suppose for the sake of contradiction that there exists $j_2 \in [j_1 : j' + 1]$ such that $|\mathscr{R}_{j_2}|$ is odd and let j_2 denote the smallest such value. As $|\mathscr{R}_{j_1}|$ is even, we must have that $|\mathscr{R}_{j_2-1}|$ is even implying that $j_2 - 1 \in [j_1 : j' + 1) \cap \textsc{Starts}$. However, this means that $\mathscr{R}_{j_2}.last.t = 0$, a contradiction to the fact that $\mathscr{R}_{j''}.last.t > 0$ for all $j'' \in (j_1 : j' + 1]$. □

Using Claim 6.53 and item 9 of Fact 6.5, in order to show $\mathscr{R}^A_{j'+1}.last.\beta \neq \mathscr{R}^B_{j'+1}.last.\beta$, it is sufficient to show $\mathscr{R}^A_{j_1+1}.last.\beta \neq \mathscr{R}^B_{j_1+1}.last.\beta$.

We now focus on showing $\mathscr{R}^A_{j_1+1}.last.\beta \neq \mathscr{R}^B_{j_1+1}.last.\beta$. Suppose not, then we have using $j_1 \in \mathfrak{E}$(90) that $(\Gamma^A_{j_1}, \tilde{\Gamma}^A_{j_1}) = (\tilde{\Gamma}^B_{j_1}, \Gamma^B_{j_1})$ and $\Gamma^A_{j_1} \neq \tilde{\Gamma}^A_{j_1}$. Using the definition of Γ, we get,

$$\begin{aligned}(\Gamma^A_{j_1}, \tilde{\Gamma}^A_{j_1}) = (\tilde{\Gamma}^B_{j_1}, \Gamma^B_{j_1}) &\implies \Gamma^A_{j_1} \neq \Gamma^B_{j_1} && (\text{As } \Gamma^A_{j_1} \neq \tilde{\Gamma}^A_{j_1})\\ &\implies \mathsf{TC}(\psi^A_{j_1} \| \sigma^A_{j_1}) \neq \mathsf{TC}(\psi^B_{j_1} \| \sigma^B_{j_1}) && (\text{As } j_1 \in \mathfrak{E}(90))\\ &\implies \psi^A_{j_1} \| \sigma^A_{j_1} \neq \psi^B_{j_1} \| \sigma^B_{j_1}.\end{aligned}$$

However, due to item 5 of Fact 6.5 (we have $[j_1 : j'+1) \notin \textsc{Starts}$ due to Claim 6.53), this means that $\psi^A_{j'} \| \sigma^A_{j'} \neq \psi^B_{j'} \| \sigma^B_{j'}$, a contradiction to the fact that $\mathsf{turn}(j') = 0$.

- We start by showing the following helper claims.

Claim 6.54. *For all $j'' \in (j' : j]$, we have that $|\psi_j| - |\psi_{j''}| = j - j''$. Moreover, for all $C \in \{A, B\}$, we have $\psi^C_{j''} \| \sigma^C_{j''} = \left(\psi^C_j \| \sigma^C_j\right)[1 : |\psi_{j''}| + 1]$.*

Proof. Proof by backwards induction on j''. For the base case $j'' = j$, the claim is trivial. We show the statement holds for $j'' \in (j' : j)$ assuming it holds for $j'' + 1$. As $|\mathscr{R}_{j''}| = |\mathscr{R}_{j''+1}| = |\mathscr{R}_{i+1}|$ are both even, we have that $j'' \notin \textsc{Starts}$, implying by item 5 of Fact 6.5, that $|\psi_j| - |\psi_{j''}| = |\psi_j| - |\psi_{j''+1}| + 1 = j - j''$ and

$$\psi^C_{j''} \| \sigma^C_{j''} = \psi^C_{j''+1} = \left(\psi^C_j \| \sigma^C_j\right)[1 : |\psi_{j''+1}|] = \left(\psi^C_j \| \sigma^C_j\right)[1 : |\psi_{j''}| + 1],$$

by the induction hypothesis as desired. □

Claim 6.55. *For all $j'' \in [j' : j]$, we have that $|\pi_{j''+1}| - |\pi_{j+1}| = j - j''$.*

Proof. Proof by backwards induction on j''. For the base case $j'' = j$, the claim is trivial. We show the statement holds for $j'' \in [j' : j)$ assuming it holds for $j'' + 1$. As $|\mathscr{R}_{j''+1}| = |\mathscr{R}_{i+1}|$ is even, we have by item 5 of Fact 6.5 that $|\pi_{j''+1}| - |\pi_{j+1}| = |\pi_{j''+2}| - |\pi_{j+1}| + 1 = j - j''$ by the induction hypothesis as desired. □

Define $j_1 \in (j' : j]$ to be the smallest such that $\mathsf{turn}(j_1) = 1$. As $\mathsf{turn}(j) = 1$, the value j_1 is well defined. Moreover, as $\mathsf{turn}(j') = 0$, we have that $\mathsf{turn}(j_1 - 1) = 0$. We claim that:

Claim 6.56. *$\sigma^A_{j_1} \neq \sigma^B_{j_1}$ and $|\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)| = |\psi_{j_1}|$.*

Proof. We first show that

$$\psi^A_{j_1} \| \sigma^A_{j_1} \neq \psi^B_{j_1} \| \sigma^B_{j_1} \qquad \text{and} \qquad \psi^A_{j_1} = \psi^B_{j_1}. \tag{38}$$

The former follows from $\mathsf{turn}(j_1) = 1$ and the definition of $\mathsf{turn}(\cdot)$. For the latter, note that either $|\mathscr{R}_{j_1-1}|$ is odd, which together with the fact that $|\mathscr{R}_{j_1}|$ is even means that

$j_1 - 1 \in \textsc{Starts}_B \implies \psi^A_{j_1} = \psi^B_{j_1} = \varepsilon$, or $|\mathscr{R}_{j_1-1}|$ is even, which together with the fact that $|\mathscr{R}_{j_1}|$ is even means that $j_1 - 1 \notin \textsc{Starts}$ implying that:

$$\begin{aligned}
\psi^A_{j_1} &= \psi^A_{j_1-1} \| \sigma^A_{j_1-1} && \text{(Fact 6.5, item 5)} \\
&= \psi^B_{j_1-1} \| \sigma^B_{j_1-1} && \text{(As } \mathsf{turn}(j_1-1) = 0 \text{ and } |\mathscr{R}_{j_1-1}| \text{ is even)} \\
&= \psi^B_{j_1}. && \text{(Fact 6.5, item 5)}
\end{aligned}$$

From Equation 38, we get that $\sigma^A_{j_1} \neq \sigma^B_{j_1}$. Moreover, combining Equation 38 with Claim 6.54, we also get $\left(\psi^A_j \| \sigma^A_j\right)[1 : |\psi_{j_1}| + 1] \neq \left(\psi^B_j \| \sigma^B_j\right)[1 : |\psi_{j_1}| + 1]$ and $\left(\psi^A_j \| \sigma^A_j\right)[1 : |\psi_{j_1}|] = \left(\psi^B_j \| \sigma^B_j\right)[1 : |\psi_{j_1}|]$ implying that $|\mathsf{LCP}(\psi^A_j \| \sigma^A_j, \psi^B_j \| \sigma^B_j)| = |\psi_{j_1}|$ and the claim follows. □

Using Claim 6.56, we have:

$$\begin{aligned}
\sigma^A_{j_1} \neq \sigma^B_{j_1} &\implies \pi^A_{j_1}[|\pi_{j_1}|] \neq \pi^B_{j_1}[|\pi_{j_1}|] && \text{(Fact 6.5, item 5 and } |\mathscr{R}_{j_1}| \text{ is even)} \\
&\implies \pi^A_{i+1}[|\pi_{j_1}|] \neq \pi^B_{i+1}[|\pi_{j_1}|] && \text{(Corollary 6.14 and } |\mathscr{R}_{j_1}| = |\mathscr{R}_{i+1}|) \\
&\implies \pi^A_{i+1}(|\pi_{j+1}| : |\pi_{j_1}|] \neq \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{j_1}|] \\
& && \text{(As } |\pi_{j+1}| < |\pi_{j_1}| \text{ by Claim 6.55)} \\
&\implies |\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|])| \leq |\pi_{j_1}| - |\pi_{j+1}| - 1.
\end{aligned}$$

Next, as $|\mathscr{R}_{j_1}|$ is even and item 5 of Fact 6.5, we have that $|\pi_{j_1}| - 1 = |\pi_{j_1+1}|$. Plugging this in, we get

$$|\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|])| \leq |\pi_{j_1+1}| - |\pi_{j+1}|. \tag{39}$$

Observe that from Claim 6.54 and Claim 6.55, we can conclude that $|\psi_j| - |\psi_{j_1}| = j - j_1 = |\pi_{j_1+1}| - |\pi_{j+1}|$. Using this, we can continue Equation 39 as

$$\begin{aligned}
|\psi_j| - |\psi_{j_1}| &\geq |\mathsf{LCP}(\pi^A_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|], \pi^B_{i+1}(|\pi_{j+1}| : |\pi_{i+1}|])| \\
&> \frac{8}{9} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) && \text{(As } \mathsf{tax}_{1,i}(j) > 0) \\
&= \frac{8}{9} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) + \frac{8}{9} \cdot (|\pi_{j_1+1}| - |\pi_{j+1}|) \\
&= \frac{8}{9} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) + \frac{8}{9} \cdot (|\psi_j| - |\psi_{j_1}|) \\
& && \text{(As } |\psi_j| - |\psi_{j_1}| = |\pi_{j_1+1}| - |\pi_{j+1}|) \\
&\geq \frac{4}{9} \cdot (|\psi_{j_1}| + 1) + \frac{8}{9} \cdot (|\psi_j| - |\psi_{j_1}|). && \text{(Lemma 6.13 and } |\mathscr{R}_{j_1}| = |\mathscr{R}_{i+1}|)
\end{aligned}$$

This rearranges to $|\psi_j| + 1 > 5 \cdot (|\psi_{j_1}| + 1)$. In particular, together with Claim 6.54, this means that $j - j_1 = |\psi_j| - |\psi_{j_1}| > 4$.

Define $j_2 \in (j_1 : j]$ be the largest such that $\mathscr{R}_{j_2}.last.t = 0$. We claim that j_2 is well defined as j_1+1 is one such value. Indeed, if not, then $\mathscr{R}_{j_1+1}.last.t > 0$ implying item 11

of Fact 6.5 that $|\psi_{j_1}| + 1 \geq \mathscr{R}_{j_1+1}.last.r - \mathscr{R}_{j_1+1}.last.t$. Moreover, as $\mathscr{R}_{j_1+1}.last.t > 0$, we get from item 9 of Fact 6.5 that $|\psi_{j_1}| + 1 \geq \mathscr{R}_j.last.r - \mathscr{R}_j.last.t = \frac{1}{2} \cdot (|\psi_j| + 1)$ as $j \in \mathfrak{E}(80)$. This contradicts the fact that $|\psi_j| + 1 > 5 \cdot (|\psi_{j_1}| + 1)$. We claim that:

Claim 6.57. *We have $j_2 - j_1 > \frac{1}{4} \cdot (|\psi_j| + 1)$. Moreover, for all $j'' \in [j_1 : j_2]$, we have $\mathscr{R}_{j''}.last.t = 0$ and for all $j'' \in (j_2 : j]$, we have $\mathscr{R}_{j''}.last.t = \mathscr{R}_j.last.t$.*

Proof. Due to item 11 of Fact 6.5 and the fact that $j \in \mathfrak{E}(80)$, we have $\mathscr{R}_j.last.t > 0 \implies j_2 < j$. Due to our choice of j_2 this means that $\mathscr{R}_{j_2+1}.last.t > 0$ implying by item 9 of Fact 6.5 that $\mathscr{R}_{j''}.last.t = \mathscr{R}_j.last.t$ for all $j'' \in (j_2 : j]$. We next show that $\mathscr{R}_{j''}.last.t = 0$ for all $j'' \in [j_1 : j_2]$. Suppose not and let $j'' \in [j_1 : j_2]$ be such that $\mathscr{R}_{j''}.last.t > 0$. Then, we would get from item 9 of Fact 6.5 that $\mathscr{R}_{j_2}.last.t > 0$, a contradiction.

It remains to show that $j_2 - j_1 > \frac{1}{4} \cdot (|\psi_j| + 1)$. This is because:

$$
\begin{aligned}
j_2 - j_1 &= |\psi_{j_2}| - |\psi_{j_1}| && \text{(Claim 6.54)} \\
&= \mathscr{R}_{j_2+1}.last.r - \mathscr{R}_{j_2+1}.last.t - (|\psi_{j_1}| + 1) \\
&\qquad \text{(As Claim 6.57 implies } j_2 \in \mathfrak{E}(90)\text{)} \\
&= \mathscr{R}_j.last.r - \mathscr{R}_j.last.t - (|\psi_{j_1}| + 1) \\
&\qquad \text{(Fact 6.5, item 9 and } |\mathscr{R}_{j''}| \text{ is even for all } j'' \in (j_2 : j]\text{)} \\
&= \frac{1}{2} \cdot (|\psi_j| + 1) - (|\psi_{j_1}| + 1) && \text{(As } j \in \mathfrak{E}(80)\text{)} \\
&> \frac{1}{4} \cdot (|\psi_j| + 1)\,. && \text{(As } |\psi_j| + 1 > 5 \cdot (|\psi_{j_1}| + 1)\text{)}
\end{aligned}
$$

□

Consider now the iterations $\in [j_1 : j_2)$. As $|\mathscr{R}_{j''}| = |\mathscr{R}_{i+1}|$ for all $j'' \in [j_1 : j_2]$, we have that $[j_1 : j_2) \subseteq \mathfrak{E}(87)$. However, $[j_1 : j_2) \subseteq \mathfrak{E}(87)$ and $\mathscr{R}_{j''}.last.t = 0$ for all $j'' \in [j_1 : j_2]$ is only possible if $\Gamma^A_{j''} = \tilde{\Gamma}^A_{j''}$ for all $j'' \in [j_1 : j_2)$. We next claim that:

Claim 6.58. $\sum_{j''=j_1}^{j_2-1} \mathbb{1}\left(\Gamma^A_{j''} \neq \Gamma^B_{j''}\right) \geq \frac{4}{5} \cdot (j_2 - j_1)$.

Proof. By Claim 6.57, we have $j_2 > j_1 \implies j_2 - 1 \geq j_1$. Combining with Claim 6.54, we get that $|\psi_{j_2-1}| \geq |\psi_{j_1}|$ implying by Claim 6.56 and the definition of $\mathsf{LCP}(\cdot)$ that $|\mathsf{LCP}((\psi^A_j \| \sigma^A_j)[1 : |\psi_{j_2-1}| + 1], (\psi^B_j \| \sigma^B_j)[1 : |\psi_{j_2-1}| + 1])| = |\psi_{j_1}|$. Next, we apply Claim 6.54 to get $|\mathsf{LCP}(\psi^A_{j_2-1} \| \sigma^A_{j_2-1}, \psi^B_{j_2-1} \| \sigma^B_{j_2-1})| = |\psi_{j_1}|$ Plugging into Definition 3.6, we have that

$$
\begin{aligned}
\Delta(\overline{\mathsf{TC}}(\psi^A_{j_2-1} \| \sigma^A_{j_2-1}), \overline{\mathsf{TC}}(\psi^B_{j_2-1} \| \sigma^B_{j_2-1})) &\geq \left(1 - 10^{-5}\right) \cdot (|\psi_{j_2-1}| + 1 - |\psi_{j_1}|) \\
&\geq \frac{4}{5} \cdot (|\psi_{j_2-1}| + 1 - |\psi_{j_1}|)
\end{aligned}
$$

$$\geq \frac{4}{5} \cdot (j_2 - j_1)\,. \qquad \text{(Claim 6.54)}$$

From the definition of $\Delta(\cdot)$ and $\overline{\mathsf{TC}}(\cdot)$, we get:

$$\frac{4}{5} \cdot (j_2 - j_1) \leq \sum_{z=1}^{|\psi_{j_2-1}|+1} \mathbb{1}\left(\mathsf{TC}\left(\left(\psi^A_{j_2-1} \| \sigma^A_{j_2-1}\right)[1:z]\right) \neq \mathsf{TC}\left(\left(\psi^B_{j_2-1} \| \sigma^B_{j_2-1}\right)[1:z]\right)\right).$$

For all $z \in [|\psi_{j_1}|]$, we have by Claim 6.56 that $\left(\psi^A_j \| \sigma^A_j\right)[1:z] = \left(\psi^B_j \| \sigma^B_j\right)[1:z]$ which implies by Claim 6.54 that $\left(\psi^A_{j_2-1} \| \sigma^A_{j_2-1}\right)[1:z] = \left(\psi^B_{j_2-1} \| \sigma^B_{j_2-1}\right)[1:z]$ in turn implying that $\mathsf{TC}\left(\left(\psi^A_{j_2-1} \| \sigma^A_{j_2-1}\right)[1:z]\right) = \mathsf{TC}\left(\left(\psi^B_{j_2-1} \| \sigma^B_{j_2-1}\right)[1:z]\right)$. Thus, we get:

$$\begin{aligned}
\frac{4}{5} \cdot (j_2 - j_1) &\leq \sum_{z=|\psi_{j_1}|+1}^{|\psi_{j_2-1}|+1} \mathbb{1}\left(\mathsf{TC}\left(\left(\psi^A_{j_2-1} \| \sigma^A_{j_2-1}\right)[1:z]\right) \neq \mathsf{TC}\left(\left(\psi^B_{j_2-1} \| \sigma^B_{j_2-1}\right)[1:z]\right)\right) \\
&\leq \sum_{z=|\psi_{j_1}|+1}^{|\psi_{j_2-1}|+1} \mathbb{1}\left(\mathsf{TC}\left(\left(\psi^A_{j} \| \sigma^A_{j}\right)[1:z]\right) \neq \mathsf{TC}\left(\left(\psi^B_{j} \| \sigma^B_{j}\right)[1:z]\right)\right) \\
&\qquad \text{(Claim 6.54)} \\
&\leq \sum_{j''=j_1}^{j_2-1} \mathbb{1}\left(\mathsf{TC}\left(\psi^A_{j''} \| \sigma^A_{j''}\right) \neq \mathsf{TC}\left(\psi^B_{j''} \| \sigma^B_{j''}\right)\right) \qquad \text{(Claim 6.54)} \\
&\leq \sum_{j''=j_1}^{j_2-1} \mathbb{1}\left(\Gamma^A_{j''} \neq \Gamma^B_{j''}\right). \qquad \text{(Definition of } \Gamma \text{ as } |\mathscr{R}_{j''}| \text{ is even)}
\end{aligned}$$

□

Combined with $\Gamma^A_{j''} = \tilde{\Gamma}^A_{j''}$ for all $j'' \in [j_1 : j_2)$, Claim 6.58 gives that for at least $\frac{4}{5} \cdot (j_2 - j_1)$ values of $j'' \in [j_1 : j_2)$, we have $\tilde{\Gamma}^A_{j''} \neq \Gamma^B_{j''} \implies 2 \cdot \mathsf{corr}_{j''} \geq \ell_{j''}$. As $|\mathscr{R}_{j''}| = |\mathscr{R}_{i+1}|$ for all $j'' \in [j_1 : j_2]$, this gives:

$$\begin{aligned}
60 \cdot \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} &\geq 60 \cdot \sum_{j''=j_1}^{j_2-1} \mathsf{corr}_{j''} \\
&\geq 24 \cdot (j_2 - j_1) \cdot \ell^*_{i+1} \\
&\geq 6 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) \qquad \text{(Claim 6.57)} \\
&\geq 5 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) + \ell^*_{i+1} \cdot (|\pi_{j'+1}| - |\pi_{j+1}|) \\
&\qquad \text{(Claim 6.54, Claim 6.55)} \\
&\geq 15 \cdot \ell^*_{i+1} + 2 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) + \ell^*_{i+1} \cdot (|\pi_{j'+1}| - |\pi_{j+1}|)\,. \\
&\qquad \text{(As } |\psi_j| + 1 > 5 \cdot (|\psi_{j_1}| + 1) \geq 5)
\end{aligned}$$

as desired.

□

6.2.8 Lemmas Concerning $\mathsf{G}(\cdot)$ and $\mathsf{B}(\cdot)$

Lemma 6.59. *Let $i \in \textsc{Starts}_{\mathrm{F}}$ and $i' \in (i : \textsc{Stop}(i)) \cap \textsc{Starts}_{\mathrm{B}}$ be such that $|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|$. We have for all $j \in \{i'\} \cup \textsc{Range}(i') \setminus \{num\}$ satisfying $|\mathscr{R}_j| = |\mathscr{R}_{i'+1}|$ that:*

$$50 \cdot (|\pi_{i'+1}| - |\pi_{j+1}|) \leq \mathsf{tax}_{1,i'}(j) + 1000 \cdot \mathsf{B}_i(i').$$

Proof. For all $j \in \{i'\} \cup \textsc{Range}(i') \setminus \{num\} \implies j \neq i$ satisfying $|\mathscr{R}_j| = |\mathscr{R}_{i'+1}|$, we have that $|\pi_{j+1}| \leq |\pi_{i'+1}|$ by Lemma 6.13. Also, $j \in \{i'\} \cup \textsc{Range}(i') \subseteq \textsc{Range}(i)$ by Lemma 6.7, we get $|\pi_{i+1}| = \mathscr{R}_j[|\mathscr{R}_{i+1}|].r$ using item 8 of Fact 6.5. Using Lemma 6.6, this gives $|\pi_{i+1}| \leq |\pi_{j+1}|$. We claim that:

$$\begin{aligned} &|\mathsf{LCP}(\pi^A_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|], \pi^B_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|])| \\ &\qquad - |\mathsf{LCP}(\pi^A_{i'+1}(|\pi_{j+1}| : |\pi_{i'+1}|], \pi^B_{i'+1}(|\pi_{j+1}| : |\pi_{i'+1}|])| \leq |\pi_{j+1}| - |\pi_{i+1}|. \end{aligned} \tag{40}$$

Indeed, either $|\mathsf{LCP}(\pi^A_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|], \pi^B_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|])| \leq |\pi_{j+1}| - |\pi_{i+1}|$ in which case there is nothing to show or $|\mathsf{LCP}(\pi^A_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|], \pi^B_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|])| > |\pi_{j+1}| - |\pi_{i+1}|$, in which case Equation 40 follows by the definition of $\mathsf{LCP}(\cdot)$ and the fact that $|\pi_{i+1}| \leq |\pi_{j+1}| \leq |\pi_{i'+1}|$. Equation 40 gives:

$$\begin{aligned} &\mathsf{tax}_{1,i'}(j) + 1000 \cdot \mathsf{B}_i(i') \\ &\quad \geq 900 \cdot |\mathsf{LCP}(\pi^A_{i'+1}(|\pi_{j+1}| : |\pi_{i'+1}|], \pi^B_{i'+1}(|\pi_{j+1}| : |\pi_{i'+1}|])| - 800 \cdot (|\pi_{i'+1}| - |\pi_{j+1}|) \\ &\qquad + 1000 \cdot \mathsf{B}_i(i') && \text{(Definition of } \mathsf{tax}_1(\cdot)) \\ &\quad \geq 900 \cdot |\mathsf{LCP}(\pi^A_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|], \pi^B_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|])| \\ &\qquad - 900 \cdot (|\pi_{j+1}| - |\pi_{i+1}|) - 800 \cdot (|\pi_{i'+1}| - |\pi_{j+1}|) + 1000 \cdot \mathsf{B}_i(i') && \text{(Equation 40)} \\ &\quad \geq 900 \cdot |\mathsf{LCP}(\pi^A_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|], \pi^B_{i'+1}(|\pi_{i+1}| : |\pi_{i'+1}|])| \\ &\qquad - 900 \cdot (|\pi_{i'+1}| - |\pi_{i+1}|) + 100 \cdot (|\pi_{i'+1}| - |\pi_{j+1}|) + 1000 \cdot \mathsf{B}_i(i') \\ &\quad \geq 100 \cdot \mathsf{B}_i(i') + 100 \cdot (|\pi_{i'+1}| - |\pi_{j+1}|) && \text{(Definition of } \mathsf{G}(\cdot) \text{ and } \mathsf{B}(\cdot)) \\ &\quad \geq 50 \cdot (|\pi_{i'+1}| - |\pi_{j+1}|)\,. \end{aligned}$$

□

Lemma 6.60. *Let $i \in \textsc{Starts}_{\mathrm{F}}$ and $i' \in (i : \textsc{Stop}(i)) \cap \textsc{Starts}_{\mathrm{B}}$ be such that i' is indirect and $|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|$. We have:*

- *If $\mathsf{G}_i(i') < |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}|$, then, for all $j' \in [i' : \textsc{Stop}(i')]$, we have $\mathsf{G}_i(i') = \mathsf{G}_i(j')$ and $\mathsf{B}_i(j') = \mathsf{B}_i(i') + |\pi_{j'+1}| - |\pi_{i'+1}|$. Moreover, we have:*

$$\mathsf{D}_i(i') - \mathsf{D}_i(\textsc{Mid}(i')) + \mathsf{spare}_i(i') \geq 1.$$

- *If $\mathsf{G}_i(i') \geq |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}|$, then $\mathsf{B}_i(\textsc{Stop}(i')) = \mathsf{B}_{\textsc{Mid}(i')}(\textsc{Stop}(i'))$ and $\mathsf{D}_i(\textsc{Mid}(i')) = 0$ and $\mathsf{spare}_i(\textsc{Stop}(i')) \leq \mathsf{spare}_{\textsc{Mid}(i')}(\textsc{Stop}(i'))$.*

Proof. We prove each part separately using the following claim in both the parts:

Claim 6.61. *For all $j' \in [i' : \textsc{Stop}(i')]$ and $C \in \{A, B\}$, we have $\pi^C_{j'+1,\leq|\pi_{\textsc{Mid}(i')+1}|} = \pi^C_{i'+1,\leq|\pi_{\textsc{Mid}(i')+1}|}$.*

Proof. As the parties only add/remove one symbol from π in every iteration, it is sufficient to show that $|\pi_{\textsc{Mid}(i')+1}| \leq |\pi_{j'+1}|$ for all $j' \in [i' : \textsc{Stop}(i')]$. This follows from Lemma 6.15 and the fact that $\textsc{Stop}(i') = \textsc{Stop}(\textsc{Mid}(i'))$ by Lemma 6.9. □

- If $\mathsf{G}_i(i') < |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}|$, then by the definition of $\mathsf{G}(\cdot)$ and $\mathsf{LCP}(\cdot)$, we get (using h to denote $|\pi_{i+1}| + \mathsf{G}_i(i') + 1 \leq |\pi_{\textsc{Mid}(i')+1}|$):

$$\pi^A_{i'+1}(|\pi_{i+1}| : h) = \pi^B_{i'+1}(|\pi_{i+1}| : h) \qquad \text{and} \qquad \pi^A_{i'+1}[h] = \pi^B_{i'+1}[h].$$

As $h \leq |\pi_{\textsc{Mid}(i')+1}|$, we get by Claim 6.61 that, for all $j' \in [i' : \textsc{Stop}(i')]$, we have:

$$\pi^A_{j'+1}(|\pi_{i+1}| : h) = \pi^B_{j'+1}(|\pi_{i+1}| : h) \qquad \text{and} \qquad \pi^A_{j'+1}[h] = \pi^B_{j'+1}[h].$$

It follows that by the definition of $\mathsf{G}(\cdot)$ and $\mathsf{LCP}(\cdot)$ that $\mathsf{G}_i(j') = h - 1 - |\pi_{i+1}| = \mathsf{G}_i(i')$. By the definition of $\mathsf{B}(\cdot)$, we also get:

$$\mathsf{B}_i(j') - \mathsf{B}_i(i') = |\pi_{j'+1}| - |\pi_{i'+1}| - \mathsf{G}_i(j') + \mathsf{G}_i(i') = |\pi_{j'+1}| - |\pi_{i'+1}|,$$

as desired. Next, we claim that:

Claim 6.62. *For all $l \in (|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|]$, it holds that $\mathsf{latest}(\textsc{Mid}(i'), l) = \mathsf{latest}(i', l)$.*

Proof. Suppose not. Then, there is an $l \in (|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|]$ such that $\mathsf{latest}(\textsc{Mid}(i'), l) \in (i' : \textsc{Mid}(i')]$. By definition of $\mathsf{latest}(\cdot)$, we get that $|\pi_{\mathsf{latest}(\textsc{Mid}(i'),l)+1}| = l$ and $|\mathscr{R}_{\mathsf{latest}(\textsc{Mid}(i'),l)}|$ is odd implying by item 5 of Fact 6.5 that $|\pi_{\mathsf{latest}(\textsc{Mid}(i'),l)}| = l - 1 < |\pi_{\textsc{Mid}(i')+1}|$. As $\mathsf{latest}(\textsc{Mid}(i'), l) \in (i' : \textsc{Mid}(i')]$, this is a contradiction to Lemma 6.13. □

Also, note that by definition of $\textsc{Mid}(\cdot)$, we can apply Lemma 6.13 on $i', \textsc{Mid}(i')$. We get that $|\pi_{\textsc{Mid}(i')+1}| < |\pi_{i'+1}|$. Using this and the definition of $\mathsf{D}(\cdot)$, we get:

$$\begin{aligned}
&\mathsf{D}_i(\textsc{Mid}(i')) \\
&\qquad = |\{|\pi_{i+1}| < l \leq |\pi_{\textsc{Mid}(i')+1}| \mid \Gamma^A_{\mathsf{latest}(\textsc{Mid}(i'),l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(\textsc{Mid}(i'),l),\geq\mathsf{depth}(i)}\}| \\
&\qquad = |\{|\pi_{i+1}| < l \leq |\pi_{\textsc{Mid}(i')+1}| \mid \Gamma^A_{\mathsf{latest}(i',l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(i',l),\geq\mathsf{depth}(i)}\}| \\
&\qquad\qquad \text{(Claim 6.62)} \\
&\qquad \leq |\{|\pi_{i+1}| < l \leq |\pi_{i'}| \mid \Gamma^A_{\mathsf{latest}(i',l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(i',l),\geq\mathsf{depth}(i)}\}|. \\
&\qquad\qquad \text{(As } |\pi_{\textsc{Mid}(i')+1}| < |\pi_{i'+1}|\text{)}
\end{aligned}$$

As $|\mathscr{R}_{i'}|$ is odd, we have by item 5 of Fact 6.5 that $|\pi_{i'+1}| = |\pi_{i'}| + 1$ and $\mathsf{latest}(i', l) = \mathsf{latest}(i' - 1, l)$ for all $l \in [|\pi_{i'}|]$. This gives:

$$\mathsf{D}_i(i' - 1) = |\{|\pi_{i+1}| < l \leq |\pi_{i'}| \mid \Gamma^A_{\mathsf{latest}(i'-1,l),\geq\mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(i'-1,l),\geq\mathsf{depth}(i)}\}|$$

$$= |\{|\pi_{i+1}| < l \le |\pi_{i'}| \mid \Gamma^A_{\mathsf{latest}(i',l),\ge \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(i',l),\ge \mathsf{depth}(i)}\}|.$$

By definition of $\mathsf{D}(\cdot)$, we also have:

$$\mathsf{D}_i(i') = |\{|\pi_{i+1}| < l \le |\pi_{i'+1}| \mid \Gamma^A_{\mathsf{latest}(i',l),\ge \mathsf{depth}(i)} \neq \Gamma^B_{\mathsf{latest}(i',l),\ge \mathsf{depth}(i)}\}|.$$

As $|\pi_{i'+1}| = |\pi_{i'}| + 1$, it follows that $\mathsf{D}_i(\textsc{Mid}(i')) \le \mathsf{D}_i(i'-1) \le \mathsf{D}_i(i')$. Consequently, we have $\mathsf{D}_i(i') - \mathsf{D}_i(\textsc{Mid}(i')) \ge \mathsf{D}_i(i') - \mathsf{D}_i(i'-1) \ge \mathbb{1}(\mathsf{D}_i(i') > \mathsf{D}_i(i'-1))$. Using the definition of $\mathsf{spare}(\cdot)$, this gives:

$$\begin{aligned}
&\mathsf{D}_i(i') - \mathsf{D}_i(\textsc{Mid}(i')) + \mathsf{spare}_i(i') \\
&\quad \ge \mathbb{1}(\mathsf{D}_i(i') > \mathsf{D}_i(i'-1)) + \mathbb{1}(\mathsf{B}_i(i') > 0 \wedge (i' \notin \mathfrak{E}(70) \vee \mathsf{D}_i(i') = \mathsf{D}_i(i'-1))) \\
&\quad \ge \mathbb{1}(\mathsf{D}_i(i') > \mathsf{D}_i(i'-1)) + \mathbb{1}(\mathsf{B}_i(i') > 0 \wedge \mathsf{D}_i(i') = \mathsf{D}_i(i'-1)).
\end{aligned}$$

We next use the fact that $\mathsf{B}_i(i') = |\pi_{i'+1}| - |\pi_{i+1}| - \mathsf{G}_i(i') \ge |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}| - \mathsf{G}_i(i') > 0$ to get

$$\begin{aligned}
\mathsf{D}_i(i') - \mathsf{D}_i(\textsc{Mid}(i')) + \mathsf{spare}_i(i') &\ge \mathbb{1}(\mathsf{D}_i(i') > \mathsf{D}_i(i'-1)) + \mathbb{1}(\mathsf{D}_i(i') = \mathsf{D}_i(i'-1)) \\
&\ge 1. \qquad (\text{As } \mathsf{D}_i(i') \ge \mathsf{D}_i(i'-1))
\end{aligned}$$

- If $\mathsf{G}_i(i') \ge |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}|$, we use the definition of $\mathsf{G}(\cdot)$ and Claim 6.61 to get

$$\begin{aligned}
&\pi^A_{i'+1}(|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|] = \pi^B_{i'+1}(|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|] \\
&\implies \pi^A_{\textsc{Stop}(i')+1}(|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|] = \pi^B_{\textsc{Stop}(i')+1}(|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|].
\end{aligned} \tag{41}$$

Using Equation 41, we derive:

$$\begin{aligned}
&\mathsf{G}_i(\textsc{Stop}(i')) \\
&\quad = |\mathsf{LCP}(\pi^A_{\textsc{Stop}(i')+1}(|\pi_{i+1}| : |\pi_{\textsc{Stop}(i')+1}|], \pi^B_{\textsc{Stop}(i')+1}(|\pi_{i+1}| : |\pi_{\textsc{Stop}(i')+1}|])| \\
&\quad = |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}| \\
&\qquad + |\mathsf{LCP}(\pi^A_{\textsc{Stop}(i')+1}(|\pi_{\textsc{Mid}(i')+1}| : |\pi_{\textsc{Stop}(i')+1}|], \pi^B_{\textsc{Stop}(i')+1}(|\pi_{\textsc{Mid}(i')+1}| : |\pi_{\textsc{Stop}(i')+1}|])| \\
&\quad = |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}| + \mathsf{G}_{\textsc{Mid}(i')}(\textsc{Stop}(i')).
\end{aligned}$$

Using the definition of $\mathsf{B}(\cdot)$, this rearranges to $\mathsf{B}_i(\textsc{Stop}(i')) = \mathsf{B}_{\textsc{Mid}(i')}(\textsc{Stop}(i'))$. To show $\mathsf{D}_i(\textsc{Mid}(i')) = 0$, we argue:

$$\begin{aligned}
&\mathsf{G}_i(i') \ge |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}| \\
&\implies \pi^A_{i'+1}(|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|] = \pi^B_{i'+1}(|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|] \\
&\implies \pi^A_{\textsc{Mid}(i')+1}(|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|] = \pi^B_{\textsc{Mid}(i')+1}(|\pi_{i+1}| : |\pi_{\textsc{Mid}(i')+1}|] \qquad (\text{Claim 6.61}) \\
&\implies \mathsf{G}_i(\textsc{Mid}(i')) = |\pi_{\textsc{Mid}(i')+1}| - |\pi_{i+1}| \\
&\implies \mathsf{B}_i(\textsc{Mid}(i')) = 0 \qquad (\text{Definition of } \mathsf{B}(\cdot)) \\
&\implies \mathsf{D}_i(\textsc{Mid}(i')) = 0. \qquad (\text{Lemma 6.24})
\end{aligned}$$

We next prove $\mathsf{spare}_i(\textsc{Stop}(i')) \leq \mathsf{spare}_{\textsc{Mid}(i')}(\textsc{Stop}(i'))$ If $\mathsf{spare}_i(\textsc{Stop}(i')) = 0$, there is nothing to show so we assume otherwise and show $\mathsf{spare}_{\textsc{Mid}(i')}(\textsc{Stop}(i')) = 1$. By the definition of $\mathsf{spare}_i(\textsc{Stop}(i'))$, we get $\mathsf{B}_i(\textsc{Stop}(i')) > 0$ and $(\textsc{Stop}(i') \notin \mathfrak{E}(70) \vee \mathsf{D}_i(\textsc{Stop}(i')) = \mathsf{D}_i(\textsc{Stop}(i') - 1))$. From $\mathsf{B}_i(\textsc{Stop}(i')) > 0$ and $\mathsf{B}_i(\textsc{Stop}(i')) = \mathsf{B}_{\textsc{Mid}(i')}(\textsc{Stop}(i'))$, we conclude that $\mathsf{B}_{\textsc{Mid}(i')}(\textsc{Stop}(i')) > 0$.

Now, in order to show that $\mathsf{spare}_{\textsc{Mid}(i')}(\textsc{Stop}(i')) = 1$, all the remains to be shown is that $\big(\textsc{Stop}(i') \notin \mathfrak{E}(70) \vee \mathsf{D}_{\textsc{Mid}(i')}(\textsc{Stop}(i')) = \mathsf{D}_{\textsc{Mid}(i')}(\textsc{Stop}(i') - 1)\big)$. This clearly holds if $\textsc{Stop}(i') \notin \mathfrak{E}(70)$, so we assume that $\mathsf{D}_i(\textsc{Stop}(i')) = \mathsf{D}_i(\textsc{Stop}(i') - 1)$. As i' in indirect, we have $|\mathscr{R}_{\textsc{Stop}(i')}|$ is odd which means (using item 5 of Fact 6.5) that $|\pi_{\textsc{Stop}(i')+1}| = |\pi_{\textsc{Stop}(i')}| + 1$ and $\mathsf{latest}(\textsc{Stop}(i'), l) = \mathsf{latest}(\textsc{Stop}(i') - 1, l)$ for all $l \in [|\pi_{\textsc{Stop}(i')}|]$ and $\mathsf{latest}(\textsc{Stop}(i'), |\pi_{\textsc{Stop}(i')+1}|) = \textsc{Stop}(i')$. We get from the definition of $\mathsf{D}(\cdot)$ that:

$$\begin{aligned}
\mathsf{D}_i(\textsc{Stop}(i')) = \mathsf{D}_i(\textsc{Stop}(i') - 1) &\implies \Gamma^A_{\textsc{Stop}(i'),\geq \mathsf{depth}(i)} = \Gamma^B_{\textsc{Stop}(i'),\geq \mathsf{depth}(i)} \\
&\implies \Gamma^A_{\textsc{Stop}(i'),\geq \mathsf{depth}(\textsc{Mid}(i'))} = \Gamma^B_{\textsc{Stop}(i'),\geq \mathsf{depth}(\textsc{Mid}(i'))} \\
&\implies \mathsf{D}_{\textsc{Mid}(i')}(\textsc{Stop}(i')) = \mathsf{D}_{\textsc{Mid}(i')}(\textsc{Stop}(i') - 1),
\end{aligned}$$

finishing the proof.

□

6.2.9 Lemmas Concerning $\mathsf{extra}(\cdot)$

Lemma 6.63. *Consider $i \in \textsc{Starts}_{\mathrm{B}}$ and all $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ such that $|\pi_{j+1}| \leq |\pi_{i+1}|$. For all $\eta \geq \eta_1 \geq 0$ and $\eta' \geq \eta'_1 \geq 0$, we have:*

$$\mathsf{extra}_i(\eta, \eta', j) \leq \mathsf{extra}_i(\eta_1, \eta'_1, j).$$

Proof. We have:

$$\begin{aligned}
&\mathsf{extra}_i(\eta, \eta', j) \\
&\quad = \ell^*_{i+1} \cdot \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30} - \mathsf{tax}_0(\eta, j), 35\left(|\pi_{i+1}| - |\pi_{j+1}|\right) - \mathsf{tax}_0(\eta', j)\right) \\
&\quad \leq \ell^*_{i+1} \cdot \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30} - \mathsf{tax}_0(\eta_1, j), 35\left(|\pi_{i+1}| - |\pi_{j+1}|\right) - \mathsf{tax}_0(\eta'_1, j)\right) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Lemma 6.42)} \\
&\quad \leq \mathsf{extra}_i(\eta_1, \eta'_1, j).
\end{aligned}$$

□

Lemma 6.64. *Consider $i \in \textsc{Starts}_{\mathrm{B}}$ and $j' < j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ such that $|\mathscr{R}_{j''}| = |\mathscr{R}_{i+1}|$ for all $j'' \in (j' : j]$ and $\mathsf{turn}(j'') = \mathsf{turn}(j)$ for all $j'' \in [j' : j]$. For all*

$0 \le z < 1$ *and all* $1000 \ge \eta \ge \eta' \ge \frac{3}{1-z}$*, we have:*

$$10^4 \cdot \mathsf{E}_i^{\mathrm{B}}(j') + \mathsf{extra}_i(\eta, \eta', j')$$
$$\le 10^4 \cdot \mathsf{E}_i^{\mathrm{B}}(j) + \mathsf{extra}_i(\eta, \eta', j) - z\eta'\ell_j^* \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0).$$

Proof. Note that:

$$\begin{aligned}
\mathsf{extra}_i(\eta, \eta', j') &\le \ell_{i+1}^* \cdot \left(\frac{|\pi_{i+1}| - |\pi_{\mathrm{PREV}(i)+1}|}{30} - \mathsf{tax}_0(\eta, j') \right) \\
&\le \frac{\ell_{i+1}^*}{30} \cdot \left(|\pi_{i+1}| - |\pi_{\mathrm{PREV}(i)+1}| \right) - \ell_j^* \cdot \mathsf{tax}_0(\eta, j') && (\text{As } |\mathscr{R}_j| = |\mathscr{R}_{i+1}|) \\
&\le \frac{\ell_{i+1}^*}{30} \cdot \left(|\pi_{i+1}| - |\pi_{\mathrm{PREV}(i)+1}| \right) - \ell_j^* \cdot \mathsf{tax}_0(\eta, j) \\
&\quad + 5\eta \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} - z\eta\ell_j^* \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0) \\
&&& (\text{Lemma 6.45}) \\
&\le \frac{\ell_{i+1}^*}{30} \cdot \left(|\pi_{i+1}| - |\pi_{\mathrm{PREV}(i)+1}| \right) - \ell_j^* \cdot \mathsf{tax}_0(\eta, j) \\
&\quad + 5000 \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} - z\eta'\ell_j^* \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0) \\
&&& (\text{As } \eta' \le \eta \le 1000) \\
&\le \ell_{i+1}^* \cdot \left(\frac{|\pi_{i+1}| - |\pi_{\mathrm{PREV}(i)+1}|}{30} - \mathsf{tax}_0(\eta, j) \right) \\
&\quad + 5000 \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} - z\eta'\ell_j^* \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0). \\
&&& (\text{As } |\mathscr{R}_j| = |\mathscr{R}_{i+1}|)
\end{aligned}$$

Similarly,

$$\begin{aligned}
\mathsf{extra}_i(\eta, \eta', j') &\le \ell_{i+1}^* \cdot \left(35 \left(|\pi_{i+1}| - |\pi_{j'+1}| \right) - \mathsf{tax}_0(\eta', j') \right) \\
&\le 35 \cdot \ell_{i+1}^* \cdot \left(|\pi_{i+1}| - |\pi_{j'+1}| \right) - \ell_j^* \cdot \mathsf{tax}_0(\eta', j') && (\text{As } |\mathscr{R}_j| = |\mathscr{R}_{i+1}|) \\
&\le 35 \cdot \ell_{i+1}^* \cdot \left(|\pi_{i+1}| - |\pi_{j+1}| \right) - \ell_j^* \cdot \mathsf{tax}_0(\eta', j') && (\text{As } |\pi_{j+1}| \le |\pi_{j'+1}|) \\
&\le 35 \cdot \ell_{i+1}^* \cdot \left(|\pi_{i+1}| - |\pi_{j+1}| \right) - \ell_j^* \cdot \mathsf{tax}_0(\eta', j) \\
&\quad + 5\eta' \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} - z\eta'\ell_j^* \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0) \\
&&& (\text{Lemma 6.45}) \\
&\le 35 \cdot \ell_{i+1}^* \cdot \left(|\pi_{i+1}| - |\pi_{j+1}| \right) - \ell_j^* \cdot \mathsf{tax}_0(\eta', j)
\end{aligned}$$

$$+ 5000 \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} - z\eta'\ell^*_j \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0)$$

(As $\eta' \le \eta \le 1000$)

$$\le \ell^*_{i+1} \cdot (35\,(|\pi_{i+1}| - |\pi_{j+1}|) - \mathsf{tax}_0(\eta', j))$$
$$+ 5000 \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} - z\eta'\ell^*_j \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0).$$

(As $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$)

Combining the last two inequalities, we have that:

$$\mathsf{extra}_i(\eta, \eta', j') \le \ell^*_{i+1} \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30} - \mathsf{tax}_0(\eta, j), 35\,(|\pi_{i+1}| - |\pi_{j+1}|) - \mathsf{tax}_0(\eta', j)\right)$$
$$+ 5000 \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} - z\eta'\ell^*_j \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0)$$
$$\le \mathsf{extra}_i(\eta, \eta', j)$$
$$+ 5000 \sum_{j''=j'+1}^{j} \mathsf{corr}_{j''} - z\eta'\ell^*_j \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0)$$

(Definition of $\mathsf{extra}(\cdot)$)

$$\le \mathsf{extra}_i(\eta, \eta', j) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) - 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j')$$
$$- z\eta'\ell^*_j \cdot \sum_{j''=j'+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0). \qquad \text{(Lemma 6.39)}$$

The lemma follows after a simple rearrangement. □

Lemma 6.65. *Let $i \in \textsc{Starts}_{\mathrm{B}}$ and $i' \in (i : \textsc{Stop}(i)) \cap \mathfrak{E}(80)$ be such that i' is indirect and $|\mathscr{R}_{i'}| = |\mathscr{R}_{i+1}|$. We have:*

$$\mathsf{extra}_i(i') + 3 \cdot \ell^*_{i+1} \cdot (|\psi_{i'}| + 1) \le \mathsf{extra}_i(225, 225, \textsc{Stop}(i')) + \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i')).$$

Proof. By definition of $\mathsf{extra}(\cdot)$, we derive:

$$\mathsf{extra}_i(i') = \mathsf{extra}_i(225, 10, i')$$
$$= \ell^*_{i+1} \cdot \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30} - \mathsf{tax}_0(225, i'), 35\,(|\pi_{i+1}| - |\pi_{i'+1}|) - \mathsf{tax}_0(10, i')\right)$$
$$\le \ell^*_{i+1} \cdot \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30}, 35\,(|\pi_{i+1}| - |\pi_{i'+1}|)\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(10, i')$$

(Lemma 6.42)

$$\leq \ell^*_{i+1} \cdot \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30}, 35\left(|\pi_{i+1}| - |\pi_{\textsc{Stop}(i')+1}|\right)\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(10, i')$$

(Lemma 6.10)

$$\leq \ell^*_{i+1} \cdot \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30}, 35\left(|\pi_{i+1}| - |\pi_{\textsc{Stop}(i')+1}|\right)\right) - 3 \cdot \ell^*_{i+1} \cdot (|\psi_{i'}| + 1)$$

(Lemma 6.44)

$$\leq \mathsf{extra}_i(225, 225, \textsc{Stop}(i')) + \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i')) - 3 \cdot \ell^*_{i+1} \cdot (|\psi_{i'}| + 1)\,.$$

(Definition of $\mathsf{extra}(\cdot)$)

The lemma follows after a simple rearrangement. □

Lemma 6.66. *Consider $i \in \textsc{Starts}_{\mathrm{B}}$ and $j' < j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ such that $|\mathscr{R}_{j''}| = |\mathscr{R}_{i+1}|$ for all $j'' \in (j' : j]$. Suppose that $j \in \mathfrak{E}(80)$, $\mathsf{tax}_{1,i}(j) > 0$, $\mathsf{turn}(j) = 1$, and $\mathsf{turn}(j') = 0$. We have that:*

$$10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j') + \mathsf{extra}_i(225, 225, j') + 150 \cdot \ell^*_{i+1} \cdot (|\pi_{j'+1}| - |\pi_{j+1}|) \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(j).$$

Proof. We have due to Corollary 6.43 that:

$$\mathsf{extra}_i(225, 225, j') \leq \ell^*_{i+1} \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30}, 35\left(|\pi_{i+1}| - |\pi_{j'+1}|\right)\right).$$

As $|\mathscr{R}_{j''}|$ is even for all $j'' \in (j' : j]$, we have by item 5 of Fact 6.5 that $|\pi_{j+1}| \leq |\pi_{j'+1}|$ implying:

$$\begin{aligned}
\mathsf{extra}_i(225, 225, j') &\leq \ell^*_{i+1} \min\left(\frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30}, 35\left(|\pi_{i+1}| - |\pi_{j+1}|\right)\right) \\
&\leq \mathsf{extra}_i(225, 225, j) + \ell^*_{i+1} \cdot \mathsf{tax}_0(225, j) && \text{(Definition of } \mathsf{extra}(\cdot)\text{)} \\
&\leq \mathsf{extra}_i(j) + \ell^*_{i+1} \cdot \mathsf{tax}_0(225, j) && \text{(Lemma 6.63)} \\
&\leq \mathsf{extra}_i(j) + 300 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) + 2250 \cdot \ell^*_{i+1} && \text{(Lemma 6.51)} \\
&\leq \mathsf{extra}_i(j) + 10^4 \cdot \sum_{i'=j'+1}^{j} \mathsf{corr}_{i'} - 150 \cdot \ell^*_{i+1} \cdot (|\pi_{j'+1}| - |\pi_{j+1}|) \\
& && \text{(Lemma 6.52)} \\
&\leq \mathsf{extra}_i(j) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) - 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j') - 150 \cdot \ell^*_{i+1} \cdot (|\pi_{j'+1}| - |\pi_{j+1}|)\,. \\
& && \text{(Lemma 6.39)}
\end{aligned}$$

The lemma follows after a simple rearrangement. □

6.2.10 Proof of Lemmas 6.17, 6.18, 6.19, and 6.20

In this section, we present our proofs of Lemmas 6.17, 6.18, 6.19, and 6.20. These lemmas will be shown together by the following indiction based approach: We shall show by induction that for all $D \geq 0$, Lemma 6.17 and Lemma 6.18 hold for $j - i = D$ and Lemma 6.19 and Lemma 6.20 hold for $\textsc{Stop}(i) - i = D$.

For the base case $D = 0$, observe that Lemma 6.17 and Lemma 6.18 are trivial if $j = i$ and Lemma 6.19 and Lemma 6.20 are trivial as $\textsc{Stop}(i) - i > 0$ for all $i \in \textsc{Starts}$. To finish the induction, we take an arbitrary $D > 0$ and, assuming the induction hypothesis holds for all numbers $< D$, show that it holds for D as well.

To this end, fix $D > 0$. We first show that Lemma 6.19 and Lemma 6.20 hold if $\textsc{Stop}(i) - i = D$ (under the induction hypothesis).

Proof of Lemma 6.19. Let $i \in \textsc{Starts}_{\mathrm{F}}$ be indirect and satisfy $\textsc{Stop}(i) - i = D$. By definition of $\textsc{Mid}(\cdot)$, we have $|\mathscr{R}_{\textsc{Mid}(i)}| = |\mathscr{R}_{i+1}|$ and therefore $\textsc{Mid}(i)$ is good for i. Furthermore, as i is indirect, we have $|\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{i+1}|$ is odd implying that $\textsc{Mid}(i) < \textsc{Stop}(i)$, which in turn means that $\textsc{Mid}(i) - i < D$. By the induction hypothesis, Lemma 6.17 holds for $i, \textsc{Mid}(i)$ and we have:

$$\begin{aligned}
\sum_{i'=i+1}^{\textsc{Mid}(i)} \ell^*_{i'} &\le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Mid}(i)) + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Mid}(i)) + 150\mathsf{B}_i(\textsc{Mid}(i)) - 2500 \cdot \mathsf{D}_i(\textsc{Mid}(i))) \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Mid}(i)) + \ell^*_{i+1} \cdot \mathsf{G}_i(\textsc{Mid}(i)) && \text{(Lemma 6.24)} \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Mid}(i)) + \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{i+1}|\right) && \text{(Definition of } \mathsf{G}(\cdot)) \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Mid}(i)) + \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right). && \text{(Lemma 6.10)}
\end{aligned}$$

By Lemma 6.9, we have $\textsc{Mid}(i) \in \textsc{Starts}_{\mathrm{B}}$ and $\textsc{Stop}(\textsc{Mid}(i)) = \textsc{Stop}(i)$. Furthermore, as i is indirect, we have that $|\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{\textsc{Mid}(i)+1}| = |\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{i+1}| - 1$ is even, and thus $\textsc{Stop}(i)$ is good for $\textsc{Mid}(i)$. Applying Lemma 6.18 on $\textsc{Mid}(i)$ and $\textsc{Stop}(i)$ (note that $\textsc{Mid}(i) > i \implies \textsc{Stop}(i) - \textsc{Mid}(i) < D$), we get

$$\begin{aligned}
\sum_{i'=\textsc{Mid}(i)+1}^{\textsc{Stop}(i)} \ell^*_{i'} &\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + \mathsf{extra}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + 3 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\quad - 2 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + 3 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\quad - 2 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) - \ell^*_{\textsc{Mid}(i)+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)) \\
&\quad + \frac{1}{30} \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Prev}(\textsc{Mid}(i))+1}|\right) && \text{(Definition of } \mathsf{extra}(\cdot)) \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + 3 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\quad - 2 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) - \ell^*_{\textsc{Mid}(i)+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)) \\
&\quad + \frac{1}{30} \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{i+1}|\right) && \text{(Lemma 6.9)} \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + 3 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\quad - \frac{59}{30} \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) - \ell^*_{\textsc{Mid}(i)+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)) \\
&&& \text{(Lemma 6.10)}
\end{aligned}$$

$$
\begin{aligned}
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + 3.3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\quad - \frac{649}{300} \cdot \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) - 1.1 \cdot \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Definition of } \ell^*\text{)} \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + \left(\frac{3}{1.1} + \frac{349}{600}\right) \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\quad - \frac{649}{300} \cdot \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) - 1.1 \cdot \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)) \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + \frac{3}{1.1} \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\quad - \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) - 1.1 \cdot \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Lemma 6.13)} \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + \frac{3}{1.1} \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\quad - \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)). \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Corollary 6.43)}
\end{aligned}
$$

Adding the two equations, we get:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(i)} \ell^*_{i'} &\le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Mid}(i)) + \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) \\
&\qquad + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + \frac{3}{1.1} \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) \\
&\qquad - \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Mid}(i)+1}| - |\pi_{\textsc{Stop}(i)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)) \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Mid}(i)) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) \\
&\qquad + \frac{3}{1.1} \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(i)}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i)),
\end{aligned}
$$

as desired. □

Proof of Lemma 6.20. Let $i \in \textsc{Starts}_{\mathrm{B}}$ be indirect and satisfy $\textsc{Stop}(i) - i = D$. By definition of $\textsc{Mid}(\cdot)$, we have $|\mathscr{R}_{\textsc{Mid}(i)}| = |\mathscr{R}_{i+1}|$ and therefore $\textsc{Mid}(i)$ is good for i. Furthermore, as i is indirect, we have $|\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{i+1}|$ is odd implying that $\textsc{Mid}(i) < \textsc{Stop}(i)$, which in turn means that $\textsc{Mid}(i) - i < D$. By the induction hypothesis, Lemma 6.18 holds for $i, \textsc{Mid}(i)$ and we have:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Mid}(i)} \ell^*_{i'} &\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Mid}(i)) + \mathsf{extra}_i(\textsc{Mid}(i)) + 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Mid}(i)}| + 1\right) \\
&\qquad - 2 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right) - \ell^*_{i+1} \cdot \mathbb{1}\left(\textsc{Mid}(i) \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(\textsc{Mid}(i)) \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Mid}(i)) + \mathsf{extra}_i(\textsc{Mid}(i)) + 4 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right) \\
&\qquad - \ell^*_{i+1} \cdot \mathbb{1}\left(\textsc{Mid}(i) \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(\textsc{Mid}(i)) \qquad \text{(Lemma 6.13)} \\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Mid}(i)) + \mathsf{extra}_i(\textsc{Mid}(i)) + 4 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right)
\end{aligned}
$$

$$
\begin{aligned}
&\quad - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\textsc{Mid}(i)) && \text{(Lemma 6.9)}\\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Mid}(i)) + 35 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(10, \textsc{Mid}(i))\\
&\quad + 4 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\textsc{Mid}(i)) && \text{(Definition of } \mathsf{extra}(\cdot))\\
&\le 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Mid}(i)) + 39 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\textsc{Mid}(i)).\\
& && \text{(Corollary 6.43)}
\end{aligned}
$$

By Lemma 6.9, we have $\textsc{Mid}(i) \in \textsc{Starts}_{\mathrm{F}}$ and $\textsc{Stop}(\textsc{Mid}(i)) = \textsc{Stop}(i)$. Furthermore, as i is indirect, we have $|\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{\textsc{Mid}(i)+1}| = |\mathscr{R}_{\textsc{Stop}(i)}| - |\mathscr{R}_{i+1}| - 1$ is even, and thus $\textsc{Stop}(i)$ is good for $\textsc{Mid}(i)$. Applying Lemma 6.17 on $\textsc{Mid}(i)$ and $\textsc{Stop}(i)$ (note that $\textsc{Mid}(i) > i \implies \textsc{Stop}(i) - \textsc{Mid}(i) < D$), we get

$$
\begin{aligned}
&\sum_{i'=\textsc{Mid}(i)+1}^{\textsc{Stop}(i)} \ell^*_{i'}\\
&\quad \le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i),\mathsf{depth}(\textsc{Mid}(i))}(\textsc{Stop}(i))\\
&\qquad + \ell^*_{\textsc{Mid}(i)+1} \cdot \left(\mathsf{G}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + 150\mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right)\\
&\qquad + \ell^*_{\textsc{Mid}(i)+1} \cdot \left(\mathsf{G}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + \mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right)\\
&\qquad - 2500 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \mathsf{spare}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\\
&\quad \le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i),\mathsf{depth}(\textsc{Mid}(i))}(\textsc{Stop}(i))\\
&\qquad + \ell^*_{\textsc{Mid}(i)+1} \cdot \left(150\mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right)\\
&\qquad + 2 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(\mathsf{G}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) + \mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right)\\
&\qquad - 2500 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \mathsf{spare}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\\
&\quad \le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i),\mathsf{depth}(\textsc{Mid}(i))}(\textsc{Stop}(i)) + 2 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\pi_{\textsc{Stop}(i)+1}| - |\pi_{\textsc{Mid}(i)+1}|\right)\\
&\qquad + \ell^*_{\textsc{Mid}(i)+1} \cdot \left(150\mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right)\\
&\qquad - 2500 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \mathsf{spare}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) && \text{(Definition of } \mathsf{G}(\cdot) \text{ and } \mathsf{B}(\cdot))\\
&\quad \le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i),\mathsf{depth}(\textsc{Mid}(i))}(\textsc{Stop}(i)) + 4 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right)\\
&\qquad + \ell^*_{\textsc{Mid}(i)+1} \cdot \left(150\mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right)\\
&\qquad - 2500 \cdot \ell^*_{\textsc{Mid}(i)+1} \cdot \mathsf{spare}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) && \text{(Lemma 6.16)}\\
&\quad \le 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i),\mathsf{depth}(\textsc{Mid}(i))}(\textsc{Stop}(i)) + 5 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right)\\
&\qquad + \ell^*_{\textsc{Mid}(i)+1} \cdot \left(150\mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right)\\
&\qquad - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(i)}(\textsc{Stop}(i)). && \text{(Definition of } \ell^*)
\end{aligned}
$$

Adding the two equations, we get:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(i)} \ell^*_{i'} \le{}& 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Mid}(i)) + 39 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\textsc{Mid}(i))\\
&+ 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i),\mathsf{depth}(\textsc{Mid}(i))}(\textsc{Stop}(i)) + 5 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right)
\end{aligned}
$$

$$
\begin{aligned}
&\quad + \ell^*_{\textsc{Mid}(i)+1} \cdot \left(150\mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right) \\
&\quad - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) \\
&\leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Mid}(i)) + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(i),\mathsf{depth}(\textsc{Mid}(i))}(\textsc{Stop}(i)) \\
&\quad + \ell^*_{\textsc{Mid}(i)+1} \cdot \left(150\mathsf{B}_{\textsc{Mid}(i)}(\textsc{Stop}(i)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(i)}(\textsc{Stop}(i))\right) \\
&\quad + 44 \cdot \ell^*_{i+1} \cdot \left(|\pi_{i+1}| - |\pi_{\textsc{Mid}(i)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\textsc{Mid}(i)) \\
&\quad - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(i)}(\textsc{Stop}(i)),
\end{aligned}
$$

as desired. □

We now show that Lemma 6.17 and Lemma 6.18 hold if $j - i = D$ (under the induction hypothesis).

Proof of Lemma 6.17. Let $i \in \textsc{Starts}_{\mathrm{F}}$ and $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ be such that j is good for i and $j - i = D$. Recall that $D > 0$ and therefore, we have $j > i$ implying by the definition of good that $|\mathscr{R}_j|$ is odd. Define $j_1 \in [i : j)$ to be the largest such that j_1 is good for i. Observe that j_1 is well defined as i is good for i. Also, note that $j_1 - i < j - i = D$. If $j_1 = j - 1$, we have by Lemma 6.17 on i, j_1 that:

$$
\begin{aligned}
\sum_{i'=i+1}^{j} \ell^*_{i'} &= \sum_{i'=i+1}^{j_1} \ell^*_{i'} + \ell^*_j \\
&\leq \ell^*_j + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j_1) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(j_1)) \\
&\quad - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) \\
&\leq \ell^*_j + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(j)) \\
&\quad - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j) && \text{(Lemma 6.25)} \\
&\leq \ell^*_{i+1} + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(j)) \\
&\quad - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j),
\end{aligned}
$$

as the fact that both $j - 1$ and j are good for i implies that $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ in turn implying that $\ell^*_j = \ell^*_{i+1}$. Now, as $|\mathscr{R}_j|$ is odd, we have by item 5 of Fact 6.5 that $\pi^C_{j+1} = \pi^C_j \| \sigma^C_j$ for all $C \in \{A, B\}$. By definition of $\mathsf{B}(\cdot)$, this means that $\mathsf{B}_i(j) \geq \mathsf{B}_i(j-1) = \mathsf{B}_i(j_1)$. Also, by definition of $\mathsf{G}(\cdot)$ and $\mathsf{B}(\cdot)$, we have

$$
\begin{aligned}
1 + \mathsf{G}_i(j_1) + \mathsf{B}_i(j_1) &\leq 1 + |\pi_{j_1+1}| - |\pi_{i+1}| \\
&\leq 1 + |\pi_j| - |\pi_{i+1}| && \text{(As } j_1 = j - 1\text{)} \\
&\leq |\pi_{j+1}| - |\pi_{i+1}| && \text{(As } |\mathscr{R}_j| \text{ is odd and Fact 6.5, item 5)} \\
&\leq \mathsf{G}_i(j) + \mathsf{B}_i(j). && \text{(Definition of } \mathsf{G}(\cdot) \text{ and } \mathsf{B}(\cdot)\text{)}
\end{aligned}
$$

Plugging this in and using $\mathsf{B}_i(j) \geq \mathsf{B}_i(j_1)$, we get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j) + 150\mathsf{B}_i(j) - 2500 \cdot \mathsf{D}_i(j)) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j).$$

The remainder of this proof deals with the case $j_1 < j - 1$. In this case, by our choice of j_1 we have that $j_1 + 1 < j$ is not good for i implying that $|\mathscr{R}_{j_1+1}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{j_1}|$ (we have $|\mathscr{R}_{j_1+1}| > |\mathscr{R}_{i+1}|$ due to item 3 of Fact 6.5) implying that $j_1 \in \mathfrak{E}(70) \subseteq \textsc{Starts}_{\mathrm{B}}$ by item 2 of Fact 6.5. As $j_1 < j \leq \textsc{Stop}(i)$, we have by Lemma 6.7 that $\textsc{Stop}(j_1) \leq \textsc{Stop}(i)$. We claim that:

Claim 6.67. *Either $j = \textsc{Stop}(j_1) + 1$ and $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ or $j = \textsc{Stop}(j_1) = \textsc{Stop}(i)$ and $|\mathscr{R}_j| > |\mathscr{R}_{i+1}|$. In either case, we have that j_1 is indirect.*

Proof. As $\textsc{Stop}(j_1) \leq \textsc{Stop}(i)$, we have the following two cases:

- **When $\textsc{Stop}(j_1) < \textsc{Stop}(i)$:** In this case, we first use Lemma 6.12 to get that $|\mathscr{R}_{\textsc{Stop}(j_1)+1}| = |\mathscr{R}_{i+1}|$ and j_1 is indirect. Observe that the claim follows if we show that $j = \textsc{Stop}(j_1) + 1$. Indeed, $j \leq \textsc{Stop}(j_1) + 1$ as otherwise $|\mathscr{R}_{\textsc{Stop}(j_1)+1}| = |\mathscr{R}_{i+1}|$ implies that $\textsc{Stop}(j_1) + 1 < j$ is good for i contradicting the choice of j_1. Also $j \geq \textsc{Stop}(j_1) + 1$, as either $j = \textsc{Stop}(i) > \textsc{Stop}(j_1)$ or by the definition of good, we have $|\mathscr{R}_j| = |\mathscr{R}_{i+1}| < |\mathscr{R}_{j_1+1}|$ implying that $j \geq \textsc{Stop}(j_1) + 1$ by the definition of $\textsc{Stop}(\cdot)$.
- **When $\textsc{Stop}(j_1) = \textsc{Stop}(i)$:** As $j_1 < j \leq \textsc{Stop}(i) = \textsc{Stop}(j_1)$, we have that $j \in \textsc{Range}(j_1)$ and therefore, using item 3 of Fact 6.5 and the fact that j is good for i, we have that $j = \textsc{Stop}(i)$ and $|\mathscr{R}_j| \geq |\mathscr{R}_{j_1+1}| > |\mathscr{R}_{i+1}|$. Using the fact that $j = \textsc{Stop}(i)$ is good for i, we have by Lemma 6.12 that j_1 is indirect.

□

As $\textsc{Stop}(j_1) \in \{j - 1, j\}$ and j_1 is indirect, we derive:

$$\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} &= \sum_{i'=i+1}^{j_1} \ell^*_{i'} + \sum_{i'=j_1+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \\
&\leq 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j_1) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(j_1)) \\
&\quad - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) + \sum_{i'=j_1+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \\
&\qquad\qquad \text{(Induction hypothesis and } j_1 < j \leq \textsc{Stop}(i)) \\
&\leq 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j_1) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(j_1)) \\
&\quad + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{j_1}(\textsc{Mid}(j_1)) + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(j_1),\mathsf{depth}(\textsc{Mid}(j_1))}(\textsc{Stop}(j_1))
\end{aligned}$$

$$
\begin{aligned}
&+ \ell^*_{\textsc{Mid}(j_1)+1} \cdot \left(150 \cdot \mathsf{B}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\right)\\
&+ 44 \cdot \ell^*_{j_1+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{j_1+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1))\\
&- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) - 2500 \cdot \ell^*_{j_1+1} \cdot \mathsf{spare}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)).
\end{aligned}
$$

(Induction hypothesis)

We continue using the definition of ℓ^* which implies that $\ell^*_{j_1+1} = 1.1 \cdot \ell^*_{i+1}$ and $\ell^*_{\textsc{Mid}(j_1)+1} = 1.1^2 \cdot \ell^*_{i+1}$. This gives:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j_1) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(j_1))\\
&+ 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{j_1}(\textsc{Mid}(j_1)) + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(j_1),\mathsf{depth}(\textsc{Mid}(j_1))}(\textsc{Stop}(j_1))\\
&+ \ell^*_{i+1} \cdot \left(200 \cdot \mathsf{B}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)) - 3025 \cdot \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\right)\\
&+ 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1))\\
&- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)).
\end{aligned}
$$

Next, we upper bound the term $10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(j_1),\mathsf{depth}(\textsc{Mid}(j_1))}(\textsc{Stop}(j_1))$ using Lemma 6.27 on $i, \textsc{Mid}(j_1)$. Observe that Lemma 6.27 is applicable due to the guarantees form Lemma 6.9. As the right hand side in Lemma 6.27 is always non-negative and $\ell^*_{\textsc{Mid}(j_1)+1} > \ell^*_{i+1}$, we get:

$$
\begin{aligned}
&10^4 \left(\mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(j_1),\mathsf{depth}(i)}(\textsc{Stop}(j_1)) - \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(j_1),\mathsf{depth}(\textsc{Mid}(j_1))}(\textsc{Stop}(j_1))\right)\\
&\quad \geq 5000 \cdot \ell^*_{i+1} \cdot \max\left(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1)) - \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\right)\\
&\quad \geq 2750 \cdot \ell^*_{i+1} \cdot \max\left(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1)) - \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\right)\\
&\quad \geq 2500 \cdot \ell^*_{i+1} \cdot \left(\mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1)) - \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\right)\\
&\qquad + 250 \cdot \ell^*_{i+1} \cdot \max\left(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1)) - \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\right)\\
&\quad \geq 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) - 2750 \cdot \ell^*_{i+1} \cdot \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\\
&\qquad + 250 \cdot \ell^*_{i+1} \cdot \max\left(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))\right).
\end{aligned}
$$

Using this inequality, we continue as:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j_1) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(j_1))\\
&+ 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{j_1}(\textsc{Mid}(j_1)) + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(j_1),\mathsf{depth}(i)}(\textsc{Stop}(j_1))\\
&- 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) + 2750 \cdot \ell^*_{i+1} \cdot \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\\
&- 250 \cdot \ell^*_{i+1} \cdot \max\left(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))\right)\\
&+ \ell^*_{i+1} \cdot \left(200 \cdot \mathsf{B}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)) - 3025 \cdot \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\right)\\
&+ 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1))\\
&- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)).
\end{aligned}
$$

We continue by bounding $\mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j_1) + \cdot \mathsf{E}^{\mathrm{B}}_{j_1}(\textsc{Mid}(j_1)) + \mathsf{E}^{\mathrm{F}}_{\textsc{Mid}(j_1),\mathsf{depth}(i)}(\textsc{Stop}(j_1))$ using

Lemma 6.30.

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \le\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(j_1)) \\ & - 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) + 2750 \cdot \ell^*_{i+1} \cdot \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)) \\ & - 250 \cdot \ell^*_{i+1} \cdot \max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\ & + \ell^*_{i+1} \cdot \left(200 \cdot \mathsf{B}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)) - 3025 \cdot \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))\right) \\ & + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1)) \\ & - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)).\end{aligned}$$

Next, we upper bound $200 \cdot \mathsf{B}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))$ by $250 \cdot \mathsf{D}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))$ using Lemma 6.24 and simplify. We also swap the terms $\mathsf{D}_i(j_1)$ and $\mathsf{D}_i(\textsc{Stop}(j_1))$.

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \le\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & - 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\ & - 250 \cdot \ell^*_{i+1} \cdot \max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\ & + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1)) \\ & - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)).\end{aligned}$$

We now consider two cases based on the cases in Lemma 6.60.

- **When $\mathsf{G}_i(j_1) < |\pi_{\textsc{Mid}(j_1)+1}| - |\pi_{i+1}|$:** In this case, Lemma 6.60 says that $\mathsf{G}_i(j_1) = \mathsf{G}_i(\textsc{Stop}(j_1))$ and $\mathsf{B}_i(\textsc{Stop}(j_1)) = \mathsf{B}_i(j_1) + |\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{j_1+1}|$. Plugging these in, we get:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \le\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) - 150 \cdot \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{j_1+1}|\right) \\ & + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & - 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\ & - 250 \cdot \ell^*_{i+1} \cdot \max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\ & + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1)) \\ & - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)).\end{aligned}$$

  Using the fact that $\mathsf{spare}(\cdot)$ and $\mathsf{tax}_1(\cdot)$ are non-negative, we have:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \le\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) - 150 \cdot \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{j_1+1}|\right) \\ & + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1)))\end{aligned}$$

$$
\begin{aligned}
&- 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\
&- 250 \cdot \ell^*_{i+1} \cdot \max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\
&+ 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1).
\end{aligned}
$$

Considering two sub-cases based on Claim 6.67, we get

– **When $j = \textsc{Stop}(j_1) + 1$ and $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$:** In this case, the "furthermore" part of Lemma 6.16 gives $|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{j_1+1}| = |\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|$ and we can simplify as:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
&+ \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
&- 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\
&- 250 \cdot \ell^*_{i+1} \cdot \max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\
&- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1).
\end{aligned}
$$

Finally, we note that the term $\max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1)))$ is non-negative and upper bound $\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1)) + \mathsf{spare}_i(j_1)$ by 1 using Lemma 6.60 to get:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
&+ \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
&- 2500 \cdot \ell^*_{i+1}.
\end{aligned} \tag{42}
$$

– **When $j = \textsc{Stop}(j_1) = \textsc{Stop}(i)$ and $|\mathscr{R}_j| > |\mathscr{R}_{i+1}|$:** In this case, we first assume that $50 \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) \leq |\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|$ and derive:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) - 150 \cdot \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{j_1+1}|\right) \\
&+ \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
&- 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\
&- 250 \cdot \ell^*_{i+1} \cdot \max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\
&+ \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1).
\end{aligned}
$$

Now, note that the terms $\max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1)))$ and $|\pi_{\textsc{Stop}(j_1)+1}| -$

$|\pi_{j_1+1}|$ are non-negative (using Lemma 6.16 for the latter). This gives:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\ & + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & - 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\ & + \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1).\end{aligned}$$

We upper bound $\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1)) + \mathsf{spare}_i(j_1)$ by 1 using Lemma 6.60 as in the previous case to get:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\ & + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & + \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right) - 2500 \cdot \ell^*_{i+1}.\end{aligned} \tag{43}$$

If our assumption does not hold, then we have $50 \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) > |\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|$. We first use the fact that the terms $\mathsf{spare}_i(j_1)$ and $|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{j_1+1}|$ are non-negative (using Lemma 6.16 for the latter) and $\max(0, \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) \geq \mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))$ to get:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\ & + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & - 2500 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\ & - 250 \cdot \ell^*_{i+1} \cdot (\mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))) \\ & + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right).\end{aligned} \tag{44}$$

To continue, we derive:

$$\begin{aligned}\mathsf{D}_i(j_1) - \mathsf{D}_i(\textsc{Mid}(j_1)) &\geq \left(1 - 10^{-5}\right) \cdot \mathsf{B}_i(j_1) - \mathsf{B}_i(\textsc{Mid}(j_1)) && \text{(Lemma 6.24)} \\ &\geq \mathsf{B}_i(j_1) - \mathsf{B}_i(\textsc{Mid}(j_1)) - 10^{-5} \cdot (|\pi_{j_1+1}| - |\pi_{i+1}|) \\ & && \text{(Definition of } \mathsf{B}(\cdot)) \\ &\geq \mathsf{B}_i(j_1) - \mathsf{B}_i(\textsc{Mid}(j_1)) - 10^{-5} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right). \\ & && \text{(Lemma 6.16)}\end{aligned}$$

Similarly, we also have:

$$\mathsf{D}_i(\textsc{Stop}(j_1)) - \mathsf{D}_i(\textsc{Mid}(j_1))$$

$$
\begin{aligned}
&\geq \left(1 - 10^{-5}\right) \cdot \mathsf{B}_i(\textsc{Stop}(j_1)) - \mathsf{B}_i(\textsc{Mid}(j_1)) && \text{(Lemma 6.24)}\\
&\geq \mathsf{B}_i(\textsc{Stop}(j_1)) - \mathsf{B}_i(\textsc{Mid}(j_1)) - 10^{-5} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right) \\
& && \text{(Definition of } \mathsf{B}(\cdot)\text{)}\\
&\geq \mathsf{B}_i(j_1) + |\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{j_1+1}| - \mathsf{B}_i(\textsc{Mid}(j_1)) \\
&\qquad - 10^{-5} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right) && \text{(Lemma 6.60)}\\
&\geq \mathsf{B}_i(j_1) - \mathsf{B}_i(\textsc{Mid}(j_1)) - 10^{-5} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right). && \text{(Lemma 6.16)}
\end{aligned}
$$

Plugging these two into Equation 44, we get:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
& + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
& - 2750 \cdot \ell^*_{i+1} \cdot \left(\mathsf{B}_i(j_1) - \mathsf{B}_i(\textsc{Mid}(j_1)) - 10^{-5} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right)\right) \\
& + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right).
\end{aligned}
$$

Due to Lemma 6.60, we have that $\mathsf{B}_i(j_1) - \mathsf{B}_i(\textsc{Mid}(j_1)) = |\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|$. Plugging in, we get:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
& + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
& - 2750 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}| - 10^{-5} \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right)\right) \\
& + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right).
\end{aligned}
$$

Now, we use our assumption that $|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}| < 50 \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right)$ and simplify:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
& + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
& - 2500 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right).
\end{aligned}
$$

Finally, we use Lemma 6.13 to conclude:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
& + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
& - 2500 \cdot \ell^*_{i+1}.
\end{aligned} \tag{45}
$$

- **When $\mathsf{G}_i(j_1) \geq |\pi_{\textsc{Mid}(j_1)+1}| - |\pi_{i+1}|$:** In this case, Lemma 6.60 says that $\mathsf{D}_i(\textsc{Mid}(j_1)) = 0$ and $\mathsf{spare}_i(\textsc{Stop}(j_1)) \leq \mathsf{spare}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))$. Plugging these in, we get:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{D}_i(j_1) \\ & - 250 \cdot \ell^*_{i+1} \cdot \max(0, \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1)) \\ & - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j_1) - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(\textsc{Stop}(j_1)).\end{aligned}$$

  Now, note that the terms $\max(0, \mathsf{D}_i(\textsc{Stop}(j_1)))$ and $\mathsf{spare}_i(j_1)$ are non-negative. Therefore, we have:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) + 150\mathsf{B}_i(j_1) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{D}_i(j_1) \\ & + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1)) \\ & - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(\textsc{Stop}(j_1)).\end{aligned}$$

  Next, we use Lemma 6.24 to bound $2500\mathsf{D}_i(j_1) \geq 1150 \cdot \mathsf{B}_i(j_1)$. Putting this in, and simplifying, we get:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j_1) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\ & - 1000 \cdot \ell^*_{i+1} \cdot \mathsf{B}_i(j_1) \\ & + 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1)) \\ & - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(\textsc{Stop}(j_1)).\end{aligned}$$

  To continue, we note from the definition of $\mathsf{G}(\cdot)$ that

$$\begin{aligned}\mathsf{G}_i(j_1) &\leq |\pi_{j_1+1}| - |\pi_{i+1}| \\ &\leq |\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}| && \text{(Lemma 6.16)} \\ &\leq \mathsf{G}_i(\textsc{Stop}(j_1)) + \mathsf{B}_i(\textsc{Stop}(j_1)) && \text{(Definition of } \mathsf{G}(\cdot) \text{ and } \mathsf{B}(\cdot)) \\ &\leq \mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)). && \text{(As } \mathsf{B}(\cdot) \geq 0)\end{aligned}$$

  Plugging in, we get:

$$\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1))$$

$$
\begin{aligned}
&+ \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
&- 1000 \cdot \ell^*_{i+1} \cdot \mathsf{B}_i(j_1) \\
&+ 50 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1)) \\
&- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(\textsc{Stop}(j_1)).
\end{aligned}
$$

Finally, Lemma 6.59 says that $50 \cdot \left(|\pi_{j_1+1}| - |\pi_{\textsc{Mid}(j_1)+1}|\right) \leq \mathsf{tax}_{1,j_1}(\textsc{Mid}(j_1)) + 1000 \cdot \mathsf{B}_i(j_1)$. This gives us:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
&+ \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
&- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(\textsc{Stop}(j_1)).
\end{aligned} \tag{46}
$$

Observe that the inequalities showed in Equation 42, Equation 43, Equation 45, and Equation 46 in the cases considered above can be summarized as:

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
&+ \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
&+ \ell^*_{i+1} \cdot \mathbb{1}\left(\textsc{Stop}(j_1) = \textsc{Stop}(i) \wedge |\mathscr{R}_{\textsc{Stop}(j_1)}| \neq |\mathscr{R}_{i+1}|\right) \cdot \left(|\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|\right) \\
&- 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(\textsc{Stop}(j_1)).
\end{aligned} \tag{47}
$$

We again consider the two sub-cases given by Claim 6.67.

- **When $j = \textsc{Stop}(j_1) + 1$ and $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$:** In this case, we have

$$
\begin{aligned}
\sum_{i'=i+1}^{j} \ell^*_{i'} &\leq \sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} + \ell^*_j && (\text{As } j = \textsc{Stop}(j_1) + 1) \\
&\leq \ell^*_{i+1} + \sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} && (\text{As } |\mathscr{R}_j| = |\mathscr{R}_{i+1}|) \\
&\leq \ell^*_{i+1} + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) \\
&\quad + \ell^*_{i+1} \cdot (\mathsf{G}_i(\textsc{Stop}(j_1)) + 150\mathsf{B}_i(\textsc{Stop}(j_1)) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
&\quad - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(\textsc{Stop}(j_1)). && (\text{Equation 47})
\end{aligned}
$$

Now, as $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ is odd, we have by item 5 of Fact 6.5 that $\pi^C_{j+1} = \pi^C_j \| \sigma^C_j$ for all $C \in \{A, B\}$. By definition of $\mathsf{B}(\cdot)$, this means that $\mathsf{B}_i(j) \geq \mathsf{B}_i(j-1) = \mathsf{B}_i(\textsc{Stop}(j_1))$. Also, by definition of $\mathsf{G}(\cdot)$ and $\mathsf{B}(\cdot)$, we have

$$
1 + \mathsf{G}_i(\textsc{Stop}(j_1)) + \mathsf{B}_i(\textsc{Stop}(j_1)) = 1 + |\pi_{\textsc{Stop}(j_1)+1}| - |\pi_{i+1}|
$$

$$
\begin{aligned}
&= 1 + |\pi_j| - |\pi_{i+1}| && \text{(As } j = \textsc{Stop}(j_1) + 1\text{)} \\
&= |\pi_{j+1}| - |\pi_{i+1}| \\
&= \mathsf{G}_i(j) + \mathsf{B}_i(j).
\end{aligned}
$$

Plugging this in and using $\mathsf{B}_i(j) \geq \mathsf{B}_i(\textsc{Stop}(j_1))$, we get:

$$
\begin{aligned}
\sum_{i'=i+1}^{j} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(\textsc{Stop}(j_1)) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j) + 150\mathsf{B}_i(j) - 2500 \cdot \mathsf{D}_i(\textsc{Stop}(j_1))) \\
& - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(\textsc{Stop}(j_1)).
\end{aligned}
$$

To finish, we use the fact that $j = \textsc{Stop}(j_1) + 1$ and apply Lemma 6.25. This gives:

$$
\begin{aligned}
\sum_{i'=i+1}^{j} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j) + 150\mathsf{B}_i(j) - 2500 \cdot \mathsf{D}_i(j)) \\
& - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j).
\end{aligned}
$$

- **When $j = \textsc{Stop}(j_1) = \textsc{Stop}(i)$ and $|\mathscr{R}_j| > |\mathscr{R}_{i+1}|$:** In this case, we simply substitute $j = \textsc{Stop}(j_1)$ in Equation 47 to get:

$$
\begin{aligned}
\sum_{i'=i+1}^{j} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i,\mathsf{depth}(i)}(j) + \ell^*_{i+1} \cdot (\mathsf{G}_i(j) + 150\mathsf{B}_i(j) - 2500 \cdot \mathsf{D}_i(j)) \\
& + \ell^*_{i+1} \cdot \mathbb{1}\left(j = \textsc{Stop}(i) \wedge |\mathscr{R}_j| \neq |\mathscr{R}_{i+1}|\right) \cdot (|\pi_{j+1}| - |\pi_{i+1}|) \\
& - 2500 \cdot \ell^*_{i+1} \cdot \mathsf{spare}_i(j).
\end{aligned}
$$

Lemma 6.17 follows by observing that $|\pi_{j+1}| - |\pi_{i+1}| = \mathsf{G}_i(j) + \mathsf{B}_i(j)$ by definition.

□

Proof of Lemma 6.18. Let $i \in \textsc{Starts}_{\mathrm{B}}$ and all $j \in \{i\} \cup \textsc{Range}(i) \setminus \{num\}$ be such that j is good for i and $j - i = D$. Recall that $D > 0$ and therefore, we have $j > i$ implying by the definition of good that $|\mathscr{R}_j|$ is even. This proof is divided into two parts. In both parts, we make use of the following claim:

Claim 6.68. *Let $j_1 \in (i : j) \cap \mathfrak{E}(80)$ be indirect and satisfy $|\mathscr{R}_{j_1}| = |\mathscr{R}_{i+1}|$ and $\textsc{Stop}(j_1) \leq j$. We have:*

$$
\begin{aligned}
\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq\ & 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Stop}(j_1)) + \mathsf{extra}_i(225, 225, \textsc{Stop}(j_1)) + 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_1)}| + 1\right) \\
& - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{\textsc{Stop}(j_1)+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\textsc{Stop}(j_1)).
\end{aligned}
$$

Proof. We derive:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} &\leq \sum_{i'=i+1}^{j_1} \ell^*_{i'} + \sum_{i'=j_1+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \\ &\leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_{j_1}| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) \\ &\quad - \ell^*_{i+1} \cdot \mathbb{1}\left(j_1 \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(j_1) + \sum_{i'=j_1+1}^{\textsc{Stop}(j_1)} \ell^*_{i'}. \qquad \text{(Induction hypothesis)}\end{aligned}$$

Due to the fact that $j_1 \in \mathfrak{E}(80)$ and the induction hypothesis, we have:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} &\leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_{j_1}| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) \\ &\quad - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j_1) + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{j_1,\mathsf{depth}(j_1)}(\textsc{Mid}(j_1)) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)) \\ &\quad + \frac{3}{1.1} \cdot \ell^*_{j_1+1} \cdot \left(|\psi_{\textsc{Stop}(j_1)}| + 1\right) - \ell^*_{j_1+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_1)).\end{aligned}$$

We continue using the definition of ℓ^* which implies that $\ell^*_{j_1+1} = 1.1 \cdot \ell^*_{i+1}$. Due to Corollary 6.43, this gives:

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} &\leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_{j_1}| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) \\ &\quad - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j_1) + 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{j_1,\mathsf{depth}(j_1)}(\textsc{Mid}(j_1)) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1)) \\ &\quad + 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_1)}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_1)).\end{aligned}$$

We continue by bounding $\mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{E}^{\mathrm{F}}_{j_1,\mathsf{depth}(j_1)}(\textsc{Mid}(j_1)) + \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(j_1)}(\textsc{Stop}(j_1))$ using Lemma 6.34.

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} &\leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Stop}(j_1)) + \mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_{j_1}| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) \\ &\quad - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j_1) + 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_1)}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_1)).\end{aligned}$$

Now, we upper bound the terms $\mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_{j_1}| + 1)$ by an application of Lemma 6.65.

$$\begin{aligned}\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} &\leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Stop}(j_1)) + \mathsf{extra}_i(225, 225, \textsc{Stop}(j_1)) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) \\ &\quad - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j_1) + 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_1)}| + 1\right).\end{aligned}$$

Finally, we use Lemma 6.10 to get that $|\pi_{j_1+1}| = |\pi_{\textsc{Stop}(j_1)+1}|$. As $\mathsf{tax}_{1,i}(j_1)$ is only a function

of i and $|\pi_{j_1+1}|$, we also have that $\mathsf{tax}_{1,i}(j_1) = \mathsf{tax}_{1,i}(\textsc{Stop}(j_1))$. This gives:

$$\sum_{i'=i+1}^{\textsc{Stop}(j_1)} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(\textsc{Stop}(j_1)) + \mathsf{extra}_i(225, 225, \textsc{Stop}(j_1)) + 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_1)}| + 1\right)$$
$$- 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{\textsc{Stop}(j_1)+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\textsc{Stop}(j_1)).$$

□

We now state the first part of our proof, where we show Lemma 6.18 in the case that $\mathbb{1}\left(j \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(j) > 0$. Later, we show Lemma 6.18 in the case $\mathbb{1}\left(j \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(j) = 0$.

When $\mathbb{1}\left(j \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(j) > 0$. In this case, we first claim that $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$. Indeed, if not, then as $j > i$ is good for i, we must have $j = \textsc{Stop}(i)$ implying by item 7 of Fact 6.5 that $j \in \mathfrak{E}(84) \cup \mathfrak{E}(73) \cup \mathfrak{E}(88)$. However, this means that $j \notin \mathfrak{E}(80)$, contradicting the fact that $\mathbb{1}\left(j \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(j) > 0$.

Define $j_1 \in [i : j)$ to be the largest such that $|\mathscr{R}_{j_1}| \neq |\mathscr{R}_{i+1}|$. We note that j_1 is well defined as $|\mathscr{R}_i| \neq |\mathscr{R}_{i+1}|$. Also, as we showed that $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$, we have for all $j' \in (j_1 : j]$ that

$$|\mathscr{R}_{j'}| = |\mathscr{R}_{i+1}|. \tag{48}$$

Next, we show that:

Claim 6.69. *If $j_1 > i$, then $j_1 = \textsc{Stop}(j_2)$ for some $j_2 \in (i : j_1) \cap \mathfrak{E}(80)$ that is indirect and satisfies $|\mathscr{R}_{j_2}| = |\mathscr{R}_{i+1}|$.*

Proof. Define $j_2 \in (i : j_1]$ to be the largest such that $|\mathscr{R}_{j_2}| = |\mathscr{R}_{i+1}|$. Observe that j_2 is well defined as $i + 1 \in (i : j_1]$ is one such value and that $j_2 < j_1$ by definition of j_1. As $j_2 < j_1$, we have $|\mathscr{R}_{j_2+1}| \neq |\mathscr{R}_{i+1}|$ by our choice of j_2. Combining with item 3 of Fact 6.5 (note that $j_2 + 1 \in \textsc{Range}(i)$ as $j_2 < j_1 < j$), we get that $|\mathscr{R}_{j_2+1}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{j_2}|$.

Due to item 2 of Fact 6.5, this is possible only if $j_2 \in \mathfrak{E}(80)$. We next show that $\textsc{Stop}(j_2) < j$. This is because, if not, then $j_2 < j_1 < j$ implies that $j \in \textsc{Range}(j_2)$ which, with item 3 of Fact 6.5, means that $|\mathscr{R}_j| \geq |\mathscr{R}_{j_2+1}| = |\mathscr{R}_{j_2}| + 1 = |\mathscr{R}_{i+1}| + 1$, contradicting Equation 48. As $\textsc{Stop}(j_2) < j \leq \textsc{Stop}(i)$, we have by Lemma 6.12 that j_2 is indirect and we have $|\mathscr{R}_{\textsc{Stop}(j_2)+1}| = |\mathscr{R}_{i+1}|$.

It remains to show that $j_1 = \textsc{Stop}(j_2)$. For this, note by our choice of j_2 that $|\mathscr{R}_{\textsc{Stop}(j_2)+1}| = |\mathscr{R}_{i+1}|$ is possible only if $j_1 \leq \textsc{Stop}(j_2)$. Furthermore, $j_1 \geq \textsc{Stop}(j_2)$, as otherwise, by Equation 48, we have that $|\mathscr{R}_{\textsc{Stop}(j_2)}| = |\mathscr{R}_{i+1}|$. This means that

$$|\mathscr{R}_{\textsc{Stop}(j_2)}| = |\mathscr{R}_{j_2}| < |\mathscr{R}_{j_2+1}|,$$

a contradiction to item 3 of Fact 6.5. □

Corollary 6.70. *If $j_1 > i$, then $|\mathscr{R}_{j_1}|$ is even and $j_1 \notin \textsc{Starts}$.*

Proof. Let j_2 be as promised by Claim 6.69. We have by Claim 6.69 that

$$\begin{aligned}
|\mathscr{R}_{j_1}| - |\mathscr{R}_{i+1}| &= |\mathscr{R}_{\textsc{Stop}(j_2)}| - |\mathscr{R}_{i+1}| && (\text{As } j_1 = \textsc{Stop}(j_2)) \\
&= |\mathscr{R}_{\textsc{Stop}(j_2)}| - |\mathscr{R}_{j_2}| && (\text{As } |\mathscr{R}_{j_2}| = |\mathscr{R}_{i+1}|) \\
&= |\mathscr{R}_{\textsc{Stop}(j_2)}| - |\mathscr{R}_{j_2+1}| + 1, && (\text{As } j_2 \in \mathfrak{E}(80))
\end{aligned}$$

is even as j_2 is indirect. As $i \in \textsc{Starts}_{\mathrm{B}}$, this implies that $|\mathscr{R}_{j_1}|$ is even. To see why $j_1 \notin \textsc{Starts}$, note simply that $|\mathscr{R}_{j_1}|$ and $|\mathscr{R}_{j_1+1}|$ are both even (the latter due to Equation 48 implying that $j_1 \notin \textsc{Starts}$. □

This allows us to claim that:

$$\begin{aligned}
\sum_{i'=i+1}^{j_1} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(225, 225, j_1) + 3 \cdot \ell^*_{i+1} \cdot \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1) \\
- 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j_1).
\end{aligned} \tag{49}$$

Indeed, either $j_1 = i$ and Equation 49 follows because all terms are 0, or $j_1 > i$, in which case, Equation 49 follows by applying Claim 6.68 on the value j_2 promised by Claim 6.69. We next show that:

Claim 6.71. *For all $j' \in (j_1 : j]$, we have $|\pi_{j'}| - |\pi_{j'+1}| = 1$ and*

$$|\psi_{j'}| + 1 - \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1) = j' - j_1.$$

Proof. For the first equation, we simply observe that $|\mathscr{R}_{j'}|$ is even (Equation 48) and apply item 5 of Fact 6.5. For the second equation, we proceed by induction. The base case is $j' = j_1 + 1$ which holds because either $j_1 = i$ and $|\psi_{j'}| = |\psi_{i+1}| = 0$ or $j_1 > i$ in which case, by Corollary 6.70 and item 5 of Fact 6.5, we have $|\psi_{j'}| + 1 - (|\psi_{j_1}| + 1) = 1 = j' - j_1$, as desired.

We now suppose the statement holds for $j' \in (j_1 : j)$ and show that it holds for $j' + 1$. By Equation 48, we have $|\mathscr{R}_{j'}|$ and $|\mathscr{R}_{j'+1}|$ are both even. This means that $j' \notin \textsc{Starts}$, which when combined with item 5 of Fact 6.5 yields

$$|\psi_{j'+1}| + 1 - \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1) = |\psi_{j'}| + 2 - \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1) = j' + 1 - j_1,$$

using the induction hypothesis, as desired. □

Corollary 6.72. *We have:*

$$\sum_{i'=j_1+1}^{j} \ell^*_{i'} = 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1 - \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1)) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{j_1+1}| - |\pi_{j+1}|)\,.$$

Proof. We simplify the right hand side using Claim 6.71. We get:

$$3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1 - \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1)) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{j_1+1}| - |\pi_{j+1}|)$$

$$= 3 \cdot \ell^*_{i+1} \cdot (j - j_1) - 2 \cdot \ell^*_{i+1} \cdot (j - j_1)$$
$$= \ell^*_{i+1} \cdot (j - j_1)\,.$$

By Equation 48 and the definition of ℓ^*, we have that $\sum_{i'=j_1+1}^{j} \ell^*_{i'} = \ell^*_{i+1} \cdot (j - j_1)$ finishing the proof. □

Adding Corollary 6.72 and Equation 49, we get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(225, 225, j_1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1)$$
$$- 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j_1).$$

Now, apply Lemma 6.41 to get (note that the condition in Lemma 6.41 is satisfied as $|\pi_{j_1+1}| - |\pi_{j+1}| = j - j_1 > 0$ by Claim 6.71):

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(225, 225, j_1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1)$$
$$- 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + 100\ell^*_{i+1} \cdot (|\pi_{j_1+1}| - |\pi_{j+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j). \tag{50}$$

We now show:

Claim 6.73. *For all $j' \in [j_1 : j)$, we have $\mathsf{turn}(j') \leq \mathsf{turn}(j' + 1)$.*

Proof. By Equation 48, we have that $|\mathscr{R}_{j'+1}|$ is even. Assume first that $|\mathscr{R}_{j'}|$ is also even. This means that $j' \notin$ Starts, which gives:

$$\begin{aligned}
\mathsf{turn}(j') &= \mathbb{1}\left(\psi^A_{j'} \| \sigma^A_{j'} \neq \psi^B_{j'} \| \sigma^B_{j'}\right) && \text{(Definition of } \mathsf{turn}(\cdot)\text{)} \\
&= \mathbb{1}\left(\psi^A_{j'+1} \neq \psi^B_{j'+1}\right) && \text{(Fact 6.5, item 5 and } j' \notin \textsc{Starts}\text{)} \\
&\leq \mathbb{1}\left(\psi^A_{j'+1} \| \sigma^A_{j'+1} \neq \psi^B_{j'+1} \| \sigma^B_{j'+1}\right) \\
&= \mathsf{turn}(j' + 1), && \text{(Definition of } \mathsf{turn}(\cdot)\text{)}
\end{aligned}$$

as desired. On the other hand, if $|\mathscr{R}_{j'}|$ is odd, then $j' = j_1$ as otherwise, we have contradiction to Equation 48. We claim that $j' = j_1$ and $|\mathscr{R}_{j'}|$ is odd can happen only if $j_1 = i$. Indeed, suppose that $j' = j_1 > i$, we have a contradiction to Corollary 6.70. However, $j' = j_1 = i$ means that $\mathsf{turn}(j') = \mathsf{turn}(i) = 0 \leq \mathsf{turn}(j' + 1)$ and we are done.

□

Owing to Claim 6.73, we have the following sub-cases:

- **When $\mathsf{turn}(j_1) = \mathsf{turn}(j)$:** In this case, Claim 6.73 says that $\mathsf{turn}(j') = \mathsf{turn}(j)$ for all $j' \in [j_1 : j]$. This together with Equation 48 means that we can apply Lemma 6.64 (on j_1, j with $z = 0.98$) to bound the term $10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(225, 225, j_1)$ in Equation 50.

We get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(225, 225, j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1)$$
$$- 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + 100 \cdot \ell^*_{i+1} \cdot (|\pi_{j_1+1}| - |\pi_{j+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j)$$
$$- 0.98 \cdot 225 \cdot \ell^*_j \cdot \sum_{j''=j_1+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0).$$

Simplifying using the observation that $0.98 \cdot 225 > 200$ and using Lemma 6.63, we get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|)$$
$$+ 100 \cdot \ell^*_{i+1} \cdot (|\pi_{j_1+1}| - |\pi_{j+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j)$$
$$- 200 \cdot \ell^*_j \cdot \sum_{j''=j_1+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0).$$

As $|\pi_{j_1+1}| - |\pi_{j+1}| = j - j_1$ by Claim 6.71 and $\ell^*_j = \ell^*_{i+1}$ by Equation 48, Lemma 6.18 now follows from the following claim:

Claim 6.74. $j - j_1 \leq 2 \cdot \sum_{j''=j_1+1}^{j} \mathbb{1}(\mathsf{turn}(j) = 1 \vee \mathscr{R}_{j''}.last.t > 0)$.

Proof. If $\mathsf{turn}(j) = 1$, there is nothing to show so suppose for contradiction that $\mathsf{turn}(j) = 0$ and $j - j_1 > 2 \cdot \sum_{j''=j_1+1}^{j} \mathbb{1}(\mathscr{R}_{j''}.last.t > 0)$. Let $j_3 \in (j_1 : j]$ be the smallest such that $\mathscr{R}_{j_3}.last.t > 0$. Observe that j_3 is well defined as $\mathscr{R}_j.last.t > 0$ due to the fact that $j \in \mathfrak{E}(80)$ and item 11 of Fact 6.5. By item 9 of Fact 6.5 (the conditions in item 9 of Fact 6.5 are satisfied due to Equation 48) we have that $(\mathscr{R}_{j'}.last.r, \mathscr{R}_{j'}.last.t) = (\mathscr{R}_j.last.r, \mathscr{R}_j.last.t)$ for all $j' \in [j_3 : j]$. In particular, this means that $\sum_{j''=j_1+1}^{j} \mathbb{1}(\mathscr{R}_{j''}.last.t > 0) \geq j - j_3 + 1$ and we get:

$$j - j_1 > 2 \cdot \sum_{j''=j_1+1}^{j} \mathbb{1}(\mathscr{R}_{j''}.last.t > 0) \geq 2 \cdot (j - j_3 + 1), \tag{51}$$

implying that $j_3 - 1 > \frac{j+j_1}{2} > j_1$. By our choice of j_3, this means that $\mathscr{R}_{j_3-1}.last.t = 0$ which, along with $\mathscr{R}_{j_3}.last.t > 0$ implies that $j_3 - 1 \in \mathfrak{E}(90)$, in turn implying that $\mathscr{R}_{j_3}.last.r - \mathscr{R}_{j_3}.last.t = |\psi_{j_3}|$. We derive:

$$\begin{aligned} |\psi_{j_3}| &= \mathscr{R}_{j_3}.last.r - \mathscr{R}_{j_3}.last.t \\ &= \mathscr{R}_j.last.r - \mathscr{R}_j.last.t && \text{(As } (\mathscr{R}_{j_3}.last.r, \mathscr{R}_{j_3}.last.t) = (\mathscr{R}_j.last.r, \mathscr{R}_j.last.t)\text{)} \\ &= \frac{|\psi_j| + 1}{2}. && \text{(As } j \in \mathfrak{E}(80)\text{)} \end{aligned}$$

In order to continue, we invoke Claim 6.71 to get $|\psi_j| + 1 \geq j - j_1$. This gives:

$$\begin{aligned}
|\psi_{j_3}| &\leq |\psi_j| + 1 - \frac{j - j_1}{2} \\
&< |\psi_j| + 1 - (j - j_3 + 1) && \text{(Equation 51)} \\
&\leq |\psi_j| + 1 - (|\psi_j| - |\psi_{j_3}| + 1) && \text{(Claim 6.71)} \\
&= |\psi_{j_3}|,
\end{aligned}$$

a contradiction. □

- **When $\mathsf{turn}(j_1) < \mathsf{turn}(j)$:** As $\mathsf{turn}(\cdot)$ takes values in $\{0, 1\}$, we have in this case that $\mathsf{turn}(j_1) = 0$ and $\mathsf{turn}(j) = 1$. We continue Equation 50 using Lemma 6.66.

$$\begin{aligned}
\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) \\
- \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j),
\end{aligned}$$

and Lemma 6.18 follows.

When $\mathbb{1}\left(j \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(j) = 0$. In this case, in order to show the lemma, we have to show that:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|). \tag{52}$$

We now show Equation 52 by considering the following sub-cases:

- **When $|\mathscr{R}_j| > |\mathscr{R}_{i+1}|$:** As j is good for i, this can only happen if $j = \textsc{Stop}(i)$. Define $j_1 \in (i : j]$ to be the largest such that $|\mathscr{R}_{j_1}| = |\mathscr{R}_{i+1}|$. Observe that j_1 is well defined as $i+1$ is one such value. Due to our assumption that $|\mathscr{R}_j| > |\mathscr{R}_{i+1}|$, we have that $j_1 < j$ implying by our choice of j_1 that $|\mathscr{R}_{j_1+1}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{j_1}|$ (we have $|\mathscr{R}_{j_1+1}| \geq |\mathscr{R}_{i+1}|$ due to item 3 of Fact 6.5). By item 2 of Fact 6.5, it follows that $j_1 \in \mathfrak{E}(80)$.

  We next show that $\textsc{Stop}(j_1) = j = \textsc{Stop}(i)$. Indeed $\textsc{Stop}(j_1) \leq \textsc{Stop}(i)$ due to Lemma 6.7. Moreover, $\textsc{Stop}(j_1) \geq \textsc{Stop}(i)$ as otherwise, we get that $|\mathscr{R}_{\textsc{Stop}(j_1)+1}| = |\mathscr{R}_{i+1}|$ from Lemma 6.12 but this contradicts the choice of j_1. As $\textsc{Stop}(j_1) = j = \textsc{Stop}(i)$ is good for i, we have by Lemma 6.12 that j_1 is indirect. Plugging in $\textsc{Stop}(j_1) = j$ in Claim 6.68, we get:

$$\begin{aligned}
\sum_{i'=i+1}^{j} \ell^*_{i'} &\leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(225, 225, j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) \\
&\quad - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(j) \\
&\leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|).
\end{aligned}$$

as $\mathsf{tax}_1(\cdot)$ is non-negative and Lemma 6.63.

For the rest of this proof, we assume that $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$. We next deal with the sub-case $\sigma_j^A \neq \sigma_j^B$.

- **When $\boldsymbol{\sigma_j^A \neq \sigma_j^B}$:** Define S to be the (possibly empty) set $S = (i : j) \cap \{j' \in \textsc{Starts} \mid |\mathscr{R}_{j'}| = |\mathscr{R}_{i+1}|\}$. Let $j_1 < j_2 < \cdots < j_{|S|}$ be the elements of S in increasing order. As $j \leq \textsc{Stop}(i)$, we have by item 3 of Fact 6.5 that $S \subseteq \mathfrak{E}(80) \subseteq \textsc{Starts}_{\mathrm{F}}$. We adopt the convention that $j_{|S|+1} = j$ for notational convenience. First, observe that for all $z \in [|S|]$, we have

$$|\mathscr{R}_{j_{z+1}}| = |\mathscr{R}_{i+1}| = |\mathscr{R}_{j_z}| < |\mathscr{R}_{j_z+1}|,$$

implying by definition of $\textsc{Stop}(\cdot)$ that $\textsc{Stop}(j_z) < j_{z+1}$. As $j_{z+1} \leq j \leq \textsc{Stop}(i)$ for $z \in [|S|]$, we have by Lemma 6.12 that j_z is indirect and $|\mathscr{R}_{\textsc{Stop}(j_z)+1}| = |\mathscr{R}_{i+1}|$. We claim that:

Claim 6.75. *For all $z \in [|S|]$, and all $j' \in (\textsc{Stop}(j_z) : j_{z+1}]$, we have $|\mathscr{R}_{j'}| = |\mathscr{R}_{i+1}|$. Furthermore, for all $j' \in (i : j_1]$, we have $|\mathscr{R}_{j'}| = |\mathscr{R}_{i+1}|$.*

Proof. Proof by contradiction. Let $z \in [|S|]$ and $j' \in (\textsc{Stop}(j_z) : j_{z+1}]$ be the smallest such that $|\mathscr{R}_{j'}| \neq |\mathscr{R}_{i+1}|$. As $j' \leq j$, we have $j' \in \textsc{Range}(i)$ implying by item 3 of Fact 6.5 that $|\mathscr{R}_{j'}| > |\mathscr{R}_{i+1}|$. As $|\mathscr{R}_{\textsc{Stop}(j_z)+1}| = |\mathscr{R}_{i+1}|$, we have $j' > \textsc{Stop}(j_z) + 1$ implying by our choice of j' that $|\mathscr{R}_{j'}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{j'-1}|$. Due to item 2 of Fact 6.5, this means that $j' - 1 \in \mathfrak{E}(80)$. However, as $j_z < j' - 1 < j_{z+1}$, we have $(j_z : j_{z+1}) \cap S \neq \emptyset$, a contradiction to our ordering of the elements of S.

The proof for the furthermore part is similar, and we include it here for completeness. Proof by contradiction. Let $j' \in (i : j_1]$ be the smallest such that $|\mathscr{R}_{j'}| \neq |\mathscr{R}_{i+1}|$. As $j' \leq j$, we have $j' \in \textsc{Range}(i)$ implying by item 3 of Fact 6.5 that $|\mathscr{R}_{j'}| > |\mathscr{R}_{i+1}|$. Also, note that $j' > i + 1$ implying by our choice of j' that $|\mathscr{R}_{j'}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{j'-1}|$. Due to item 2 of Fact 6.5, this means that $j' - 1 \in \mathfrak{E}(80)$. However, as $i < j' - 1 < j_1$, we have $(i : j_1) \cap S \neq \emptyset$, a contradiction to our ordering of the elements of S.

□

Claim 6.76. *For all $z \in [|S|]$ and $j' \in [\textsc{Stop}(j_z) : j_{z+1}]$, we have $|\pi_{\textsc{Stop}(j_z)+1}| - |\pi_{j'+1}| = j' - \textsc{Stop}(j_z) = |\psi_{j'}| - |\psi_{\textsc{Stop}(j_z)}|$.*

Proof. Proof by induction. The base case $j' = \textsc{Stop}(j_z)$ is trivial. We show the claim for $j' \in (\textsc{Stop}(j_z) : j_{z+1}]$, by assuming it holds for $j' - 1$. First, note that as $|\mathscr{R}_{j'}|$ is even (Claim 6.75), we have by item 5 of Fact 6.5 that $|\pi_{\textsc{Stop}(j_z)+1}| - |\pi_{j'+1}| = |\pi_{\textsc{Stop}(j_z)+1}| - |\pi_{j'}| + 1 = j' - \textsc{Stop}(j_z)$ by the induction hypothesis. We now claim that $|\mathscr{R}_{j'-1}|$ is even as well. If $j' > \textsc{Stop}(j_z) + 1$, this follows from Claim 6.75. If not, then $j' = \textsc{Stop}(j_z) + 1$ and we can conclude $|\mathscr{R}_{j'-1}|$ is even from the fact

that j_z is indirect, and $|\mathscr{R}_{j_z+1}| = |\mathscr{R}_{j_z}| + 1 = |\mathscr{R}_{i+1}| + 1$ is odd. As $|\mathscr{R}_{j'-1}|$ and $|\mathscr{R}_{j'}|$ are both even, we have $j'-1 \notin \textsc{Starts}$, and therefore, by item 5 of Fact 6.5 that $|\psi_{j'}| - |\psi_{\textsc{Stop}(j_z)}| = |\psi_{j'-1}| + 1 - |\psi_{\textsc{Stop}(j_z)}| = j' - \textsc{Stop}(j_z)$, using the induction hypothesis as desired. □

Claim 6.77. *For all $1 \le z < |S|$ such that $\mathscr{R}_{\textsc{Stop}(j_z)+1}.last.t = 0$, we have $|\psi_{\textsc{Stop}(j_z)}| + 1 \le |\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|$.*

Proof. As $1 \le z < |S|$, we have that $j_{z+1} \in S \subseteq \mathfrak{E}(80)$. Due to item 11 of Fact 6.5, this means that $\mathscr{R}_{j_{z+1}}.last.t > 0$. Let $j' \in (\textsc{Stop}(j_z) : j_{z+1}]$ be the smallest such that $\mathscr{R}_{j'}.last.t > 0$. Observe j' is well defined as $\mathscr{R}_{j_{z+1}}.last.t > 0$ and $j' > \textsc{Stop}(j_z)+1$ as $\mathscr{R}_{\textsc{Stop}(j_z)+1}.last.t = 0$. The latter together with our choice of j' implies that $\mathscr{R}_{j'-1}.last.t = 0 \implies j'-1 \in \mathfrak{E}(90)$. We derive:

$$\begin{aligned}
|\psi_{\textsc{Stop}(j_z)}| + 1 &\le |\psi_{j'-1}| + 1 && \text{(Claim 6.76)}\\
&= \mathscr{R}_{j'}.last.r - \mathscr{R}_{j'}.last.t && (\text{As } j'-1 \in \mathfrak{E}(90))\\
&= \mathscr{R}_{j_{z+1}}.last.r - \mathscr{R}_{j_{z+1}}.last.t && \text{(Fact 6.5, item 9 and Claim 6.75)}\\
&= \frac{|\psi_{j_{z+1}}| + 1}{2} && (\text{As } j_{z+1} \in \mathfrak{E}(80))\\
&= \frac{|\pi_{\textsc{Stop}(j_z)+1}| - |\pi_{j_{z+1}+1}| + |\psi_{\textsc{Stop}(j_z)}| + 1}{2} && \text{(Claim 6.76)}\\
&= \frac{|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}| + |\psi_{\textsc{Stop}(j_z)}| + 1}{2}, && \text{(Lemma 6.10)}
\end{aligned}$$

and the claim follows via a simple rearrangement. □

We now analyze $\sum_{i'=i+1}^{j} \ell^*_{i'}$. As $i < j_1 < \textsc{Stop}(j_1) < j_2 < \cdots < j$, we have:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \le \sum_{i'=i+1}^{j_1} \ell^*_{i'} + \sum_{z=1}^{|S|} \sum_{i'=j_z+1}^{\textsc{Stop}(j_z)} \ell^*_{i'} + \sum_{z=1}^{|S|} \sum_{i'=\textsc{Stop}(j_z)+1}^{j_{z+1}} \ell^*_{i'}$$

Due to Claim 6.75, we have $|\mathscr{R}_{j'}| = |\mathscr{R}_{i+1}|$ is even for all $j' \in (i : j_1]$. Combining with item 5 of Fact 6.5, we get that $|\pi_{i+1}| - |\pi_{j_1+1}| = j_1 - i$. Also, combining with the definition of ℓ^*, we get that $\ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) = \ell^*_{i+1} \cdot (j_1 - i) = \sum_{i'=i+1}^{j_1} \ell^*_{i'}$. Using this and similar results for the intervals $(\textsc{Stop}(j_z) : j_{z+1}]$ for $z \in [|S|]$, we get

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \le \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) + \sum_{z=1}^{|S|} \sum_{i'=j_z+1}^{\textsc{Stop}(j_z)} \ell^*_{i'} + \sum_{z=1}^{|S|} \ell^*_{i+1} \cdot \left(|\pi_{\textsc{Stop}(j_z)+1}| - |\pi_{j_{z+1}+1}|\right).$$

Invoking Lemma 6.10 and telescoping, we get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \le \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + \sum_{z=1}^{|S|} \sum_{i'=j_z+1}^{\textsc{Stop}(j_z)} \ell^*_{i'}.$$

We now apply Lemma 6.19 on j_z for $z \in [|S|]$ to get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \le \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + \sum_{z=1}^{|S|} 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{j_z,\mathsf{depth}(j_z)}(\textsc{Mid}(j_z)) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(j_z)}(\textsc{Stop}(j_z)) + \sum_{z=1}^{|S|} \frac{3}{1.1} \cdot \ell^*_{j_z+1} \cdot \left(|\psi_{\textsc{Stop}(j_z)}| + 1\right) - \ell^*_{j_z+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_z)).$$

We continue using the definition of ℓ^* which implies that $\ell^*_{j_z+1} = 1.1 \cdot \ell^*_{i+1}$. This with Corollary 6.43 gives:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \le \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + \sum_{z=1}^{|S|} 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{j_z,\mathsf{depth}(j_z)}(\textsc{Mid}(j_z)) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(j_z)}(\textsc{Stop}(j_z)) + \sum_{z=1}^{|S|} 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_z)}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_z)).$$

We continue by bounding $\mathsf{E}^{\mathrm{F}}_{j_z,\mathsf{depth}(j_z)}(\textsc{Mid}(j_z)) + \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(j_z)}(\textsc{Stop}(j_z))$ using Lemma 6.34.

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \le \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + \sum_{z=1}^{|S|} 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{i}(\textsc{Stop}(j_z)) - 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{i}(j_z) + \sum_{z=1}^{|S|} 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_z)}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_z)).$$

We continue with an application of Lemma 6.39 on the intervals $(\textsc{Stop}(j_z) : j_{z+1}]$ for $z \in [|S|]$ and the interval $(i : j_1]$ (the conditions of Lemma 6.39 are satisfied due to Claim 6.75) and noting that $\mathsf{E}^{\mathrm{B}}_{i}(i) = 0$:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \le \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + \sum_{z=1}^{|S|} 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{i}(\textsc{Stop}(j_z)) - 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{i}(j_z) + \sum_{z=1}^{|S|} 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{i}(j_{z+1}) - 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{i}(\textsc{Stop}(j_z)) - 10^4 \cdot \sum_{z=1}^{|S|} \sum_{l=|\pi_{j_{z+1}+1}|+1}^{|\pi_{\textsc{Stop}(j_z)+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} - 10^4 \cdot \sum_{z=1}^{|S|} \sum_{i'=\textsc{Stop}(j_z)+1}^{j_{z+1}} \mathsf{corr}_{i'}$$

$$+ 10^4 \cdot \mathsf{E}_i^{\mathrm{B}}(j_1) - 10^4 \cdot \sum_{i'=i+1}^{j_1} \mathsf{corr}_{i'} - 10^4 \cdot \sum_{l=|\pi_{j_1+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)}$$
$$+ \sum_{z=1}^{|S|} 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_z)}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_z)).$$

Telescoping all the $\mathsf{E}^{\mathrm{B}}(\cdot)$ terms, we get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}_i^{\mathrm{B}}(j) + \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|)$$
$$- 10^4 \cdot \sum_{z=1}^{|S|} \sum_{l=|\pi_{j_{z+1}+1}|+1}^{|\pi_{\textsc{Stop}(j_z)+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} - 10^4 \cdot \sum_{z=1}^{|S|} \sum_{i'=\textsc{Stop}(j_z)+1}^{j_{z+1}} \mathsf{corr}_{i'}$$
$$- 10^4 \cdot \sum_{i'=i+1}^{j_1} \mathsf{corr}_{i'} - 10^4 \cdot \sum_{l=|\pi_{j_1+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)}$$
$$+ \sum_{z=1}^{|S|} 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_z)}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_z)).$$

Next, we use Lemma 6.10 to get $|\pi_{j_z+1}| = |\pi_{\textsc{Stop}(j_z)+1}|$. Using this fact to combine all the $\mathsf{corr}_{\mathsf{latest}(i,l)}$ terms and using $\sum_{i'=i+1}^{j_1} \mathsf{corr}_{i'} \geq 0$, we have:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}_i^{\mathrm{B}}(j) + \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) - 10^4 \cdot \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)}$$
$$- 10^4 \cdot \sum_{z=1}^{|S|} \sum_{i'=\textsc{Stop}(j_z)+1}^{j_{z+1}} \mathsf{corr}_{i'}$$
$$+ \sum_{z=1}^{|S|} 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\textsc{Stop}(j_z)}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_z)).$$

We get using Claim 6.76 that :

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}_i^{\mathrm{B}}(j) + \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) - 10^4 \cdot \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)}$$
$$- 10^4 \cdot \sum_{z=1}^{|S|} \sum_{i'=\textsc{Stop}(j_z)+1}^{j_{z+1}} \mathsf{corr}_{i'}$$
$$+ \sum_{z=1}^{|S|} 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{j_{z+1}}| + 1\right) - \ell^*_{i+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(j_z)).$$

We now deal with the terms $3 \cdot \left(|\psi_{j_{z+1}}| + 1\right) - \mathsf{tax}_0(225, \textsc{Stop}(j_z))$ for $z \in [|S|]$. If $S = \emptyset$, these terms just disappear. Otherwise, if $z = |S|$, we upper bound it simply by $3 \cdot \left(|\psi_{j_{|S|+1}}| + 1\right) = 3 \cdot (|\psi_j| + 1)$. For $z < |S|$, we have that $j_{z+1} \in S \subseteq \mathfrak{E}(80)$. If $\mathscr{R}_{\textsc{Stop}(j_z)+1}.last.t > 0$, we apply Lemma 6.52 on $\textsc{Stop}(j_z), j_{z+1}$ (the conditions of Lemma 6.39 are satisfied due to Claim 6.75). If $\mathscr{R}_{\textsc{Stop}(j_z)+1}.last.t = 0$, we use Claim 6.77 to get that $3 \cdot \left(|\psi_{\textsc{Stop}(j_z)}| + 1\right) - \mathsf{tax}_0(225, \textsc{Stop}(j_z)) \leq 3 \cdot \left(|\psi_{\textsc{Stop}(j_z)}| + 1\right) \leq 3 \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right)$. We get:

$$\begin{aligned}\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) - 10^4 \cdot \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)} \\ + \sum_{\substack{1 \leq z < |S| \\ \mathscr{R}_{\textsc{Stop}(j_z)+1}.last.t = 0}} 3 \cdot \ell^*_{i+1} \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right) \\ + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1)\,.\end{aligned}$$

Now, note by Lemma 6.13 that $|\pi_{i+1}| - |\pi_{j_1+1}| \geq 0$. Also, by Claim 6.76 and Lemma 6.10, we have that $|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}| = |\pi_{\textsc{Stop}(j_z)+1}| - |\pi_{j_{z+1}+1}| \geq 0$. Thus, we get

$$\begin{aligned}|\pi_{i+1}| - |\pi_{j+1}| &\geq |\pi_{j_1+1}| - |\pi_{j+1}| \\ &= \sum_{z=1}^{|S|} |\pi_{j_z+1}| - |\pi_{j_{z+1}+1}| \\ &\geq \sum_{\substack{1 \leq z < |S| \\ \mathscr{R}_{\textsc{Stop}(j_z)+1}.last.t = 0}} |\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|.\end{aligned}$$

Plugging this in, we get:

$$\begin{aligned}\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + 4 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) \\ - 10^4 \cdot \sum_{l=|\pi_{j+1}|+1}^{|\pi_{i+1}|} \mathsf{corr}_{\mathsf{latest}(i,l)}.\end{aligned}$$

Use Lemma 6.36 to get:

$$\begin{aligned}\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + 4 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2250 \cdot \ell^*_{i+1} \\ + \ell^*_{i+1} \cdot \min\left(0, \frac{|\pi_{i+1}| - |\pi_{\textsc{Prev}(i)+1}|}{30} - 500 \cdot (|\pi_{i+1}| - |\pi_{j+1}|)\right).\end{aligned}$$

Finally, note by Lemma 6.51 that $\mathsf{tax}_0(10, j) \leq 27 \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + 100$ and

$\mathsf{tax}_0(225, j) \leq 470 \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + 2250$. Plugging these in and using the definition of extra, we get

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) + \mathsf{extra}_i(j),$$

as desired.

Owing to this result, we can now assume for the rest of the proof that $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ and $\sigma^A_j = \sigma^B_j$. We first claim that $\sigma^A_j = \sigma^B_j$ implies that $\mathsf{turn}(j) = \mathsf{turn}(j-1)$. Indeed, as $\sigma^A_j = \sigma^B_j$, we have that $\mathsf{turn}(j) = \mathbb{1}\left(\psi^A_j \neq \psi^B_j\right)$. Now, either $|\mathscr{R}_{j-1}|$ is odd, which means that $\mathsf{turn}(j-1) = 0$ and, as $|\mathscr{R}_j|$ is even, implies that $j - 1 \in \mathfrak{E}(70)$ which means that $\psi^A_j = \psi^B_j = \varepsilon$ and therefore, $\mathsf{turn}(j) = 0 = \mathsf{turn}(j-1)$, or $|\mathscr{R}_{j-1}|$ and $|\mathscr{R}_j|$ are both even, in which case, we have $j - 1 \notin \textsc{Starts}$, and by item 5 of Fact 6.5, that

$$\mathsf{turn}(j) = \mathbb{1}\left(\psi^A_j \neq \psi^B_j\right) = \mathbb{1}\left(\psi^A_{j-1}\|\sigma^A_{j-1} \neq \psi^B_{j-1}\|\sigma^B_{j-1}\right) = \mathsf{turn}(j-1).$$

Define $j_1 \in [i : j)$ to be the largest such that j_1 is good for i. Observe that j_1 is well defined as i is good for i. Also, note that $j_1 - i < j - i = D$. We have:

- **When $j_1 = j - 1$:** We have by Lemma 6.18 on i, j_1 that:

$$\begin{aligned}\sum_{i'=i+1}^{j} \ell^*_{i'} &\leq \sum_{i'=i+1}^{j_1} \ell^*_{i'} + \ell^*_j \\ &\leq \ell^*_j + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1) \\ &\quad - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|) - \ell^*_{i+1} \cdot \mathbb{1}\left(j_1 \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,i}(j_1).\end{aligned}$$

  As we have $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$, we have that $\ell^*_j = \ell^*_{i+1}$. Also, note that as $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ is even, we have that $j - 1 = j_1 \notin \mathfrak{E}(80)$. Using this, we get:

$$\begin{aligned}\sum_{i'=i+1}^{j} \ell^*_{i'} &\leq \ell^*_{i+1} + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1) \\ &\quad - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j_1+1}|).\end{aligned}$$

  Again using the fact that $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ is even, we have by item 5 of Fact 6.5 that $|\pi_{j+1}| = |\pi_j| - 1 = |\pi_{j_1+1}| - 1$. This yields:

$$\begin{aligned}\sum_{i'=i+1}^{j} \ell^*_{i'} &\leq 3 \cdot \ell^*_{i+1} + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j_1) + \mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1) \\ &\quad - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|).\end{aligned}$$

  Now, as $j_1 < j \leq \textsc{Stop}(i)$ is good for i, we have that either $j_1 = i$ or $|\mathscr{R}_{j_1}| = |\mathscr{R}_{i+1}|$

is even. In the former case, we have $|\psi_j| = |\psi_{i+1}| = 0$ as $i \in \text{STARTS}_\text{B}$ and in the latter case, we have from the fact that $|\mathscr{R}_{j_1}| = |\mathscr{R}_j|$ is even that $j_1 \notin \text{STARTS}$ which, by item 5 of Fact 6.5, means that $|\psi_{j_1+1}| = |\psi_{j_1}| + 1$. Thus, in either case, we get that $|\psi_j| = \mathbb{1}(j_1 \neq i) \cdot (|\psi_{j_1}| + 1)$. Plugging this, we get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\text{B}}_i(j_1) + \mathsf{extra}_i(j_1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|).$$

Finally, we use Lemma 6.64 on with $j' = j_1$. Note that the conditions of the lemma are satisfies as we have $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ and $\mathsf{turn}(j) = \mathsf{turn}(j-1)$. We get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\text{B}}_i(j) + \mathsf{extra}_i(j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|),$$

which is exactly Equation 52.

- **When $j_1 < j-1$:** In this case, by our choice of j_1, we have that $j_1+1 < j$ is not good for i. This is possible only if $i < j_1 < \text{STOP}(i)$. By definition of good, the latter implies that $|\mathscr{R}_{j_1+1}| > |\mathscr{R}_{i+1}| = |\mathscr{R}_{j_1}|$ (we have $|\mathscr{R}_{j_1+1}| > |\mathscr{R}_{i+1}|$ due to item 3 of Fact 6.5) implying that $j_1 \in \mathfrak{E}(80) \subseteq \text{STARTS}_\text{F}$ by item 2 of Fact 6.5. As $j_1 < j \leq \text{STOP}(i)$, we have by Lemma 6.7 that $\text{STOP}(j_1) \leq \text{STOP}(i)$. We claim that:

  Claim 6.78. *We have $j = \text{STOP}(j_1) + 1$ and j_1 is indirect.*

  Proof. We have $j \geq \text{STOP}(j_1) + 1$, because otherwise $j \in \text{RANGE}(j_1)$ which means due to item 3 of Fact 6.5 that

  $$|\mathscr{R}_{i+1}| = |\mathscr{R}_j| \geq |\mathscr{R}_{j_1+1}| > |\mathscr{R}_{i+1}|,$$

  a contradiction. As $\text{STOP}(i) \geq j \geq \text{STOP}(j_1) + 1$, we have by Lemma 6.12 that $|\mathscr{R}_{\text{STOP}(j_1)+1}| = |\mathscr{R}_{i+1}|$ and j_1 is indirect. As $|\mathscr{R}_{\text{STOP}(j_1)+1}| = |\mathscr{R}_{i+1}|$, we must have $j \leq \text{STOP}(j_1) + 1$, as otherwise, we have a contradiction to the choice of j_1.

  □

  Using Claim 6.68 (the conditions in Claim 6.68 are satisfied due to Claim 6.78), we derive:

$$\begin{aligned}\sum_{i'=i+1}^{j} \ell^*_{i'} &\leq \sum_{i'=i+1}^{\text{STOP}(j_1)} \ell^*_{i'} + \ell^*_j \\ &\leq 10^4 \cdot \mathsf{E}^{\text{B}}_i(\text{STOP}(j_1)) + \mathsf{extra}_i(225, 225, \text{STOP}(j_1)) + 3 \cdot \ell^*_{i+1} \cdot \left(|\psi_{\text{STOP}(j_1)}| + 1\right) \\ &\quad - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{\text{STOP}(j_1)+1}|) - \ell^*_{i+1} \cdot \mathsf{tax}_{1,i}(\text{STOP}(j_1)) + \ell^*_j.\end{aligned}$$

We now plug in $j = \textsc{Stop}(j_1) + 1$ and use the fact that $\mathsf{tax}_1(\cdot)$ is non-negative and $\ell^*_j = \ell^*_{i+1}$ along with Lemma 6.63.

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j-1) + \mathsf{extra}_i(j-1) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_{j-1}| + 1) \\ - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_j|) + \ell^*_{i+1}.$$

Next, we use Lemma 6.64 on with $j' = j - 1$. Note that the conditions of the lemma are satisfies as we have $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ and $\mathsf{turn}(j) = \mathsf{turn}(j-1)$. We get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_{j-1}| + 1) - 2\ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_j|) + \ell^*_{i+1}.$$

Now, as $j_1 \in \mathfrak{E}(80)$ is indirect (Claim 6.78) and $|\mathscr{R}_{j_1}| = |\mathscr{R}_{i+1}|$, we have that $|\mathscr{R}_{\textsc{Stop}(j_1)}|$ is even. Using this and the fact that $\textsc{Stop}(j_1) = j - 1 < \textsc{Stop}(i)$, we have by item 3 and item 7 of Fact 6.5 that $j - 1 \in \mathfrak{E}(88) \implies j - 1 \notin \textsc{Starts}$. By item 5 of Fact 6.5, this gives $|\psi_{j-1}| + 1 = |\psi_j|$. We get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_j| + 1).$$

Finally, as $|\mathscr{R}_j| = |\mathscr{R}_{i+1}|$ is even, we have $|\pi_{j+1}| + 1 = |\pi_j|$ by item 5 of Fact 6.5 and we get:

$$\sum_{i'=i+1}^{j} \ell^*_{i'} \leq 10^4 \cdot \mathsf{E}^{\mathrm{B}}_i(j) + \mathsf{extra}_i(j) + 3 \cdot \ell^*_{i+1} \cdot (|\psi_j| + 1) - 2 \cdot \ell^*_{i+1} \cdot (|\pi_{i+1}| - |\pi_{j+1}|).$$

□

6.2.11 Finishing the Proof of Theorem 6.4

We now finish by showing Theorem 6.4.

Finishing the proof of Theorem 6.4. To finish the proof, we have to show that:

$$\sum_{i<num} \ell^*_i \leq 8 \cdot \ell^*_1 \cdot |\mathsf{LCP}\left(\pi^A_{num}, \pi^B_{num}\right)| + 10^5 \cdot \sum_{i<num} \mathsf{corr}_i. \tag{53}$$

Let $a = |\mathfrak{E}(84)|$. Define $i_0 = 0$ and $i_1 < i_2 < \cdots < i_a$ to be the elements of $\mathfrak{E}(84)$ in increasing order. Observe that $i_z \in \textsc{Starts}$ for all $0 \leq z \leq a$. Also, by definition of $\textsc{Stop}(\cdot)$, we have for $0 \leq z < a$ that $\textsc{Stop}(i_z) = i_{z+1}$. Furthermore, for $0 \leq z < a$, observe that $|\mathscr{R}_{\textsc{Stop}(i_z)}| - |\mathscr{R}_{i_z+1}| = |\mathscr{R}_{i_{z+1}}| - |\mathscr{R}_{i_{z+1}}| = |\mathscr{R}_{i_{z+1}}| - 1$ as $i_z \in \mathfrak{E}(84) \cup \{0\}$. Using now that $i_{z+1} \in \mathfrak{E}(84)$, this means that $|\mathscr{R}_{\textsc{Stop}(i_z)}| - |\mathscr{R}_{i_z+1}|$ is odd implying that i_z is indirect for

all $0 \leq z < a$. We have:

$$\begin{aligned}
\sum_{i=1}^{i_a} \ell_i^* &= \sum_{z=1}^{a} \sum_{i=i_{z-1}+1}^{i_z} \ell_i^* \\
&= \sum_{z=1}^{a} \sum_{i=i_{z-1}+1}^{\textsc{Stop}(i_{z-1})} \ell_i^* && \text{(As } \textsc{Stop}(i_z) = i_{z+1} \text{ for } 0 \leq z < a\text{)} \\
&\leq \sum_{z=1}^{a} 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i_{z-1},\mathsf{depth}(i_{z-1})}(\textsc{Mid}(i_{z-1})) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i_{z-1})}(\textsc{Stop}(i_{z-1})) \\
&\quad + \sum_{z=1}^{a} \frac{3}{1.1} \cdot \ell^*_{i_{z-1}+1} \cdot \left(|\psi_{\textsc{Stop}(i_{z-1})}| + 1\right) - \ell^*_{i_{z-1}+1} \cdot \mathsf{tax}_0(225, \textsc{Stop}(i_{z-1})). \\
& && \text{(Lemma 6.19 as } i_z \text{ is indirect for } 0 \leq z < a\text{)}
\end{aligned}$$

To continue, we use Lemma 6.44 noting that $\textsc{Stop}(i_{z-1}) = i_z \in \mathfrak{E}(84)$. We get:

$$\sum_{i=1}^{i_a} \ell_i^* \leq \sum_{z=1}^{a} 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{i_{z-1},\mathsf{depth}(i_{z-1})}(\textsc{Mid}(i_{z-1})) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{\textsc{Mid}(i_{z-1})}(i_z).$$

To continue, we invoke Lemma 6.29 with $i = i_{z-1}$, $i' = \textsc{Mid}(i_{z-1})$, and $j = \textsc{Stop}(i_{z-1}) = i_z$ (note that the condition of the lemma are satisfied due to Lemma 6.9 and the fact that $|\pi_{i_z+1}| = 0$). We get

$$\sum_{i=1}^{i_a} \ell_i^* \leq \sum_{z=1}^{a} 3 \cdot 10^4 \cdot \sum_{i'=i_{z-1}+1}^{i_z} \mathsf{corr}_{i'} \leq 10^5 \cdot \sum_{i'=1}^{i_a} \mathsf{corr}_{i'}.$$

Thus, in order to show Equation 53, it is sufficient to show that:

$$\sum_{i=i_a+1}^{num-1} \ell_i^* \leq 8 \cdot \ell_1^* \cdot |\mathsf{LCP}\left(\pi^A_{num}, \pi^B_{num}\right)| + 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i. \tag{54}$$

We now focus on showing Equation 54. Note that if $i_a = num - 1$, then there is nothing to show, so we assume $i_a < num - 1$. Now, for $b > 0$ and a sequence J of b iterations $j_1 < j_2 < \cdots j_b < num$, we say that J is 'nice' if $j_1 = i_a$ and the following hold for all $1 \leq z < b$:

- If z is odd, we have $j_z \in \textsc{Starts}_{\mathrm{F}}$. If $z > 1$ is odd, we additionally have $j_z \in \mathfrak{E}(80) \subseteq \textsc{Starts}_{\mathrm{F}}$. If z is even, we have $j_z \in \textsc{Starts}_{\mathrm{B}}$.
- $z = |\mathscr{R}_{j_z+1}| = |\mathscr{R}_{j_{z+1}}|$.
- $\textsc{Stop}(j_z) \geq num - 1$.

Claim 6.79. *There exists a $b > 1$ and a nice sequence J of b iterations such that $j_b = num - 1$.*

Proof. Proof by contradiction. Suppose that for all nice sequences of at least 2 iterations, we have $j_b < num - 1$. Pick one such sequence J with the largest value of j_b. Observe that J is well defined as the sequence J with only the iterations $i_a, i_a + 1$ is a nice sequence (using the fact that $i_a \in \mathfrak{E}(84) \cup \{0\}$ is fixed by our choice of a).

Let $j_1, j_2, \cdots, j_{b-1}, j_b$ be the iterations in J. Observe that $j_b < num - 1 \leq \textsc{Stop}(j_{b-1})$. By our choice of J, the sequence $j_1, j_2, \cdots, j_{b-1}, j_b + 1$ is not nice. Using the definition of nice, this is only possible if $|\mathscr{R}_{j_b}| = |\mathscr{R}_{j_{b-1}+1}| \neq |\mathscr{R}_{j_b+1}|$. Now, as $j_b < \textsc{Stop}(j_{b-1})$ implies that $j_b + 1 \in \textsc{Range}(j_{b-1})$ which, together with $|\mathscr{R}_{j_{b-1}+1}| \neq |\mathscr{R}_{j_b+1}|$ and item 3 of Fact 6.5 gives us that $|\mathscr{R}_{j_b}| = |\mathscr{R}_{j_{b-1}+1}| < |\mathscr{R}_{j_b+1}|$.

Due to item 2 of Fact 6.5, this is possible only if $j_b \in \mathfrak{E}(70) \cup \mathfrak{E}(80)$. As $|\mathscr{R}_{j_b}| = |\mathscr{R}_{j_{b-1}+1}| = b - 1$, we additionally get that $|\mathscr{R}_{j_b+1}| = b$ and $j_b \in \mathfrak{E}(80) \subseteq \textsc{Starts}_{\mathrm{F}}$ if b is odd and $j_b \in \textsc{Starts}_{\mathrm{B}}$ otherwise. Combining, this with the fact that the sequence $j_1, j_2, \cdots, j_{b-1}, j_b, j_b + 1$ is not nice (again due to the choice of J, we have that $\textsc{Stop}(j_b) < num - 1 \leq \textsc{Stop}(j_{b-1})$. Due to Lemma 6.12, this means that $|\mathscr{R}_{\textsc{Stop}(j_b)+1}| = |\mathscr{R}_{j_{b-1}+1}|$. However, this means that the sequence $j_1, j_2, \cdots, j_{b-1}, \textsc{Stop}(j_b) + 1$ is nice, contradicting the choice of J.

□

For the rest of the proof, fix $b > 1$ and J to be those promised by Claim 6.79. As J is nice, we derive:

$$\begin{aligned}
\sum_{i=i_a+1}^{num-1} \ell_i^* &= \sum_{i=j_1+1}^{j_b} \ell_i^* && \text{(As } j_1 = i_a \text{ and } j_b = num - 1\text{)} \\
&= \sum_{z=1}^{b-1} \sum_{i=j_z+1}^{j_{z+1}} \ell_i^* && \text{(As } j_z < j_{z+1} \text{ for all } 1 \leq z < b\text{)} \\
&= \sum_{\text{odd } z=1}^{b-1} \sum_{i=j_z+1}^{j_{z+1}} \ell_i^* + \sum_{\text{even } z=1}^{b-1} \sum_{i=j_z+1}^{j_{z+1}} \ell_i^*.
\end{aligned}$$

To continue, we use Lemma 6.17 for odd z and Lemma 6.18 for even z and get (note that the conditions in Lemma 6.17 and Lemma 6.18 are satisfied due to the definition of nice):

$$\begin{aligned}
\sum_{i=i_a+1}^{num-1} \ell_i^* \leq & \sum_{\text{odd } z=1}^{b-1} 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{j_z,\mathsf{depth}(j_z)}(j_{z+1}) + \ell^*_{j_z+1} \left(\mathsf{G}_{j_z}(j_{z+1}) + 150\mathsf{B}_{j_z}(j_{z+1}) - 2500 \cdot \mathsf{D}_{j_z}(j_{z+1})\right) \\
& + \sum_{\text{odd } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}(j_{z+1} = \textsc{Stop}(j_z) \wedge |\mathscr{R}_{j_z+1}| \neq |\mathscr{R}_{j_z+1}|) \left(\mathsf{G}_{j_z}(j_{z+1}) + \mathsf{B}_{j_z}(j_{z+1})\right) \\
& - \sum_{\text{odd } z=1}^{b-1} 2500 \cdot \ell^*_{j_z+1} \cdot \mathsf{spare}_{j_z}(j_{z+1}) \\
& + \sum_{\text{even } z=1}^{b-1} 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{j_z}(j_{z+1}) + \mathsf{extra}_{j_z}(j_{z+1}) + 3 \cdot \ell^*_{j_z+1} \cdot \mathbb{1}(j_{z+1} \neq j_z) \cdot \left(|\psi_{j_z+1}| + 1\right)
\end{aligned}$$

$$
\begin{aligned}
&- \sum_{\text{even } z=1}^{b-1} 2 \cdot \ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|) \\
&- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).
\end{aligned}
$$

Simplifying using the fact that $|\mathscr{R}_{j_z+1}| = |\mathscr{R}_{j_{z+1}}|$ by the definition of nice and noting that $\mathsf{spare}(\cdot)$ is non-negative and $\mathbb{1}(j_{z+1} \neq j_z) \leq 1$, we get:

$$
\begin{aligned}
\sum_{i=i_a+1}^{num-1} \ell^*_i \leq & \sum_{\text{odd } z=1}^{b-1} 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{j_z,\mathsf{depth}(j_z)}(j_{z+1}) + \ell^*_{j_z+1}\left(\mathsf{G}_{j_z}(j_{z+1}) + 150\mathsf{B}_{j_z}(j_{z+1}) - 2500 \cdot \mathsf{D}_{j_z}(j_{z+1})\right) \\
&+ \sum_{\text{even } z=1}^{b-1} 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{j_z}(j_{z+1}) + \mathsf{extra}_{j_z}(j_{z+1}) + 3 \cdot \ell^*_{j_z+1} \cdot \left(|\psi_{j_{z+1}}| + 1\right) \\
&- \sum_{\text{even } z=1}^{b-1} 2 \cdot \ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|) \\
&- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).
\end{aligned}
$$

Reordering the terms, and reindexing the term $\sum_{\text{even } z=1}^{b-1} 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{j_z}(j_{z+1})$, we get:

$$
\begin{aligned}
\sum_{i=i_a+1}^{num-1} \ell^*_i \leq & \sum_{\text{odd } z=1}^{b-1} 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{j_z,\mathsf{depth}(j_z)}(j_{z+1}) + \sum_{\text{odd } z=1}^{b-2} 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{j_{z+1}}(j_{z+2}) \\
&+ \sum_{\text{odd } z=1}^{b-1} \ell^*_{j_z+1}\left(\mathsf{G}_{j_z}(j_{z+1}) + 150\mathsf{B}_{j_z}(j_{z+1}) - 2500 \cdot \mathsf{D}_{j_z}(j_{z+1})\right) \\
&+ \sum_{\text{even } z=1}^{b-1} \mathsf{extra}_{j_z}(j_{z+1}) + 3 \cdot \ell^*_{j_z+1} \cdot \left(|\psi_{j_{z+1}}| + 1\right) - 2\ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|) \\
&- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).
\end{aligned}
$$

This is equivalent to:

$$
\begin{aligned}
\sum_{i=i_a+1}^{num-1} \ell^*_i \leq & \; 10^4 \cdot \mathbb{1}(b \text{ is even}) \cdot \mathsf{E}^{\mathrm{F}}_{j_{b-1},\mathsf{depth}(j_{b-1})}(j_b) \\
&+ \sum_{\text{odd } z=1}^{b-2} 10^4 \cdot \mathsf{E}^{\mathrm{F}}_{j_z,\mathsf{depth}(j_z)}(j_{z+1}) + 10^4 \cdot \mathsf{E}^{\mathrm{B}}_{j_{z+1}}(j_{z+2}) \\
&+ \sum_{\text{odd } z=1}^{b-1} \ell^*_{j_z+1}\left(\mathsf{G}_{j_z}(j_{z+1}) + 150\mathsf{B}_{j_z}(j_{z+1}) - 2500 \cdot \mathsf{D}_{j_z}(j_{z+1})\right)
\end{aligned}
$$

$$+\sum_{\text{even } z=1}^{b-1}\mathsf{extra}_{j_z}(j_{z+1})+3\cdot\ell^*_{j_z+1}\cdot\left(|\psi_{j_{z+1}}|+1\right)-2\ell^*_{j_z+1}\cdot\left(|\pi_{j_z+1}|-|\pi_{j_{z+1}+1}|\right)$$
$$-\sum_{\text{even } z=1}^{b-1}\ell^*_{j_z+1}\cdot\mathbb{1}\left(j_{z+1}\in\mathfrak{E}(80)\right)\cdot\mathsf{tax}_{1,j_z}(j_{z+1}).$$

Now, note that if b is even, then by the definition of nice and Claim 6.79, we have that $j_{b-1}\in\textsc{Starts}_{\mathrm{F}}$ and $j_b=num-1\le\textsc{Stop}(j_{b-1})$. This means we can use Lemma 6.28 to bound the first term. We get:

$$\sum_{i=i_a+1}^{num-1}\ell^*_i\le 10^5\cdot\mathbb{1}(b\text{ is even})\cdot\sum_{j'=j_{b-1}+1}^{j_b}\mathsf{corr}_{j'}+\sum_{\text{odd } z=1}^{b-2}10^4\cdot\mathsf{E}^{\mathrm{F}}_{j_z,\mathsf{depth}(j_z)}(j_{z+1})+10^4\cdot\mathsf{E}^{\mathrm{B}}_{j_{z+1}}(j_{z+2})$$
$$+\sum_{\text{odd } z=1}^{b-1}\ell^*_{j_z+1}\left(\mathsf{G}_{j_z}(j_{z+1})+150\mathsf{B}_{j_z}(j_{z+1})-2500\cdot\mathsf{D}_{j_z}(j_{z+1})\right)$$
$$+\sum_{\text{even } z=1}^{b-1}\mathsf{extra}_{j_z}(j_{z+1})+3\cdot\ell^*_{j_z+1}\cdot\left(|\psi_{j_{z+1}}|+1\right)-2\ell^*_{j_z+1}\cdot\left(|\pi_{j_z+1}|-|\pi_{j_{z+1}+1}|\right)$$
$$-\sum_{\text{even } z=1}^{b-1}\ell^*_{j_z+1}\cdot\mathbb{1}\left(j_{z+1}\in\mathfrak{E}(80)\right)\cdot\mathsf{tax}_{1,j_z}(j_{z+1}).$$

Again by the definition of nice, we have for odd $z\in[b-2]$ that $j_z\in\textsc{Starts}_{\mathrm{F}}$, $j_{z+1}\in(j_z:\textsc{Stop}(j_z))\cap\textsc{Starts}_{\mathrm{B}}$, and $j_{z+2}\in\textsc{Range}(j_{z+1})\setminus\{num\}$. As $|\mathscr{R}_{j_{z+1}+1}|=|\mathscr{R}_{j_{z+2}}|$, we have by Lemma 6.13 that $|\pi_{j_{z+2}+1}|\le|\pi_{j_{z+1}+1}|$ and we can use Lemma 6.29 to get:

$$\sum_{i=i_a+1}^{num-1}\ell^*_i\le 10^5\cdot\mathbb{1}(b\text{ is even})\cdot\sum_{j'=j_{b-1}+1}^{j_b}\mathsf{corr}_{j'}+\sum_{\text{odd } z=1}^{b-2}10^5\cdot\sum_{j'=j_z+1}^{j_{z+2}}\mathsf{corr}_{j'}$$
$$+\sum_{\text{odd } z=1}^{b-1}\ell^*_{j_z+1}\left(\mathsf{G}_{j_z}(j_{z+1})+150\mathsf{B}_{j_z}(j_{z+1})-2500\cdot\mathsf{D}_{j_z}(j_{z+1})\right)$$
$$+\sum_{\text{even } z=1}^{b-1}\mathsf{extra}_{j_z}(j_{z+1})+3\cdot\ell^*_{j_z+1}\cdot\left(|\psi_{j_{z+1}}|+1\right)-2\ell^*_{j_z+1}\cdot\left(|\pi_{j_z+1}|-|\pi_{j_{z+1}+1}|\right)$$
$$-\sum_{\text{even } z=1}^{b-1}\ell^*_{j_z+1}\cdot\mathbb{1}\left(j_{z+1}\in\mathfrak{E}(80)\right)\cdot\mathsf{tax}_{1,j_z}(j_{z+1}).$$

This is equivalent to (note that $j_1=i_a$ and $j_b=num-1$ by Claim 6.79):

$$\sum_{i=i_a+1}^{num-1}\ell^*_i\le 10^5\cdot\sum_{i=i_a+1}^{num-1}\mathsf{corr}_i$$
$$+\sum_{\text{odd } z=1}^{b-1}\ell^*_{j_z+1}\left(\mathsf{G}_{j_z}(j_{z+1})+150\mathsf{B}_{j_z}(j_{z+1})-2500\cdot\mathsf{D}_{j_z}(j_{z+1})\right)$$

$$+ \sum_{\text{even } z=1}^{b-1} \mathsf{extra}_{j_z}(j_{z+1}) + 3 \cdot \ell^*_{j_z+1} \cdot \left(|\psi_{j_{z+1}}| + 1\right) - 2\ell^*_{j_z+1} \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right)$$
$$- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).$$

By definition of $\mathsf{extra}(\cdot)$, we derive:

$$\sum_{i=i_a+1}^{num-1} \ell^*_i \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} \ell^*_{j_z+1} \left(\mathsf{G}_{j_z}(j_{z+1}) + 150\mathsf{B}_{j_z}(j_{z+1}) - 2500 \cdot \mathsf{D}_{j_z}(j_{z+1})\right)$$
$$+ \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \left(\frac{|\pi_{j_z+1}| - |\pi_{\textsc{Prev}(j_z)+1}|}{30} - \mathsf{tax}_0(225, j_{z+1})\right)$$
$$+ \sum_{\text{even } z=1}^{b-1} 3 \cdot \ell^*_{j_z+1} \cdot \left(|\psi_{j_{z+1}}| + 1\right) - 2\ell^*_{j_z+1} \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right)$$
$$- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).$$

Continuing using Lemma 6.24, we have:

$$\sum_{i=i_a+1}^{num-1} \ell^*_i \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} \ell^*_{j_z+1} \left(\mathsf{G}_{j_z}(j_{z+1}) - 2300\mathsf{B}_{j_z}(j_{z+1})\right)$$
$$+ \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \left(\frac{|\pi_{j_z+1}| - |\pi_{\textsc{Prev}(j_z)+1}|}{30} - \mathsf{tax}_0(225, j_{z+1})\right)$$
$$+ \sum_{\text{even } z=1}^{b-1} 3 \cdot \ell^*_{j_z+1} \cdot \left(|\psi_{j_{z+1}}| + 1\right) - 2\ell^*_{j_z+1} \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right)$$
$$- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).$$

Now, we claim that for even $z < b-1$ we have that $\textsc{Prev}(j_z) = j_{z-1}$. For this, we need to show that $|\mathscr{R}_{j_{z-1}+1}| = |\mathscr{R}_{j_z}|$ and $|\mathscr{R}_{j'+1}| \neq |\mathscr{R}_{j_z}|$ for all $j' \in (j_{z-1} : j_z) \cap \textsc{Starts}$. The former is due to the definition of nice while the latter is because $j' \in (j_{z-1} : j_z) \cap \textsc{Starts} \implies j' \in (j_{z-1} : j_z) \cap (\mathfrak{E}(70) \cup \mathfrak{E}(80))$ by choice of $i_a = j_1$, which in turn implies that $|\mathscr{R}_{j'+1}| = |\mathscr{R}_{j'}| + 1 \ge |\mathscr{R}_{j_{z-1}+1}| + 1 = |\mathscr{R}_{j_z}| + 1$ as $j' \in \textsc{Range}(j_{z-1})$ by definition of nice and item 3 of Fact 6.5. Plugging in, we get

$$\sum_{i=i_a+1}^{num-1} \ell^*_i \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} \ell^*_{j_z+1} \left(\mathsf{G}_{j_z}(j_{z+1}) - 2300\mathsf{B}_{j_z}(j_{z+1})\right)$$
$$+ \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \left(\frac{|\pi_{j_z+1}| - |\pi_{j_{z-1}+1}|}{30} - \mathsf{tax}_0(225, j_{z+1})\right)$$

$$+\sum_{\text{even } z=1}^{b-1} 3\cdot\ell^*_{j_z+1}\cdot\left(|\psi_{j_{z+1}}|+1\right)-2\ell^*_{j_z+1}\cdot\left(|\pi_{j_z+1}|-|\pi_{j_{z+1}+1}|\right)$$
$$-\sum_{\text{even } z=1}^{b-1}\ell^*_{j_z+1}\cdot\mathbb{1}\left(j_{z+1}\in\mathfrak{E}(80)\right)\cdot\mathsf{tax}_{1,j_z}(j_{z+1}).$$

To continue, we need the following claim:

Claim 6.80. *For all even $1<z<b$, we have*

$$3\cdot\left(|\psi_{j_{z+1}}|+1\right)-\mathsf{tax}_0(225,j_{z+1})$$
$$\leq 6\cdot\mathbb{1}\left(\mathsf{turn}(j_{z+1})=0\wedge z+1=b\wedge\pi^A_{j_{z+1}}\|\psi^A_{j_{z+1}}\neq\pi^B_{j_{z+1}}\|\psi^B_{j_{z+1}}\right)\cdot\left(|\pi_{j_z+1}|-|\pi_{j_{z-1}+1}|\right).$$

Proof. To start, note that $|\mathscr{R}_{j_{z+1}}|=z$ is even. If $\mathsf{turn}(j_{z+1})=1$, then, we have from Lemma 6.42 that the left hand side is non-positive and there is nothing to show. If $\pi^A_{j_{z+1}}\|\psi^A_{j_{z+1}}=\pi^B_{j_{z+1}}\|\psi^B_{j_{z+1}}$, then by the definition of $\mathsf{tax}_0(225,\cdot)$, we have that the left hand side is non-positive and there is nothing to show. Also, if $z+1<b$, we have by the definition of nice that $j_{z+1}\in\mathfrak{E}(80)$ which together with Lemma 6.44 means again that the left hand side is non-positive and there is nothing to show.

If none of these conditions holds, we have due to Corollary 6.43 that:

$$3\cdot\left(|\psi_{j_{z+1}}|+1\right)-\mathsf{tax}_0(225,j_{z+1})\leq 3\cdot\left(|\psi_{j_{z+1}}|+1\right).$$

Using Lemma 6.13 (the conditions in Lemma 6.13 are satisfied due to the definition of nice), we get:

$$3\cdot\left(|\psi_{j_{z+1}}|+1\right)-\mathsf{tax}_0(225,j_{z+1})\leq 6\cdot\left(|\pi_{j_z+1}|-|\pi_{j_{z+1}+1}|\right),$$

implying that it is enough to show that $|\pi_{j_{z-1}+1}|\leq|\pi_{j_{z+1}+1}|$. To see this, we use the definition of nice to conclude that $j_{z+1}\in\textsc{Range}(j_{z-1})$ and we have:

$$\begin{aligned}
|\pi_{j_{z+1}+1}| &= |\pi_{j_{z+1}}|-1 && \text{(Fact 6.5, item 5 as } |\mathscr{R}_{j_{z+1}}|=z \text{ is even)}\\
&> \mathscr{R}_{j_{z+1}}[z-1].r-1 && \text{(Lemma 6.6 as } |\mathscr{R}_{j_{z+1}}|=z \text{ is even)}\\
&= |\pi_{j_{z-1}+1}|-1, && \text{(Fact 6.5, item 8 as } j_{z+1}\in\textsc{Range}(j_{z-1}))
\end{aligned}$$

and the result follows as all quantities are integers.

□

Using Claim 6.80, we get:

$$\sum_{i=i_a+1}^{num-1}\ell^*_i\leq 10^5\cdot\sum_{i=i_a+1}^{num-1}\mathsf{corr}_i+\sum_{\text{odd } z=1}^{b-1}\ell^*_{j_z+1}\left(\mathsf{G}_{j_z}(j_{z+1})-2300\mathsf{B}_{j_z}(j_{z+1})\right)$$
$$+\sum_{\text{even } z=1}^{b-1}\ell^*_{j_z+1}\cdot\left(\frac{|\pi_{j_z+1}|-|\pi_{j_{z-1}+1}|}{30}\right)$$

$$+ \sum_{\text{even } z=1}^{b-1} 6 \cdot \ell^*_{j_z+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_{z+1}) = 0 \wedge z+1 = b \wedge \pi^A_{j_{z+1}} \| \psi^A_{j_{z+1}} \neq \pi^B_{j_{z+1}} \| \psi^B_{j_{z+1}}\right) \times \left(|\pi_{j_z+1}| - |\pi_{j_{z-1}+1}|\right)$$

$$- \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right)$$

$$- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).$$

To continue, we use the definition of $\mathsf{G}(\cdot)$ and $\mathsf{B}(\cdot)$ to get:

$$\sum_{i=i_a+1}^{num-1} \ell^*_i \leq 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} \ell^*_{j_z+1} \left(\mathsf{G}_{j_z}(j_{z+1}) - 2300\mathsf{B}_{j_z}(j_{z+1})\right)$$

$$+ \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \left(\frac{\mathsf{G}_{j_{z-1}}(j_z) + \mathsf{B}_{j_{z-1}}(j_z)}{30}\right)$$

$$+ \sum_{\text{even } z=1}^{b-1} 6 \cdot \ell^*_{j_z+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_{z+1}) = 0 \wedge z+1 = b \wedge \pi^A_{j_{z+1}} \| \psi^A_{j_{z+1}} \neq \pi^B_{j_{z+1}} \| \psi^B_{j_{z+1}}\right) \times \left(\mathsf{G}_{j_{z-1}}(j_z) + \mathsf{B}_{j_{z-1}}(j_z)\right)$$

$$- \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right)$$

$$- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).$$

This gives:

$$\sum_{i=i_a+1}^{num-1} \ell^*_i \leq 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} \ell^*_{j_z+1} \left(\mathsf{G}_{j_z}(j_{z+1}) - 2300\mathsf{B}_{j_z}(j_{z+1})\right)$$

$$+ \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \left(\frac{\mathsf{G}_{j_{z-1}}(j_z) + \mathsf{B}_{j_{z-1}}(j_z)}{30} + 6 \cdot \mathsf{B}_{j_{z-1}}(j_z)\right)$$

$$+ \sum_{\text{even } z=1}^{b-1} 6 \cdot \ell^*_{j_z+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_{z+1}) = 0 \wedge z+1 = b \wedge \pi^A_{j_{z+1}} \| \psi^A_{j_{z+1}} \neq \pi^B_{j_{z+1}} \| \psi^B_{j_{z+1}}\right) \times \mathsf{G}_{j_{z-1}}(j_z)$$

$$- \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right)$$

$$- \sum_{\text{even } z=1}^{b-1} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).$$

The sum in the third line is non-zero only when $z = b-1$ is even. We get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell_i^* \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} \ell_{j_z+1}^* \left(\mathsf{G}_{j_z}(j_{z+1}) - 2300\mathsf{B}_{j_z}(j_{z+1})\right) \\ + \sum_{\text{even } z=1}^{b-1} \ell_{j_z+1}^* \cdot \left(\frac{\mathsf{G}_{j_{z-1}}(j_z) + \mathsf{B}_{j_{z-1}}(j_z)}{30} + 6 \cdot \mathsf{B}_{j_{z-1}}(j_z)\right) \\ + 6 \cdot \ell_{j_{b-1}+1}^* \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi_{j_b}^A \| \psi_{j_b}^A \ne \pi_{j_b}^B \| \psi_{j_b}^B\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell_{j_z+1}^* \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right) \\ - \sum_{\text{even } z=1}^{b-1} \ell_{j_z+1}^* \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).\end{aligned}$$

To continue, we reindex the second line and get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell_i^* \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} \ell_{j_z+1}^* \left(\mathsf{G}_{j_z}(j_{z+1}) - 2300\mathsf{B}_{j_z}(j_{z+1})\right) \\ + \sum_{\text{odd } z=1}^{b-2} \ell_{j_{z+1}+1}^* \cdot \left(\frac{\mathsf{G}_{j_z}(j_{z+1}) + \mathsf{B}_{j_z}(j_{z+1})}{30} + 6 \cdot \mathsf{B}_{j_z}(j_{z+1})\right) \\ + 6 \cdot \ell_{j_{b-1}+1}^* \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi_{j_b}^A \| \psi_{j_b}^A \ne \pi_{j_b}^B \| \psi_{j_b}^B\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell_{j_z+1}^* \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right) \\ - \sum_{\text{even } z=1}^{b-1} \ell_{j_z+1}^* \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).\end{aligned}$$

Using the definition of ℓ^* and nice, we have $\ell_{j_{z+1}+1}^* = 1.1 \cdot \ell_{j_z+1}^*$ for all $1 < z < b-1$. This allows us to merge the first two lines to get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell_i^* \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} \ell_{j_z+1}^* \left(1.12 \cdot \mathsf{G}_{j_z}(j_{z+1}) - 2280\mathsf{B}_{j_z}(j_{z+1})\right) \\ + 6 \cdot \ell_{j_{b-1}+1}^* \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi_{j_b}^A \| \psi_{j_b}^A \ne \pi_{j_b}^B \| \psi_{j_b}^B\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell_{j_z+1}^* \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right) \\ - \sum_{\text{even } z=1}^{b-1} \ell_{j_z+1}^* \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).\end{aligned}$$

Noting that $\mathsf{B}(\cdot)$ and $\mathsf{tax}_1(\cdot)$ are non-negative, we get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell^*_i \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + \sum_{\text{odd } z=1}^{b-1} 1.12 \cdot \ell^*_{j_z+1} \cdot \mathsf{G}_{j_z}(j_{z+1}) - \sum_{\text{odd } z=1}^{b-3} 2280 \cdot \ell^*_{j_z+1} \cdot \mathsf{B}_{j_z}(j_{z+1}) \\ + 6 \cdot \ell^*_{j_{b-1}+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi^A_{j_b} \| \psi^A_{j_b} \neq \pi^B_{j_b} \| \psi^B_{j_b}\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|) \\ - \sum_{\text{even } z=1}^{b-2} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).\end{aligned}$$

Separating the $z = 1$ term in the first line and reindexing, we get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell^*_i \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + 1.12 \cdot \ell^*_{j_1+1} \cdot \mathsf{G}_{j_1}(j_2) \\ + \sum_{\text{even } z=1}^{b-2} 1.12 \cdot \ell^*_{j_{z+1}+1} \cdot \mathsf{G}_{j_{z+1}}(j_{z+2}) - 2280 \cdot \ell^*_{j_{z-1}+1} \cdot \mathsf{B}_{j_{z-1}}(j_z) \\ + 6 \cdot \ell^*_{j_{b-1}+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi^A_{j_b} \| \psi^A_{j_b} \neq \pi^B_{j_b} \| \psi^B_{j_b}\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|) \\ - \sum_{\text{even } z=1}^{b-2} \ell^*_{j_z+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).\end{aligned}$$

Using the definition of ℓ^* and nice, we have $\ell^*_{j_{z+1}+1} = 1.1 \cdot \ell^*_{j_z+1}$ for all $1 < z < b-1$. This allows us to get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell^*_i \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + 1.12 \cdot \ell^*_{j_1+1} \cdot \mathsf{G}_{j_1}(j_2) \\ + \sum_{\text{even } z=1}^{b-2} 1.12 \cdot \ell^*_{j_{z+1}+1} \cdot \mathsf{G}_{j_{z+1}}(j_{z+2}) - 1500 \cdot \ell^*_{j_{z+1}+1} \cdot \mathsf{B}_{j_{z-1}}(j_z) \\ + 6.6\ell^*_{j_{b-2}+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi^A_{j_b} \| \psi^A_{j_b} \neq \pi^B_{j_b} \| \psi^B_{j_b}\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|) \\ - \sum_{\text{even } z=1}^{b-2} 0.9 \cdot \ell^*_{j_{z+1}+1} \cdot \mathbb{1}\left(j_{z+1} \in \mathfrak{E}(80)\right) \cdot \mathsf{tax}_{1,j_z}(j_{z+1}).\end{aligned}$$

Next, we note by the definition of nice that $j_{z+1} \in \mathfrak{E}(80)$ for all even $z \leq b-2$. We get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell_i^* \leq 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + 1.12 \cdot \ell^*_{j_1+1} \cdot \mathsf{G}_{j_1}(j_2) \\ + \sum_{\text{even } z=1}^{b-2} \ell^*_{j_{z+1}+1} \cdot \left(1.12 \cdot \mathsf{G}_{j_{z+1}}(j_{z+2}) - 1500 \cdot \mathsf{B}_{j_{z-1}}(j_z) - 0.9 \cdot \mathsf{tax}_{1,j_z}(j_{z+1})\right) \\ + 6.6\ell^*_{j_{b-2}+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi^A_{j_b}\|\psi^A_{j_b} \neq \pi^B_{j_b}\|\psi^B_{j_b}\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|).\end{aligned}$$

Now, note that

$$\begin{aligned}\ell^*_{j_{b-2}+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi^A_{j_b}\|\psi^A_{j_b} \neq \pi^B_{j_b}\|\psi^B_{j_b}\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) \\ \leq \ell^*_{j_1+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_3) = 0 \wedge b = 3 \wedge \pi^A_{j_3}\|\psi^A_{j_3} \neq \pi^B_{j_3}\|\psi^B_{j_3}\right) \cdot \mathsf{G}_{j_1}(j_2) \\ + \sum_{\text{even } z=1}^{b-2} \ell^*_{j_{z+1}+1} \cdot \mathsf{G}_{j_{z+1}}(j_{z+2}).\end{aligned}$$

Indeed, either b is even, in which case the left hand side is 0 and there is nothing to show, or $b = 3$, in which case $\ell^*_{j_{b-2}+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_b) = 0 \wedge b \text{ is odd } \wedge \pi^A_{j_b}\|\psi^A_{j_b} \neq \pi^B_{j_b}\|\psi^B_{j_b}\right) \cdot \mathsf{G}_{j_{b-2}}(j_{b-1}) = \ell^*_{j_1+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_3) = 0 \wedge \pi^A_{j_3}\|\psi^A_{j_3} \neq \pi^B_{j_3}\|\psi^B_{j_3}\right) \cdot \mathsf{G}_{j_1}(j_2)$ and we are done or $b > 3$ is odd, in which case the inequality follows by substituting $z = b-3$ in the right hand side. This gives:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell_i^* \leq 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + 1.12 \cdot \ell^*_{j_1+1} \cdot \mathsf{G}_{j_1}(j_2) \\ + \sum_{\text{even } z=1}^{b-2} \ell^*_{j_{z+1}+1} \cdot \left(8 \cdot \mathsf{G}_{j_{z+1}}(j_{z+2}) - 1500 \cdot \mathsf{B}_{j_{z-1}}(j_z) - 0.9 \cdot \mathsf{tax}_{1,j_z}(j_{z+1})\right) \\ + 6.6 \cdot \ell^*_{j_1+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_3) = 0 \wedge b = 3 \wedge \pi^A_{j_3}\|\psi^A_{j_3} \neq \pi^B_{j_3}\|\psi^B_{j_3}\right) \cdot \mathsf{G}_{j_1}(j_2) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|).\end{aligned}$$

In order to continue, we apply the Lemma 6.59 on j_{z-1}, j_z, and j_{z+1} for even $z \leq b-2$. Note that the conditions in Lemma 6.59 are satisfied due to the definition of nice. We get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell_i^* \leq 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + 1.12 \cdot \ell^*_{j_1+1} \cdot \mathsf{G}_{j_1}(j_2) \\ + \sum_{\text{even } z=1}^{b-2} \ell^*_{j_{z+1}+1} \cdot \left(8 \cdot \mathsf{G}_{j_{z+1}}(j_{z+2}) - 45 \cdot \left(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\right)\right) \\ + 6.6 \cdot \ell^*_{j_1+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_3) = 0 \wedge b = 3 \wedge \pi^A_{j_3}\|\psi^A_{j_3} \neq \pi^B_{j_3}\|\psi^B_{j_3}\right) \cdot \mathsf{G}_{j_1}(j_2)\end{aligned}$$

$$- \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|).$$

Next, note by the definition of G that, for even $z \le b-2$, we have $\mathsf{G}_{j_{z+1}}(j_{z+2}) \le |\pi_{j_{z+2}+1}| - |\pi_{j_{z+1}+1}|$. Applying Lemma 6.15, gives us $|\pi_{j_{z+1}+1}| = \min_{j' \in [j_z : \textsc{Stop}(j_{z+1})] \setminus \{num\}} |\pi_{j'+1}| \le \min_{j' \in [j_z : j_{z+2}]} |\pi_{j'+1}|$ by the definition of nice. Combining, we get $\mathsf{G}_{j_{z+1}}(j_{z+2}) \le |\pi_{j_{z+2}+1}| + \min_{j' \in [j_z : j_{z+2}]} |\pi_{j'+1}| - 2 \cdot |\pi_{j_{z+1}+1}|$ which with Lemma 6.11 gives $\mathsf{G}_{j_{z+1}}(j_{z+2}) \le 2 \cdot \big(|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|\big)$. Plugging in, we get:

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell^*_i \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + 1.12 \cdot \ell^*_{j_1+1} \cdot \mathsf{G}_{j_1}(j_2) \\ + 6.6 \cdot \ell^*_{j_1+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_3) = 0 \wedge b = 3 \wedge \pi^A_{j_3} \| \psi^A_{j_3} \ne \pi^B_{j_3} \| \psi^B_{j_3}\right) \cdot \mathsf{G}_{j_1}(j_2) \\ - \sum_{\text{even } z=1}^{b-1} 2\ell^*_{j_z+1} \cdot (|\pi_{j_z+1}| - |\pi_{j_{z+1}+1}|).\end{aligned}$$

Observe that, if $b = 2$, then the last term is 0. Otherwise, if $b > 2$, we have by the definition of nice and Lemma 6.13 that, for all even $z \le b-1$, it holds that $|\pi_{j_z+1}| \ge |\pi_{j_{z+1}+1}|$. This gives (using $\ell^*_{j_2+1} > \ell^*_{j_1+1}$ if $b > 2$):

$$\begin{aligned}\sum_{i=i_a+1}^{num-1} \ell^*_i \le 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_i + 1.12 \cdot \ell^*_{j_1+1} \cdot \mathsf{G}_{j_1}(j_2) - 2 \cdot \mathbb{1}(b > 2) \cdot \ell^*_{j_1+1} \cdot (|\pi_{j_2+1}| - |\pi_{j_3+1}|) \\ + 6.6 \cdot \ell^*_{j_1+1} \cdot \mathbb{1}\left(\mathsf{turn}(j_3) = 0 \wedge b = 3 \wedge \pi^A_{j_3} \| \psi^A_{j_3} \ne \pi^B_{j_3} \| \psi^B_{j_3}\right) \cdot \mathsf{G}_{j_1}(j_2).\end{aligned} \tag{55}$$

We now show the following claims:

Claim 6.81. *If $b > 2$, then for $C \in \{A, B\}$, we have $\pi^C_{j_2+1}[1 : |\pi_{j_3+1}|] = \pi^C_{num}[1 : |\pi_{j_3+1}|]$.*

Proof. As the parties only add/remove one symbol from π in every iteration, it is sufficient to show that $|\pi_{j_3+1}| \le |\pi_{j'+1}|$ for all $j' \in [j_2 : num)$. This follows from Lemma 6.13 if $b = 3$ and Lemma 6.15 if $b > 3$. □

Claim 6.82. $1.12 \cdot \mathsf{G}_{j_1}(j_2) - 2 \cdot \mathbb{1}(b > 2) \cdot (|\pi_{j_2+1}| - |\pi_{j_3+1}|) \le 1.12 \cdot |\mathsf{LCP}\left(\pi^A_{num}, \pi^B_{num}\right)|$.

Proof. If $b = 2$, then by Claim 6.79, we have $j_2 = num - 1$ and we get from the definition of $\mathsf{G}(\cdot)$ that $1.12 \cdot \mathsf{G}_{j_1}(j_2) = 1.12 \cdot |\mathsf{LCP}(\pi^A_{num}(|\pi_{j_1+1}| : |\pi_{num}|], \pi^B_{num}(|\pi_{j_1+1}| : |\pi_{num}|])| = 1.12 \cdot |\mathsf{LCP}(\pi^A_{num}, \pi^B_{num})|$ as $j_1 = i_a \implies |\pi_{j_1+1}| = 0$. Otherwise, we have $b > 2$ and we derive:

$$\begin{aligned}&1.12 \cdot \mathsf{G}_{j_1}(j_2) - 2 \cdot (|\pi_{j_2+1}| - |\pi_{j_3+1}|) \\ &\quad \le 1.12 \cdot \mathsf{G}_{j_1}(j_2) - 1.12 \cdot (|\pi_{j_2+1}| - |\pi_{j_3+1}|) && \text{(As } |\pi_{j_2+1}| \ge |\pi_{j_3+1}|) \\ &\quad \le 1.12 \cdot |\mathsf{LCP}(\pi^A_{j_2+1}(|\pi_{j_1+1}| : |\pi_{j_2+1}|], \pi^B_{j_2+1}(|\pi_{j_1+1}| : |\pi_{j_2+1}|])| - 1.12 \cdot (|\pi_{j_2+1}| - |\pi_{j_3+1}|) \\ &&& \text{(Definition of } \mathsf{G}(\cdot))\end{aligned}$$

$$
\begin{aligned}
&\leq 1.12 \cdot |\mathsf{LCP}(\pi^A_{j_2+1}(|\pi_{j_1+1}| : |\pi_{j_3+1}|], \pi^B_{j_2+1}(|\pi_{j_1+1}| : |\pi_{j_3+1}|])| && \text{(As } |\pi_{j_2+1}| \geq |\pi_{j_3+1}|\text{)}\\
&\leq 1.12 \cdot |\mathsf{LCP}(\pi^A_{j_2+1}[1 : |\pi_{j_3+1}|], \pi^B_{j_2+1}[1 : |\pi_{j_3+1}|])| && \text{(As } j_1 = i_a \implies |\pi_{j_1+1}| = 0\text{)}\\
&\leq 1.12 \cdot |\mathsf{LCP}(\pi^A_{num}[1 : |\pi_{j_3+1}|], \pi^B_{num}[1 : |\pi_{j_3+1}|])| && \text{(Claim 6.81)}\\
&\leq 1.12 \cdot |\mathsf{LCP}(\pi^A_{num}, \pi^B_{num})|. && \text{(Definition of } \mathsf{LCP}(\cdot)\text{)}
\end{aligned}
$$

□

Claim 6.83. *If $b = 3$, $\mathsf{turn}(j_3) = 0$, and $\pi^A_{j_3}\|\psi^A_{j_3} \neq \pi^B_{j_3}\|\psi^B_{j_3}$, we have $\mathsf{G}_{j_1}(j_2) = |\mathsf{LCP}(\pi^A_{num}, \pi^B_{num})|$.*

Proof. By definition of nice and Claim 6.79, we have $j_3 = num - 1$ and $|\mathscr{R}_{j_3}|$ is even. Due to the latter, we have by the definition of $\mathsf{turn}(\cdot)$ that $\psi^A_{j_3}\|\sigma^A_{j_3} = \psi^B_{j_3}\|\sigma^B_{j_3}$. This together with item 5 of Fact 6.5 gives us that $\psi^A_{j_3}\|\pi^A_{j_3}[|\pi_{j_3}|] = \psi^B_{j_3}\|\pi^B_{j_3}[|\pi_{j_3}|]$. However, as $\pi^A_{j_3}\|\psi^A_{j_3} \neq \pi^B_{j_3}\|\psi^B_{j_3}$, this is only possible if $\pi^A_{j_3}[1 : |\pi_{j_3}|) \neq \pi^B_{j_3}[1 : |\pi_{j_3}|)$ which using item 5 of Fact 6.5 and $j_3 = num - 1$ means that $\pi^A_{num} \neq \pi^B_{num}$, which when combined with Claim 6.81 gives $\pi^A_{j_2+1}[1 : |\pi_{num}|] \neq \pi^B_{j_2+1}[1 : |\pi_{num}|]$ implying that

$$
\begin{aligned}
\mathsf{G}_{j_1}(j_2) &= |\mathsf{LCP}(\pi^A_{j_2+1}(|\pi_{j_1+1}| : |\pi_{j_2+1}|], \pi^B_{j_2+1}(|\pi_{j_1+1}| : |\pi_{j_2+1}|])|\\
&= |\mathsf{LCP}(\pi^A_{j_2+1}, \pi^B_{j_2+1})| && \text{(As } j_1 = i_a \implies |\pi_{j_1+1}| = 0\text{)}\\
&= |\mathsf{LCP}(\pi^A_{j_2+1}[1 : |\pi_{num}|], \pi^B_{j_2+1}[1 : |\pi_{num}|])| && \text{(As } \pi^A_{j_2+1}[1 : |\pi_{num}|] \neq \pi^B_{j_2+1}[1 : |\pi_{num}|]\text{)}\\
&= |\mathsf{LCP}(\pi^A_{num}, \pi^B_{num})|. && \text{(Claim 6.81 and } j_3 = num - 1\text{)}
\end{aligned}
$$

□

Plugging in Claim 6.82 and Claim 6.83 into Equation 55, we get:

$$\sum_{i=i_a+1}^{num-1} \ell^*_i \leq 10^5 \cdot \sum_{i=i_a+1}^{num-1} \mathsf{corr}_{j'} + 8 \cdot \ell^*_{j_1+1} \cdot |\mathsf{LCP}\left(\pi^A_{num}, \pi^B_{num}\right)|,$$

and Equation 54 follows as $j_1 = i_a \implies \ell^*_{j_1+1} = \ell^*_1$ by definition of ℓ^*.

□

6.3 Proof of Theorem 6.2

This section is dedicated to proving Theorem 6.2. We will need the following definition

Definition 6.84. *For $C \in \{A, B\}$, $i \in [R/(P+1)+1]$, and $j \in [|\boldsymbol{\mathcal{S}}^C_i|]$, define the value $\mathsf{last}^C_i(j)$ as:*

$$\mathsf{last}^C_i(j) = \max\{j' \in [i] \mid |\boldsymbol{\mathcal{S}}^C_{j'}| = j \text{ and } j' - 1 \in \{0\} \cup \mathfrak{E}^C(52)\}.$$

As the value of $|\boldsymbol{\mathcal{S}}^C|$ increases by at most 1 in every iteration, and increases only when party C executes Line 52, we have that the $\max(\cdot)$ in the definition above is always over a non-empty set, and is thus, well defined. We will omit the subscript i when $i = R/(P+1)+1$. Some properties of the function $\mathsf{last}^C_i(\cdot)$ are captured in the following lemma.

Lemma 6.85. *It holds for all $C \in \{A, B\}$ that:*

1. *For all $i \in [R/(P+1)+1]$ and all $j < j' \in [|\boldsymbol{\mathcal{S}}_i^C|]$, we have $\mathsf{last}_i^C(j) < \mathsf{last}_i^C(j')$.*
2. *For all $i' \leq i \in [R/(P+1)+1]$ and all $j \in [|\boldsymbol{\mathcal{S}}_i^C|]$ such that $i' \geq \mathsf{last}_i^C(j)$, we have $|\boldsymbol{\mathcal{S}}_{i'}^C| \geq j$ and $\boldsymbol{\mathcal{S}}_{i'}^C[j] = \boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C[j]$.*
3. *For all $i \in [R/(P+1)]$ and all $j \in [\min(|\boldsymbol{\mathcal{S}}_i^C|, |\boldsymbol{\mathcal{S}}_{i+1}^C|)]$, we have $\mathsf{last}_i^C(j) = \mathsf{last}_{i+1}^C(j)$.*
4. *For all $i \in [R/(P+1)+1]$ and all $1 \leq j < |\boldsymbol{\mathcal{S}}_i^C|$, we have $\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C = \boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j+1)-1}^C$.*
5. *For all $i \in [R/(P+1)+1]$, we have $\boldsymbol{\mathcal{S}}_i^C.last = \boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_i^C|)}^C.last$.*

Proof. We have that:

1. By Definition 6.84, we have that $|\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C| = j$. Under the conditions of the lemma, this extends to $j = |\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C| < j' \leq |\boldsymbol{\mathcal{S}}_i^C|$. As $|\boldsymbol{\mathcal{S}}^C|$ increases by at most 1 in every iteration, and increases only if party C executes Line 52, $|\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C| < j' \leq |\boldsymbol{\mathcal{S}}_i^C|$ implies that there is an iteration i' such that $\mathsf{last}_i^C(j) < i' \leq i$ such that $|\boldsymbol{\mathcal{S}}_{i'}^C| = j'$ and $i' - 1 \in \mathfrak{E}^C(52)$. In particular we get that $\mathsf{last}_i^C(j') \geq i' > \mathsf{last}_i^C(j)$.

2. We first show that $|\boldsymbol{\mathcal{S}}_{i'}^C| \geq j$ by contradiction. Suppose that $|\boldsymbol{\mathcal{S}}_{i'}^C| < j$. Under the conditions of the lemma, this extends to $|\boldsymbol{\mathcal{S}}_{i'}^C| < j \leq |\boldsymbol{\mathcal{S}}_i^C|$. As $|\boldsymbol{\mathcal{S}}^C|$ increases by at most 1 in every iteration, and increases only if party C executes Line 52, $|\boldsymbol{\mathcal{S}}_{i'}^C| < j \leq |\boldsymbol{\mathcal{S}}_i^C|$ implies that there is an iteration $i' < i'' \leq i$ such that $|\boldsymbol{\mathcal{S}}_{i''}^C| = j$ and $i'' - 1 \in \mathfrak{E}^C(52)$. As $\mathsf{last}_i^C(j) \leq i'$, this contradicts Definition 6.84.

   We now show that $\boldsymbol{\mathcal{S}}_{i'}^C[j] = \boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C[j]$. Suppose not. Observe that, in our protocol, the only way the parties can change the j^{th} entry in $\boldsymbol{\mathcal{S}}$ is by removing it in one iteration and adding a different one in a subsequent iteration. Thus, $\boldsymbol{\mathcal{S}}_{i'}^C[j] = \boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C[j]$ and $i' \geq \mathsf{last}_i^C(j)$ implies that there is an iteration $\mathsf{last}_i^C(j) < i'' \leq i' \leq i$ such that $|\boldsymbol{\mathcal{S}}_{i''}^C| = j$ and $i'' - 1 \in \mathfrak{E}^C(52)$. However, this contradicts Definition 6.84.

3. We observe from Definition 6.84 that, if $\mathsf{last}_i^C(j) \neq \mathsf{last}_{i+1}^C(j)$ for some j, then, $\mathsf{last}_{i+1}^C(j) = i + 1$ and therefore $i \in \mathfrak{E}^C(52)$ and $j = |\boldsymbol{\mathcal{S}}_{i+1}^C| = |\boldsymbol{\mathcal{S}}_i^C| + 1$. In particular, $j \notin [\min(|\boldsymbol{\mathcal{S}}_i^C|, |\boldsymbol{\mathcal{S}}_{i+1}^C|)] = [|\boldsymbol{\mathcal{S}}_i^C|]$ and we have a contradiction.

4. We first show that $|\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C| = |\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j+1)-1}^C| = j$. Indeed, $|\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C| = j$ is straightforward by Definition 6.84. Also, by Definition 6.84 and the fact that $j \geq 1$, we get that $|\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j+1)}^C| = j + 1$ and $\mathsf{last}_i^C(j+1) - 1 \in \mathfrak{E}^C(52)$. Together, this gives $|\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j+1)-1}^C| = |\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j+1)}^C| - 1 = j$ as desired.

   We now show that, for all $j' \in [j]$, we have that $\boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j)}^C[j'] = \boldsymbol{\mathcal{S}}_{\mathsf{last}_i^C(j+1)-1}^C[j']$. Let $j' \in [j]$. As $j' \leq j < j+1$, we have by item 1 that $\mathsf{last}_i^C(j') \leq \mathsf{last}_i^C(j) < \mathsf{last}_i^C(j+1) \implies$

$\mathsf{last}_i^C(j') \leq \mathsf{last}_i^C(j) \leq \mathsf{last}_i^C(j+1) - 1$ as all quantities are integers. By item 2, this gives:

$$\boldsymbol{\mathcal{S}}^C_{\mathsf{last}_i^C(j)}[j'] = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}_i^C(j')}[j'] = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}_i^C(j+1)-1}[j'],$$

as desired.

5. By item 2, we get $\boldsymbol{\mathcal{S}}_i^C.last = \boldsymbol{\mathcal{S}}_i^C[|\boldsymbol{\mathcal{S}}_i^C|] = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_i^C|)}[|\boldsymbol{\mathcal{S}}_i^C|]$. Due to Definition 6.84, we have $|\boldsymbol{\mathcal{S}}^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_i^C|)}| = |\boldsymbol{\mathcal{S}}_i^C|$ and can extend to $\boldsymbol{\mathcal{S}}_i^C.last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_i^C|)}.last$.

□

With Definition 6.84 and Lemma 6.85, we can now prove Theorem 6.2.

Proof of Theorem 6.2. To start, observe that if $\mathcal{A}'$ is such that $\forall C \in \{A, B\} : \Pi'^C_{\mathcal{A}'}(x^A, x^B) = \Pi^C(x^A, x^B)$, then we can set $\mathcal{A}''$ to be the adversary that does not corrupt any of the messages by any of the parties. When the protocol Π' is run with $\mathcal{A}''$, the parties execute Line 52 for the first $\frac{S}{1100KP}$ iterations (our choice of parameters ensures that $\frac{S}{1100KP}$ is an integer), and exchange $\perp$s afterwards. This, taking the adversary $\mathcal{A}''$ and setting $num = \frac{S}{1100KP} + 1$ satisfies all the requirements of Theorem 6.2.

We can therefore, assume that $\exists C \in \{A, B\} : \Pi'^C_{\mathcal{A}'}(x^A, x^B) \neq \Pi^C(x^A, x^B)$. We assume that $C = A$ without loss of generality. We define:

Definition 6.86. *We define* Sync *to be the set containing all* $j \in [\min(|\boldsymbol{\mathcal{S}}^A|, |\boldsymbol{\mathcal{S}}^B|)]$ *such that* $\mathsf{last}^A(j) = \mathsf{last}^B(j)$ *and we have*

$$(\mathscr{P}^A_{\mathsf{last}^A(j)}, |\boldsymbol{\mathcal{S}}^A_{\mathsf{last}^A(j)}|) = (\mathscr{P}^B_{\mathsf{last}^B(j)}, |\boldsymbol{\mathcal{S}}^B_{\mathsf{last}^B(j)}|).$$

Observe that $1 \in \mathsf{Sync}$. Let $M = \max(\mathsf{Sync})$ denote the largest element in Sync. Note that $M \leq \min(|\boldsymbol{\mathcal{S}}^A|, |\boldsymbol{\mathcal{S}}^B|)$. For $1 \leq j < M$ and $C \in \{A, B\}$, define,

$$\mathsf{lo}(j) = \max\{j' \in \mathsf{Sync} \mid j' \leq j\}.$$
$$\mathsf{hi}(j) = \min\{j' \in \mathsf{Sync} \mid j' > j\}.$$
$$\mathsf{tip}^C(j) = \begin{cases} \mathsf{hi}(j) & , |\mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}| \text{ is odd} \\ 1 + \max\{\mathsf{lo}(j) \leq j' < \mathsf{hi}(j) \mid |\mathscr{R}^C_{\mathsf{last}^C(j')}| \text{ is odd}\} & , |\mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}| \text{ is even} \end{cases}.$$

If the max in the definition of $\mathsf{tip}(\cdot)$ is over an empty set, we define $\mathsf{tip}^C(j) = \mathsf{lo}(j)$. As $1, M \in \mathsf{Sync}$, both $\mathsf{lo}(j)$ and $\mathsf{hi}(j)$ are well defined for all $1 \leq j < M$ and $\mathsf{lo}(j) < \mathsf{hi}(j)$.

Claim 6.87. *Let* $C \in \{A, B\}$. *For all* $1 \leq j < M$ *and* $\mathsf{tip}^C(j) \leq j' \leq \mathsf{hi}(j)$, *we have:*

$$|\psi^C_{\mathsf{last}^C(j')}| = |\psi^C_{\mathsf{last}^C(\mathsf{hi}(j))}| + j' - \mathsf{hi}(j).$$

Proof. Proof by backwards induction on j'. The base case $j' = \mathsf{hi}(j)$ is trivial. We show the statement holds for $\mathsf{tip}^C(j) \leq j' < \mathsf{hi}(j)$ by assuming it holds for $j' + 1$. As we assume

that $\mathsf{tip}^C(j) < \mathsf{hi}(j)$, we have by the definition of $\mathsf{tip}(\cdot)$ that $|\mathscr{R}^C_{\mathsf{last}^C(j'')}|$ is even for all $j'' \in [\mathsf{tip}^C(j) : \mathsf{hi}(j)]$.

In particular, we get that $|\mathscr{R}^C_{\mathsf{last}^C(j')}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j'+1)}|$ are both even. Applying item 4 of Lemma 6.85, we get that $|\mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j'+1)}|$ are both even. As $\mathsf{last}^C(j'+1)-1 \in \mathfrak{E}^C(52)$ by Definition 6.84, we get from the fact that $|\mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j'+1)}|$ are both even that $|\psi^C_{\mathsf{last}^C(j'+1)}| = |\psi^C_{\mathsf{last}^C(j'+1)-1}| + 1$. This gives:

$$\begin{aligned}
|\psi^C_{\mathsf{last}^C(j')}| &= |\psi^C_{\mathsf{last}^C(j'+1)-1}| && \text{(Lemma 6.85, item 4)}\\
&= |\psi^C_{\mathsf{last}^C(j'+1)}| - 1 && \text{(As } |\psi^C_{\mathsf{last}^C(j'+1)}| = |\psi^C_{\mathsf{last}^C(j'+1)-1}| + 1\text{)}\\
&= |\psi^C_{\mathsf{last}^C(\mathsf{hi}(j))}| - \mathsf{hi}(j) + j' + 1 - 1 && \text{(Induction hypothesis)}\\
&= |\psi^C_{\mathsf{last}^C(\mathsf{hi}(j))}| - \mathsf{hi}(j) + j',
\end{aligned}$$

and the result follows. □

Claim 6.88. *Let $C \in \{A, B\}$. For all $1 \leq j < M$ such that $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}|$ is even and $\mathsf{tip}^C(j) > \mathsf{lo}(j)$, we have:*

$$|\psi^C_{\mathsf{last}^C(\mathsf{tip}^C(j))}| = 0.$$

Proof. Under the assumptions of the lemma, we have by the definition of $\mathsf{tip}(\cdot)$ that $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{tip}^C(j)-1)}|$ is odd and $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{tip}^C(j))}|$ is even. Applying item 4 of Lemma 6.85, we get that $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{tip}^C(j))-1}|$ is odd and $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{tip}^C(j))}|$ is even. As $\mathsf{last}^C(\mathsf{tip}^C(j))-1 \in \mathfrak{E}^C(52)$ by Definition 6.84, we get from the fact that $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{tip}^C(j))-1}|$ is odd and $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{tip}^C(j))}|$ is even that $|\psi^C_{\mathsf{last}^C(\mathsf{tip}^C(j))}| = 0$ as desired. □

Corollary 6.89. *For all $1 \leq j < M$, we have $\mathsf{tip}^A(j) = \mathsf{tip}^B(j)$.*

Proof. Suppose first that there exists a $C \in \{A, B\}$ such that $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}|$ is odd. In this case, as $\mathsf{hi}(j) \in \mathsf{Sync}$ by definition, we have from Definition 6.86 that $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}|$ is odd for all $C \in \{A, B\}$ as well implying that $\mathsf{tip}^A(j) = \mathsf{tip}^B(j) = \mathsf{hi}(j)$.

For the rest of the proof, we assume that $|\mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}|$ is even for all $C \in \{A, B\}$. Suppose for the sake of contradiction that $\mathsf{tip}^A(j) \neq \mathsf{tip}^B(j)$ and assume without loss of generality that $\mathsf{tip}^A(j) < \mathsf{tip}^B(j)$. As $\mathsf{lo}(j) \leq \mathsf{tip}^A(j)$, we get:

$$\begin{aligned}
|\psi^B_{\mathsf{last}^B(\mathsf{hi}(j))}| &= |\psi^B_{\mathsf{last}^B(\mathsf{tip}^B(j))}| + \mathsf{hi}(j) - \mathsf{tip}^B(j) && \text{(Claim 6.87)}\\
&= \mathsf{hi}(j) - \mathsf{tip}^B(j) && \text{(Claim 6.88)}\\
&< |\psi^A_{\mathsf{last}^A(\mathsf{tip}^B(j)-1)}| + \mathsf{hi}(j) - \mathsf{tip}^B(j) + 1\\
&\leq |\psi^A_{\mathsf{last}^A(\mathsf{hi}(j))}| && \text{(Claim 6.87)}\\
&= |\psi^B_{\mathsf{last}^B(\mathsf{hi}(j))}|, && \text{(As } \mathsf{hi}(j) \in \mathsf{Sync} \text{ and Definition 6.86)}
\end{aligned}$$

a contradiction. □

Owing to Corollary 6.89, we henceforth omit the superscript C in $\mathsf{tip}^C(\cdot)$ and simply write $\mathsf{tip}(j)$. We also note that:

Claim 6.90. *If* $1 \leq j < M$ *and* $j \notin \mathsf{Sync}$*, then we have* $\mathsf{lo}(j) = \mathsf{lo}(j-1)$ *and* $\mathsf{hi}(j) = \mathsf{hi}(j-1)$ *and* $\mathsf{tip}(j) = \mathsf{tip}(j-1)$.

Proof. Note that $j \notin \mathsf{Sync}$ implies that $j > 1$. The first two follow straightforwardly from the definitions. For the third, note that $\mathsf{tip}(j)$ is determined by $\mathsf{lo}(j)$ and $\mathsf{hi}(j)$ and therefore $\mathsf{tip}(j) = \mathsf{tip}(j-1)$. □

Claim 6.91. *For all* $1 \leq j < M$ *and all* $\mathsf{tip}(j) \leq j' \leq \mathsf{hi}(j)$*, the following hold:*

1. *For* $C \in \{A, B\}$*, we have:*

$$\exists j'' \in (\mathsf{tip}(j) : j'] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90) \implies \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t > 0.$$

2. *We have:*

$$\left(\mathscr{R}^A_{\mathsf{last}^A(j')}.last, |\pi^A_{\mathsf{last}^A(j')}|, |\psi^A_{\mathsf{last}^A(j')}|\right) = \left(\mathscr{R}^B_{\mathsf{last}^B(j')}.last, |\pi^B_{\mathsf{last}^B(j')}|, |\psi^B_{\mathsf{last}^B(j')}|\right).$$

3. *For* $C \in \{A, B\}$*, we have:*

$$\begin{aligned}\exists j'' \in (\mathsf{tip}(j) : j'] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90)\\ \implies \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t\\ \implies \nexists j'' \in (j' : \mathsf{hi}(j)] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90).\end{aligned}$$

4. *For* $C \in \{A, B\}$*, we have* $\mathscr{R}^C_{\mathsf{last}^C(j')}.last.\alpha = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\alpha$ *and*

$$\mathscr{R}^C_{\mathsf{last}^C(j')}.last.\beta = \begin{cases} \diamond & , \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & , \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}.$$

Proof. Suppose first that $\mathsf{tip}(j) = \mathsf{hi}(j)$. In this case, we also have $\mathsf{tip}(j) = j' = \mathsf{hi}(j)$ and the claim is straightforward due to Definition 6.86 as $\mathsf{hi}(j) \in \mathsf{Sync}$. So assume throughout that $\mathsf{tip}(j) < \mathsf{hi}(j)$. By the definition of $\mathsf{tip}(\cdot)$, this means that $|\mathscr{R}^C_{\mathsf{last}^C(j'')}|$ is even for all $j'' \in [\mathsf{tip}(j) : \mathsf{hi}(j)]$ and all $C \in \{A, B\}$.

It follows that, for all $j'' \in (\mathsf{tip}(j) : \mathsf{hi}(j)]$ and all $C \in \{A, B\}$, we have that $|\mathscr{R}^C_{\mathsf{last}^C(j''-1)}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j'')}|$ are both even. Due to item 4 of Lemma 6.85, this means that $|\mathscr{R}^C_{\mathsf{last}^C(j'')-1}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j'')}|$ are both even. As $\mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(52)$ by Definition 6.84, this is only possible if $\mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(87)$ for all $j'' \in (\mathsf{tip}(j) : \mathsf{hi}(j)]$.

For item 1, we proceed by induction on j'. The base case $j' = \mathsf{tip}(j)$ is trivial. We show the claim for $j' \in (\mathsf{tip}(j) : \mathsf{hi}(j)]$ by assuming it holds for $j' - 1$. Let $C \in \{A, B\}$. We showed that $\mathsf{last}^C(j') - 1 \in \mathfrak{E}^C(87)$. If $\mathsf{last}^C(j') - 1 \notin \mathfrak{E}^C(90)$, we derive:

$$\exists j'' \in (\mathsf{tip}(j) : j'] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90)$$

$$\implies \exists j'' \in (\mathsf{tip}(j) : j') : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90)$$
$$\implies \mathscr{R}^C_{\mathsf{last}^C(j'-1)}.last.t > 0 \qquad \text{(Induction hypothesis)}$$
$$\implies \mathscr{R}^C_{\mathsf{last}^C(j')-1}.last.t > 0 \qquad \text{(Lemma 6.85, item 4)}$$
$$\implies \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t > 0. \qquad \text{(As } \mathsf{last}^C(j') - 1 \in \mathfrak{E}^C(87) \setminus \mathfrak{E}^C(90)\text{)}$$

Otherwise, if $\mathsf{last}^C(j') - 1 \in \mathfrak{E}^C(90)$, we get that $\mathscr{R}^C_{\mathsf{last}^C(j')}.last.t > 0$ by Line 90 and the proof is complete.

For the remaining parts, we proceed by backwards induction on j'. The base case $j' = \mathsf{hi}(j)$ is straightforward due to Definition 6.86 as $\mathsf{hi}(j) \in \mathsf{Sync}$. We show the statement holds for $\mathsf{tip}(j) \leq j' < \mathsf{hi}(j)$ by assuming it holds for $j' + 1$. Recall that $\mathsf{last}^C(j' + 1) - 1 \in \mathfrak{E}^C(87)$. We have:

1. The fact that $\mathsf{last}^C(j' + 1) - 1 \in \mathfrak{E}^C(87)$ implies that for $C \in \{A, B\}$, the tuple $\left(\mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last, |\pi^C_{\mathsf{last}^C(j'+1)}|, |\psi^C_{\mathsf{last}^C(j'+1)}|\right)$ completely determines the tuple $\left(\mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last, |\pi^C_{\mathsf{last}^C(j'+1)-1}|, |\psi^C_{\mathsf{last}^C(j'+1)-1}|\right)$ for $C \in \{A, B\}$. Thus, our induction hypothesis that $\left(\mathscr{R}^A_{\mathsf{last}^A(j'+1)}.last, |\pi^A_{\mathsf{last}^A(j'+1)}|, |\psi^A_{\mathsf{last}^A(j'+1)}|\right) = \left(\mathscr{R}^B_{\mathsf{last}^B(j'+1)}.last, |\pi^B_{\mathsf{last}^B(j'+1)}|, |\psi^B_{\mathsf{last}^B(j'+1)}|\right)$ implies

$$\left(\mathscr{R}^A_{\mathsf{last}^A(j'+1)-1}.last, |\pi^A_{\mathsf{last}^A(j'+1)-1}|, |\psi^A_{\mathsf{last}^A(j'+1)-1}|\right) = \left(\mathscr{R}^B_{\mathsf{last}^B(j'+1)-1}.last, |\pi^B_{\mathsf{last}^B(j'+1)-1}|, |\psi^B_{\mathsf{last}^B(j'+1)-1}|\right),$$

   which using item 4 of Lemma 6.85 implies that

$$\left(\mathscr{R}^A_{\mathsf{last}^A(j')}.last, |\pi^A_{\mathsf{last}^A(j')}|, |\psi^A_{\mathsf{last}^A(j')}|\right) = \left(\mathscr{R}^B_{\mathsf{last}^B(j')}.last, |\pi^B_{\mathsf{last}^B(j')}|, |\psi^B_{\mathsf{last}^B(j')}|\right),$$

2. If $\mathsf{last}^C(j' + 1) - 1 \notin \mathfrak{E}^C(90)$, then we have $\mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.t = \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t$ by item 4 of Lemma 6.85 implying that:

$$\exists j'' \in (\mathsf{tip}(j) : j'] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90)$$
$$\iff \exists j'' \in (\mathsf{tip}(j) : j' + 1] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90),$$
$$\mathscr{R}^C_{\mathsf{last}^C(j')}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t$$
$$\iff \mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t,$$
$$\nexists j'' \in (j' : \mathsf{hi}(j)] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90)$$
$$\iff \nexists j'' \in (j' + 1 : \mathsf{hi}(j)] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90).$$

   and the claim follows easily from the induction hypothesis. On the other hand, if $\mathsf{last}^C(j' + 1) - 1 \in \mathfrak{E}^C(90)$, then by Line 90, we have $\mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.t = 0 = \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t$ by item 4 of Lemma 6.85. By item 1, we get $\nexists j'' \in (\mathsf{tip}(j) : j'] :$

$\mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90)$.

This means that it is sufficient to show that $\mathscr{R}^C_{\mathsf{last}^C(j')}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t$. If not, then we have $\mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t = 0 \implies \mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t$. By the induction hypothesis, this means that $\nexists j'' \in (\mathsf{tip}(j) : j'+1] : \mathsf{last}^C(j'') - 1 \in \mathfrak{E}^C(90)$, a contradiction to the assumption that $\mathsf{last}^C(j'+1) - 1 \in \mathfrak{E}^C(90)$.

3. As $\mathsf{last}^C(j'+1) - 1 \in \mathfrak{E}^C(87)$ for $C \in \{A, B\}$, we have that

$$\begin{aligned}
\mathscr{R}^C_{\mathsf{last}^C(j')}.last.\alpha &= \mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.\alpha && \text{(Lemma 6.85, item 4)} \\
&= \mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.\alpha \\
&= \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\alpha. && \text{(Induction hypothesis)}
\end{aligned}$$

If $\mathsf{last}^C(j'+1) - 1 \notin \mathfrak{E}^C(90)$, we get $\left(\mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.t, \mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.\beta\right) = \left(\mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.t, \mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.\beta\right)$ implying that

$$\begin{aligned}
\mathscr{R}^C_{\mathsf{last}^C(j')}.last.\beta &= \mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.\beta && \text{(Lemma 6.85, item 4)} \\
&= \mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.\beta \\
&= \begin{cases} \diamond & , \mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & , \mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}. \\
& && \text{(Induction hypothesis)}
\end{aligned}$$

The proof is done as we have $\mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.t = \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t$ by item 4 of Lemma 6.85. On the other hand, if $\mathsf{last}^C(j'+1) - 1 \in \mathfrak{E}^C(90)$, then we have by Line 90 and item 3 that $0 = \mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(j'+1)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t$ by the induction hypothesis. As $\mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.t = \mathscr{R}^C_{\mathsf{last}^C(j')}.last.t$ by item 4 of Lemma 6.85, this means that it is sufficient to show that $\mathscr{R}^C_{\mathsf{last}^C(j')}.last.\beta = \diamond$. The latter is because

$$\begin{aligned}
\mathscr{R}^C_{\mathsf{last}^C(j')}.last.\beta &= \mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.\beta && \text{(Lemma 6.85, item 4)} \\
&= \diamond. && (\text{As } \mathscr{R}^C_{\mathsf{last}^C(j'+1)-1}.last.t = 0)
\end{aligned}$$

□

Next, for $1 \leq j < |\boldsymbol{\mathcal{S}}^A|$, define the set:

$$\mathsf{boss}(j) = \begin{cases} \{A, B\} & , \{j, j+1\} \subseteq \mathsf{Sync} \\ \{A\} & , M \leq j < |\boldsymbol{\mathcal{S}}^A| \\ \{\arg\min_{C \in \{A,B\}} \min_{k \in [\mathsf{lo}(j):\mathsf{tip}(j)]} |\pi^C_{\mathsf{last}^C(k)}|\} & , \{j, j+1\} \not\subseteq \mathsf{Sync} \wedge 1 \leq j < M \end{cases},$$

where the ties in $\arg\min$ are broken arbitrarily. Note that $\mathsf{boss}(j)$ is well defined as

$j+1 \in \mathsf{Sync} \implies j < M$ and therefore, the three cases are disjoint. Also, observe that $\mathsf{boss}(j)$ is singleton except when $\{j, j+1\} \subseteq \mathsf{Sync}$. Define $\overline{\mathsf{boss}}(j) = \{A, B\} \setminus \mathsf{boss}(j)$. We have:

Claim 6.92. *For all $1 \leq j < |\boldsymbol{\mathcal{S}}^A|$ and $C \in \mathsf{boss}(j)$, we have $j < |\boldsymbol{\mathcal{S}}^C|$.*

Proof. For $j < M$, we simply derive $j < M \leq \min\left(|\boldsymbol{\mathcal{S}}^A|, |\boldsymbol{\mathcal{S}}^B|\right) \leq |\boldsymbol{\mathcal{S}}^C|$. Otherwise, we have $j \geq M \implies \mathsf{boss}(j) = \{A\}$ and the claim follows easily. □

Claim 6.93. *For all $1 \leq j < |\boldsymbol{\mathcal{S}}^A|$, we have:*

$$j \notin \mathsf{Sync} \implies \mathsf{boss}(j) = \mathsf{boss}(j-1).$$

Proof. Suppose that $j \notin \mathsf{Sync}$ implying in particular that $j \neq M$. If $M < j$, then $M \leq j-1$, and therefore $\mathsf{boss}(j) = \mathsf{boss}(j-1) = \{A\}$. On the other hand if $j < M$, then $j \notin \mathsf{Sync}$ implies due to Claim 6.90 that $\mathsf{lo}(j) = \mathsf{lo}(j-1)$ and $\mathsf{tip}(j) = \mathsf{tip}(j-1)$. We have

$$\begin{aligned}\mathsf{boss}(j) &= \{\arg\min_{C \in \{A,B\}} \min_{k \in [\mathsf{lo}(j):\mathsf{tip}(j)]} |\pi^C_{\mathsf{last}^C(k)}|\} \\ &= \{\arg\min_{C \in \{A,B\}} \min_{k \in [\mathsf{lo}(j-1):\mathsf{tip}(j-1)]} |\pi^C_{\mathsf{last}^C(k)}|\} = \mathsf{boss}(j-1),\end{aligned}$$

as desired. □

We are now ready to define the adversary $\mathcal{A}''$ that along with $num = |\boldsymbol{\mathcal{S}}^A|$ shows Theorem 6.2. To define $\mathcal{A}''$, we need to define a pair of functions $(\mathcal{A}''^A, \mathcal{A}''^B)$ where $\mathcal{A}''^A, \mathcal{A}''^B : X^A \times X^B \to (\Sigma^*)^R$. We shall only define these functions for the pair of inputs (x^A, x^B) as this partial definition is all that is needed for Theorem 6.2. We first define the values of $\mathcal{A}''^A_{\leq (num-1)(P+1)}(x^A, x^B)$ and $\mathcal{A}''^B_{\leq (num-1)(P+1)}(x^A, x^B)$. We do this in $num-1$ steps and after step j, for $j \in [num-1]$, we would have defined $\mathcal{A}''^A_{\leq j(P+1)}(x^A, x^B)$ and $\mathcal{A}''^B_{\leq j(P+1)}(x^A, x^B)$. This partial definition is sufficient to determine the values of the variables $\mathscr{P}^C_{j'}(\mathcal{A}''), \mathscr{Q}^C_{j'}(\mathcal{A}''), \boldsymbol{\mathcal{S}}^C_{j'}(\mathcal{A}'')$ for $C \in \{A, B\}$ and $j' \in [j+1]$ and whether or not $[j] \subseteq \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$. We will maintain:

Lemma 6.94. *We have that:*

1. *For all $j' \in [j]$ and $C \in \mathsf{boss}(j')$, we have $\boldsymbol{\mathcal{S}}^C_{j'+1}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j'+1)}.last$.*
2. *The set $[j] \subseteq \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$ and for all $j' \in [j+1]$, we have*
$$\mathscr{Q}^A_{j'}(\mathcal{A}'') = \mathscr{Q}^B_{j'}(\mathcal{A}'') \qquad \text{and} \qquad |\boldsymbol{\mathcal{S}}^A_{j'}(\mathcal{A}'')| = |\boldsymbol{\mathcal{S}}^B_{j'}(\mathcal{A}'')| = j'.$$
3. *If $1 \leq j < M$, then, for all $C \in \overline{\mathsf{boss}}(j')$, the following hold*[14]*:*

[14] As usual, $\overline{C}$ denotes the unique element in $\{A, B\}$ that is different from C.

(a) If $j < \mathsf{tip}(j)$*, then*

$$\pi^C_{j+1}(\mathcal{A}'')\left[1 : \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right].$$

(b) If $j+1 \geq \mathsf{tip}(j)$*, then*

$$\left(\mathscr{R}'^C_{j+1}(\mathcal{A}'').last, \pi^C_{j+1}(\mathcal{A}''), \psi^C_{j+1}(\mathcal{A}'')\right) = \left(\mathscr{R}'^C_{\mathsf{last}^C(j+1)}.last, \pi^C_{\mathsf{last}^C(j+1)}, \psi^C_{\mathsf{last}^C(j+1)}\right).$$

Furthermore, we have $\mathscr{R}^C_{j+1}(\mathcal{A}'').last.\alpha = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\alpha$ *and*

$$\mathscr{R}^C_{j+1}(\mathcal{A}'').last.\beta = \begin{cases} \diamond & ,\mathscr{R}^C_{j+1}(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^C_{j+1}(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}.$$

4. For $j' \in [j+1] \cap \mathsf{Sync}$ *and all* $C \in \{A, B\}$*, we have* $\boldsymbol{\mathcal{S}}^C_{j'}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j')}.last$.

The definitions of $\mathcal{A}''^A_{\leq 0}(x^A, x^B)$ and $\mathcal{A}''^B_{\leq 0}(x^A, x^B)$ are trivial and they satisfy Lemma 6.94 trivially. Assume that, for some $1 \leq j < |\boldsymbol{\mathcal{S}}^A|$, the values of $\mathcal{A}''^A_{\leq (j-1)(P+1)}(x^A, x^B)$ and $\mathcal{A}''^B_{\leq (j-1)(P+1)}(x^A, x^B)$ have been defined and they satisfy Lemma 6.94. We now define the values of $\mathcal{A}''^A_{(j-1)(P+1)+j'}(x^A, x^B)$ and $\mathcal{A}''^B_{(j-1)(P+1)+j'}(x^A, x^B)$ for $j' \in [P+1]$ and show that Lemma 6.94 holds also for $\mathcal{A}''^A_{\leq j(P+1)}(x^A, x^B)$ and $\mathcal{A}''^B_{\leq j(P+1)}(x^A, x^B)$.

As $\mathcal{A}''^C_{j(P+1)}(x^A, x^B) = \left(\tilde{\mathscr{P}}^C_j(\mathcal{A}''), |\tilde{\boldsymbol{\mathcal{S}}}^C_j(\mathcal{A}'')|, \tilde{\Gamma}^C_j(\mathcal{A}'')\right)$ for $C \in \{A, B\}$ we need to define, for $C \in \{A, B\}$, the values of $\tilde{\mathscr{P}}^C_j(\mathcal{A}'')$, $|\tilde{\boldsymbol{\mathcal{S}}}^C_j(\mathcal{A}'')|$, $\tilde{\Gamma}^C_j(\mathcal{A}'')$, and $\mathcal{A}''^C_{(j-1)(P+1)+j'}(x^A, x^B)$ for $j' \in [P]$. For $C \in \{A, B\}$, we define:

$$\tilde{\mathscr{P}}^C_j(\mathcal{A}'') = \mathscr{P}^C_j(\mathcal{A}'') \qquad |\tilde{\boldsymbol{\mathcal{S}}}^C_j(\mathcal{A}'')| = |\boldsymbol{\mathcal{S}}^C_j(\mathcal{A}'')|. \tag{56}$$

For $C \in \mathsf{boss}(j)$, define $\tilde{\Gamma}^C_j(\mathcal{A}'') = \tilde{\Gamma}^C_{\mathsf{last}^C(j+1)-1}$ and for $j' \in [P]$,

$$\mathcal{A}''^C_{(j-1)(P+1)+j'}(x^A, x^B) = \mathcal{A}'^C_{(\mathsf{last}^C(j+1)-2)(P+1)+j'}(x^A, x^B). \tag{57}$$

It remains to define the values $\tilde{\Gamma}^C_j(\mathcal{A}'')$ and $\mathcal{A}''^C_{(j-1)(P+1)+j'}(x^A, x^B)$ for $j' \in [P]$ and $C \in \overline{\mathsf{boss}}(j)$. For this, consider the following cases:

- $\boldsymbol{1 \leq j < M}$**:** If there exists a $z < \mathsf{tip}(j)$ such that $|\pi^C_j(\mathcal{A}'')| = |\pi^C_{\mathsf{last}^C(z+1)-1}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(z+1)-1}|$ is odd, then, denoting by z the largest such value, define, for $j' \in [P]$:

$$\mathcal{A}''^C_{(j-1)(P+1)+j'}(x^A, x^B) = \mathcal{A}'^C_{(\mathsf{last}^C(z+1)-2)(P+1)+j'}(x^A, x^B). \tag{58}$$

  If no such z exists, define $\mathcal{A}''^C_{(j-1)(P+1)+j'}(x^A, x^B) = \perp$ for all $j' \in [P]$.

- $\boldsymbol{M \leq j < |\mathcal{S}^A|}$**:** Define $\mathcal{A}''^C_{(j-1)(P+1)+j'}(x^A, x^B) = \perp$ for $j' \in [P]$.

It remains to define the value of $\tilde{\Gamma}^C_j(\mathcal{A}'')$ for $C \in \overline{\mathsf{boss}}(j)$. Before defining this, we note that having defined $\mathcal{A}''^C_{(j-1)(P+1)+j'}(x^A, x^B)$ for $j' \in [P]$ and $C \in \{A, B\}$, we have also defined

the value of $\Gamma_j^C(\mathcal{A}'')$ for $C \in \{A, B\}$. Also, as $\mathsf{boss}(j)$ is always non-empty, we have also defined the value of $\tilde{\Gamma}_j^{\overline{C}}(\mathcal{A}'')$ where $\overline{C}$ denotes the unique element in $\{A, B\}$ that is different from C. If $\Gamma_j^{\overline{C}}(\mathcal{A}'') = \tilde{\Gamma}_j^{\overline{C}}(\mathcal{A}'')$, we define:

$$\tilde{\Gamma}_j^C(\mathcal{A}'') = \Gamma_j^C(\mathcal{A}''). \tag{59}$$

Otherwise, let h be the smallest such that $\Gamma_{j,h}^{\overline{C}}(\mathcal{A}'') \neq \tilde{\Gamma}_{j,h}^{\overline{C}}(\mathcal{A}'')$. Define:

$$\tilde{\Gamma}_j^C(\mathcal{A}'') = \begin{cases} \Gamma_j^C(\mathcal{A}'')|_{h \leftarrow \Gamma_{j,h}^{\overline{C}}(\mathcal{A}'')} & , \Gamma_{j,h}^C(\mathcal{A}'') = \tilde{\Gamma}_{j,h}^{\overline{C}}(\mathcal{A}'') \\ \Gamma_j^C(\mathcal{A}'')|_{h \leftarrow \tilde{\Gamma}_{j,h}^{\overline{C}}(\mathcal{A}'')} & , \Gamma_{j,h}^C(\mathcal{A}'') \neq \tilde{\Gamma}_{j,h}^{\overline{C}}(\mathcal{A}'') \end{cases}. \tag{60}$$

In the above definition, $\Gamma_j^C(\mathcal{A}'')|_{h \leftarrow \gamma}$ denotes $\Gamma_j^C(\mathcal{A}'')$ with coordinate h set to γ. In order to show that these definitions satisfy Lemma 6.94, we will need the following claims:

Claim 6.95. *We have for all $C \in \mathsf{boss}(j)$ that*

$$\boldsymbol{\mathcal{S}}_j^C(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}.last \qquad \text{and} \qquad |\boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}| = j.$$

Proof. Note by Claim 6.92 that $j < |\boldsymbol{\mathcal{S}}^C|$. This means that we can apply item 4 of Lemma 6.85 on $\mathsf{boss}(j)$ to get $\boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j)} = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}$.

From Definition 6.84, we immediately get that $|\boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j)}| = |\boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}| = j$ and the second part of the claim holds. Moreover, due to the foregoing equality it is sufficient to show that $\boldsymbol{\mathcal{S}}_j^C(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j)}.last$ in order to show the first part of the claim. If $j \in \mathsf{Sync}$, this follows from item 4 of the induction hypothesis of Lemma 6.94. Otherwise, we have $j \notin \mathsf{Sync}$ implying in particular that $j > 1$ and $C \in \mathsf{boss}(j-1)$ by Claim 6.93. We have by item 1 of the induction hypothesis of Lemma 6.94 that $\boldsymbol{\mathcal{S}}_j^C(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j)}.last$, as desired. □

Claim 6.96. *We have for all $C \in \mathsf{boss}(j)$ and $j' \in [P+1]$ that:*

$$\mathcal{A}''^C_{(j-1)(P+1)+j'}(x^A, x^B) = \mathcal{A}'^C_{(\mathsf{last}^C(j+1)-2)(P+1)+j'}(x^A, x^B).$$

Proof. For $j' \in [P]$, this simply follows from Equation 57. For $j' = P+1$, we have

$$\begin{aligned}
\mathcal{A}''^C_{j(P+1)}(x^A, x^B) &= \left(\tilde{\mathscr{P}}_j^C(\mathcal{A}''), |\tilde{\boldsymbol{\mathcal{S}}}_j^C(\mathcal{A}'')|, \tilde{\Gamma}_j^C(\mathcal{A}'')\right) \\
&= \left(\mathscr{P}_j^C(\mathcal{A}''), |\boldsymbol{\mathcal{S}}_j^C(\mathcal{A}'')|, \tilde{\Gamma}_j^C(\mathcal{A}'')\right) && \text{(Equation 56)} \\
&= \left(\mathscr{P}_j^C(\mathcal{A}''), |\boldsymbol{\mathcal{S}}_j^C(\mathcal{A}'')|, \tilde{\Gamma}^C_{\mathsf{last}^C(j+1)-1}\right) && (\text{As } \tilde{\Gamma}_j^C(\mathcal{A}'') = \tilde{\Gamma}^C_{\mathsf{last}^C(j+1)-1}) \\
&= \left(\mathscr{P}_j^C(\mathcal{A}''), j, \tilde{\Gamma}^C_{\mathsf{last}^C(j+1)-1}\right) && \text{(Induction hypothesis Lemma 6.94, item 2)} \\
&= \left(\mathscr{P}^C_{\mathsf{last}^C(j+1)-1}, |\boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}|, \tilde{\Gamma}^C_{\mathsf{last}^C(j+1)-1}\right). && \text{(Claim 6.95)}
\end{aligned}$$

By Definition 6.84 and the fact that $j \geq 1$, we get that $\mathsf{last}^C(j+1)-1 \in \mathfrak{E}^C(52)$. This gives:

$$\begin{aligned}\mathcal{A}''^C_{j(P+1)}(x^A, x^B) &= \left(\mathscr{P}^C_{\mathsf{last}^C(j+1)-1}, |\boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}|, \tilde{\Gamma}^C_{\mathsf{last}^C(j+1)-1}\right) \\ &= \left(\tilde{\mathscr{P}}^C_{\mathsf{last}^C(j+1)-1}, |\tilde{\boldsymbol{\mathcal{S}}}^C_{\mathsf{last}^C(j+1)-1}|, \tilde{\Gamma}^C_{\mathsf{last}^C(j+1)-1}\right) && \text{(Line 52)} \\ &= \mathcal{A}'^C_{(\mathsf{last}^C(j+1)-1)(P+1)}.\end{aligned}$$

□

Claim 6.97. *If $\{j, j+1\} \not\subseteq \mathsf{Sync}$, we have $\Gamma^A_j(\mathcal{A}'') = \tilde{\Gamma}^A_j(\mathcal{A}'') \iff \Gamma^B_j(\mathcal{A}'') = \tilde{\Gamma}^B_j(\mathcal{A}'')$.*

Proof. Observe from the definition of $\mathsf{boss}(\cdot)$ that $\{j, j+1\} \not\subseteq \mathsf{Sync}$ implies that $\mathsf{boss}(j)$ is singleton. Let C be the unique element in $\mathsf{boss}(j)$ and $\overline{C}$ be the unique element not in $\mathsf{boss}(j)$. If $\Gamma^C_j(\mathcal{A}'') = \tilde{\Gamma}^C_j(\mathcal{A}'')$, we have by Equation 59 that $\tilde{\Gamma}^{\overline{C}}_j(\mathcal{A}'') = \Gamma^{\overline{C}}_j(\mathcal{A}'')$ and we are done. Otherwise, let h be the smallest such that $\Gamma^C_{j,h}(\mathcal{A}'') \neq \tilde{\Gamma}^C_{j,h}(\mathcal{A}'')$. We show that $\Gamma^{\overline{C}}_{j,h}(\mathcal{A}'') \neq \tilde{\Gamma}^{\overline{C}}_{j,h}(\mathcal{A}'')$ and the result follows. If $\Gamma^{\overline{C}}_{j,h}(\mathcal{A}'') = \tilde{\Gamma}^C_{j,h}(\mathcal{A}'')$, we have by Equation 60 that

$$\tilde{\Gamma}^{\overline{C}}_{j,h}(\mathcal{A}'') = \Gamma^C_{j,h}(\mathcal{A}'') \neq \tilde{\Gamma}^C_{j,h}(\mathcal{A}'') = \Gamma^{\overline{C}}_{j,h}(\mathcal{A}''),$$

as desired. Otherwise, if $\Gamma^{\overline{C}}_{j,h}(\mathcal{A}'') \neq \tilde{\Gamma}^C_{j,h}(\mathcal{A}'')$, we have

$$\tilde{\Gamma}^{\overline{C}}_{j,h}(\mathcal{A}'') = \tilde{\Gamma}^C_{j,h}(\mathcal{A}'') \neq \Gamma^{\overline{C}}_{j,h}(\mathcal{A}''),$$

as desired. □

We now show that these definitions satisfy Lemma 6.94.

Proof of Lemma 6.94. First, we show item 1 of Lemma 6.94. Due to the induction hypothesis, it is sufficient to show for all $C \in \mathsf{boss}(j)$ that

$$\boldsymbol{\mathcal{S}}^C_{j+1}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)}.last. \tag{61}$$

To see why Equation 61 holds, note from Claim 6.95 that $\boldsymbol{\mathcal{S}}^C_j(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}.last$. This means that party C starts iteration j in the execution of Π' with $\mathcal{A}''$ and iteration $\mathsf{last}^C(j+1)-1$ in the execution of Π' with $\mathcal{A}'$ with the same values of $(\mathscr{R}, \pi, \psi, p)$. Due to Claim 6.96, the symbols received by the party C in these two iterations are also the same and due to Equation 56 and Definition 6.84, party C executes Line 52 in both these iterations. It follows from Algorithm 4 that $\boldsymbol{\mathcal{S}}^C_{j+1}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)}.last$.

Next, we show item 2 of Lemma 6.94. Due to the induction hypothesis, it is sufficient to show that $j \in \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$ and

$$\mathscr{Q}^A_{j+1}(\mathcal{A}'') = \mathscr{Q}^B_{j+1}(\mathcal{A}'') \qquad \text{and} \qquad |\boldsymbol{\mathcal{S}}^A_{j+1}(\mathcal{A}'')| = |\boldsymbol{\mathcal{S}}^B_{j+1}(\mathcal{A}'')| = j+1.$$

We have $j \in \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$ due to Equation 56. It follows that for $C \in \{A, B\}$, we have $|\boldsymbol{\mathcal{S}}^C_{j+1}(\mathcal{A}'')| = |\boldsymbol{\mathcal{S}}^C_j(\mathcal{A}'')| + 1 = j+1$ and all that remains to be shown is that

$\mathcal{Q}^A_{j+1}(\mathcal{A}'') = \mathcal{Q}^B_{j+1}(\mathcal{A}'')$. If $\{j, j+1\} \subseteq \mathsf{Sync}$, then $\mathsf{boss}(j) = \{A, B\}$ by the definition of $\mathsf{boss}(\cdot)$. Using the previous part, we get:

$$\begin{aligned}
\mathcal{Q}^A_{j+1}(\mathcal{A}'') &= \mathcal{Q}^A_{\mathsf{last}^A(j+1)} && \text{(Equation 61)} \\
&= \mathcal{Q}^B_{\mathsf{last}^B(j+1)} && \text{(As } j+1 \in \mathsf{Sync} \text{ and Definition 6.86)} \\
&= \mathcal{Q}^B_{j+1}(\mathcal{A}''). && \text{(Equation 61)}
\end{aligned}$$

Now, suppose that $\{j, j+1\} \not\subseteq \mathsf{Sync}$. Observe from Algorithm 4 that, for $j \in \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$ and $C \in \{A, B\}$, the value of $\mathcal{Q}^C_{j+1}(\mathcal{A}'')$ is determined independently of C given $\mathcal{Q}^C_j(\mathcal{A}'')$ and whether or not $\Gamma^C_j(\mathcal{A}'') = \tilde{\Gamma}^C_j(\mathcal{A}'')$. Thus, due to Claim 6.97 and the fact that $\mathcal{Q}^A_j(\mathcal{A}'') = \mathcal{Q}^B_j(\mathcal{A}'')$, we also have $\mathcal{Q}^A_{j+1}(\mathcal{A}'') = \mathcal{Q}^B_{j+1}(\mathcal{A}'')$ as desired.

Next, we show item 3 of Lemma 6.94. Observe that this is non-trivial only if $1 \leq j < M$ and $\overline{\mathsf{boss}}(j)$ is non-empty. In turn, as $\mathsf{boss}(j)$ is always non-empty by definition, this part is non-trivial only if $\mathsf{boss}(j)$ and $\overline{\mathsf{boss}}(j)$ are singleton, so we assume this throughout. Let C be the unique element in $\overline{\mathsf{boss}}(j)$ and $\overline{C}$ be the unique element in $\mathsf{boss}(j)$. We first show item 3a of Lemma 6.94. We start by claiming:

$$\pi^C_j(\mathcal{A}'') \left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))} \left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right]. \tag{62}$$

To show Equation 62, we consider two cases. First, we assume that $j \notin \mathsf{Sync}$ implying in particular that $j > 1$. Additionally, $j \notin \mathsf{Sync}$ also implies that $\mathsf{tip}(j-1) = \mathsf{tip}(j)$ by Claim 6.90 and $\mathsf{boss}(j-1) = \mathsf{boss}(j) = \{\overline{C}\}$ by Claim 6.93. In this case, we have by item 3a of the induction hypothesis of Lemma 6.94 that:

$$\pi^C_j(\mathcal{A}'') \left[1 : \min_{j' \in [j:\mathsf{tip}(j-1)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j-1))} \left[1 : \min_{j' \in [j:\mathsf{tip}(j-1)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right].$$

Using $\mathsf{tip}(j-1) = \mathsf{tip}(j)$, we get Equation 62, as desired. On the other hand, if $j \in \mathsf{Sync}$, then $j = \mathsf{lo}(j)$ by definition and we have by item 4 of the induction hypothesis of Lemma 6.94 that $\boldsymbol{\mathcal{S}}^C_j(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j)}.last \implies \pi^C_j(\mathcal{A}'') = \pi^C_{\mathsf{last}^C(j)}$. To show Equation 62, we actually show a stronger statement that, for all $j'' \in [j : \mathsf{tip}(j)]$, we have:

$$\pi^C_j(\mathcal{A}'') \left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] = \pi^C_{\mathsf{last}^C(j'')} \left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right].$$

As $\pi^C_j(\mathcal{A}'') = \pi^C_{\mathsf{last}^C(j)}$, the foregoing equation clearly holds for $j'' = j$. Suppose for the sake of contradiction that there is a $j'' \in (j : \mathsf{tip}(j)]$ such that the foregoing equation does not hold for j''. Let j'' be the smallest such value. We have by our choice of j'' that

$$\begin{aligned}
\pi^C_j(\mathcal{A}'') \left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] &= \pi^C_{\mathsf{last}^C(j''-1)} \left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] \\
&\neq \pi^C_{\mathsf{last}^C(j'')} \left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right].
\end{aligned}$$

It follows that there is an $h \in [\min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|]$ such that $\pi^{C}_{\mathsf{last}^{C}(j''-1)}[h] \neq \pi^{C}_{\mathsf{last}^{C}(j'')}[h]$. However, as $j = \mathsf{lo}(j)$ and $h \in [\min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|] \subseteq [\min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{C}_{\mathsf{last}^{C}(j')}|]$ (recall that $\mathsf{boss}(j) = \{\overline{C}\}$ and the definition of $\mathsf{boss}(\cdot)$) and $\mathsf{last}^{C}(j'') - 1 \in \mathfrak{E}^{C}(52)$ by Definition 6.84, we have

$$\pi^{C}_{\mathsf{last}^{C}(j'')}[h] = \pi^{C}_{\mathsf{last}^{C}(j'')-1}[h] = \pi^{C}_{\mathsf{last}^{C}(j''-1)}[h],$$

by item 4 of Lemma 6.85, a contradiction. Next, we show that:

$$|\pi^{C}_{j}(\mathcal{A}'')| = |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| \qquad \text{and} \qquad |\pi^{C}_{j+1}(\mathcal{A}'')| = |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|. \tag{63}$$

Indeed, we have $\mathscr{Q}^{A}_{j}(\mathcal{A}'') = \mathscr{Q}^{B}_{j}(\mathcal{A}'')$ by item 2 of induction hypothesis of Lemma 6.94 implying that:

$$\begin{aligned}
|\pi^{C}_{j}(\mathcal{A}'')| &= |\pi^{\overline{C}}_{j}(\mathcal{A}'')| \\
&= |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)-1}| && \text{(Claim 6.95 and } \mathsf{boss}(j) = \{\overline{C}\}) \\
&= |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}|. && \text{(Lemma 6.85, item 4)}
\end{aligned}$$

Moreover, as $\mathscr{Q}^{A}_{j+1}(\mathcal{A}'') = \mathscr{Q}^{B}_{j+1}(\mathcal{A}'')$ by item 2 of Lemma 6.94, we also have:

$$|\pi^{C}_{j+1}(\mathcal{A}'')| = |\pi^{\overline{C}}_{j+1}(\mathcal{A}'')| = |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|. \qquad \text{(Equation 61 and } \mathsf{boss}(j) = \{\overline{C}\})$$

Now, recall that $j \in \mathfrak{E}^{A}(\mathcal{A}'', 52) \cap \mathfrak{E}^{B}(\mathcal{A}'', 52)$ from item 2 of Lemma 6.94. Thus, we have that either $j \in \mathfrak{E}^{C}(\mathcal{A}'', 67)$ or $j \in \mathfrak{E}^{C}(\mathcal{A}'', 77)$. We have the following cases:

- **If $|\boldsymbol{\pi}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| \geq \min_{j' \in (j:\mathsf{tip}(j)]} |\boldsymbol{\pi}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|$:** In this case, as $j \in \mathfrak{E}^{C}(\mathcal{A}'', 67)$ or $j \in \mathfrak{E}^{C}(\mathcal{A}'', 77)$, we have:

  $$\pi^{C}_{j+1}(\mathcal{A}'')\left[1 : \min\left(|\pi^{C}_{j}(\mathcal{A}'')|, |\pi^{C}_{j+1}(\mathcal{A}'')|\right)\right] = \pi^{C}_{j}(\mathcal{A}'')\left[1 : \min\left(|\pi^{C}_{j}(\mathcal{A}'')|, |\pi^{C}_{j+1}(\mathcal{A}'')|\right)\right].$$

  Due to the fact that $j < \mathsf{tip}(j)$ and Equation 63, this gives:

  $$\pi^{C}_{j+1}(\mathcal{A}'')\left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] = \pi^{C}_{j}(\mathcal{A}'')\left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right]. \tag{64}$$

  The foregoing equation allows us to derive:

  $$\begin{aligned}
  \pi^{C}_{j+1}(\mathcal{A}'')\left[1 : \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] &= \pi^{C}_{j+1}(\mathcal{A}'')\left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] \\
  &\qquad \text{(As } |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| \geq \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|) \\
  &= \pi^{C}_{j}(\mathcal{A}'')\left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] && \text{(Equation 64)} \\
  &= \pi^{C}_{\mathsf{last}^{C}(\mathsf{tip}(j))}\left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] && \text{(Equation 62)}
  \end{aligned}$$

$$= \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right].$$
(As $|\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| \geq \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|$)

- **If $|\boldsymbol{\pi}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| < \min_{j' \in (j:\mathsf{tip}(j)]} |\boldsymbol{\pi}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|$:** Using Equation 63, we get that $|\pi^C_j(\mathcal{A}'')| < |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(\mathsf{tip}(j))}|$. We have by Claim 6.91 that $|\pi^A_{\mathsf{last}^A(\mathsf{tip}(j))}| = |\pi^B_{\mathsf{last}^B(\mathsf{tip}(j))}|$ which implies that $|\pi^C_j(\mathcal{A}'')| < |\pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}|$.

  As $|\pi^C_j(\mathcal{A}'')| < |\pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}|$, there exists a $1 \leq z < \mathsf{tip}(j)$ such that $|\pi^C_j(\mathcal{A}'')| = |\pi^C_{\mathsf{last}^C(z+1)-1}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(z+1)-1}|$ is odd. Moreover, for the largest such z, we have that:
  $$\pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : |\pi^C_{\mathsf{last}^C(z+1)}|\right] = \pi^C_{\mathsf{last}^C(z+1)} = \pi^C_{\mathsf{last}^C(z+1)-1} \| \sigma^C_{\mathsf{last}^C(z+1)-1},$$
  as $|\mathscr{R}^C_{\mathsf{last}^C(z+1)-1}|$ is odd and $\mathsf{last}^C(z+1)-1 \in \mathfrak{C}^C(52)$ by definition. We can conclude that:
  $$\pi^C_{\mathsf{last}^C(z+1)-1} = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : |\pi^C_{\mathsf{last}^C(z+1)}| - 1\right]. \tag{65}$$
  $$\sigma^C_{\mathsf{last}^C(z+1)-1} = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[|\pi^C_{\mathsf{last}^C(z+1)}|\right]. \tag{66}$$

  From Equation 65, we can conclude that
  $$\begin{aligned}
  |\pi^C_{\mathsf{last}^C(z+1)}| - 1 &= |\pi^C_{\mathsf{last}^C(z+1)-1}| \\
  &= |\pi^C_j(\mathcal{A}'')| && (\text{As } |\pi^C_j(\mathcal{A}'')| = |\pi^C_{\mathsf{last}^C(z+1)-1}|) \\
  &= |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}|. && (\text{Equation 63})
  \end{aligned}$$

  This allows us to continue Equation 65 as:
  $$\begin{aligned}
  \pi^C_{\mathsf{last}^C(z+1)-1} &= \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : |\pi^C_{\mathsf{last}^C(z+1)}| - 1\right] \\
  &= \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}|\right] \\
  &= \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] \\
  &&& (\text{As } |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| < \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|) \\
  &= \pi^C_j(\mathcal{A}'')\left[1 : \min_{j' \in [j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right] && (\text{Equation 62}) \\
  &= \pi^C_j(\mathcal{A}'')\left[1 : |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}|\right] && (\text{As } |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| < \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|) \\
  &= \pi^C_j(\mathcal{A}'')\left[1 : |\pi^C_j(\mathcal{A}'')|\right] && (\text{Equation 63}) \\
  &= \pi^C_j(\mathcal{A}'').
  \end{aligned}$$

  Consider now iteration j in the execution of Π' with $\mathcal{A}''$ and iteration $\mathsf{last}^C(z+1)-1$ in

the execution of Π' with $\mathcal{A}'$ from the perspective of party C. As $\pi^C_{\mathsf{last}^C(z+1)-1} = \pi^C_j(\mathcal{A}'')$, the value of π is the same for both these iterations. Moreover, due to Equation 58, the first P symbols received by party C in these two iterations are the same. Finally, as $|\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| < \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}| \leq |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|$, we have that $|\mathscr{R}|$ is odd in both the iterations. It follows from Algorithm 5 and Equation 66 that

$$\sigma^C_j(\mathcal{A}'') = \sigma^C_{\mathsf{last}^C(z+1)-1} = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))} \left[|\pi^C_{\mathsf{last}^C(z+1)}| \right].$$

We next claim that:

$$|\pi^C_{j+1}(\mathcal{A}'')| = \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|. \tag{67}$$

Indeed, we have $|\pi^C_{j+1}(\mathcal{A}'')| \geq \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|$ as $j < \mathsf{tip}(j)$ and Equation 63. We also have that $|\pi^C_{j+1}(\mathcal{A}'')| \leq \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|$ as otherwise, as both the quantities are integers, we have

$$\begin{aligned}
|\pi^C_{j+1}(\mathcal{A}'')| &\geq \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}| + 1 \\
&> |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| + 1 && (\text{As } |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| < \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|) \\
&\geq |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)-1}| + 1 && (\text{Lemma 6.85, item 4}) \\
&\geq |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}| && (\text{As } \mathsf{last}^{\overline{C}}(j+1) - 1 \in \mathfrak{E}^C(52) \text{ by Definition 6.84}) \\
&\geq |\pi^C_{j+1}(\mathcal{A}'')|, && (\text{Equation 63})
\end{aligned}$$

a contradiction. Also, as $|\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}| < |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|$, we have by Equation 63 that $|\pi^C_j(\mathcal{A}'')| < |\pi^C_{j+1}(\mathcal{A}'')|$ which together with the fact that $j \in \mathfrak{E}^C(\mathcal{A}'', 52)$ implies $\pi^C_{j+1}(\mathcal{A}'') = \pi^C_j(\mathcal{A}'') \| \sigma^C_j(\mathcal{A}'')$ This yields:

$$\begin{aligned}
&\pi^C_{j+1}(\mathcal{A}'') \left[1 : \min_{j' \in (j:\mathsf{tip}(j)]} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}| \right] \\
&\quad = \pi^C_{j+1}(\mathcal{A}'') \left[1 : |\pi^C_{j+1}(\mathcal{A}'')| \right] && (\text{Equation 67}) \\
&\quad = \pi^C_{j+1}(\mathcal{A}'') \\
&\quad = \pi^C_j(\mathcal{A}'') \| \sigma^C_j(\mathcal{A}'') \\
&\quad = \pi^C_{\mathsf{last}^C(z+1)-1} \| \sigma^C_j(\mathcal{A}'') && (\text{As } \pi^C_{\mathsf{last}^C(z+1)-1} = \pi^C_j(\mathcal{A}'')) \\
&\quad = \pi^C_{\mathsf{last}^C(z+1)-1} \| \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))} \left[|\pi^C_{\mathsf{last}^C(z+1)}| \right] \\
&\qquad && (\text{As } \sigma^C_j(\mathcal{A}'') = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))} \left[|\pi^C_{\mathsf{last}^C(z+1)}| \right]) \\
&\quad = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))} \left[1 : |\pi^C_{\mathsf{last}^C(z+1)}| - 1 \right] \| \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))} \left[|\pi^C_{\mathsf{last}^C(z+1)}| \right] && (\text{Equation 65}) \\
&\quad = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))} \left[1 : |\pi^C_{\mathsf{last}^C(z+1)}| \right] \\
&\quad = \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))} \left[1 : |\pi^C_{\mathsf{last}^C(z+1)-1}| + 1 \right] && (\text{Equation 65})
\end{aligned}$$

$$= \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : |\pi^C_j(\mathcal{A}'')| + 1\right] \qquad (\text{As } |\pi^C_j(\mathcal{A}'')| = |\pi^C_{\mathsf{last}^C(z+1)-1}|)$$
$$= \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : |\pi^C_{j+1}(\mathcal{A}'')|\right] \qquad (\text{As } \pi^C_{j+1}(\mathcal{A}'') = \pi^C_j(\mathcal{A}'')\|\sigma^C_j(\mathcal{A}''))$$
$$= \pi^C_{\mathsf{last}^C(\mathsf{tip}(j))}\left[1 : \min_{j' \in (j:\mathsf{tip}(j))} |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j')}|\right], \qquad (\text{Equation 67})$$

as desired.

Next, we show item 3b of Lemma 6.94. We first claim that, for $C', C'' \in \{A, B\}$, we have:

$$\left(\mathscr{R}'^{C'}_{j+1}(\mathcal{A}'').last, |\pi^{C'}_{j+1}(\mathcal{A}'')|, |\psi^{C'}_{j+1}(\mathcal{A}'')|\right) = \left(\mathscr{R}'^{C''}_{\mathsf{last}^{C''}(j+1)}.last, |\pi^{C''}_{\mathsf{last}^{C''}(j+1)}|, |\psi^{C''}_{\mathsf{last}^{C''}(j+1)}|\right). \tag{68}$$

Indeed, as $j < \mathsf{hi}(j)$, we can invoke Claim 6.91 to conclude:

$$\left(\mathscr{R}'^{C}_{\mathsf{last}^C(j+1)}.last, |\pi^{C}_{\mathsf{last}^C(j+1)}|, |\psi^{C}_{\mathsf{last}^C(j+1)}|\right) = \left(\mathscr{R}'^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}.last, |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|, |\psi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|\right)$$
$$(\text{Claim 6.91})$$
$$= \left(\mathscr{R}'^{\overline{C}}_{j+1}(\mathcal{A}'').last, |\pi^{\overline{C}}_{j+1}(\mathcal{A}'')|, |\psi^{\overline{C}}_{j+1}(\mathcal{A}'')|\right)$$
$$(\text{Equation 61 and } \mathsf{boss}(j) = \{\overline{C}\})$$
$$= \left(\mathscr{R}'^{C}_{j+1}(\mathcal{A}'').last, |\pi^{C}_{j+1}(\mathcal{A}'')|, |\psi^{C}_{j+1}(\mathcal{A}'')|\right).$$
$$(\text{As } \mathscr{Q}^A_{j+1}(\mathcal{A}'') = \mathscr{Q}^B_{j+1}(\mathcal{A}''))$$

We now break the proof in to the following cases:

- $\boldsymbol{j+1 > \mathsf{tip}(j)}$**:** As both quantities are integers, we have that $j \geq \mathsf{tip}(j) \implies \mathsf{tip}(j) \leq j < \mathsf{hi}(j)$ by definition of $\mathsf{hi}(\cdot)$. We claim that:

$$\left(\mathscr{R}'^{C}_{j}(\mathcal{A}'').last, \pi^C_j(\mathcal{A}''), \psi^C_j(\mathcal{A}'')\right) = \left(\mathscr{R}'^{C}_{\mathsf{last}^C(j)}.last, \pi^C_{\mathsf{last}^C(j)}, \psi^C_{\mathsf{last}^C(j)}\right). \tag{69}$$

Indeed, either $j \in \mathsf{Sync}$, in which case Equation 69 follows due to item 4 of the induction hypothesis of Lemma 6.94, or $j \notin \mathsf{Sync}$ implying in particular that $j > 1$. Additionally, $j \notin \mathsf{Sync}$ also implies that $\mathsf{tip}(j-1) = \mathsf{tip}(j)$ by Claim 6.90 and $\mathsf{boss}(j-1) = \mathsf{boss}(j) = \{\overline{C}\}$ by Claim 6.93. It follows that $j \geq \mathsf{tip}(j-1)$ and Equation 69 follows by item 3b of the induction hypothesis of Lemma 6.94. We next claim that:

Claim 6.98. *The quantities $|\mathscr{R}^C_{\mathsf{last}^C(j+1)-1}|$, $|\mathscr{R}^C_{\mathsf{last}^C(j+1)}|$ are both even. Moreover, for $C' \in \{A, B\}$, the quantities $|\mathscr{R}^{C'}_j(\mathcal{A}'')|$ and $|\mathscr{R}^{C'}_{j+1}(\mathcal{A}'')|$ are both even.*

Proof. We first show that $|\mathscr{R}^{C'}_{\mathsf{last}^{C'}(j)}|$ and $|\mathscr{R}^{C'}_{\mathsf{last}^{C'}(j+1)}|$ are both even for $C' \in \{A, B\}$. This is because $\mathsf{tip}(j) < \mathsf{hi}(j)$, and therefore, we have by the definition of $\mathsf{tip}(\cdot)$ that $|\mathscr{R}^{C'}_{\mathsf{last}^{C'}(j'')}|$ is even for all $j'' \in [\mathsf{tip}(j) : \mathsf{hi}(j)]$, as desired.

We now prove the claim. The first part of the claim follows simply from the fact that $|\mathscr{R}^C_{\mathsf{last}^C(j)}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j+1)}|$ are both even and item 4 of Lemma 6.85. It remains to show

the "moreover" part. Note that as we showed item 2 of Lemma 6.94, it is sufficient to show that there exists $C' \in \{A, B\}$ such that $|\mathscr{R}_j^{C'}(\mathcal{A}'')|$ is even and another (possibly different) $C' \in \{A, B\}$ such that $|\mathscr{R}_{j+1}^{C'}(\mathcal{A}'')|$ is even.

For the latter, we simply note that $|\mathscr{R}_{j+1}^{\overline{C}}(\mathcal{A}'')| = |\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|$ by Equation 61 is even, while for the former, we may either have $j \in \mathsf{Sync}$ in which case, we have by item 4 of the induction hypothesis of Lemma 6.94, we have that $|\mathscr{R}_j^{C}(\mathcal{A}'')| = |\mathscr{R}^{C}_{\mathsf{last}^{C}(j)}|$ is even, or $j \notin \mathsf{Sync}$, in which case, we have $j > 1$ and $\mathsf{boss}(j-1) = \mathsf{boss}(j) = \{\overline{C}\}$ by Claim 6.93. We get that $|\mathscr{R}_j^{\overline{C}}(\mathcal{A}'')| = |\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}|$ is even by item 1 of the induction hypothesis of Lemma 6.94 and the result follows.

□

Consider now iteration j in the execution of Π' with $\mathcal{A}''$ and iteration $\mathsf{last}^C(j+1) - 1$ in the execution of Π' with $\mathcal{A}'$ from the perspective of party C. Due to Claim 6.98, the value of $|\mathscr{R}|$ is even before and after both these iterations. Furthermore, as we showed that $j \in \mathfrak{E}^C(\mathcal{A}'', 52)$ and $\mathsf{last}^C(j+1) - 1 \in \mathfrak{E}^C(52)$ by Definition 6.84, we can conclude that Line 87 is executed in both the iterations. It follows from Algorithm 6 that the values of (π, ψ) before these iterations determine the values after these iterations. Thus, as Equation 69 says $\left(\pi_j^C(\mathcal{A}''), \psi_j^C(\mathcal{A}'')\right) = \left(\pi^C_{\mathsf{last}^C(j)}, \psi^C_{\mathsf{last}^C(j)}\right) = \left(\pi^C_{\mathsf{last}^C(j+1)-1}, \psi^C_{\mathsf{last}^C(j+1)-1}\right)$ by item 4 of Lemma 6.85, we must also have:

$$\left(\pi_{j+1}^C(\mathcal{A}''), \psi_{j+1}^C(\mathcal{A}'')\right) = \left(\pi^C_{\mathsf{last}^C(j+1)}, \psi^C_{\mathsf{last}^C(j+1)}\right). \tag{70}$$

Next, comparing the two iterations again, we claim that:

Claim 6.99. $\mathscr{R}_{j+1}^C(\mathcal{A}'').last.\alpha = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\alpha$.

Proof. If $j \in \mathsf{Sync}$, we have:

$$\begin{aligned}
\mathscr{R}_{j+1}^C(\mathcal{A}'').last.\alpha &= \mathscr{R}_j^C(\mathcal{A}'').last.\alpha && (\text{As } j \in \mathfrak{E}^C(\mathcal{A}'', 87)) \\
&= \mathscr{R}^C_{\mathsf{last}^C(j)}.last.\alpha && (\text{Induction hypothesis Lemma 6.94, item 4}) \\
&= \mathscr{R}^C_{\mathsf{last}^C(j+1)-1}.last.\alpha && (\text{Lemma 6.85, item 4}) \\
&= \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\alpha && (\text{As } \mathsf{last}^C(j+1) - 1 \in \mathfrak{E}^C(87)) \\
&= \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\alpha. && (\text{Claim 6.91})
\end{aligned}$$

If $j \notin \mathsf{Sync}$, we have in particular that $j > 1$. Additionally, $j \notin \mathsf{Sync}$ also implies that $\mathsf{tip}(j-1) = \mathsf{tip}(j)$ by Claim 6.90 and $\mathsf{boss}(j-1) = \mathsf{boss}(j) = \{\overline{C}\}$ by Claim 6.93. It follows that $j \geq \mathsf{tip}(j-1)$ and we get:

$$\mathscr{R}_{j+1}^C(\mathcal{A}'').last.\alpha = \mathscr{R}_j^C(\mathcal{A}'').last.\alpha \qquad (\text{As } j \in \mathfrak{E}^C(\mathcal{A}'', 87))$$

$$= \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j-1))}.last.\alpha \quad \text{(Induction hypothesis Lemma 6.94, item 3b)}$$
$$= \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\alpha. \quad \text{(Claim 6.90)}$$

□

Claim 6.100. *It holds that:*

$$\mathscr{R}^C_j(\mathcal{A}'').last.\beta = \begin{cases} \diamond & ,\mathscr{R}^C_j(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^C_j(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}.$$

Proof. If $j \in \mathsf{Sync}$, then $j = \mathsf{lo}(j)$ by definition of $\mathsf{lo}(\cdot)$ and $j+1 > \mathsf{tip}(j) \implies j = \mathsf{lo}(j) = \mathsf{tip}(j)$. We have by Claim 6.91 that:

$$\mathscr{R}^C_j(\mathcal{A}'').last.\beta = \mathscr{R}^C_{\mathsf{last}^C(j)}.last.\beta \quad \text{(Induction hypothesis Lemma 6.94, item 4)}$$
$$= \begin{cases} \diamond & ,\mathscr{R}^C_{\mathsf{last}^C(j)}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^C_{\mathsf{last}^C(j)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases} \quad \text{(Claim 6.91)}$$
$$= \begin{cases} \diamond & ,\mathscr{R}^C_j(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^C_j(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}. \quad \text{(Induction hypothesis Lemma 6.94, item 4)}$$

If $j \notin \mathsf{Sync}$, we have in particular that $j > 1$. Additionally, $j \notin \mathsf{Sync}$ also implies that $\mathsf{tip}(j-1) = \mathsf{tip}(j)$ by Claim 6.90 and $\mathsf{boss}(j-1) = \mathsf{boss}(j) = \{\overline{C}\}$ by Claim 6.93. It follows that $j \geq \mathsf{tip}(j-1)$ and we get:

$$\mathscr{R}^C_j(\mathcal{A}'').last.\beta = \begin{cases} \diamond & ,\mathscr{R}^C_j(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j-1))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j-1))}.last.\beta & ,\mathscr{R}^C_j(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j-1))}.last.t \end{cases},$$

by item 3b of the induction hypothesis of Lemma 6.94 and the claim follows using Claim 6.90. □

Claim 6.101. *We have:*

$$\mathscr{R}^C_{j+1}(\mathcal{A}'').last.\beta = \begin{cases} \diamond & ,\mathscr{R}^C_{j+1}(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^C_{j+1}(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}.$$

Proof. Recall that $j \in \mathfrak{E}^C(\mathcal{A}'', 87)$. In the case that $j \notin \mathfrak{E}^C(\mathcal{A}'', 90)$, we obtain $\left(\mathscr{R}^C_j(\mathcal{A}'').last.t, \mathscr{R}^C_j(\mathcal{A}'').last.\beta\right) = \left(\mathscr{R}^C_{j+1}(\mathcal{A}'').last.t, \mathscr{R}^C_{j+1}(\mathcal{A}'').last.\beta\right)$ allowing us to get:

$$\mathscr{R}^C_{j+1}(\mathcal{A}'').last.\beta = \mathscr{R}^C_j(\mathcal{A}'').last.\beta$$

$$= \begin{cases} \diamond & ,\mathscr{R}^C_j(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^C_j(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}$$

(Claim 6.100)

$$= \begin{cases} \diamond & ,\mathscr{R}^C_{j+1}(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^C_{j+1}(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases},$$

(As $\mathscr{R}^C_j(\mathcal{A}'').last.t = \mathscr{R}^C_{j+1}(\mathcal{A}'').last.t$)

as desired. In the other case that $j \in \mathfrak{E}^C(\mathcal{A}'', 90)$, we have $0 = \mathscr{R}^C_j(\mathcal{A}'').last.t \neq \mathscr{R}^C_{j+1}(\mathcal{A}'').last.t$. Using Equation 68 and Equation 69, we get $\mathscr{R}^C_{\mathsf{last}^C(j)}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.t \implies \mathscr{R}^C_{\mathsf{last}^C(j+1)-1}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.t$ by item 4 of Lemma 6.85. As $\mathsf{last}^C(j+1) - 1 \in \mathfrak{E}^C(87)$, this is possible only if $\mathsf{last}^C(j+1) - 1 \in \mathfrak{E}^C(90)$.

Next, we apply item 3 of Claim 6.91 to conclude that $\mathscr{R}^C_{\mathsf{last}^C(j+1)-1}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t$. Again using Equation 68 and Equation 69, we get $\mathscr{R}^C_j(\mathcal{A}'').last.t \neq \mathscr{R}^C_{j+1}(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t$. Moreover, as we have shown item 2 of Lemma 6.94, we get that $\mathscr{R}^{\overline{C}}_j(\mathcal{A}'').last.t \neq \mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'').last.t$. Due to Claim 6.98, the last two are possible only if $j \in \mathfrak{E}^A(\mathcal{A}'', 90) \cap \mathfrak{E}^B(\mathcal{A}'', 90)$.

As $\mathscr{R}^C_{j+1}(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t$, we need to show that

$$\mathscr{R}^C_{j+1}(\mathcal{A}'').last.\beta = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta. \tag{71}$$

As $\mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t$, we have:

$$\begin{aligned} \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta &= \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\beta && \text{(Claim 6.91, item 4)} \\ &= \mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}.last.\beta && \text{(Claim 6.91, item 2)} \\ &= \mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'').last.\beta, && \text{(Equation 61 and } \mathsf{boss}(j) = \{\overline{C}\}) \end{aligned}$$

implying that Equation 71 follows once we show that $\mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'').last.\beta = \mathscr{R}^C_{j+1}(\mathcal{A}'').last.\beta$. In this proof, we assume for simplicity that $C = B$ as the other case is symmetric. We need to show that $\mathscr{R}^A_{j+1}(\mathcal{A}'').last.\beta = \mathscr{R}^B_{j+1}(\mathcal{A}'').last.\beta$, or equivalently using the definition of β in Line 91, that $\left(\Gamma^A_{j,1}(\mathcal{A}''), \tilde{\Gamma}^A_{j,1}(\mathcal{A}'')\right) = \left(\tilde{\Gamma}^B_{j,1}(\mathcal{A}''), \Gamma^B_{j,1}(\mathcal{A}'')\right)$. We first show that $\tilde{\Gamma}^A_{j,1}(\mathcal{A}'') = \Gamma^B_{j,1}(\mathcal{A}'')$. This is because:

$$\begin{aligned} \tilde{\Gamma}^A_{j,1}(\mathcal{A}'') &= \mathscr{R}^A_{j+1}(\mathcal{A}'').last.\beta[2] \\ &= \mathscr{R}^B_{\mathsf{last}^B(j+1)}.last.\beta[2] && \text{(As } \mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'').last.\beta = \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\beta) \\ &= \mathsf{TC}(\psi^B_{\mathsf{last}^B(j+1)}) && \text{(As } \mathsf{last}^C(j+1) - 1 \in \mathfrak{E}^C(90)) \\ &= \mathsf{TC}(\psi^B_{j+1}(\mathcal{A}'')) && \text{(Equation 70)} \\ &= \Gamma^B_{j,1}(\mathcal{A}''). && \text{(As } j \in \mathfrak{E}^A(\mathcal{A}'', 90) \cap \mathfrak{E}^B(\mathcal{A}'', 90)) \end{aligned}$$

It remains to show that $\Gamma^A_{j,1}(\mathcal{A}'') = \tilde{\Gamma}^B_{j,1}(\mathcal{A}'')$. For this, we use the definition of $\tilde{\Gamma}^C_j(\mathcal{A}'')$ in Equation 59 and Equation 60. As $j \in \mathfrak{E}^A(\mathcal{A}'', 90) \cap \mathfrak{E}^B(\mathcal{A}'', 90)$, we have $\Gamma^A_j(\mathcal{A}'') \neq \tilde{\Gamma}^A_j(\mathcal{A}'')$ and $|\Gamma^A_j(\mathcal{A}'')| = |\tilde{\Gamma}^A_j(\mathcal{A}'')| = 1$ implying that Equation 60 applies with $h = 1$. Equation 60 gives $\tilde{\Gamma}^B_{j,1}(\mathcal{A}'') = \Gamma^A_{j,1}(\mathcal{A}'')$ using the fact that $\tilde{\Gamma}^A_{j,1}(\mathcal{A}'') = \Gamma^B_{j,1}(\mathcal{A}'')$ finishing the proof.

□

Combining Equation 68, Equation 70, Claim 6.99, and Claim 6.101 proves item 3b of Lemma 6.94.

- $\boldsymbol{j+1 = \mathsf{tip}(j)}$**:** In this case, we have that $\mathsf{lo}(j) \leq j < \mathsf{tip}(j)$ by definition of $\mathsf{lo}(\cdot)$. We have by item 3a of Lemma 6.94 that:

$$\pi^C_{j+1}(\mathcal{A}'')\left[1 : |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|\right] = \pi^C_{\mathsf{last}^C(j+1)}\left[1 : |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|\right].$$

Due to Equation 68, this gives:

$$\pi^C_{j+1}(\mathcal{A}'') = \pi^C_{\mathsf{last}^C(j+1)}. \tag{72}$$

Next, note that $\mathsf{hi}(j) \in \mathsf{Sync}$ implies $|\mathscr{R}^A_{\mathsf{last}^A(\mathsf{hi}(j))}| = |\mathscr{R}^B_{\mathsf{last}^B(\mathsf{hi}(j))}|$ by Definition 6.86 and consider the following subcases:

  - $\boldsymbol{|\mathscr{R}^A_{\mathsf{last}^A(\mathsf{hi}(j))}| = |\mathscr{R}^B_{\mathsf{last}^B(\mathsf{hi}(j))}|}$ **is odd:** By definition of $\mathsf{tip}(\cdot)$, this implies $\mathsf{tip}(j) = \mathsf{hi}(j)$. As $j+1 = \mathsf{tip}(j) = \mathsf{hi}(j) \in \mathsf{Sync}$, we have:

$$\begin{aligned} |\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}| &= |\mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'')| && \text{(Equation 61 and } \mathsf{boss}(j) = \{\overline{C}\}) \\ &= |\mathscr{R}^C_{j+1}(\mathcal{A}'')|, && \text{(As } \mathscr{Q}^A_{j+1}(\mathcal{A}'') = \mathscr{Q}^B_{j+1}(\mathcal{A}'')) \end{aligned}$$

    implying that $|\mathscr{R}^C_{j+1}(\mathcal{A}'')|$ is odd as well. As $|\mathscr{R}^C_{j+1}(\mathcal{A}'')|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j+1)}|$ are both odd, we must have:

$$\begin{aligned} \psi^C_{j+1}(\mathcal{A}'') = \psi^C_{\mathsf{last}^C(j+1)} = \varepsilon. \\ \mathscr{R}^C_{j+1}(\mathcal{A}'').last.\alpha = \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\alpha = \diamond. \\ \mathscr{R}^C_{j+1}(\mathcal{A}'').last.\beta = \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\beta = \diamond. \end{aligned}$$

    Combining the foregoing equation, Equation 68, Equation 72, and the fact that $j+1 = \mathsf{hi}(j)$ proves item 3b of Lemma 6.94.

  - $\boldsymbol{|\mathscr{R}^A_{\mathsf{last}^A(\mathsf{hi}(j))}| = |\mathscr{R}^B_{\mathsf{last}^B(\mathsf{hi}(j))}|}$ **is even:** In this case, as $\mathsf{lo}(j) \leq j < j+1 = \mathsf{tip}(j)$, we have from the definition of $\mathsf{tip}(\cdot)$ that $|\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j)}|$ are both odd and $|\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j+1)}|$ are both even. It follows by item 4 of Lemma 6.85 that $|\mathscr{R}^{C'}_{\mathsf{last}^{C'}(j+1)-1}|$ is odd and $|\mathscr{R}^{C'}_{\mathsf{last}^{C'}(j+1)}|$ is even for $C' \in \{A, B\}$. We claim that:

Claim 6.102. *For $C' \in \{A, B\}$, we have that $|\mathscr{R}_j^{C'}(\mathcal{A}'')|$ is odd and $|\mathscr{R}_{j+1}^{C'}(\mathcal{A}'')|$ is even.*

Proof. Note that as we showed item 2 of Lemma 6.94, it is sufficient to show that there exists $C' \in \{A, B\}$ such that $|\mathscr{R}_j^{C'}(\mathcal{A}'')|$ is odd and another (possibly different) $C' \in \{A, B\}$ such that $|\mathscr{R}_{j+1}^{C'}(\mathcal{A}'')|$ is even. For the former, note that either $j \in \mathsf{Sync}$ in which case, we have by item 4 of the induction hypothesis of Lemma 6.94 that $|\mathscr{R}_j^C(\mathcal{A}'')| = |\mathscr{R}^C_{\mathsf{last}^C(j)}|$ is odd, or $j \notin \mathsf{Sync}$ implying in particular that $j > 1$. Additionally, $j \notin \mathsf{Sync}$ also implies that $\mathsf{tip}(j-1) = \mathsf{tip}(j)$ by Claim 6.90 and $\mathsf{boss}(j-1) = \mathsf{boss}(j) = \{\overline{C}\}$ by Claim 6.93. We get $|\mathscr{R}_j^{\overline{C}}(\mathcal{A}'')| = |\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j)}|$ is odd from item 1 of the induction hypothesis of Lemma 6.94. Finally, by Equation 61, we have that $|\mathscr{R}_{j+1}^{\overline{C}}(\mathcal{A}'')| = |\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|$ is even. □

Consider now iteration j in the execution of Π' with $\mathcal{A}''$ and iteration $\mathsf{last}^C(j+1)-1$ in the execution of Π' with $\mathcal{A}'$ from the perspective of party C. Due to Claim 6.102, the value of $|\mathscr{R}|$ is odd before both the iterations and even after both the iterations. Furthermore, as we showed that $j \in \mathfrak{E}^C(\mathcal{A}'', 52)$ and $\mathsf{last}^C(j+1) - 1 \in \mathfrak{E}^C(52)$ by Definition 6.84, we can conclude that Line 70 is executed in both the iterations and we get:

$$\psi_{j+1}^C(\mathcal{A}'') = \psi^C_{\mathsf{last}^C(j+1)} = \varepsilon \quad \text{and} \quad \mathscr{R}_{j+1}^C(\mathcal{A}'').last.\beta = \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\beta = \diamond. \tag{73}$$

We next claim that

$$\mathscr{R}_{j+1}^C(\mathcal{A}'').last.\beta = \begin{cases} \diamond & ,\mathscr{R}_{j+1}^C(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}_{j+1}^C(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}. \tag{74}$$

Indeed, we have:

$$\begin{aligned} \mathscr{R}_{j+1}^C(\mathcal{A}'').last.\beta &= \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\beta \\ &= \begin{cases} \diamond & ,\mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases} && \text{(Claim 6.91)} \\ &= \begin{cases} \diamond & ,\mathscr{R}_{j+1}^C(\mathcal{A}'').last.t \neq \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}_{j+1}^C(\mathcal{A}'').last.t = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}, && \text{(Equation 68)} \end{aligned}$$

as desired. As $j \in \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$ and we have Claim 6.102, we can

conclude that $j \in \mathfrak{E}^A(\mathcal{A}'', 70) \cap \mathfrak{E}^B(\mathcal{A}'', 70)$. We claim that:

$$\mathscr{R}^C_{j+1}(\mathcal{A}'').last.\alpha = \mathscr{R}^C_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\alpha. \tag{75}$$

Before showing Equation 75, we observe that the combination of Equation 68, Equation 72, Equation 73 , Equation 74, and Equation 75 proves item 3b of Lemma 6.94, and thus showing Equation 75 finishes the proof of item 3b of Lemma 6.94. Note that:

$$\begin{aligned}
\mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'').last.\alpha &= \mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}.last.\alpha && \text{(Equation 61)}\\
&= \mathscr{R}^{C}_{\mathsf{last}^{C}(j+1)}.last.\alpha && \text{(Claim 6.91, item 2)}\\
&= \mathscr{R}^{C}_{\mathsf{last}^{C}(\mathsf{hi}(j))}.last.\alpha, && \text{(Claim 6.91, item 4)}
\end{aligned}$$

and therefore, Equation 75 follows once we show $\mathscr{R}^C_{j+1}(\mathcal{A}'').last.\alpha = \mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'').last.\alpha$. Assume for simplicity that $C = B$ as the other case is symmetric. We have to show that $\mathscr{R}^A_{j+1}(\mathcal{A}'').last.\alpha = \mathscr{R}^B_{j+1}(\mathcal{A}'').last.\alpha$, or equivalently, using Line 70 that

$$\begin{aligned}
&\left(\mathscr{R}^A_{\mathrm{F},j+1}(\mathcal{A}'')[h^A].r, \Gamma^A_{j,h^A}(\mathcal{A}''), \tilde{\Gamma}^A_{j,h^A}(\mathcal{A}'')\right)\\
&\qquad = \left(\mathscr{R}^B_{\mathrm{F},j+1}(\mathcal{A}'')[h^B].r, \tilde{\Gamma}^B_{j,h^B}(\mathcal{A}''), \Gamma^B_{j,h^B}(\mathcal{A}'')\right).
\end{aligned}$$

where, $h^{C'}$, for $C' \in \{A, B\}$ is the smallest such that $\Gamma^{C'}_{j,h^{C'}}(\mathcal{A}'') \neq \tilde{\Gamma}^{C'}_{j,h^{C'}}(\mathcal{A}'')$. Note that $h^{C'}$ is well defined as $j \in \mathfrak{E}^A(\mathcal{A}'', 70) \cap \mathfrak{E}^B(\mathcal{A}'', 70)$. Due to Equation 60, we have $h^A = h^B = h$, say, and using the fact that $\mathscr{Q}^A_{j+1}(\mathcal{A}'') = \mathscr{Q}^B_{j+1}(\mathcal{A}'')$, we get:

$$\mathscr{R}^A_{\mathrm{F},j+1}(\mathcal{A}'')[h^A].r = \mathscr{R}^A_{\mathrm{F},j+1}(\mathcal{A}'')[h].r = \mathscr{R}^B_{\mathrm{F},j+1}(\mathcal{A}'')[h].r = \mathscr{R}^B_{\mathrm{F},j+1}(\mathcal{A}'')[h^B].r,$$

implying that $\mathscr{R}^B_{j+1}(\mathcal{A}'').last.\alpha[1] = \mathscr{R}^A_{j+1}(\mathcal{A}'').last.\alpha[1]$. We next show that $\tilde{\Gamma}^A_{j,h}(\mathcal{A}'') = \Gamma^B_{j,h}(\mathcal{A}'')$. This is because

$$\begin{aligned}
\tilde{\Gamma}^A_{j,h}(\mathcal{A}'') &= \mathscr{R}^A_{j+1}(\mathcal{A}'').last.\alpha[3]\\
&= \mathscr{R}^B_{\mathsf{last}^B(j+1)}.last.\alpha[3] && (\text{As } \mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'').last.\alpha = \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\alpha)\\
&= \mathsf{TC}(\pi^B_{\mathsf{last}^B(j+1),>\mathscr{R}^B_{\mathsf{last}^B(j+1)}.last.\alpha[1]}) && (\text{As } \mathsf{last}^C(j+1)-1 \in \mathfrak{E}^C(70))\\
&= \mathsf{TC}(\pi^B_{\mathsf{last}^B(j+1),>\mathscr{R}^A_{j+1}(\mathcal{A}'').last.\alpha[1]})\\
&\qquad && (\text{As } \mathscr{R}^{\overline{C}}_{j+1}(\mathcal{A}'').last.\alpha = \mathscr{R}^C_{\mathsf{last}^C(j+1)}.last.\alpha)\\
&= \mathsf{TC}(\pi^B_{\mathsf{last}^B(j+1),>\mathscr{R}^B_{j+1}(\mathcal{A}'').last.\alpha[1]})\\
&\qquad && (\text{As } \mathscr{R}^B_{j+1}(\mathcal{A}'').last.\alpha[1] = \mathscr{R}^A_{j+1}(\mathcal{A}'').last.\alpha[1])\\
&= \mathsf{TC}((\pi^B_{j+1}(\mathcal{A}''))_{>\mathscr{R}^B_{j+1}(\mathcal{A}'').last.\alpha[1]}) && \text{(Equation 72)}
\end{aligned}$$

$$= \Gamma^B_{j,h}(\mathcal{A}''). \qquad \text{(Line 70)}$$

It remains to show that $\Gamma^A_{j,h}(\mathcal{A}'') = \tilde{\Gamma}^B_{j,h}(\mathcal{A}'')$. For this, we use the definition of $\tilde{\Gamma}^C_j(\mathcal{A}'')$ in Equation 59 and Equation 60. By our choice of h, we have that Equation 60 applies with h. Equation 60 gives $\tilde{\Gamma}^B_{j,h}(\mathcal{A}'') = \Gamma^A_{j,h}(\mathcal{A}'')$ as $\Gamma^B_{j,h}(\mathcal{A}'') = \tilde{\Gamma}^A_{j,h}(\mathcal{A}'')$ finishing the proof.

Finally, we show item 4 of Lemma 6.94. Due to the induction hypothesis, it is sufficient to show that, if $j+1 \in \mathsf{Sync}$, then we have $\boldsymbol{\mathcal{S}}^C_{j+1}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)}.last$ for all $C \in \{A, B\}$. Thus, we assume throughout that $j+1 \in \mathsf{Sync}$. Observe that if $j \in \mathsf{Sync}$ as well, then $\mathsf{boss}(j) = \{A, B\}$ by the definition of $\mathsf{boss}(\cdot)$ and we are done by item 1 of Lemma 6.94. This means that we can assume $j \notin \mathsf{Sync}$ implying by the definition of $\mathsf{boss}(\cdot)$ that $\mathsf{boss}(j)$ and $\overline{\mathsf{boss}}(j)$ are singleton. Let C be the unique element in $\overline{\mathsf{boss}}(j)$ and $\overline{C}$ be the unique element in $\mathsf{boss}(j)$. As we have shown Equation 61, all that remains to be shown is that $\boldsymbol{\mathcal{S}}^C_{j+1}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)}.last$. To start, observe that:

$$\begin{aligned} \mathcal{Q}^C_{j+1}(\mathcal{A}'') &= \mathcal{Q}^{\overline{C}}_{j+1}(\mathcal{A}'') && \text{(As } \mathcal{Q}^A_{j+1}(\mathcal{A}'') = \mathcal{Q}^B_{j+1}(\mathcal{A}'')\text{)} \\ &= \mathcal{Q}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}. && \text{(Equation 61)} \end{aligned}$$

As $j+1 \in \mathsf{Sync}$, we have from Definition 6.86 that $\mathscr{P}^A_{\mathsf{last}^A(j+1)} = \mathscr{P}^B_{\mathsf{last}^B(j+1)}$. As $\mathscr{Q}$ is determined by $\mathscr{P}$, we get in turn that $\mathcal{Q}^A_{\mathsf{last}^A(j+1)} = \mathcal{Q}^B_{\mathsf{last}^B(j+1)}$ implying that

$$\mathcal{Q}^C_{j+1}(\mathcal{A}'') = \mathcal{Q}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)} = \mathcal{Q}^C_{\mathsf{last}^C(j+1)}. \tag{76}$$

Next, we observe that the fact that $j+1 \in \mathsf{Sync}$ implies that $\mathsf{hi}(j) = j+1$ and consider the following cases:

- **When $|\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|$ is odd:** As $\mathsf{hi}(j) = j+1$, we have by the definition of $\mathsf{tip}(\cdot)$ that $\mathsf{hi}(j) = \mathsf{tip}(j) = j+1$. Due to Equation 76, we have in this case that $|\mathscr{R}^C_{j+1}(\mathcal{A}'')|$ and $|\mathscr{R}^C_{\mathsf{last}^C(j+1)}|$ are also odd. Observe that when $|\mathscr{R}|$ is odd, then $\mathscr{R}$ is is determined by $\mathscr{R}'$ and we have $\psi = \varepsilon$. This means that, in this case, $\boldsymbol{\mathcal{S}}.last$ is determined by $(\mathscr{Q}, \pi)$. As we have already shown Equation 76, in order to show that $\boldsymbol{\mathcal{S}}^C_{j+1}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)}.last$ it is enough to show that $\pi^C_{j+1}(\mathcal{A}'') = \pi^C_{\mathsf{last}^C(j+1)}$. This is because by item 3a of Lemma 6.94 and the fact that $\mathsf{hi}(j) = \mathsf{tip}(j) = j+1$, we have:

  $$\pi^C_{j+1}(\mathcal{A}'')\left[1 : |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(\mathsf{hi}(j))}|\right] = \pi^C_{\mathsf{last}^C(\mathsf{hi}(j))}\left[1 : |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(\mathsf{hi}(j))}|\right],$$

  and we can conclude from $\mathsf{hi}(j) = j+1$ and Equation 76 that $|\pi^C_{j+1}(\mathcal{A}'')| = |\pi^C_{\mathsf{last}^C(j+1)}| = |\pi^C_{\mathsf{last}^C(\mathsf{hi}(j))}| = |\pi^{\overline{C}}_{\mathsf{last}^{\overline{C}}(\mathsf{hi}(j))}|$ by Definition 6.86.

- **When $|\mathscr{R}^{\overline{C}}_{\mathsf{last}^{\overline{C}}(j+1)}|$ is even:** As $j+1 = \mathsf{hi}(j) \geq \mathsf{tip}(j)$, we have due to item 3b of

Lemma 6.94 that:

$$\left(\mathscr{R}'^{C}_{j+1}(\mathcal{A}'').last, \pi^{C}_{j+1}(\mathcal{A}''), \psi^{C}_{j+1}(\mathcal{A}'')\right) = \left(\mathscr{R}'^{C}_{\mathsf{last}^C(j+1)}.last, \pi^{C}_{\mathsf{last}^C(j+1)}, \psi^{C}_{\mathsf{last}^C(j+1)}\right).$$

Furthermore, we have $\mathscr{R}^{C}_{j+1}(\mathcal{A}'').last.\alpha = \mathscr{R}^{C}_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\alpha$ and

$$\mathscr{R}^{C}_{j+1}(\mathcal{A}'').last.\beta = \begin{cases} \diamond & ,\mathscr{R}^{C}_{j+1}(\mathcal{A}'').last.t \neq \mathscr{R}^{C}_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \\ \mathscr{R}^{C}_{\mathsf{last}^C(\mathsf{hi}(j))}.last.\beta & ,\mathscr{R}^{C}_{j+1}(\mathcal{A}'').last.t = \mathscr{R}^{C}_{\mathsf{last}^C(\mathsf{hi}(j))}.last.t \end{cases}.$$

As $\mathsf{hi}(j) = j+1$, this simplifies to:

$$\left(\mathscr{R}^{C}_{j+1}(\mathcal{A}'').last, \pi^{C}_{j+1}(\mathcal{A}''), \psi^{C}_{j+1}(\mathcal{A}'')\right) = \left(\mathscr{R}^{C}_{\mathsf{last}^C(j+1)}.last, \pi^{C}_{\mathsf{last}^C(j+1)}, \psi^{C}_{\mathsf{last}^C(j+1)}\right).$$

As the variable $\boldsymbol{\mathcal{S}}.last$ is determined by $(\mathscr{Q}, \pi \| \psi, \mathscr{R}.last.\alpha, \mathscr{R}.last.\beta)$, the foregoing equation and Equation 76 imply that $\boldsymbol{\mathcal{S}}^{C}_{j+1}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^{C}_{\mathsf{last}^C(j+1)}.last$ completing the proof.

□

Next, we define the values $\mathcal{A}''^{A}_{>(num-1)(P+1)}(x^A, x^B)$ and $\mathcal{A}''^{B}_{>(num-1)(P+1)}(x^A, x^B)$. For all $num \leq j \leq R/(P+1)$, $j' \in [P]$, and $C \in \{A, B\}$, we define:

$$\mathcal{A}''^{C}_{(j-1)(P+1)+j'}(x^A, x^B) = \perp \qquad \text{and} \qquad \mathcal{A}''^{C}_{j(P+1)}(x^A, x^B) = \perp^P. \tag{77}$$

With this definition of $\mathcal{A}''$ and num, we show that the requirements of Theorem 6.2 are satisfied. Observe that item 1 of Theorem 6.2 is straightforward from item 2 of Lemma 6.94.

Next, we show item 3 of Theorem 6.2. If $M < |\boldsymbol{\mathcal{S}}^A| = num$, we have $\mathsf{boss}(num-1) = \{A\}$ by definition of $\mathsf{boss}(\cdot)$ implying using item 1 of Lemma 6.94 that $\boldsymbol{\mathcal{S}}^{A}_{num}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^{A}_{\mathsf{last}^A(num)}.last$. Otherwise, as $M \leq \min\left(|\boldsymbol{\mathcal{S}}^A|, |\boldsymbol{\mathcal{S}}^B|\right)$, we must have $M = |\boldsymbol{\mathcal{S}}^A| \in \mathsf{Sync}$ implying by item 4 of Lemma 6.94 that $\boldsymbol{\mathcal{S}}^{A}_{num}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^{A}_{\mathsf{last}^A(num)}.last$.

Thus, in either case, we have $\boldsymbol{\mathcal{S}}^{A}_{num}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^{A}_{\mathsf{last}^A(num)}.last$. Due to the "furthermore" part of item 1 of Theorem 6.2, we have that $\boldsymbol{\mathcal{S}}^{A}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^{A}_{\mathsf{last}^A(num)}.last$. Combining with item 5 of Lemma 6.85, we have that $\boldsymbol{\mathcal{S}}^{A}(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^{A}.last$.

Finally, as the output of Alice is determined by $\boldsymbol{\mathcal{S}}^{A}.last$, the fact that $\boldsymbol{\mathcal{S}}^{A}.last = \boldsymbol{\mathcal{S}}^{A}(\mathcal{A}'').last$ implies:

$$\Pi'^{A}_{\mathcal{A}''}(x^A, x^B) = \Pi'^{A}_{\mathcal{A}'}(x^A, x^B) \neq \Pi^{A}(x^A, x^B),$$

and item 3 of Theorem 6.2 follows. We finish the proof by showing item 2 of Theorem 6.2 in the next subsection.

□

6.3.1 Proof of item 2 of Theorem 6.2

We start with some technical lemmas.

Lemma 6.103. *Let $C \in \{A, B\}$ and $j \in [R/(P+1)+1]$. We have for all $1 \leq z < |\boldsymbol{\mathcal{S}}_j^C|$ that $\boldsymbol{\mathcal{S}}_j^C[z].p \leq 2 \cdot \boldsymbol{\mathcal{S}}_j^C[z+1].p = 2 \cdot \ell^C_{\mathsf{last}_j^C(z+1)-1}$.*

Proof. Proof by induction on j. The base case $j = 1$ is trivial. We show the statement holds for $j+1$ assuming that it holds for j. Consider $1 \leq z < |\boldsymbol{\mathcal{S}}_{j+1}^C|$ and assume first that $z < \min(|\boldsymbol{\mathcal{S}}_j^C|, |\boldsymbol{\mathcal{S}}_{j+1}^C|)$. For all such z observe that Algorithm 4 does not change the values of $\boldsymbol{\mathcal{S}}_j^C[z]$ and $\boldsymbol{\mathcal{S}}_j^C[z+1]$ in iteration j. Furthermore, by item 3 of Lemma 6.85, we have that $\mathsf{last}_{j+1}^C(z+1) = \mathsf{last}_j^C(z+1)$. Combining and using the induction hypothesis the result clearly follows.

Now consider $\min(|\boldsymbol{\mathcal{S}}_j^C|, |\boldsymbol{\mathcal{S}}_{j+1}^C|) \leq z < |\boldsymbol{\mathcal{S}}_{j+1}^C|$. When this happens, we have in particular that $|\boldsymbol{\mathcal{S}}_j^C| < |\boldsymbol{\mathcal{S}}_{j+1}^C|$ implying that $j \in \mathfrak{E}^C(52)$ and $|\boldsymbol{\mathcal{S}}_{j+1}^C| = |\boldsymbol{\mathcal{S}}_j^C| + 1 = z + 1$. We get from Line 50 and Line 96 that

$$\boldsymbol{\mathcal{S}}_{j+1}^C[z].p = \boldsymbol{\mathcal{S}}_j^C[z].p = \boldsymbol{\mathcal{S}}_j^C.last.p = p_j^C \leq 2 \cdot \ell_j^C = 2 \cdot \boldsymbol{\mathcal{S}}_{j+1}^C[z+1].p.$$

To finish the proof, we simply note by Definition 6.84 that $j = \mathsf{last}_{j+1}^C(z+1) - 1$.

□

Lemma 6.104. *For $C \in \{A, B\}$ and $j \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)$, we have*

$$\sum_{z=|\boldsymbol{\mathcal{S}}_{j+1}^C|}^{|\boldsymbol{\mathcal{S}}_j^C|-1} \ell^C_{\mathsf{last}_j^C(z+1)-1} = \sum_{z=|\boldsymbol{\mathcal{S}}_{j+1}^C|+1}^{|\boldsymbol{\mathcal{S}}_j^C|} \boldsymbol{\mathcal{S}}_j^C[z].p \leq 22 \cdot \left(\ell_j^A + \ell_j^B + \mathsf{corr}_j\right).$$

Proof. The equality follows simply from Lemma 6.103 as we get $\sum_{z=|\boldsymbol{\mathcal{S}}_{j+1}^C|}^{|\boldsymbol{\mathcal{S}}_j^C|-1} \ell^C_{\mathsf{last}_j^C(z+1)-1} = \sum_{z=|\boldsymbol{\mathcal{S}}_{j+1}^C|}^{|\boldsymbol{\mathcal{S}}_j^C|-1} \boldsymbol{\mathcal{S}}_j^C[z+1].p = \sum_{z=|\boldsymbol{\mathcal{S}}_{j+1}^C|+1}^{|\boldsymbol{\mathcal{S}}_j^C|} \boldsymbol{\mathcal{S}}_j^C[z].p$. For the inequality, we upper bound the left hand side by $22 \cdot (\ell_j^C + \tilde{\ell}_j^C)$ and then use the definition of corr to upper bound $\tilde{\ell}_j^C \leq \ell_j^{\overline{C}} + \mathsf{corr}_j$ to finish the proof[15]. We first deal with the simple case when $j \in \mathfrak{E}^C(54)$. In this case $|\boldsymbol{\mathcal{S}}_{j+1}^C| + 1 = |\boldsymbol{\mathcal{S}}_j^C|$ and we get:

$$\sum_{z=|\boldsymbol{\mathcal{S}}_{j+1}^C|+1}^{|\boldsymbol{\mathcal{S}}_j^C|} \boldsymbol{\mathcal{S}}_j^C[z].p = \boldsymbol{\mathcal{S}}_j^C.last.p = p_j^C \leq 2 \cdot \ell_j^C,$$

by Line 50. In the other case, when $j \in \mathfrak{E}^C(56)$, we consider the value μ_j^C computed in Line 56. If $\mu_j^C = |\boldsymbol{\mathcal{S}}_j^C| + 1$, then we have by the definition of μ that:

$$\sum_{z=|\boldsymbol{\mathcal{S}}_{j+1}^C|+1}^{|\boldsymbol{\mathcal{S}}_j^C|} \boldsymbol{\mathcal{S}}_j^C[z].p \leq \sum_{z=1}^{|\boldsymbol{\mathcal{S}}_j^C|} \boldsymbol{\mathcal{S}}_j^C[z].p \leq 10 \cdot \left(\ell_j^C + \tilde{\ell}_j^C\right),$$

[15] Recall that $\overline{C}$ denotes the unique element in $\{A, B\}$ that is different from C.

Otherwise, we we use our choice of μ_j^C to conclude:

$$\sum_{z=1}^{\mu_j^C-1} \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|+1-z].p \leq 10 \cdot \left(\ell_j^C + \tilde{\ell}_j^C\right) < \sum_{z=1}^{\mu_j^C} \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|+1-z].p. \tag{78}$$

This lets us derive:

$$\begin{aligned}
\sum_{z=|\boldsymbol{\mathcal{S}}_{j+1}^C|+1}^{|\boldsymbol{\mathcal{S}}_j^C|} \boldsymbol{\mathcal{S}}_j^C[z].p &= \sum_{z=1}^{|\boldsymbol{\mathcal{S}}_j^C|-|\boldsymbol{\mathcal{S}}_{j+1}^C|} \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|+1-z].p \\
&\leq \sum_{z=1}^{\mu_j^C} \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|+1-z].p && \text{(As } |\boldsymbol{\mathcal{S}}_j^C| - |\boldsymbol{\mathcal{S}}_{j+1}^C| \leq \mu_j^C \text{ by Line 56)} \\
&= \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|].p + \sum_{z=2}^{\mu_j^C} \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|+1-z].p \\
&= \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|].p + \sum_{z=1}^{\mu_j^C-1} \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|-z].p \\
&\leq \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|].p + 2 \cdot \sum_{z=1}^{\mu_j^C-1} \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|+1-z].p && \text{(Lemma 6.103)} \\
&\leq \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|].p + 20 \cdot \left(\ell_j^C + \tilde{\ell}_j^C\right) && \text{(Equation 78)} \\
&\leq 22 \cdot \left(\ell_j^C + \tilde{\ell}_j^C\right). && \text{(As } \boldsymbol{\mathcal{S}}_j^C[|\boldsymbol{\mathcal{S}}_j^C|].p = p_j^C \leq 2 \cdot \ell_j^C \text{ by Line 50)}
\end{aligned}$$

□

Lemma 6.105. *It holds for $C \in \{A, B\}$ that:*

$$\sum_{j \in \mathfrak{E}^C(52)} \ell_j^C \cdot \mathbb{1}(\exists j < j' \leq R/(P+1) : |\boldsymbol{\mathcal{S}}_{j'+1}^C| < |\boldsymbol{\mathcal{S}}_{j+1}^C|) \leq 22 \cdot \sum_{j \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)} \left(\ell_j^A + \ell_j^B + \mathsf{corr}_j\right).$$

Proof. Let J be the set of all $j \in \mathfrak{E}^C(52)$ such that there exists $j < j' \leq R/(P+1)$ satisfying $|\boldsymbol{\mathcal{S}}_{j'+1}^C| < |\boldsymbol{\mathcal{S}}_{j+1}^C|$. We start by claiming that:

Claim 6.106. *For all $j \in J$, there exists $j'' \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)$ and $z \in (|\boldsymbol{\mathcal{S}}_{j''+1}^C| : |\boldsymbol{\mathcal{S}}_{j''}^C|]$ such that (j'', z) determines j and $\ell_j^C = \boldsymbol{\mathcal{S}}_{j''}^C[z].p$.*

We show Claim 6.106 later but use it to get:

$$\begin{aligned}
&\sum_{j \in \mathfrak{E}^C(52)} \ell_j^C \cdot \mathbb{1}(\exists j < j' \leq R/(P+1) : |\boldsymbol{\mathcal{S}}_{j'+1}^C| < |\boldsymbol{\mathcal{S}}_{j+1}^C|) \\
&\quad \leq \sum_{j \in J} \ell_j^C
\end{aligned}$$

$$\leq \sum_{j'' \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)} \sum_{z=|\boldsymbol{\mathcal{S}}^C_{j''+1}|+1}^{|\boldsymbol{\mathcal{S}}^C_{j''}|} \boldsymbol{\mathcal{S}}^C_{j''}[z].p \qquad \text{(Claim 6.106)}$$

$$\leq 22 \cdot \sum_{j'' \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)} \left(\ell^A_{j''} + \ell^B_{j''} + \mathsf{corr}_{j''}\right). \qquad \text{(Lemma 6.104)}$$

We now show Claim 6.106.

Proof of Claim 6.106. Define j'' to be the smallest $j < j' \leq R/(P+1)$ such that $|\boldsymbol{\mathcal{S}}^C_{j'+1}| < |\boldsymbol{\mathcal{S}}^C_{j+1}|$ and $z = |\boldsymbol{\mathcal{S}}^C_{j+1}|$. Note that j'' is well defined as $j \in J$. By our choice of j'', we must have $|\boldsymbol{\mathcal{S}}^C_{j''+1}| < |\boldsymbol{\mathcal{S}}^C_{j+1}| \leq |\boldsymbol{\mathcal{S}}^C_{j''}|$ implying that $j'' \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)$ and $z \in (|\boldsymbol{\mathcal{S}}^C_{j''+1}| : |\boldsymbol{\mathcal{S}}^C_{j''}|]$.

In order to show that the pair (j'', z) determines j, we show that $j+1 = \mathsf{last}^C_{j''}(z)$. Suppose not. As $z = |\boldsymbol{\mathcal{S}}^C_{j+1}|$ and $j \in \mathfrak{E}^C(52)$, this is only possible if there exists $j+1 < j''' \leq j''$ such that $|\boldsymbol{\mathcal{S}}^C_{j'''}| = z$ and $j'''-1 \in \mathfrak{E}^C(52)$. However, this means that $|\boldsymbol{\mathcal{S}}^C_{j'''-1}| = z-1$ contradicting the choice of j''.

Finally, to show that $\ell^C_j = \boldsymbol{\mathcal{S}}^C_{j''}[z].p$, we use item 2 of Lemma 6.85 that says $\boldsymbol{\mathcal{S}}^C_{j''}[z].p = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C_{j''}(z)}[z].p = \boldsymbol{\mathcal{S}}^C_{j+1}[|\boldsymbol{\mathcal{S}}^C_{j+1}|].p = \boldsymbol{\mathcal{S}}^C_{j+1}.last.p$. The last term equals ℓ^C_j as $j \in \mathfrak{E}^C(52)$. □

□

Lemma 6.107. *For all $j \in [num]$, there exists $C \in \{A, B\}$ such that $\ell^A_j(\mathcal{A}'') = \ell^B_j(\mathcal{A}'') = \ell^C_{\mathsf{last}^C(j)}$.*

Proof. Fix $j \in [num]$. We first show that there exists $C \in \{A, B\}$ such that $\mathscr{Q}^C_j(\mathcal{A}'') = \mathscr{Q}^C_{\mathsf{last}^C(j)}$. If $j \in \mathsf{Sync}$, we let C be an arbitrary element in $\{A, B\}$ and the claim follows from item 4 of Lemma 6.94. On the other hand, if $j \notin \mathsf{Sync}$, we have in particular that $j > 1$. In this case, we let C be an arbitrary element in $\mathsf{boss}(j-1)$ (recall that $\mathsf{boss}(\cdot)$ is always non-empty by definition). We get by item 1 of Lemma 6.94 that $\mathscr{Q}^C_j(\mathcal{A}'') = \mathscr{Q}^C_{\mathsf{last}^C(j)}$, as desired.

Let $C \in \{A, B\}$ be as above. Use item 2 of Lemma 6.94 to conclude that $\mathscr{Q}^A_j(\mathcal{A}'') = \mathscr{Q}^B_j(\mathcal{A}'') = \mathscr{Q}^C_{\mathsf{last}^C(j)}$. As ℓ is determined by $\mathscr{Q}$, we get:

$$\ell^A_j(\mathcal{A}'') = \ell^B_j(\mathcal{A}'') = \ell^C_{\mathsf{last}^C(j)}.$$

□

Lemma 6.108. *It holds that:*

$$\sum_{j \in [num] \setminus \mathsf{Sync}} \ell^A_j(\mathcal{A}'') + \ell^B_j(\mathcal{A}'') \leq 300 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 50 \cdot \sum_{C \in \{A,B\}} \sum_{j \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)} \left(\ell^A_j + \ell^B_j\right).$$

Proof. We start by claiming that:

Claim 6.109. *For all $j \in [num] \setminus \mathsf{Sync}$, there exists a $C \in \{A, B\}$ and $j' \in [R/(P+1)]$ such that (C, j') determines j and*[16]*:*

$$\ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') \leq 2.2 \cdot (\mathsf{corr}_{j'} + \ell_{j'}^{\overline{C}} \cdot \mathbb{1}(j' \in \mathfrak{E}^{\overline{C}}(52)) \cdot \mathbb{1}(\exists j' < j'' \leq R/(P+1) : |\boldsymbol{\mathcal{S}}_{j''+1}^{\overline{C}}| < |\boldsymbol{\mathcal{S}}_{j'+1}^{\overline{C}}|)).$$

We show Claim 6.109 later but assuming it for now, we get:

$$\begin{aligned}
&\sum_{j \in [num] \setminus \mathsf{Sync}} \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') \\
&\quad \leq 2.2 \cdot \sum_{C \in \{A,B\}} \sum_{j'=1}^{R/(P+1)} \ell_{j'}^{\overline{C}} \cdot \mathbb{1}(j' \in \mathfrak{E}^{\overline{C}}(52)) \cdot \mathbb{1}(\exists j' < j'' \leq R/(P+1) : |\boldsymbol{\mathcal{S}}_{j''+1}^{\overline{C}}| < |\boldsymbol{\mathcal{S}}_{j'+1}^{\overline{C}}|) \\
&\qquad + 2.2 \cdot \sum_{C \in \{A,B\}} \sum_{j'=1}^{R/(P+1)} \mathsf{corr}_{j'} \\
&\quad \leq 5 \cdot \sum_{j'=1}^{R/(P+1)} \mathsf{corr}_{j'} + 2.2 \cdot \sum_{C \in \{A,B\}} \sum_{j' \in \mathfrak{E}^{\overline{C}}(52)} \ell_{j'}^{\overline{C}} \cdot \mathbb{1}(\exists j' < j'' \leq R/(P+1) : |\boldsymbol{\mathcal{S}}_{j''+1}^{\overline{C}}| < |\boldsymbol{\mathcal{S}}_{j'+1}^{\overline{C}}|) \\
&\quad \leq 5 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 2.2 \cdot \sum_{C \in \{A,B\}} \sum_{j \in \mathfrak{E}^{C}(52)} \ell_j^{C} \cdot \mathbb{1}(\exists j < j' \leq R/(P+1) : |\boldsymbol{\mathcal{S}}_{j'+1}^{C}| < |\boldsymbol{\mathcal{S}}_{j+1}^{C}|) \\
&\quad \leq 5 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 50 \cdot \sum_{C \in \{A,B\}} \sum_{j \in \mathfrak{E}^{C}(54) \cup \mathfrak{E}^{C}(56)} \left(\ell_j^A + \ell_j^B + \mathsf{corr}_j\right) \qquad \text{(Lemma 6.105)} \\
&\quad \leq 5 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 50 \cdot \sum_{C \in \{A,B\}} \sum_{j \in \mathfrak{E}^{C}(54) \cup \mathfrak{E}^{C}(56)} \left(\ell_j^A + \ell_j^B\right) + 50 \cdot \sum_{C \in \{A,B\}} \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j \\
&\quad \leq 300 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 50 \cdot \sum_{C \in \{A,B\}} \sum_{j \in \mathfrak{E}^{C}(54) \cup \mathfrak{E}^{C}(56)} \left(\ell_j^A + \ell_j^B\right).
\end{aligned}$$

It remains to show Claim 6.109.

Proof of Claim 6.109. Let $C \in \{A, B\}$ be the one promised by Lemma 6.107 and $j' = \mathsf{last}^C(j) - 1$. By Definition 6.84, we have that $|\boldsymbol{\mathcal{S}}_{j'+1}^{C}| = j$ and it follows that (C, j') determines j. Definition 6.84 also says that $j' \in \mathfrak{E}^C(52)$. We claim that:

$$\ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') \leq 2.2 \cdot \ell_{j'}^{C}. \tag{79}$$

As $\ell_j^A(\mathcal{A}'') = \ell_j^B(\mathcal{A}'') = \ell_{j'+1}^C$ by Lemma 6.107, it is sufficient to show that $\ell_{j'+1}^C \leq 1.1 \cdot \ell_{j'}^C$. In turn, due to Line 50, it is sufficient to show that $\boldsymbol{\mathcal{S}}_{j'+1}^{C}.last.p \leq 1.1 \cdot \ell_{j'}^C$ and $500KP \cdot 1.1^{|\mathscr{R}_{j'+1}^C|} \leq 1.1 \cdot \ell_{j'}^C$. For the former, note that $j' \in \mathfrak{E}^C(52)$ implies that $\boldsymbol{\mathcal{S}}_{j'+1}^{C}.last.p \leq \ell_{j'}^C$ while for the latter use $j' \in \mathfrak{E}^C(52)$ to conclude $|\mathscr{R}_{j'+1}^C| \leq |\mathscr{R}_{j'}^C| + 1$, which using Line 50 implies

[16] Recall that $\overline{C}$ denotes the unique element in $\{A, B\}$ that is different from C.

$500KP \cdot 1.1^{|\mathscr{R}^C_{j'+1}|} \leq 1.1 \cdot 500KP \cdot 1.1^{|\mathscr{R}^C_{j'}|} \leq 1.1 \cdot \ell^C_{j'}$. Consider now the following cases:

- **$\mathsf{corr}_{j'} > 0$:** In this case, we have by definition of corr that $\mathsf{corr}_{j'} \geq \min\left(\ell^C_{j'}, \tilde{\ell}^C_{j'}\right)$. As $j' \in \mathfrak{E}^C(52)$, we must have $\mathscr{P}^C_{j'} = \tilde{\mathscr{P}}^C_{j'} \implies \ell^C_{j'} = \tilde{\ell}^C_{j'}$. Plugging in, we get $\mathsf{corr}_{j'} \geq \ell^C_{j'}$ which, together with Equation 79 implies Claim 6.109.

- **$\mathsf{corr}_{j'} = 0$:** In this case, we first note that:

$$\begin{aligned}
(\tilde{\mathscr{P}}^{\overline{C}}_{j'}, |\tilde{\boldsymbol{\mathcal{S}}}^{\overline{C}}_{j'}|) &= (\mathscr{P}^C_{j'}, |\boldsymbol{\mathcal{S}}^C_{j'}|) && (\text{As } \mathsf{corr}_{j'} = 0)\\
&= (\tilde{\mathscr{P}}^C_{j'}, |\tilde{\boldsymbol{\mathcal{S}}}^C_{j'}|) && (\text{As } j' \in \mathfrak{E}^C(52))\\
&= (\mathscr{P}^{\overline{C}}_{j'}, |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'}|). && (\text{As } \mathsf{corr}_{j'} = 0)
\end{aligned}$$

  It follows that $j' \in \mathfrak{E}^C(52) \cap \mathfrak{E}^{\overline{C}}(52)$ and $\ell^C_{j'} = \ell^{\overline{C}}_{j'}$. Observe from Algorithm 6 that the former together with $(\mathscr{P}^C_{j'}, |\boldsymbol{\mathcal{S}}^C_{j'}|) = (\mathscr{P}^{\overline{C}}_{j'}, |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'}|)$ and $\mathsf{corr}_{j'} = 0$ implies that $(\mathscr{P}^C_{j'+1}, |\boldsymbol{\mathcal{S}}^C_{j'+1}|) = (\mathscr{P}^{\overline{C}}_{j'+1}, |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}|)$ which, in particular means that $|\boldsymbol{\mathcal{S}}^C_{j'+1}| = |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}| = j$ by Definition 6.84. We claim that there exists $j' \leq j'' \leq R/(P+1)$ such that $|\boldsymbol{\mathcal{S}}^{\overline{C}}_{j''+1}| < |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}|$. Proving this claim suffices as we must have $j' < j''$ implying:

$$\ell^C_{j'} = \ell^{\overline{C}}_{j'} = \ell^{\overline{C}}_{j'} \cdot \mathbb{1}(j' \in \mathfrak{E}^{\overline{C}}(52)) \cdot \mathbb{1}(\exists j' < j'' \leq R/(P+1) : |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j''+1}| < |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}|),$$

  and Equation 79 finishes the proof of Claim 6.109. Suppose for contradiction that $|\boldsymbol{\mathcal{S}}^{\overline{C}}_{j''+1}| \geq |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}|$ for all $j' \leq j'' \leq R/(P+1)$. Due to item 3 of Lemma 6.85, this means that $\mathsf{last}^{\overline{C}}(|\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}|) = \mathsf{last}^{\overline{C}}_{j'+1}(|\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}|)$. We get that:

$$\begin{aligned}
\mathsf{last}^{\overline{C}}(j) &= \mathsf{last}^{\overline{C}}(|\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}|) && (\text{As } |\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}| = j)\\
&= \mathsf{last}^{\overline{C}}_{j'+1}(|\boldsymbol{\mathcal{S}}^{\overline{C}}_{j'+1}|)\\
&= j' + 1 && (\text{Definition 6.84})\\
&= \mathsf{last}^C(j). && (\text{As } j' = \mathsf{last}^C(j) - 1)
\end{aligned}$$

  The results in this paragraph satisfy all conditions of Definition 6.86 and thus, show that $j \in \mathsf{Sync}$, a contradiction.

□

□

Lemma 6.110. *Let $1 \leq j < num$ be such that $\{j, j+1\} \subseteq \mathsf{Sync}$. Then, we have for $C \in \{A, B\}$ that $\mathsf{corr}^C_j(\mathcal{A}'') = \mathsf{corr}^C_{\mathsf{last}^C(j+1)-1}$.*

Proof. As $j \in \mathsf{Sync}$, we have using item 4 of Lemma 6.94 that $\boldsymbol{\mathcal{S}}^C_j(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j)}.last$ for $C \in \{A, B\}$. Applying item 4 of Lemma 6.85, we get $\boldsymbol{\mathcal{S}}^C_j(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}.last$ for $C \in \{A, B\}$.

Observe from the definition of $\mathsf{boss}(\cdot)$ that $\{j, j+1\} \subseteq \mathsf{Sync}$ implies that $\mathsf{boss}(j) = \{A, B\}$. Thus, by Claim 6.96, we have for all $C \in \{A, B\}$ and $j' \in [P+1]$ that:

$$\mathcal{A}''^{C}_{(j-1)(P+1)+j'}(x^A, x^B) = \mathcal{A}'^{C}_{(\mathsf{last}^C(j+1)-2)(P+1)+j'}(x^A, x^B). \tag{80}$$

Fix an arbitrary $C \in \{A, B\}$ and consider now iteration j in the execution of Π' with $\mathcal{A}''$ and iteration $\mathsf{last}^C(j+1)-1$ in the execution of Π' with $\mathcal{A}'$ from the perspective of party C. As we showed that $j \in \mathfrak{C}^C(\mathcal{A}'', 52)$ in item 1 of Theorem 6.2 and $\mathsf{last}^C(j+1)-1 \in \mathfrak{C}^C(52)$ by Definition 6.84, we have that Line 52 is executed in both the iterations. Furthermore, as $\boldsymbol{\mathcal{S}}^C_j(\mathcal{A}'').last = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}^C(j+1)-1}.last$ for $C \in \{A, B\}$, the value of $\boldsymbol{\mathcal{S}}.last$ is the same before both the iterations, and due to Equation 80, the symbols received by party C are the same in both the iterations. It follows that $\mathsf{corr}^C_j(\mathcal{A}'') = \mathsf{corr}^C_{\mathsf{last}^C(j+1)-1}$, as desired. □

Lemma 6.111. *It holds that:*

$$\sum_{j<num} \mathsf{corr}_j(\mathcal{A}'') \leq 1000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 150 \cdot \sum_{C\in\{A,B\}} \sum_{j\in\mathfrak{C}^C(54)\cup\mathfrak{C}^C(56)} \left(\ell^A_j + \ell^B_j\right).$$

Proof. Note that:

$$\sum_{j<num} \mathsf{corr}_j(\mathcal{A}'') \leq \sum_{\substack{j<num \\ \{j,j+1\}\subseteq\mathsf{Sync}}} \mathsf{corr}_j(\mathcal{A}'') + \sum_{\substack{j<num \\ \{j,j+1\}\not\subseteq\mathsf{Sync}}} \mathsf{corr}_j(\mathcal{A}'').$$

Recall that $\mathsf{corr}_j(\mathcal{A}'') = \mathsf{corr}^A_j(\mathcal{A}'') + \mathsf{corr}^B_j(\mathcal{A}'')$ for all $j \in [R/(P+1)]$. We bound the first term by using Lemma 6.110 to get $\mathsf{corr}_j(\mathcal{A}'') = \mathsf{corr}^A_{\mathsf{last}^A(j+1)-1} + \mathsf{corr}^B_{\mathsf{last}^B(j+1)-1}$. This gives:

$$\begin{aligned}\sum_{j<num} \mathsf{corr}_j(\mathcal{A}'') &\leq \sum_{\substack{j<num \\ \{j,j+1\}\subseteq\mathsf{Sync}}} \sum_{C\in\{A,B\}} \mathsf{corr}^C_{\mathsf{last}^C(j+1)-1} + \sum_{\substack{j<num \\ \{j,j+1\}\not\subseteq\mathsf{Sync}}} \mathsf{corr}_j(\mathcal{A}'') \\ &\leq \sum_{C\in\{A,B\}} \sum_{\substack{j<num \\ \{j,j+1\}\subseteq\mathsf{Sync}}} \mathsf{corr}^C_{\mathsf{last}^C(j+1)-1} + \sum_{\substack{j<num \\ \{j,j+1\}\not\subseteq\mathsf{Sync}}} \mathsf{corr}_j(\mathcal{A}'').\end{aligned}$$

As for $C \in \{A, B\}$, the value of $\mathsf{last}^C(j+1)$ is distinct for all $1 \leq j < |\boldsymbol{\mathcal{S}}^C|$, we get:

$$\begin{aligned}\sum_{j<num} \mathsf{corr}_j(\mathcal{A}'') &\leq \sum_{C\in\{A,B\}} \sum_{j=1}^{R/(P+1)} \mathsf{corr}^C_j + \sum_{\substack{j<num \\ \{j,j+1\}\not\subseteq\mathsf{Sync}}} \mathsf{corr}_j(\mathcal{A}'') \\ &\leq \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + \sum_{\substack{j<num \\ \{j,j+1\}\not\subseteq\mathsf{Sync}}} \mathsf{corr}_j(\mathcal{A}'').\end{aligned}$$

For $1 \leq j < num$ and $C \in \{A, B\}$, we have by definition of corr that[17] $\mathsf{corr}^C_j(\mathcal{A}'') \leq$

[17] $\overline{C}$ denotes the unique element in $\{A, B\}$ that is different from C.

$\max\left(\ell_j^C(\mathcal{A}''), \widetilde{\ell_j^C}(\mathcal{A}'')\right)$. As $j \in \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$ by item 2 of Lemma 6.94, we must have $\mathscr{P}_j^{\overline{C}}(\mathcal{A}'') = \tilde{\mathscr{P}}_j^{\overline{C}}(\mathcal{A}'') \implies \ell_j^{\overline{C}}(\mathcal{A}'') = \widetilde{\ell_j^{\overline{C}}}(\mathcal{A}'')$. Combining with Lemma 6.107, we get $\ell_j^C(\mathcal{A}'') = \widetilde{\ell_j^C}(\mathcal{A}'')$. This implies that $\mathsf{corr}_j^C(\mathcal{A}'') \le \ell_j^C(\mathcal{A}'')$ in turn implying that $\mathsf{corr}_j(\mathcal{A}'') = \mathsf{corr}_j^A(\mathcal{A}'') + \mathsf{corr}_j^B(\mathcal{A}'') \le \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'')$. Plugging in, we get:

$$\begin{aligned}
\sum_{j<num} \mathsf{corr}_j(\mathcal{A}'') &\le \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + \sum_{\substack{j<num \\ \{j,j+1\} \not\subseteq \mathsf{Sync}}} \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') \\
&\le \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + \sum_{\substack{j<num \\ j \notin \mathsf{Sync}}} \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') + \sum_{\substack{j<num \\ j+1 \notin \mathsf{Sync}}} \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') \\
&\le \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + \sum_{\substack{j<num \\ j \notin \mathsf{Sync}}} \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') + \sum_{\substack{1<j\le num \\ j \notin \mathsf{Sync}}} \ell_{j-1}^A(\mathcal{A}'') + \ell_{j-1}^B(\mathcal{A}'').
\end{aligned}$$

Next, note that, for all $1 < j \le num$ and $C \in \{A, B\}$, we have by Line 50 that $\ell_j^C(\mathcal{A}'') \ge p_j^C(\mathcal{A}'')/2 = \boldsymbol{\mathcal{S}}_j^C(\mathcal{A}'').last.p/2$. As $j - 1 \in \mathfrak{E}^A(\mathcal{A}'', 52) \cap \mathfrak{E}^B(\mathcal{A}'', 52)$ by item 2 of Lemma 6.94, we get $\ell_j^C(\mathcal{A}'') \ge \ell_{j-1}^C(\mathcal{A}'')/2$. Plugging in, we get:

$$\begin{aligned}
\sum_{j<num} \mathsf{corr}_j(\mathcal{A}'') &\le \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + \sum_{\substack{j<num \\ j \notin \mathsf{Sync}}} \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') + 2 \cdot \sum_{\substack{1<j\le num \\ j \notin \mathsf{Sync}}} \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') \\
&\le \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 3 \cdot \sum_{j \in [num] \setminus \mathsf{Sync}} \ell_j^A(\mathcal{A}'') + \ell_j^B(\mathcal{A}'') \\
&\le 1000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 150 \cdot \sum_{C \in \{A,B\}} \sum_{j \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)} \left(\ell_j^A + \ell_j^B\right). \\
&\qquad \text{(Lemma 6.108)}
\end{aligned}$$

□

To continue, we define, for $i \in [R/(P+1)+1]$ and $j \in [\min(|\boldsymbol{\mathcal{S}}_i^A|, |\boldsymbol{\mathcal{S}}_i^B|)]$,

$$\mathsf{ok}_i(j) = \mathbb{1}(\mathscr{P}^A_{\mathsf{last}_i^A(j)} = \mathscr{P}^B_{\mathsf{last}_i^B(j)}).$$

Also, define, for $i \in [R/(P+1)+1]$ and $C \in \{A, B\}$,

$$\mathsf{sync}_i = \sum_{j=1}^{\min(|\boldsymbol{\mathcal{S}}_i^A|, |\boldsymbol{\mathcal{S}}_i^B|)-1} \min(\ell^A_{\mathsf{last}_i^A(j+1)-1}, \ell^B_{\mathsf{last}_i^B(j+1)-1}) \cdot \mathsf{ok}_i(j+1).$$

$$\mathsf{total}_i^C = \sum_{j=1}^{|\boldsymbol{\mathcal{S}}_i^C|-1} \ell^C_{\mathsf{last}_i^C(j+1)-1}.$$

$$\zeta_i = 8000 \cdot \sum_{j=1}^{i-1} \mathsf{corr}_j + 9 \cdot \mathsf{sync}_i - 4 \cdot \sum_{C \in \{A,B\}} \mathsf{total}_i^C.$$

When we omit the subscript i in the above definitions, we mean $i = R/(P+1)+1$.

Lemma 6.112. *For $i \in [R/(P+1)]$, and $j \in [\min(|\boldsymbol{\mathcal{S}}_i^A|, |\boldsymbol{\mathcal{S}}_i^B|)] \cap [\min(|\boldsymbol{\mathcal{S}}_{i+1}^A|, |\boldsymbol{\mathcal{S}}_{i+1}^B|)]$, we have $\mathsf{ok}_i(j) = \mathsf{ok}_{i+1}(j)$*

Proof. Direct calculation using item 3 of Lemma 6.85:

$$\mathsf{ok}_i(j) = \mathbb{1}(\mathscr{P}^A_{\mathsf{last}_i^A(j)} = \mathscr{P}^B_{\mathsf{last}_i^B(j)}) = \mathbb{1}(\mathscr{P}^A_{\mathsf{last}_{i+1}^A(j)} = \mathscr{P}^B_{\mathsf{last}_{i+1}^B(j)}) = \mathsf{ok}_{i+1}(j).$$

□

Lemma 6.113. *For $i \in [R/(P+1)+1]$, we have $2 \cdot \mathsf{sync}_i \le \sum_{C \in \{A,B\}} \mathsf{total}_i^C$.*

Proof. We directly derive:

$$\begin{aligned}
2 \cdot \mathsf{sync}_i &\le \sum_{j=1}^{\min(|\boldsymbol{\mathcal{S}}_i^A|,|\boldsymbol{\mathcal{S}}_i^B|)-1} \ell^A_{\mathsf{last}_i^A(j+1)-1} + \sum_{j=1}^{\min(|\boldsymbol{\mathcal{S}}_i^A|,|\boldsymbol{\mathcal{S}}_i^B|)-1} \ell^B_{\mathsf{last}_i^B(j+1)-1} \\
&\le \sum_{j=1}^{|\boldsymbol{\mathcal{S}}_i^A|-1} \ell^A_{\mathsf{last}_i^A(j+1)-1} + \sum_{j=1}^{|\boldsymbol{\mathcal{S}}_i^B|-1} \ell^B_{\mathsf{last}_i^B(j+1)-1} \\
&\le \mathsf{total}_i^A + \mathsf{total}_i^B = \sum_{C \in \{A,B\}} \mathsf{total}_i^C.
\end{aligned}$$

□

Lemma 6.114. *It holds that:*

$$\zeta \ge \frac{S}{20} \qquad \textit{and} \qquad \zeta - \mathsf{sync} \ge \frac{1}{4} \cdot \sum_{C \in \{A,B\}} \sum_{i \in \mathfrak{C}^C(54) \cup \mathfrak{C}^C(56)} \left(\ell_i^A + \ell_i^B\right).$$

We prove this lemma in the next subsection, but first show that item 2 of Theorem 6.2 follows from this lemma.

Proof of item 2 of Theorem 6.2 assuming Lemma 6.114. We have:

$$\begin{aligned}
\sum_{i<num} \ell_i^A(\mathcal{A}'') + \ell_i^B(\mathcal{A}'') &\ge \sum_{i=1}^{\min(|\boldsymbol{\mathcal{S}}^A|,|\boldsymbol{\mathcal{S}}^B|)-1} \ell_i^A(\mathcal{A}'') + \ell_i^B(\mathcal{A}'') \\
&\ge \sum_{i=1}^{\min(|\boldsymbol{\mathcal{S}}^A|,|\boldsymbol{\mathcal{S}}^B|)-1} \min\left(\ell^A_{\mathsf{last}^A(i)}, \ell^B_{\mathsf{last}^B(i)}\right) && \text{(Lemma 6.107)} \\
&\ge \sum_{i=1}^{\min(|\boldsymbol{\mathcal{S}}^A|,|\boldsymbol{\mathcal{S}}^B|)-1} \min\left(\ell^A_{\mathsf{last}^A(i+1)-1}, \ell^B_{\mathsf{last}^B(i+1)-1}\right) \\
& && \text{(Lemma 6.85, item 4)}
\end{aligned}$$

$$\geq \mathsf{sync} \qquad \text{(Definition of } \mathsf{sync}(\cdot)\text{)}$$
$$\geq \frac{\zeta}{9} - 1000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j \qquad \text{(Definition of } \zeta(\cdot)\text{)}$$
$$\geq \frac{S}{180} - 1000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j \qquad \text{(Lemma 6.114)}$$
$$\geq \frac{S}{500}. \qquad \text{(As } \mathsf{corr}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta_2 S\text{)}$$

We also have:

$$\sum_{j<num} \mathsf{corr}_j(\mathcal{A}'') \leq 1000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 150 \cdot \sum_{C\in\{A,B\}} \sum_{j\in\mathfrak{E}^C(54)\cup\mathfrak{E}^C(56)} \left(\ell_j^A + \ell_j^B\right)$$
(Lemma 6.111)
$$\leq 1000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 600 \cdot (\zeta - \mathsf{sync}) \qquad \text{(Lemma 6.114)}$$
$$\leq 1000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 600 \cdot \left(\zeta - 9 \cdot \mathsf{sync} + 4 \cdot \sum_{C\in\{A,B\}} \mathsf{total}^C\right)$$
(Lemma 6.113)
$$\leq 1000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j + 600 \cdot 8000 \cdot \sum_{j=1}^{R/(P+1)} \mathsf{corr}_j \qquad \text{(Definition of } \zeta(\cdot)\text{)}$$
$$\leq 10^7 \theta_2 S. \qquad \text{(As } \mathsf{corr}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta_2 S\text{)}$$

□

6.3.2 Proof of Lemma 6.114

We start with the following technical lemma.

Lemma 6.115. *Let $C \in \{A, B\}$ and $i \in [R/(P+1)+1]$. For all $1 \leq j < |\boldsymbol{\mathcal{S}}_i^C|$, we have*

$$\ell^C_{\mathsf{last}_i^C(j+1)-1} = \ell^C_{\mathsf{last}_i^C(j)} \leq 2\ell^C_{\mathsf{last}_i^C(j+1)} \leq 2.2 \cdot \ell^C_{\mathsf{last}_i^C(j+1)-1}.$$

Proof. The equality follows directly from item 4 of Lemma 6.85 and the fact that $\boldsymbol{\mathcal{S}}$ determines ℓ. Next, we have by Definition 6.84 that $\mathsf{last}_i^C(j+1) - 1 \in \mathfrak{E}^C(52)$ implying that $p^C_{\mathsf{last}_i^C(j+1)} = \boldsymbol{\mathcal{S}}^C_{\mathsf{last}_i^C(j+1)}.last.p = \ell^C_{\mathsf{last}_i^C(j+1)-1}$.

Now for the first inequality, note by Line 50 that $2\ell^C_{\mathsf{last}_i^C(j+1)} \geq p^C_{\mathsf{last}_i^C(j+1)} = \ell^C_{\mathsf{last}_i^C(j+1)-1}$, while for the second inequality, note that $\mathsf{last}_i^C(j+1) - 1 \in \mathfrak{E}^C(52)$ implies $|\mathscr{R}^C_{\mathsf{last}_i^C(j+1)}| \leq$

$|\mathscr{R}^C_{\mathsf{last}^C_i(j+1)-1}| + 1$ giving

$$\begin{aligned}\ell^C_{\mathsf{last}^C_i(j+1)} &= \max\left(500KP \cdot 1.1^{|\mathscr{R}^C_{\mathsf{last}^C_i(j+1)}|}, p^C_{\mathsf{last}^C_i(j+1)}\right) \\ &\leq 1.1 \cdot \max\left(500KP \cdot 1.1^{|\mathscr{R}^C_{\mathsf{last}^C_i(j+1)-1}|}, p^C_{\mathsf{last}^C_i(j+1)}\right) \leq 1.1 \cdot \ell^C_{\mathsf{last}^C_i(j+1)-1}.\end{aligned}$$

□

Corollary 6.116. *For $C \in \{A, B\}$ and $i \in [R/(P+1)+1]$ such that $|\boldsymbol{\mathcal{S}}^C_i| > 1$, we have $\frac{10}{11} \cdot \ell^C_i \leq \ell^C_{\mathsf{last}^C_i(|\boldsymbol{\mathcal{S}}^C_i|)-1} \leq 2 \cdot \ell^C_i$.*

Proof. By Lemma 6.115, we have that $\ell^C_{\mathsf{last}^C_i(|\boldsymbol{\mathcal{S}}^C_i|)} \leq 1.1 \cdot \ell^C_{\mathsf{last}^C_i(|\boldsymbol{\mathcal{S}}^C_i|)-1} \leq 2.2 \cdot \ell^C_{\mathsf{last}^C_i(|\boldsymbol{\mathcal{S}}^C_i|)}$ and by item 5 of Lemma 6.85 and the fact that $\boldsymbol{\mathcal{S}}.last$ determines ℓ, we have that $\ell^C_i = \ell^C_{\mathsf{last}^C_i(|\boldsymbol{\mathcal{S}}^C_i|)}$. □

We now analyze the quantities sync and total, dedicating a lemma for each one of them.

Lemma 6.117. *Let $i \in [R/(P+1)]$.*

1. *If $\mathsf{corr}_i = 0$ and $i \in \mathfrak{E}^A(52) \cap \mathfrak{E}^B(52)$, then*
$$\mathsf{sync}_{i+1} - \mathsf{sync}_i \geq \frac{1}{2}(\ell^A_i + \ell^B_i).$$
2. *If $\min(|\boldsymbol{\mathcal{S}}^A_{i+1}|, |\boldsymbol{\mathcal{S}}^B_{i+1}|) \geq \min(|\boldsymbol{\mathcal{S}}^A_i|, |\boldsymbol{\mathcal{S}}^B_i|)$, we have $\mathsf{sync}_{i+1} \geq \mathsf{sync}_i$.*
3. *If $\min(|\boldsymbol{\mathcal{S}}^A_{i+1}|, |\boldsymbol{\mathcal{S}}^B_{i+1}|) + 1 \geq |\boldsymbol{\mathcal{S}}^A_i| = |\boldsymbol{\mathcal{S}}^B_i|$ and $\mathscr{P}^A_i \neq \mathscr{P}^B_i$, then $\mathsf{sync}_{i+1} \geq \mathsf{sync}_i$.*
4. *If $|\boldsymbol{\mathcal{S}}^B_i| < |\boldsymbol{\mathcal{S}}^A_i|$ and $|\boldsymbol{\mathcal{S}}^B_i| - 1 = |\boldsymbol{\mathcal{S}}^B_{i+1}| \leq |\boldsymbol{\mathcal{S}}^A_{i+1}|$, we have*
$$\mathsf{sync}_{i+1} - \mathsf{sync}_i \geq -\min\left(2 \cdot \ell^B_i, \frac{2}{3} \cdot \ell^A_{\mathsf{last}^A_i(|\boldsymbol{\mathcal{S}}^B_i|)-1} + \frac{1}{3} \cdot \ell^B_{\mathsf{last}^B_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}\right).$$
An analogous claim holds with the roles of Alice and Bob reversed.
5. *It holds that:*
$$\mathsf{sync}_{i+1} - \mathsf{sync}_i \geq -22 \cdot \left(\ell^A_i + \ell^B_i + \mathsf{corr}_i\right).$$

Proof. To start, using the notation $z = \min(|\boldsymbol{\mathcal{S}}^A_i|, |\boldsymbol{\mathcal{S}}^B_i|, |\boldsymbol{\mathcal{S}}^A_{i+1}|, |\boldsymbol{\mathcal{S}}^B_{i+1}|)$, we claim that

$$\begin{aligned}&\sum_{j=1}^{z-1} \min(\ell^A_{\mathsf{last}^A_i(j+1)-1}, \ell^B_{\mathsf{last}^B_i(j+1)-1}) \cdot \mathsf{ok}_i(j+1) \\ &\qquad = \sum_{j=1}^{z-1} \min(\ell^A_{\mathsf{last}^A_{i+1}(j+1)-1}, \ell^B_{\mathsf{last}^B_{i+1}(j+1)-1}) \cdot \mathsf{ok}_{i+1}(j+1).\end{aligned} \tag{81}$$

Indeed, we have:

$$\begin{aligned}
&\sum_{j=1}^{z-1} \min(\ell^A_{\mathsf{last}_i^A(j+1)-1}, \ell^B_{\mathsf{last}_i^B(j+1)-1}) \cdot \mathsf{ok}_i(j+1) \\
&\qquad = \sum_{j=1}^{z-1} \min(\ell^A_{\mathsf{last}_i^A(j+1)-1}, \ell^B_{\mathsf{last}_i^B(j+1)-1}) \cdot \mathsf{ok}_{i+1}(j+1) && \text{(Lemma 6.112)} \\
&\qquad = \sum_{j=1}^{z-1} \min(\ell^A_{\mathsf{last}_{i+1}^A(j+1)-1}, \ell^B_{\mathsf{last}_{i+1}^B(j+1)-1}) \cdot \mathsf{ok}_{i+1}(j+1). && \text{(Lemma 6.85, item 3)}
\end{aligned}$$

We now prove each part in turn using Equation 81 in each part.

1. As $\mathsf{corr}_i = 0$ and $i \in \mathfrak{E}^A(52) \cap \mathfrak{E}^B(52)$, we have $\Gamma_i^A = \tilde{\Gamma}_i^B$, $\tilde{\Gamma}_i^A = \Gamma_i^B$ and
$$(\tilde{\mathscr{P}}_i^A, |\tilde{\boldsymbol{\mathcal{S}}}_i^A|) = (\mathscr{P}_i^B, |\boldsymbol{\mathcal{S}}_i^B|) = (\tilde{\mathscr{P}}_i^B, |\tilde{\boldsymbol{\mathcal{S}}}_i^B|) = (\mathscr{P}_i^A, |\boldsymbol{\mathcal{S}}_i^A|).$$
We use $(\mathscr{P}^*, |\boldsymbol{\mathcal{S}}^*|)$ to denote the common value of the quantities above. Observe from Algorithm 6 that the equations above imply that $(\mathscr{P}_{i+1}^A, |\boldsymbol{\mathcal{S}}_{i+1}^A|) = (\mathscr{P}_{i+1}^B, |\boldsymbol{\mathcal{S}}_{i+1}^B|)$ and $|\boldsymbol{\mathcal{S}}_{i+1}^C| = |\boldsymbol{\mathcal{S}}^*| + 1$ for $C \in \{A, B\}$.
Using Definition 6.84, we additionally have $\mathsf{last}_{i+1}^C(|\boldsymbol{\mathcal{S}}^*| + 1) = i + 1$ for $C \in \{A, B\}$. This gives $\mathsf{ok}_{i+1}(|\boldsymbol{\mathcal{S}}^*|+1) = \mathbb{1}(\mathscr{P}^A_{\mathsf{last}_{i+1}^A(|\boldsymbol{\mathcal{S}}^*|+1)} = \mathscr{P}^B_{\mathsf{last}_{i+1}^B(|\boldsymbol{\mathcal{S}}^*|+1)}) = \mathbb{1}(\mathscr{P}_{i+1}^A = \mathscr{P}_{i+1}^B) = 1$ and therefore:
$$\begin{aligned}
\mathsf{sync}_{i+1} - \mathsf{sync}_i &= \min(\ell^A_{\mathsf{last}_{i+1}^A(|\boldsymbol{\mathcal{S}}^*|+1)-1}, \ell^B_{\mathsf{last}_{i+1}^B(|\boldsymbol{\mathcal{S}}^*|+1)-1}) \cdot \mathsf{ok}_{i+1}(|\boldsymbol{\mathcal{S}}^*| + 1) \\
&\qquad \text{(Equation 81 as } |\boldsymbol{\mathcal{S}}_{i+1}^C| = |\boldsymbol{\mathcal{S}}^*| + 1 \text{ for } C \in \{A, B\}) \\
&= \min(\ell^A_{\mathsf{last}_{i+1}^A(|\boldsymbol{\mathcal{S}}^*|+1)-1}, \ell^B_{\mathsf{last}_{i+1}^B(|\boldsymbol{\mathcal{S}}^*|+1)-1}) \qquad \text{(As } \mathsf{ok}_{i+1}(|\boldsymbol{\mathcal{S}}^*| + 1) = 1) \\
&= \min(\ell_i^A, \ell_i^B) \qquad \text{(As } \mathsf{last}_{i+1}^C(|\boldsymbol{\mathcal{S}}^*| + 1) = i + 1 \text{ for } C \in \{A, B\}) \\
&= \frac{1}{2}(\ell_i^A + \ell_i^B). \qquad \text{(As } \mathscr{P}_i^A = \mathscr{P}_i^B)
\end{aligned}$$

2. This part is straightforward from Equation 81 as ℓ is always non-negative.

3. If $\min(|\boldsymbol{\mathcal{S}}_{i+1}^A|, |\boldsymbol{\mathcal{S}}_{i+1}^B|) \geq |\boldsymbol{\mathcal{S}}_i^A| = |\boldsymbol{\mathcal{S}}_i^B|$, we are done by item 2. Thus, we assume that $\min(|\boldsymbol{\mathcal{S}}_{i+1}^A|, |\boldsymbol{\mathcal{S}}_{i+1}^B|) + 1 = |\boldsymbol{\mathcal{S}}_i^A| = |\boldsymbol{\mathcal{S}}_i^B|$. Let $C \in \{A, B\}$ be the minimizer of $|\boldsymbol{\mathcal{S}}_{i+1}^C|$ (breaking ties arbitrarily). We have from Equation 81 that
$$\mathsf{sync}_{i+1} - \mathsf{sync}_i = -\min(\ell^A_{\mathsf{last}_i^A(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)-1}, \ell^B_{\mathsf{last}_i^B(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)-1}) \cdot \mathsf{ok}_i(|\boldsymbol{\mathcal{S}}_{i+1}^C| + 1),$$
and it is sufficient to show that $\mathsf{ok}_i(|\boldsymbol{\mathcal{S}}_{i+1}^C| + 1) = 0$. By definition, we have $\mathsf{ok}_i(|\boldsymbol{\mathcal{S}}_{i+1}^C| + 1) = \mathbb{1}(\mathscr{P}^A_{\mathsf{last}_i^A(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)} = \mathscr{P}^B_{\mathsf{last}_i^B(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)})$. As $|\boldsymbol{\mathcal{S}}_{i+1}^C| + 1 = |\boldsymbol{\mathcal{S}}_i^A| = |\boldsymbol{\mathcal{S}}_i^B|$, we get $\mathsf{ok}_i(|\boldsymbol{\mathcal{S}}_{i+1}^C| + 1) = \mathbb{1}(\mathscr{P}^A_{\mathsf{last}_i^A(|\boldsymbol{\mathcal{S}}_i^A|)} = \mathscr{P}^B_{\mathsf{last}_i^B(|\boldsymbol{\mathcal{S}}_i^B|)})$. By item 5 of Lemma 6.85 and the fact that $\boldsymbol{\mathcal{S}}.\mathit{last}$ determined $\mathscr{P}$, we get that $\mathsf{ok}_i(|\boldsymbol{\mathcal{S}}_{i+1}^C| + 1) = \mathbb{1}(\mathscr{P}_i^A = \mathscr{P}_i^B) = 0$, as $\mathscr{P}_i^A \neq \mathscr{P}_i^B$ finishing the proof.

4. We have from Equation 81 that:

$$\begin{aligned}\mathsf{sync}_{i+1} - \mathsf{sync}_i &= -\min(\ell^A_{\mathsf{last}^A_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}, \ell^B_{\mathsf{last}^B_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}) \cdot \mathsf{ok}_i(|\boldsymbol{\mathcal{S}}^B_i|) \\ &\geq -\min(\ell^A_{\mathsf{last}^A_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}, \ell^B_{\mathsf{last}^B_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}).\end{aligned}$$

Now, note that $\min(\ell^A_{\mathsf{last}^A_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}, \ell^B_{\mathsf{last}^B_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}) \leq \ell^B_{\mathsf{last}^B_i(|\boldsymbol{\mathcal{S}}^B_i|)-1} \leq 2 \cdot \ell^B_i$ by Corollary 6.116. Also, note that $\min(\ell^A_{\mathsf{last}^A_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}, \ell^B_{\mathsf{last}^B_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}) \leq \frac{2}{3} \cdot \ell^A_{\mathsf{last}^A_i(|\boldsymbol{\mathcal{S}}^B_i|)-1} + \frac{1}{3} \cdot \ell^B_{\mathsf{last}^B_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}$ as the minmum is at most a weighted average. Combining, we get:

$$\mathsf{sync}_{i+1} - \mathsf{sync}_i \geq -\min\left(2 \cdot \ell^B_i, \frac{2}{3} \cdot \ell^A_{\mathsf{last}^A_i(|\boldsymbol{\mathcal{S}}^B_i|)-1} + \frac{1}{3} \cdot \ell^B_{\mathsf{last}^B_i(|\boldsymbol{\mathcal{S}}^B_i|)-1}\right).$$

5. Due to item 2, it is sufficient to consider the case $\min(|\boldsymbol{\mathcal{S}}^A_{i+1}|, |\boldsymbol{\mathcal{S}}^B_{i+1}|) < \min(|\boldsymbol{\mathcal{S}}^A_i|, |\boldsymbol{\mathcal{S}}^B_i|)$. We have due to Equation 81 that:

$$\mathsf{sync}_{i+1} - \mathsf{sync}_i = -\sum_{j=\min(|\boldsymbol{\mathcal{S}}^A_{i+1}|,|\boldsymbol{\mathcal{S}}^B_{i+1}|)}^{\min(|\boldsymbol{\mathcal{S}}^A_i|,|\boldsymbol{\mathcal{S}}^B_i|)-1} \min(\ell^A_{\mathsf{last}^A_i(j+1)-1}, \ell^B_{\mathsf{last}^B_i(j+1)-1}) \cdot \mathsf{ok}_i(j+1).$$

Let $C \in \{A, B\}$ be the minimizer of $|\boldsymbol{\mathcal{S}}^C_{i+1}|$ (breaking ties arbitrarily). As $|\boldsymbol{\mathcal{S}}^C_{i+1}| = \min(|\boldsymbol{\mathcal{S}}^A_{i+1}|, |\boldsymbol{\mathcal{S}}^B_{i+1}|) < \min(|\boldsymbol{\mathcal{S}}^A_i|, |\boldsymbol{\mathcal{S}}^B_i|) \leq |\boldsymbol{\mathcal{S}}^C_i|$, we must have $i \in \mathfrak{E}^C(54) \cup \mathfrak{E}^C(56)$. We get that:

$$\begin{aligned}\mathsf{sync}_{i+1} - \mathsf{sync}_i &= -\sum_{j=\min(|\boldsymbol{\mathcal{S}}^A_{i+1}|,|\boldsymbol{\mathcal{S}}^B_{i+1}|)}^{\min(|\boldsymbol{\mathcal{S}}^A_i|,|\boldsymbol{\mathcal{S}}^B_i|)-1} \min(\ell^A_{\mathsf{last}^A_i(j+1)-1}, \ell^B_{\mathsf{last}^B_i(j+1)-1}) \cdot \mathsf{ok}_i(j+1) \\ &\geq -\sum_{j=|\boldsymbol{\mathcal{S}}^C_{i+1}|}^{|\boldsymbol{\mathcal{S}}^C_i|-1} \min(\ell^A_{\mathsf{last}^A_i(j+1)-1}, \ell^B_{\mathsf{last}^B_i(j+1)-1}) \cdot \mathsf{ok}_i(j+1) \\ &\qquad \text{(As } |\boldsymbol{\mathcal{S}}^C_{i+1}| = \min(|\boldsymbol{\mathcal{S}}^A_{i+1}|, |\boldsymbol{\mathcal{S}}^B_{i+1}|) < \min(|\boldsymbol{\mathcal{S}}^A_i|, |\boldsymbol{\mathcal{S}}^B_i|) \leq |\boldsymbol{\mathcal{S}}^C_i|) \\ &\geq -\sum_{j=|\boldsymbol{\mathcal{S}}^C_{i+1}|}^{|\boldsymbol{\mathcal{S}}^C_i|-1} \ell^C_{\mathsf{last}^C_i(j+1)-1} \\ &\geq -22 \cdot \left(\ell^A_i + \ell^B_i + \mathsf{corr}_i\right). \qquad \text{(Lemma 6.104)}\end{aligned}$$

□

Lemma 6.118. *Let $C \in \{A, B\}$ and $i \in [R/(P+1)]$.*

1. *If $|\boldsymbol{\mathcal{S}}^C_i| < |\boldsymbol{\mathcal{S}}^C_{i+1}|$, then $\mathsf{total}^C_i - \mathsf{total}^C_{i+1} \geq -\ell^C_i$.*
2. *If $|\boldsymbol{\mathcal{S}}^C_i| = |\boldsymbol{\mathcal{S}}^C_{i+1}|$, then $\mathsf{total}^C_i - \mathsf{total}^C_{i+1} = 0$.*
3. *If $|\boldsymbol{\mathcal{S}}^C_i| > |\boldsymbol{\mathcal{S}}^C_{i+1}|$, then $\mathsf{total}^C_i - \mathsf{total}^C_{i+1} \geq \ell^C_{\mathsf{last}^C_i(|\boldsymbol{\mathcal{S}}^C_i|)-1} \geq \frac{10}{11} \cdot \ell^C_i$.*

4. *If* $i \in \mathfrak{E}^C(56)$ *and* $\mu_i^C \le |\boldsymbol{\mathcal{S}}_i^C| - |\tilde{\boldsymbol{\mathcal{S}}}_i^C| + \mathbb{1}(10\ell_i^C < \tilde{\ell}_i^C)$, *then*

$$\mathsf{total}_i^C - \mathsf{total}_{i+1}^C \ge 10\left(\ell_i^C + \tilde{\ell}_i^C\right).$$

5. *If* $i \in \mathfrak{E}^C(56)$ *and* $10\ell_i^C < \tilde{\ell}_i^C$ *and* $\mu_i^C > |\boldsymbol{\mathcal{S}}_i^C| - |\tilde{\boldsymbol{\mathcal{S}}}_i^C| + 1$, *then*

$$\mathsf{total}_i^C - \mathsf{total}_{i+1}^C \ge \frac{3}{2} \cdot \ell^C_{\mathsf{last}_i^C(|\tilde{\boldsymbol{\mathcal{S}}}_i^C|)-1}.$$

Proof. Note by item 3 of Lemma 6.85 that

$$\sum_{j=1}^{\min(|\boldsymbol{\mathcal{S}}_i^C|,|\boldsymbol{\mathcal{S}}_{i+1}^C|)-1} \ell^C_{\mathsf{last}_i^C(j+1)-1} = \sum_{j=1}^{\min(|\boldsymbol{\mathcal{S}}_i^C|,|\boldsymbol{\mathcal{S}}_{i+1}^C|)-1} \ell^C_{\mathsf{last}_{i+1}^C(j+1)-1}. \tag{82}$$

We prove each part separately using Equation 82 in each part.

1. As $|\boldsymbol{\mathcal{S}}_i^C| < |\boldsymbol{\mathcal{S}}_{i+1}^C|$, we must have $i \in \mathfrak{E}^C(52)$ implying $|\boldsymbol{\mathcal{S}}_i^C| + 1 = |\boldsymbol{\mathcal{S}}_{i+1}^C|$ and $\mathsf{last}_{i+1}^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|) = i+1$ by Definition 6.84. From Equation 82, we get that $\mathsf{total}_i^C - \mathsf{total}_{i+1}^C = -\ell^C_{\mathsf{last}_{i+1}^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|)-1} = -\ell_i^C$.

2. Straightforward from Equation 82.

3. As $|\boldsymbol{\mathcal{S}}_i^C| > |\boldsymbol{\mathcal{S}}_{i+1}^C|$, we have from Equation 82 that $\mathsf{total}_i^C - \mathsf{total}_{i+1}^C \ge \ell^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_i^C|)-1}$. Corollary 6.116 finishes the proof.

4. Firstly, note that $\mu_i^C \le |\boldsymbol{\mathcal{S}}_i^C| - |\tilde{\boldsymbol{\mathcal{S}}}_i^C| + \mathbb{1}(10\ell_i^C < \tilde{\ell}_i^C)$ implies $\mu_i^C \le |\boldsymbol{\mathcal{S}}_i^C|$ as $|\tilde{\boldsymbol{\mathcal{S}}}_i^C| \ge 1$. We get:

$$\begin{aligned}
\mathsf{total}_i^C - \mathsf{total}_{i+1}^C &\ge \sum_{j=|\boldsymbol{\mathcal{S}}_{i+1}^C|}^{|\boldsymbol{\mathcal{S}}_i^C|-1} \ell^C_{\mathsf{last}_i^C(j+1)-1} \\
&\qquad \text{(Equation 82 as } i \in \mathfrak{E}^C(56) \implies |\boldsymbol{\mathcal{S}}_i^C| > |\boldsymbol{\mathcal{S}}_{i+1}^C|) \\
&\ge \sum_{j=|\boldsymbol{\mathcal{S}}_{i+1}^C|+1}^{|\boldsymbol{\mathcal{S}}_i^C|} \boldsymbol{\mathcal{S}}_i^C[j].p \qquad \text{(Lemma 6.104)} \\
&\ge \sum_{j=|\boldsymbol{\mathcal{S}}_i^C|-\mu_i^C+1}^{|\boldsymbol{\mathcal{S}}_i^C|} \boldsymbol{\mathcal{S}}_i^C[j].p \\
&\qquad \text{(Line 56 as } \mu_i^C \le |\boldsymbol{\mathcal{S}}_i^C| - |\tilde{\boldsymbol{\mathcal{S}}}_i^C| + \mathbb{1}(10\ell_i^C < \tilde{\ell}_i^C)) \\
&\ge \sum_{j=1}^{\mu_i^C} \boldsymbol{\mathcal{S}}_i^C[|\boldsymbol{\mathcal{S}}_i^C| + 1 - j].p \\
&\ge 10\left(\ell_i^C + \tilde{\ell}_i^C\right). \qquad \text{(Line 56 as } \mu_i^C \le |\boldsymbol{\mathcal{S}}_i^C|)
\end{aligned}$$

5. As $10\ell_i^C < \tilde{\ell}_i^C$ and $\mu_i^C > |\boldsymbol{\mathcal{S}}_i^C| - |\tilde{\boldsymbol{\mathcal{S}}}_i^C| + 1$, we have by Line 56 that $|\boldsymbol{\mathcal{S}}_i^C| - |\boldsymbol{\mathcal{S}}_{i+1}^C| = |\boldsymbol{\mathcal{S}}_i^C| - |\tilde{\boldsymbol{\mathcal{S}}}_i^C| + 1 \geq 2$. It follows that $|\boldsymbol{\mathcal{S}}_{i+1}^C| = |\tilde{\boldsymbol{\mathcal{S}}}_i^C| - 1$ and $|\boldsymbol{\mathcal{S}}_i^C| \geq |\boldsymbol{\mathcal{S}}_{i+1}^C| + 2$. We get from Equation 82 that:

$$\begin{aligned}
\mathsf{total}_i^C - \mathsf{total}_{i+1}^C &\geq \ell^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)-1} + \ell^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|+2)-1} \\
&\geq \ell^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)-1} + \ell^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)} && \text{(Lemma 6.85, item 4)} \\
&\geq \ell^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)-1} + \frac{1}{2}\cdot \ell^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|)} && \text{(Lemma 6.115)} \\
&\geq \frac{3}{2}\cdot \ell^C_{\mathsf{last}_i^C(|\boldsymbol{\mathcal{S}}_{i+1}^C|+1)-1} && \text{(Lemma 6.85, item 4)} \\
&\geq \frac{3}{2}\cdot \ell^C_{\mathsf{last}_i^C(|\tilde{\boldsymbol{\mathcal{S}}}_i^C|)-1}. && \text{(As } |\boldsymbol{\mathcal{S}}_{i+1}^C| = |\tilde{\boldsymbol{\mathcal{S}}}_i^C| - 1)
\end{aligned}$$

□

We are now ready to prove Lemma 6.114.

Proof of Lemma 6.114. To show Lemma 6.114, we show by induction that, for all $j \in [R/(P+1)+1]$, we have

$$\zeta_j \geq \frac{1}{4}\cdot\sum_{i=1}^{j-1}\left(\ell_i^A + \ell_i^B\right) \quad \text{and} \quad \zeta_j - \mathsf{sync}_j \geq \frac{1}{4}\cdot\sum_{C\in\{A,B\}}\sum_{\substack{i\in\mathfrak{E}^C(54)\cup\mathfrak{E}^C(56)\\ i<j}}\left(\ell_i^A + \ell_i^B\right). \tag{83}$$

Then, by plugging $j = R/(P+1)+1$, we get $\zeta - \mathsf{sync} \geq \frac{1}{4}\cdot\sum_{C\in\{A,B\}}\sum_{i\in\mathfrak{E}^C(54)\cup\mathfrak{E}^C(56)}\left(\ell_i^A + \ell_i^B\right)$ and $\zeta \geq \frac{1}{4}\cdot\sum_{i=1}^{R/(P+1)}\left(\ell_i^A + \ell_i^B\right)$. Lemma 6.114 then follows as either the parties never send a string of $\perp$s in Line 50, in which case we have $\sum_{i=1}^{R/(P+1)}\left(\ell_i^A + \ell_i^B\right) \geq 250RK \geq S$ by our choice of parameters, or one of them aborts after communicating S symbols. In this case, as S symbols have been communicated by one of the parties, say C, we again get $\sum_{i=1}^{R/(P+1)}\left(\ell_i^A + \ell_i^B\right) \geq \sum_{i=1}^{R/(P+1)}\left(\ell_i^C + \tilde{\ell}_i^C - \mathsf{corr}_i\right) \geq 0.9S$ as $\mathsf{corr}_{\mathrm{L},\Pi',\mathcal{A}'}(x^A, x^B) \leq \theta_2 S$.

Now, we focus on showing Equation 83. The base case $j = 1$ holds because all quantities are 0. To show the induction step, it is sufficient to show that, for $j \in [R/(P+1)]$, we have:

$$\zeta_{j+1} - \zeta_j \geq \frac{1}{4}\cdot\left(\ell_j^A + \ell_j^B\right) \tag{84}$$

$$\left(\zeta_{j+1} - \mathsf{sync}_{j+1}\right) - \left(\zeta_j - \mathsf{sync}_j\right) \geq \frac{1}{4}\cdot\sum_{C\in\{A,B\}}\left(\ell_j^A + \ell_j^B\right)\cdot\mathbb{1}\left(j\in\mathfrak{E}^C(54)\cup\mathfrak{E}^C(56)\right). \tag{85}$$

We now break the proof into several cases.

- $\boldsymbol{\mathsf{corr}_j < \frac{1}{15}\cdot\left(\ell_j^A + \ell_j^B\right)}$**:** In this case, we start by showing that:

  Claim 6.119. *If* $\mathsf{corr}_j^A > 0$*, we have* $10\cdot\max(\ell_j^A, \tilde{\ell}_j^B) < \ell_j^B$*. An analogous result holds for Bob. It follows that* $\mathsf{corr}_j^A > 0 \implies \mathsf{corr}_j^B = 0$.

Proof. We have by definition of corr that:

$$\max\left(\ell_j^A, \tilde{\ell}_j^B\right) \leq \mathsf{corr}_j^A < \frac{1}{15} \cdot \left(\ell_j^A + \ell_j^B\right) \leq \frac{1}{15} \cdot \left(\max\left(\ell_j^A, \tilde{\ell}_j^B\right) + \ell_j^B\right).$$

Rearranging gives the result. □

We have the following subcases:

– $\boldsymbol{|\mathcal{S}_j^A| = |\mathcal{S}_j^B|}$**:** We further subdivide this case:

∗ $\boldsymbol{\mathscr{P}_j^A = \mathscr{P}_j^B}$**:** As $\mathscr{P}_j^A = \mathscr{P}_j^B$, we have that $\ell_j^A = \ell_j^B \implies \mathsf{corr}_j = 0$ by the contrapositive of Claim 6.119. As $\mathsf{corr}_j = 0$, we have

$$(\tilde{\mathscr{P}}_j^B, |\tilde{\mathcal{S}}_j^B|) = (\mathscr{P}_j^A, |\mathcal{S}_j^A|) = (\mathscr{P}_j^B, |\mathcal{S}_j^B|) = (\tilde{\mathscr{P}}_j^A, |\tilde{\mathcal{S}}_j^A|).$$

It follows that $j \in \mathfrak{E}^A(52) \cap \mathfrak{E}^B(52)$. We conclude using item 1 of Lemma 6.117 that $\mathsf{sync}_{j+1} - \mathsf{sync}_j \geq \frac{1}{2}(\ell_j^A + \ell_j^B)$. Also, by applying item 1 in Lemma 6.118 on A and B, we get that $\sum_{C\in\{A,B\}} \mathsf{total}_j^C - \sum_{C\in\{A,B\}} \mathsf{total}_{j+1}^C \geq -(\ell_j^A + \ell_j^B)$. Combining, we have:

$$\zeta_{j+1} - \zeta_j \geq \frac{9}{2} \cdot (\ell_j^A + \ell_j^B) - 4 \cdot (\ell_j^A + \ell_j^B) \geq \frac{1}{2}(\ell_j^A + \ell_j^B),$$

$$\left(\zeta_{j+1} - \mathsf{sync}_{j+1}\right) - \left(\zeta_j - \mathsf{sync}_j\right) \geq 4(\ell_j^A + \ell_j^B) - 4(\ell_j^A + \ell_j^B) \geq 0,$$

and Equation 84 and Equation 85 follow as $j \in \mathfrak{E}^A(52) \cap \mathfrak{E}^B(52)$.

∗ $\boldsymbol{\mathscr{P}_j^A \neq \mathscr{P}_j^B}$**:** We first claim that $j \in \mathfrak{E}^A(54) \cap \mathfrak{E}^B(54)$. If $\mathsf{corr}_j = 0$, this holds because we have $|\tilde{\mathcal{S}}_j^B| = |\mathcal{S}_j^A| = |\mathcal{S}_j^B| = |\tilde{\mathcal{S}}_j^A|$ and $\tilde{\mathscr{P}}_j^B = \mathscr{P}_j^A \neq \mathscr{P}_j^B = \tilde{\mathscr{P}}_j^A$. Otherwise, there exists $C \in \{A, B\}$ such that $\mathsf{corr}_j^C > 0$. Assume without loss of generality that $C = A$. By Claim 6.119, we have that $10 \cdot \max(\ell_j^A, \tilde{\ell}_j^B) < \ell_j^B$ and $\mathsf{corr}_j^B = 0$. The former implies that $\tilde{\mathscr{P}}_j^B \neq \mathscr{P}_j^B$ and $10 \cdot \tilde{\ell}_j^B < \ell_j^B$ implying in turn that $j \in \mathfrak{E}^B(54)$ while the latter implies that $|\mathcal{S}_j^A| = |\mathcal{S}_j^B| = |\tilde{\mathcal{S}}_j^A|$ and $\mathscr{P}_j^A \neq \mathscr{P}_j^B = \tilde{\mathscr{P}}_j^A$ implying that $j \in \mathfrak{E}^A(54)$. Overall, we get that $j \in \mathfrak{E}^A(54) \cap \mathfrak{E}^B(54)$.
It follows that $|\mathcal{S}_{j+1}^A| = |\mathcal{S}_{j+1}^B| = |\mathcal{S}_j^A| - 1 = |\mathcal{S}_j^B| - 1$. By item 3 of Lemma 6.117, this gives $\mathsf{sync}_{j+1} \geq \mathsf{sync}_j$ while by item 3 of Lemma 6.118 on A and B, we get that $\sum_{C\in\{A,B\}} \mathsf{total}_j^C - \sum_{C\in\{A,B\}} \mathsf{total}_{j+1}^C \geq \frac{10}{11}(\ell_j^A + \ell_j^B)$. Combining, we get:

$$\zeta_{j+1} - \zeta_j \geq \frac{40}{11} \cdot (\ell_j^A + \ell_j^B),$$

$$\left(\zeta_{j+1} - \mathsf{sync}_{j+1}\right) - \left(\zeta_j - \mathsf{sync}_j\right) \geq \frac{40}{11} \cdot (\ell_j^A + \ell_j^B),$$

and Equation 84 and Equation 85 follow.

– $\boldsymbol{|\mathcal{S}_j^A| > |\mathcal{S}_j^B|}$**:** We further subdivide this case.

* $\mathbf{10 \cdot \ell_j^A \geq \ell_j^B}$**:** By the contrapositive of Claim 6.119, we have that $\mathsf{corr}_j^A = 0$. It follows that $\ell_j^A = \tilde{\ell}_j^B \implies 10 \cdot \tilde{\ell}_j^B \geq \ell_j^B$ and $|\tilde{\boldsymbol{\mathcal{S}}}_j^B| = |\boldsymbol{\mathcal{S}}_j^A| > |\boldsymbol{\mathcal{S}}_j^B|$ implying that $j \in \overline{\mathfrak{E}^B(52)} \cap \overline{\mathfrak{E}^B(54)} \cap \overline{\mathfrak{E}^B(56)}$. In turn, this means that $|\boldsymbol{\mathcal{S}}_j^B| = |\boldsymbol{\mathcal{S}}_{j+1}^B|$.

Claim 6.120. $|\boldsymbol{\mathcal{S}}_{j+1}^B| \leq |\boldsymbol{\mathcal{S}}_{j+1}^A| < |\boldsymbol{\mathcal{S}}_j^A|$.

Proof. If $10 \cdot \tilde{\ell}_j^A < \ell_j^A$, we must have $\ell_j^A \neq \tilde{\ell}_j^A$ implying that $\tilde{\mathscr{P}}_j^A \neq \mathscr{P}_j^A$. Together, these mean that $j \in \mathfrak{E}^A(54)$ from which we get that $|\boldsymbol{\mathcal{S}}_{j+1}^A| = |\boldsymbol{\mathcal{S}}_j^A| - 1$ and the claim follows.
On the other hand, if $10 \cdot \tilde{\ell}_j^A \geq \ell_j^A$, we have by the contrapositive of Claim 6.119 that $\mathsf{corr}_j^B = 0$, implying that $\ell_j^B = \tilde{\ell}_j^A$ and $|\boldsymbol{\mathcal{S}}_j^A| > |\boldsymbol{\mathcal{S}}_j^B| = |\tilde{\boldsymbol{\mathcal{S}}}_j^A|$. Thus, we have $j \in \mathfrak{E}^A(56)$ and $|\boldsymbol{\mathcal{S}}_{j+1}^A| < |\boldsymbol{\mathcal{S}}_j^A|$ follows. Moreover, we have by Line 56 that

$$\begin{aligned}
|\boldsymbol{\mathcal{S}}_j^A| - |\boldsymbol{\mathcal{S}}_{j+1}^A| &\leq |\boldsymbol{\mathcal{S}}_j^A| - |\tilde{\boldsymbol{\mathcal{S}}}_j^A| + \mathbb{1}(10\ell_j^A < \tilde{\ell}_j^A) \\
&\leq |\boldsymbol{\mathcal{S}}_j^A| - |\boldsymbol{\mathcal{S}}_j^B| + \mathbb{1}(10\ell_j^A < \ell_j^B) && (\text{As } \mathsf{corr}_j^B = 0) \\
&\leq |\boldsymbol{\mathcal{S}}_j^A| - |\boldsymbol{\mathcal{S}}_{j+1}^B|, && (\text{As } 10 \cdot \ell_j^A \geq \ell_j^B \text{ and } |\boldsymbol{\mathcal{S}}_j^B| = |\boldsymbol{\mathcal{S}}_{j+1}^B|)
\end{aligned}$$

finishing the proof. □

As $|\boldsymbol{\mathcal{S}}_j^B| = |\boldsymbol{\mathcal{S}}_{j+1}^B|$ and we have Claim 6.120, we can apply item 2 of Lemma 6.117 to get $\mathsf{sync}_{j+1} \geq \mathsf{sync}_j$. We can also apply item 3 of Lemma 6.118 on A and item 2 of Lemma 6.118 on B get $\sum_{C \in \{A,B\}} \mathsf{total}_j^C - \sum_{C \in \{A,B\}} \mathsf{total}_{j+1}^C \geq \frac{10}{11} \cdot \ell_j^A$. Combining, we get:

$$\zeta_{j+1} - \zeta_j \geq \frac{40}{11} \cdot \ell_j^A \geq \frac{1}{4} \cdot (\ell_j^A + \ell_j^B),$$

$$\left(\zeta_{j+1} - \mathsf{sync}_{j+1}\right) - \left(\zeta_j - \mathsf{sync}_j\right) \geq \frac{40}{11} \cdot \ell_j^A \geq \frac{1}{4} \cdot (\ell_j^A + \ell_j^B),$$

and Equation 84 and Equation 85 follow.

* $\mathbf{10 \cdot \ell_j^A < \ell_j^B}$**:** By the contrapositive of Claim 6.119, we have that $\mathsf{corr}_j^B = 0$. It follows that $\tilde{\ell}_j^A = \ell_j^B$ and $|\tilde{\boldsymbol{\mathcal{S}}}_j^A| = |\boldsymbol{\mathcal{S}}_j^B| < |\boldsymbol{\mathcal{S}}_j^A|$. The former implies that $10\tilde{\ell}_j^A = 10\ell_j^B \geq \ell_j^A$ which together with the latter implies that $j \in \mathfrak{E}^A(56) \implies |\boldsymbol{\mathcal{S}}_{j+1}^A| < |\boldsymbol{\mathcal{S}}_j^A|$. We claim that:

Claim 6.121. $|\boldsymbol{\mathcal{S}}_j^B| - 1 = |\boldsymbol{\mathcal{S}}_{j+1}^B| \leq |\boldsymbol{\mathcal{S}}_{j+1}^A|$.

Proof. We first claim that $10 \cdot \tilde{\ell}_j^B < \ell_j^B$. Indeed, either $\mathsf{corr}_j^A > 0$ and the claim follows by Claim 6.119, or $\mathsf{corr}_j^A = 0 \implies \tilde{\ell}_j^B = \ell_j^A$ implying in turn that $10 \cdot \tilde{\ell}_j^B = 10 \cdot \ell_j^A < \ell_j^B$.
As $10 \cdot \tilde{\ell}_j^B < \ell_j^B$, we have in particular that $\ell_j^B \neq \tilde{\ell}_j^B$ implying that $\tilde{\mathscr{P}}_j^B \neq \mathscr{P}_j^B$. Together, these mean that $j \in \mathfrak{E}^B(54)$ from which we get that $|\boldsymbol{\mathcal{S}}_{j+1}^B| = |\boldsymbol{\mathcal{S}}_j^B| - 1$. As $j \in \mathfrak{E}^A(56)$, we also have:

$$|\boldsymbol{\mathcal{S}}_j^A| - |\boldsymbol{\mathcal{S}}_{j+1}^A| \leq |\boldsymbol{\mathcal{S}}_j^A| - |\tilde{\boldsymbol{\mathcal{S}}}_j^A| + \mathbb{1}(10\ell_j^A < \tilde{\ell}_j^A)$$

$$\leq |\boldsymbol{\mathcal{S}}_j^A| - |\boldsymbol{\mathcal{S}}_j^B| + \mathbb{1}(10\ell_j^A < \ell_j^B) \qquad (\text{As } \mathsf{corr}_j^B = 0)$$
$$\leq |\boldsymbol{\mathcal{S}}_j^A| - |\boldsymbol{\mathcal{S}}_{j+1}^B|, \qquad (\text{As } 10\ell_j^A < \ell_j^B \text{ and } |\boldsymbol{\mathcal{S}}_{j+1}^B| = |\boldsymbol{\mathcal{S}}_j^B| - 1)$$

and the claim follows by simple rearrangement.

□

Assume for now that the value μ_j^A computed by Alice in Line 56 satisfies $\mu_j^A \leq |\boldsymbol{\mathcal{S}}_j^A| - |\tilde{\boldsymbol{\mathcal{S}}}_j^A| + \mathbb{1}(10\ell_j^A < \tilde{\ell}_j^A)$. In this case, we apply item 4 of Lemma 6.117 to get $\mathsf{sync}_{j+1} - \mathsf{sync}_j \geq -2 \cdot \ell_j^B$. We also apply item 4 of Lemma 6.118 on A and item 3 of Lemma 6.118 on B get $\sum_{C\in\{A,B\}} \mathsf{total}_j^C - \sum_{C\in\{A,B\}} \mathsf{total}_{j+1}^C \geq 10\left(\ell_j^A + \tilde{\ell}_j^A\right) + \frac{10}{11}\ell_j^B \geq 10\left(\ell_j^A + \ell_j^B\right)$ as $\tilde{\ell}_j^A = \ell_j^B$. Combining, we get:

$$\zeta_{j+1} - \zeta_j \geq -18 \cdot \ell_j^B + 40\left(\ell_j^A + \ell_j^B\right) \geq 22 \cdot (\ell_j^A + \ell_j^B),$$

$$\left(\zeta_{j+1} - \mathsf{sync}_{j+1}\right) - \left(\zeta_j - \mathsf{sync}_j\right) \geq -16 \cdot \ell_j^B + 40\left(\ell_j^A + \ell_j^B\right) \geq 24 \cdot (\ell_j^A + \ell_j^B),$$

and Equation 84 and Equation 85 follow.
On the other hand, if $\mu_j^A > |\boldsymbol{\mathcal{S}}_j^A| - |\tilde{\boldsymbol{\mathcal{S}}}_j^A| + \mathbb{1}(10\ell_j^A < \tilde{\ell}_j^A)$, we apply item 4 of Lemma 6.117 to get $\mathsf{sync}_{j+1} - \mathsf{sync}_j \geq -\frac{2}{3} \cdot \ell^A_{\mathsf{last}_j^A(|\boldsymbol{\mathcal{S}}_j^B|)-1} - \frac{1}{3} \cdot \ell^B_{\mathsf{last}_j^B(|\boldsymbol{\mathcal{S}}_j^B|)-1}$. We also apply item 5 of Lemma 6.118 on A and item 3 of Lemma 6.118 on B get $\sum_{C\in\{A,B\}} \mathsf{total}_j^C - \sum_{C\in\{A,B\}} \mathsf{total}_{j+1}^C \geq \frac{3}{2} \cdot \ell^A_{\mathsf{last}_j^A(|\tilde{\boldsymbol{\mathcal{S}}}_j^A|)-1} + \ell^B_{\mathsf{last}_j^B(|\boldsymbol{\mathcal{S}}_j^B|)-1} = \frac{3}{2} \cdot \ell^A_{\mathsf{last}_j^A(|\boldsymbol{\mathcal{S}}_j^B|)-1} + \ell^B_{\mathsf{last}_j^B(|\boldsymbol{\mathcal{S}}_j^B|)-1}$ as $|\tilde{\boldsymbol{\mathcal{S}}}_j^A| = |\boldsymbol{\mathcal{S}}_j^B|$. Combining, we get:

$$\zeta_{j+1} - \zeta_j \geq \ell^B_{\mathsf{last}_j^B(|\boldsymbol{\mathcal{S}}_j^B|)-1},$$

$$\left(\zeta_{j+1} - \mathsf{sync}_{j+1}\right) - \left(\zeta_j - \mathsf{sync}_j\right) \geq \ell^B_{\mathsf{last}_j^B(|\boldsymbol{\mathcal{S}}_j^B|)-1},$$

and Equation 84 and Equation 85 follow as $\ell^B_{\mathsf{last}_j^B(|\boldsymbol{\mathcal{S}}_j^B|)-1} \geq \frac{10}{11} \cdot \ell_j^B \geq \frac{4}{5} \cdot (\ell_j^A + \ell_j^B)$ using Corollary 6.116 and the fact that $10 \cdot \ell_j^A < \ell_j^B$.

– $\boldsymbol{|\mathcal{S}_j^A| < |\mathcal{S}_j^B|}$**:** Symmetric to the case above.

- $\boldsymbol{\mathsf{corr}_j \geq \frac{1}{15} \cdot \left(\ell_j^A + \ell_j^B\right)}$**:** We apply item 5 of Lemma 6.117 to get $\mathsf{sync}_{j+1} - \mathsf{sync}_j \geq -22 \cdot \left(\ell_j^A + \ell_j^B + \mathsf{corr}_j\right)$. We also combine item 1, item 2, and item 3 of Lemma 6.118 on A and B to conclude that $\sum_{C\in\{A,B\}} \mathsf{total}_j^C - \sum_{C\in\{A,B\}} \mathsf{total}_{j+1}^C \geq -(\ell_j^A + \ell_j^B)$. Equation 84 and Equation 85 follow as:

$$\zeta_{j+1} - \zeta_j \geq 8000 \cdot \mathsf{corr}_j - 200 \cdot \left(\ell_j^A + \ell_j^B + \mathsf{corr}_j\right) - 4(\ell_j^A + \ell_j^B) \geq 250 \cdot \left(\ell_j^A + \ell_j^B\right).$$

$$\begin{aligned}\left(\zeta_{j+1} - \mathsf{sync}_{j+1}\right) - \left(\zeta_j - \mathsf{sync}_j\right) &\geq 8000 \cdot \mathsf{corr}_j - 180 \cdot \left(\ell_j^A + \ell_j^B + \mathsf{corr}_j\right) - 4(\ell_j^A + \ell_j^B) \\ &\geq 500 \cdot \left(\ell_j^A + \ell_j^B\right) - 200 \cdot \left(\ell_j^A + \ell_j^B\right) \\ &\geq 200 \cdot \left(\ell_j^A + \ell_j^B\right).\end{aligned}$$

□

References

[BE14] Mark Braverman and Klim Efremenko. List and unique coding for interactive communication in the presence of adversarial noise. In *Foundations of Computer Science (FOCS)*, pages 236–245, 2014. 4

[BGMO17] Mark Braverman, Ran Gelles, Jieming Mao, and Rafail Ostrovsky. Coding for interactive communication correcting insertions and deletions. *IEEE Transactions on Information Theory*, 63(10):6256–6270, 2017. 4

[BK12] Zvika Brakerski and Yael Tauman Kalai. Efficient interactive coding against adversarial noise. In *Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on*, pages 160–166. IEEE, 2012. 4, 5, 6, 7, 11, 12, 13, 43

[BKN14] Zvika Brakerski, Yael Tauman Kalai, and Moni Naor. Fast interactive coding against adversarial noise. *Journal of the ACM (JACM)*, 61(6):35, 2014. 4

[BR11] Mark Braverman and Anup Rao. Towards coding for maximum errors in interactive communication. In *Symposium on Theory of computing (STOC)*, pages 159–166. ACM, 2011. 4, 16

[Bra12] Mark Braverman. Towards deterministic tree code constructions. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 161–167. ACM, 2012. 4

[CHS18] Gil Cohen, Bernhard Haeupler, and Leonard J. Schulman. Explicit binary tree codes with polylogarithmic size alphabet. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 535–544. ACM, 2018. 3, 4

[EGH16] Klim Efremenko, Ran Gelles, and Bernhard Haeupler. Maximal noise in interactive communication over erasure channels and channels with feedback. *IEEE Transactions on Information Theory*, 62(8):4575–4588, 2016. 4

[EHK18] Klim Efremenko, Elad Haramaty, and Yael Kalai. Interactive coding with constant round and communication blowup. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:54, 2018. 13

[EKS18] Klim Efremenko, Gillat Kol, and Raghuvansh Saxena. Interactive coding over the noisy broadcast channel. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 507–520. ACM, 2018. 4

[Gel17] Ran Gelles. Coding for interactive communication: A survey. *Foundations and Trends® in Theoretical Computer Science*, 13(1–2):1–157, 2017. 4

[GH14] Mohsen Ghaffari and Bernhard Haeupler. Optimal Error Rates for Interactive Coding II: Efficiency and List Decoding. In *Symposium on Foundations of Computer Science (FOCS)*, FOCS, pages 394–403, 2014. 4

[GHK+16] Ran Gelles, Bernhard Haeupler, Gillat Kol, Noga Ron-Zewi, and Avi Wigderson. Towards optimal deterministic coding for interactive communication. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1922–1936. Society for Industrial and Applied Mathematics, 2016. 4

[GK17] Ran Gelles and Yael Tauman Kalai. Constant-rate interactive coding is impossible, even in constant-degree networks. In *8th Innovations in Theoretical Computer Science Conference, ITCS 2017, January 9-11, 2017, Berkeley, CA, USA*, pages 21:1–21:13, 2017. 19

[GKR19] Ran Gelles, Yael Tauman Kalai, and Govind Ramnarayan. Efficient multiparty interactive coding for insertions, deletions and substitutions. *CoRR*, abs/1901.09863, 2019. 4

[GL16] Venkatesan Guruswami and Ray Li. Efficiently decodable insertion/deletion codes for high-noise and high-rate regimes. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 620–624. IEEE, 2016. 16

[GMS11] Ran Gelles, Ankur Moitra, and Amit Sahai. Efficient and explicit coding for interactive communication. In *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, pages 768–777. IEEE, 2011. 4

[GMS14] Ran Gelles, Ankur Moitra, and Amit Sahai. Efficient coding for interactive communication. *IEEE Transactions on Information Theory*, 60(3):1899–1913, 2014. 4

[HS16] William M. Hoza and Leonard J. Schulman. The adversarial noise threshold for distributed protocols. In *Symposium on Discrete Algorithms (SODA)*, pages 240–258, 2016. 4

[JKL15] Abhishek Jain, Yael Tauman Kalai, and Allison Bishop Lewko. Interactive coding for multiparty protocols. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*, pages 1–10. ACM, 2015. 4

[MS14] Cristopher Moore and Leonard J Schulman. Tree codes and a conjecture on exponential sums. In *Innovations in theoretical computer science (ITCS)*, pages 145–154. ACM, 2014. 3, 4

[NW19] Anand Kumar Narayanan and Matthew Weidner. On decoding cohen-haeupler-schulman tree codes. *CoRR*, abs/1909.07413, 2019. 4

[Pec06] Marcin Peczarski. An improvement of the tree code construction. *Inf. Process. Lett.*, 99(3):92–95, 2006. 3, 4

[RS94] Sridhar Rajagopalan and Leonard J. Schulman. A coding theorem for distributed computation. In *Symposium on the Theory of Computing (STOC)*, pages 790–799, 1994. 4

[Sch92] Leonard J Schulman. Communication on noisy channels: A coding theorem for computation. In *Foundations of Computer Science (FOCS)*, pages 724–733. IEEE, 1992. 3, 4

[Sch93] Leonard J Schulman. Deterministic coding for interactive communication. In *Symposium on Theory of computing (STOC)*, pages 747–756. ACM, 1993. 3, 4, 16

[Sch96] Leonard J. Schulman. Coding for interactive communication. *IEEE Transactions on Information Theory*, 42(6):1745–1756, 1996. 3, 17

[SZ99] Leonard J Schulman and David Zuckerman. Asymptotically good codes correcting insertions, deletions, and transpositions. *IEEE transactions on information theory*, 45(7):2552–2557, 1999. 16

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il