Electronic Colloquium on Computational Complexity, Report No. 60 (2021)

Optimal Error Resilience of Adaptive Message Exchange

Klim Efremenko[*] Ben-Gurion University

Gillat Kol[†] Princeton University

Raghuvansh R. Saxena[‡] Princeton University

Abstract

We study the *error resilience* of the *message exchange* task: Two parties, each holding a private input, want to exchange their inputs. However, the channel connecting them is governed by an adversary that may corrupt a constant fraction of the transmissions. What is the maximum fraction of corruptions that still allows the parties to exchange their inputs?

For the non-adaptive channel, where the parties must agree in advance on the order in which they communicate, the maximum error resilience was shown to be $\frac{1}{4}$ (see [BR11], STOC 2011). The problem was also studied over the adaptive channel, where the order in which the parties communicate may not be predetermined ([GHS14], STOC 2014; [EKS20], STOC 2020). These works show that the adaptive channel admits much richer set of protocols but leave open the question of finding its maximum error resilience.

In this work, we show that the maximum error resilience of a protocol for message exchange over the adaptive channel is $\frac{5}{16}$, thereby settling the above question. Our result requires improving both the known upper bounds and the known lower bounds for the problem.

[*] klimefrem@gmail.com
[†] gillat.kol@gmail.com
[‡] rrsaxena@princeton.edu

ISSN 1433-8092

1 Introduction

We study the *error resilience* of the *message exchange* task: Alice and Bob each have a private input, and they wish to know both inputs. To achieve this, they may communicate any number of symbols over any alphabet set[1]. However, an adversary can corrupt up to θ fraction of the communicated symbols. What is the maximum[2] θ for which there exists a protocol for the message exchange task?

In the 'standard' model, where parties take turns communicating, it can be shown that the answer is $\theta = \frac{1}{4}$ (see [BR11][3]). Observe, however, that this model is rather restrictive, as the order of communication in the protocol must be determined in advance, and thus cannot depend of the parties' inputs, randomness, and on the messages they received during the protocol[4]. Since the order of turns cannot be adapted after an execution commences, these protocols are called *non-adaptive* (*a.k.a. oblivious* or *static*).

Motivated by the fact that modern communication systems often allow more than one party to transmit in a single round (*e.g.*, wireless networks), Ghaffari, Haeupler, and Sudan [GHS14], initiated the study of the message exchange problem over the *adaptive* channel, where the order in which the parties transmit is not determined in advance and both (or none of the) parties may transmit in a given round. However, the messages received in a round are only meaningful if exactly one party transmitted in this round (see subsection 1.2 and subsection 3.1 for a description of the model). In their paper [GHS14], the authors show that this modest relaxation of the standard model allows for an improved maximum error resilience. Specifically, they give a novel message exchange protocol with an error resilience of $\frac{2}{7} > \frac{1}{4}$. One key idea behind their protocol, is that it "dynamically" allocates more receiving rounds to the party that received more corruptions. This scheme was believed to be tight. In fact, [GHS14] contains a proof of optimality that was later found to contain a vulnerability.

In a recent work [EKS20], we show how to break the $\frac{2}{7}$ barrier and obtained a protocol that is resilient to $\frac{7}{24} > \frac{2}{7}$ fraction of errors. We mention that both [GHS14] and our result [EKS20] actually give more general results: They show how to simulate any protocol (designed to work over the noiseless channel) by a protocol that is resilient to $\frac{2}{7}$ and $\frac{7}{24}$ fraction of corruptions respectively. Such schemes, that convert protocols over the noiseless channel to noise resilient protocols, are called *interactive coding* schemes.

One obvious question left open by our work [EKS20] is whether $\frac{7}{24}$ is indeed the maximum error resilience of the adaptive channel. Prior to our current paper, the best known

[1] Of course, our end goal is to construct short, efficient protocols over a small alphabet.

[2] Actually, supremum.

[3] Note that $\theta > \frac{1}{4} - \delta$ for all $\delta > 0$ as the parties can encode their inputs using an error correcting code of relative distance $1 - \delta$. Also, $\theta \leq \frac{1}{4}$ as there is a party, say Alice, that 'speaks' in no more than half of the rounds. Let Alice's input be x. The adversary can corrupt the first half of the messages sent by Alice to make it look like her input is some $x' \neq x$. If this happens, Bob cannot tell whether Alice has input x or x'. We mention that [BR11] also prove that *any* task can be performed when the noise rate approaches $\frac{1}{4}$, by constructing a beautiful simulation protocol building on the groundbreaking work of [Sch96].

[4] Indeed, the $\frac{1}{4}$ impossibility result assumes that the identity of the party that communicates less is known is advance.

impossibility result for both message exchange and interactive coding ruled out protocols that tolerate a $\frac{1}{3}$ fraction of corruptions [GHS14] (also see [EGH16])[5].

1.1 Our Results

In this work, we settle the question of the maximum error resilience of the message exchange task over the adaptive channel, getting an exact constant. The maximum error resilience of different (mostly one-way) channels was and still is studied extensively by the information theory community. For many important channels, exact constants are known. This result is part of an effort to understand two-way (or multi-way) channels to the extent that one-way channels are understood.

An informal statement of our main result is given in Theorem 1.1. For a formal statement, see Theorem 4.1 and Theorem 5.1.

Theorem 1.1 (informal). *The maximum error resilience of the message exchange task over the adaptive channel is $\frac{5}{16}$.*

To prove the above theorem, we design a protocol that solves the message exchange task even in the presence of $\frac{5}{16} - \varepsilon$ fraction of adversarial errors (for every $\varepsilon > 0$). Our protocol is deterministic, computationally efficient, and consists of only $\mathcal{O}\left(1/\epsilon\right)$ communication rounds. Furthermore, it only requires the parties to communicate messages of bit length at most $n + 1$, where n is the length of their inputs.

We also show that no message exchange protocol is resilient to $\frac{5}{16}$ fraction of errors, thereby showing that our protocol is optimal. Such lower bounds are tricky, as when a message is corrupted, it may not only cause the parties to change their future messages, but can also cause them to completely change the order in which they speak. Thus, the parties can dynamically allocate more rounds to the party that received more corruptions, decreasing the length of the simulation (see [GHS14] and [EKS20] to learn more about this phenomenon).

We note that since designing a noise resilient message exchange protocol is a special case of designing an interactive coding scheme, our result also implies that no interactive coding scheme can tolerate $\frac{5}{16}$ fraction of corruptions. Also, a noise resilient protocol for message exchange implies the same noise resilience for general interactive coding, albeit, with an exponentially small rate, as the parties can simply exchange their entire inputs (which may be exponentially large) and compute the function separately. Thus, Theorem 1.1 implies

[5] The argument is simple and elegant: Consider the message exchange task with bit inputs. Denote the length of the protocol by $3N$, and assume wlog that on inputs $x = y = 0$, Bob is speaks in at most N out of the first $2N$ rounds. Consider the following adversary (only requiring N corruption): on inputs $x = 0, y = 1$, corrupt Bob's messages in the first $2N$ rounds to be consistent with $y = 0$. On inputs $x = y = 0$, corrupt Bob's messages in the last N rounds to be consistent with $y = 1$. Now, if the messages received by Alice are consistent with $y = 0$ in the first $2N$ rounds and with $y = 1$ in the last N rounds, Alice cannot tell if $y = 0$ and the adversary corrupted the end of the protocol, or if $y = 1$ and the beginning was corrupted.

that the maximum error resilience of an interactive coding scheme is $\frac{5}{16}$, if one allows an arbitrarily small rate.

1.2 The Adaptive Model

The adaptive model was defined in this context by [GHS14] and is inspired by extensively studied models in distributed computing (*e.g.* radio networks [CK85]). This model assumes that each party is equipped with a device that can either receive or transmit in every communication round. If exactly one party transmits, and the adversary decides not to corrupt the transmission, then the other party receives the transmitted message. In the case where both parties decide to transmit, neither gets a message, as neither was listening for one. Finally, if both parties decide to receive, then since there is no one transmitting, nothing can be assumed about the received messages. This means these messages are controlled by the adversary, and are not "charged" to its "corruption budget".

While it seems pessimistic to assume that the messages received by the parties when they are both receiving are determined by the adversary, this is a crucial in order to avoid "signaling"[6]. For a formal definition of this model, see section subsection 3.1, and for additional motivation for the definition, see [Hae14, GHS14].

1.3 Our Techniques

To prove our lower bound result, showing that no adaptive message exchange protocol is resilient to $\frac{5}{16}$ fraction of corruptions, we identify and measure two key parameters, Δ and L, that govern the error resilience of a protocol. We show that upper bounds on Δ and L give an upper bound on the error resilience of the protocol.

Assume that the adversary's budget is f corruptions. A natural approach for designing a resilient message exchange protocol is to have one party, say Alice, first try to convey her input to Bob. For this, she may send her input to Bob in each of the first x rounds of the protocol. How large should x be? Clearly, we want $x \geq f$, as otherwise, the adversary can target these rounds. Our lower bound shows that protocols with high error resilience have x substantially larger than f. We denote these extra rounds by Δ, *i.e.*, $x = \Delta + f$. Intuitively, a large x can allow Bob to give meaningful *feedback* to Alice about whether he already knows her input or not. Observe that if Bob still does not know Alice's input after these x rounds, then Δ corruptions must have happened, and Bob can convey this to Alice.

The second parameter, called L, counts the number of "*compensation*" rounds. Assume that Bob is unsure about Alice's input after the first x rounds, and that Alice was able to receive Bob's feedback. Then, Alice should transmit more in the remaining rounds, to allow Bob to know her input. We denote these extra transmissions by L. We remark that if Bob is unsure and Alice knows that, the rounds will have Alice transmitting and Bob

[6] For example, if we were to assume that such "simultaneous receives" can be detected, then each party can use this to signal their input to the other party.

receiving. However, if the feedback from Bob is also corrupted, then Alice may also receive in some of these rounds. In this case, these rounds have both parties receiving (we call such rounds RR-rounds). While such rounds are risky, as they are controlled by the adversary, and indeed, noise resilient protocols in prior works [GHS14, EKS20] were designed to avoid such rounds, perhaps surprisingly, our lower bound proves that they are necessary to get optimal resilience.

The parameters Δ and L also guide the construction of our error resilient protocol. We implement a mechanism that uses the extra Δ rounds in the beginning of the protocol to give suitable feedback from Bob to Alice. We note that this feedback mechanism is very different from the one developed in [EKS20] (which is not as efficient as the one in this paper, but better suited for interactive communication).

As suggested by our lower bound, our protocol has $L > 0$ compensation rounds. Scheduling these rounds is a subtle task, because, as noted above, these rounds can turn into RR-rounds in some settings. In RR-rounds, the adversary controls the messages received by the parties, and may use them to cause both parties to receive in the following round as well. This potentially allows the adversary to control many additional rounds "for free". To avoid this phenomenon, we "interleave" adaptive and non-adaptive rounds, meaning that after a round in which both parties may receive we schedule a round where exactly one party receives, and the identity of this party is decided in advance. This interleaving controls the damage done by the RR-rounds.

Even though our protocol is involved and specialized to the message exchange problem, we believe that ideas from our protocol, *e.g.*, the interleaving technique, can also be used to get higher error resilience for other interactive tasks.

1.4 Additional Related Works

The works most related to our paper are [EKS20], [GHS14], and [BR11] mentioned above.

Since the study of coding for interactive communication was initiated by Schulman [Sch92, Sch93, Sch96], numerous works have been published in this area [GMS11, BR11, Bra12, KR13, BE17, BKN14, GMS14, GHK$^+$18, EGH16, BGMO17, *e.g.*]. For a great survey of this field, see [Gel17]. It is, by now, well known that adaptive models can be much more powerful than non-adaptive models [Hae14, GH14, GHS14, AGS16, HV17, EKS18].

The question of maximum error resilience was also studied for feedback and erasure channels [EGH16, FGOS15, SW17, HSV18], and for a different adaptive model (interesting in its own right) where collisions do not occur [AGS16]. The works of [HKV15, WQC17, Ber64] show that the maximal error rate of the message transfer problem (one-way communication) can be improved in the presence of (even partial and noisy) feedback. Feedback was shown to also allow the construction of interactive codes with better rates [Pan13, GH17].

Finally, we note that the problem of message exchange without noise was extensively studied under the name of two-way source coding in the information theory community (see, *e.g.*, [Kas85, MI13] and related works), and also in many multi-party models (*e.g.* the gossiping problem in wireless radio networks).

2 Our Approach

In this section, we build the ideas behind our results in the paper.

2.1 The Lower Bound Attempt of [GHS14]

The starting point of our lower bound of $\frac{5}{16}$ is the attempt by [GHS14] to upper bound the maximum error resilience of adaptive protocols by $\frac{2}{7}$, although our proof is more involved and goes far beyond [GHS14]. We go over the attempt of [GHS14] before explaining our contributions. In all that follows, when we say that the adversary *corrupts* a party, we mean that it corrupts the messages this party receives (rather than the messages this party sends). We also use the words listening and receiving interchangeably. Without loss of generality, we will assume that all the messages sent by a party contain (at least) its input.

The [GHS14] attempt is based on the observation that if the adversary can corrupt a total of f rounds in the protocol, then Alice will need to receive more than f copies of Bob's input to be sure that the message received is indeed his input, and not something the adversary sent. A similar claim also holds for Bob. In order to receive more than f copies of Bob's input, Alice may have to receive more than $2f$ messages. In particular, this happens if the adversary uses all of its corruption in confusing Alice and Alice gets f corrupted messages that are not what Bob sent.

This observation is already enough to show that non-adaptive protocols cannot have error resilience higher than $\frac{1}{4}$ [BR11]. In a non-adaptive protocol, the rounds where each parties receives is decided before the execution of the protocol commences. If any of the parties receives at most $2f$ messages, then the adversary may use all of its corruptions on that party alone, thereby confusing that party. Thus, in order for the protocol to work, both parties should receive in more than $2f$ rounds, implying the error fraction is at most $\frac{f}{2f+2f} = \frac{1}{4}$.

[GHS14] attempt to adapt this proof to the adaptive setting. Specifically, they imagine a situation where the adversary does not corrupt the first f messages received by either of the parties. Rather, after a party has received f messages, the adversary starts corrupting that party. Importantly, the adversary does this for both the parties simultaneously in a *joint attack*, without giving them any indication that the other party is also being corrupted.

At first, corrupting both the parties may seem infeasible as the adversary will have to use twice as many errors, but this is not actually the case. Since the adversary does not indicate to any of the parties that both parties are being corrupted, both the parties will behave as if only they were being corrupted and receive more than f extra messages. Either the extra f rounds in which each of the parties receive do not intersect a lot, in which case, the protocol is long and the error resilience is low anyway, or they do intersect a lot, which is the case we analyze next.

Recall that whenever both the parties are receiving in a given round, the adversary gets to corrupt them for free. Therefore, if there are many such rounds, then the adversary may have enough budget to corrupt both the parties simultaneously. In fact, if the f extra messages for the two parties are contained in at most $\frac{3f}{2}$ rounds, then there are at least $\frac{f}{2}$ rounds where both parties are listening, and the adversary can corrupt all of the $\frac{3f}{2}$ rounds by using only f corruptions.

Thus, it seems that the adversary can derail any protocol that has at most $f+f+\frac{3f}{2}=\frac{7f}{2}$ messages, implying a maximum error resilience of at most $\frac{2}{7}$ for any protocol.

2.2 The Vulnerability in [GHS14] - Asymmetry

The [GHS14] attempt outlined above suffers from a vulnerability, which we describe next. Let p^A be the round such that Alice receives in exactly f rounds before p^A, and p^B be such that Bob receives in exactly f rounds before p^B. Further, assume without loss of generality that $p^A > p^B$. The joint attack outlined above corrupts Alice after round p^A and Bob after round p^B, but does *not* corrupt Alice between rounds p^B and p^A (because the adversary does not corrupt the first f messages received by Alice and by the definition of p^A, Alice receives f messages before p^A).

Not corrupting Alice between rounds p^B and p^A turns out to be okay as long as Bob does not receive in these rounds. In particular, if the protocol is *symmetric* and p^A is very close to p^B, then the joint attack described above works and implies that the maximum error resilience of such protocols is indeed $\frac{2}{7}$. In fact, it may seem that any protocol for a 'symmetric' problem like message exchange must be symmetric, and therefore the $\frac{2}{7}$ bound should apply. Quite astonishingly, this is not true, as is witnessed by our protocol from [EKS20] with error resilience $\frac{7}{24} > \frac{2}{7}$.

[EKS20] establishes that asymmetric protocols are actually more powerful than symmetric ones when it comes to error resilience, as it allows for meaningful feedback (see subsection 1.3 and [EKS20]). Therefore, in order to show a lower bound for all protocols, we need to understand exactly how much power does asymmetry provide a protocol.

To this end, suppose that Bob receives an additional δ messages between round p^B and p^A. These δ messages are corrupted by the adversary, and Bob can tell Alice that these δ corruptions happened between rounds p^B and p^A. As the adversary does not corrupt Alice in these rounds, Alice will receive this information from Bob correctly and know that the adversary has already spent δ corruption on Bob by round p^A.

With this information, Alice knows that the adversary only has $f-\delta$ corruptions left and she only needs to listen to $f-\delta$ rounds after round p^A. Also, Bob has already received δ messages between rounds p^B and p^A, and only needs to receive $f-\delta$ more messages after round p^A. By a similar calculation as in the foregoing section, we can conclude that a protocol that solves message exchange must have at least $f+f+\delta+\frac{3(f-\delta)}{2}$ rounds, and therefore an error resilience of at most $\frac{2f}{7f-\delta}$.

2.3 Bounding the Asymmetry - A New Attack

In the foregoing section, we did get a bound of $\frac{2f}{7f-\delta}$ on the maximum error resilience of any protocol. However, this bound is unsatisfactory as it involves an unnatural parameter δ of the protocol. To make matters worse, in the worst case $\delta = f$, and this bound reduces to the already known bound of $\frac{1}{3}$.

On the bright side, we also get that any upper bound on δ that is better than the trivial f would give us a new bound on the maximum error resilience. This is exactly the approach we take, but before we describe how we get a better upper bound on δ, we point out that a protocol with optimal error resilience should have a large number of rounds between p^B and p^A where Alice is listening. This is because a large number of rounds allows Bob to give better feedback to Alice and inform her about the corruptions on his end. For the rest of this sketch, we will assume that this number is equal to f, the largest possible. With this assumption, we get that before p^B, Bob receives in f rounds and Alice receives in 0 rounds, and in between p^B and p^A, Bob receives in δ rounds while Alice receives in f rounds, a total of $f + \delta$ rounds.

To get a better upper bound on the parameter δ, we consider a new attack, where the adversary starts corrupting *both* the parties after round p^B itself, such that both the parties think that they are the only ones being corrupted, *i.e.*, the adversary is cutting the feedback as well. It is possible that the adversary cannot sustain this attack till the end of the protocol with its budget of f corruptions. However, it is still worthwhile to consider this attack till the point where the adversary has used all of its budget. It turns out that the interesting case is when this point, say q, is before round p^A and we shall assume this henceforth.

As far as Bob is concerned, nothing has changed from the joint attack of [GHS14] to this new attack. He still gets corrupted after round p^B and thinks that he is the only one being corrupted. Thus, he will still be receiving in all the δ rounds in between p^B and p^A that he was receiving in before. However, Alice now gets a different view and starts listening in some of these δ rounds. Based on Alice's behavior, we partition the δ rounds as follows (see Figure 1 for an illustration):

1. The rounds before q where Alice is now listening. Observe that, in our new attack both the parties are listening in these rounds. Let's say that there are L such rounds.

2. The rounds before q where Alice continues to transmit. Let's say that there are Δ such rounds.

3. The rounds that are in between q and p^A. There are $\delta - \Delta - L$ such rounds. We claim that, in the interesting case, $\delta - \Delta - L \leq \Delta$. This is because, as observed above, these rounds are beneficial for the protocol only if Bob can send meaningful feedback about the corruptions in these rounds to Alice. The amount of meaningful feedback that Bob can give Alice is obviously constrained by the number of messages Bob can send to Alice. We next show that this number is Δ.

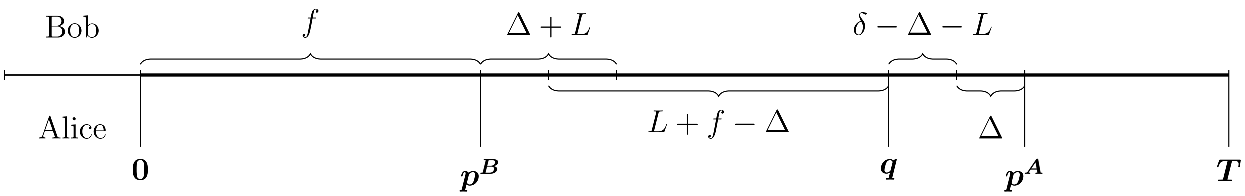

Figure 1: Depiction of the various rounds in our lower bound. The number of times Bob listens in an interval is written above the interval. The number of times Alice listens in an interval is written below the interval. The L rounds in the between p^B and q where both parties listen is depicted using overlapping braces.

> Recall that the number of messages in between p^B and p^A that Bob sends Alice is f. We simply show that $f - \Delta$ of these messages lie in between p^B and q. This is because, by definition of q, the adversary spends f corruptions between p^B and q. Δ of these corruptions are spent on Bob in the rounds where he is listening and Alice is speaking. The remaining $f - \Delta$ must have been spent on Alice implying that Alice was listening and Bob was transmitting in $f - \Delta$ rounds between p^B and q.

We conclude that $\delta \leq 2\Delta + L$ and it is enough to upper bound Δ and L in order to upper bound δ. We describe our approach for this in the next section.

2.4 Bounding Δ and L

We now describe our approach to upper bounding Δ and L.

Bounding Δ. Recall that Δ is the number of rounds in between p^B and q where Alice speaks and Bob listens in our new attack. In our new attack, after round p^B Alice thinks that she is the only one being corrupted. This means that she will aspire to listen at least $2f$ times between rounds p^B and T, where T denotes the total length of the protocol. We get that

$$2f \leq (T - q) + (q - p^B - \Delta) = T - p^B - \Delta \leq T - f - \Delta,$$

as $p^B \geq f$. It follows that $\Delta \leq T - 3f$.

Bounding L. Recall that L is the number of rounds in between p^B and q where both parties are listening. By definition of q, we have $q = p^B + f + L \geq 2f + L$. In our new attack, till round q Alice only receives corrupted messages from Bob. Thus, after round q she must receive at least f messages from Bob to be sure of his input. We get that

$$f \leq T - q \leq T - 2f - L.$$

It follows that $L \leq T - 3f$.

Plugging these bounds into our equation for δ, we get that $\delta \leq 3(T - 3f)$ and therefore, the error resilience $\frac{f}{T}$ satisfies:

$$\frac{f}{T} \leq \frac{2f}{7f - \delta} \leq \frac{2f}{16f - 3T} \implies \frac{f}{T} \leq \frac{5}{16},$$

as desired.

2.5 What Optimal Protocols Must Look Like?

Not only does our lower bound improve the state-of-the-art, the arguments behind it also provide explicit design principles that a protocol with a matching error-resilience must satisfy. We briefly go over these principles before delving deeper into our protocols. We note here that a subset of these principles apply to all protocols that break the $\frac{2}{7}$ barrier. In particular, they apply to the protocol in [EKS20].

Asymmetry and feedback. Our discussion makes it clear that Alice and Bob must necessarily play asymmetric roles in any protocol with error resilience $> \frac{2}{7}$. Specifically, one of the parties will listen more towards the beginning of the protocol and later provide feedback about the number of errors it sees to the other party. The other party will then speak more towards the end of the protocol and act on this feedback.

Consequently, even the error-resilient simulation of a non-interactive task such as message exchange must have inbuilt interaction between the two parties in the sense that the messages sent by the parties depend on the communication received by them during the protocol. This is in contrast to the protocol in [GHS14], where only the order of the messages (and not the content of the messages) depends on the communication during the protocol (the parties in the [GHS14] protocol only send their inputs).

RR-rounds are necessary. Also, any protocol that achieves an error-resilience of $\frac{5}{16}$ must exhibit the counter-intuitive feature of having "RR-rounds", *i.e.*, rounds where both parties are receiving (even when the corruptions inserted by the adversary are within its budget). The reason this is surprising is because when both the parties are receiving in the same round, then the adversary gets to corrupt them for free! Paradoxically however, when we repeat the calculations of the previous section with the parameter L (that measures the number of RR-rounds) set to 0, we get that the maximum error resilience is upper bounded by $\frac{4}{13} < \frac{5}{16}$.

This apparent paradox is resolved once one takes a closer look at the lower bound argument. It is, of course, true that RR-rounds give the adversary free corruptions and cannot help an execution. Nonetheless, they show up in the lower bound because these rounds can be converted to rounds where only one of the parties is listening in a different execution, and help that execution. In fact, if the protocol can suitably adapt, these rounds can be very flexible and be converted to rounds where Bob is speaking to Alice, if Alice is being targeted by the adversary, and to rounds where Alice is speaking to Bob when Bob is being targeted by the adversary. We ensure that RR-rounds only happen in our protocol when the adversary is corrupting both the parties more or less evenly, and there is enough slack in the analysis to accommodate such rounds.

Even though this reasoning explains why rounds where both parties listen can be helpful, it is unclear how a protocol should be designed in order to exploit them.

2.6 Our Error-Resilient Simulation

Actualizing the design principles above into a protocol requires a lot of effort. In particular, one needs to implement a feedback mechanism and schedule the RR-rounds so that they improve the overall error resilience.

Our feedback mechanism. Our feedback mechanism is inspired by the one in [EKS20], wherein a feedback mechanism was constructed over the same channel for the same reason. However, the goal in [EKS20], was to design a feedback mechanism that would allow us to simulate *any* interactive task with *any* error-resilience better than $\frac{2}{7}$. Our goal here is different. We now want a feedback mechanism that will let us perform a particular task of message exchange with the best error-resilience possible.

Focusing on a particular task allows us to simplify and strengthen the [EKS20] feedback mechanism in two ways. Firstly, for the message exchange task, we are able to take the asymmetry between Alice and Bob to the extreme. Namely, Alice does not have to receive any message at all till a round after p^B when Bob starts giving feedback. Thereafter, Bob does not have to receive any messages from Alice (other than the messages Bob asked for in his feedback).

Additionally, this asymmetry means that feedback from Bob to Alice does not have to be 'online', as was necessary in [EKS20]. Instead, Bob can receive many messages from Alice at the beginning of the protocol itself, compute the feedback 'offline' based on these messages, and later send this feedback in all of his future messages. We note that even though Bob can do an arbitrary computation on the messages received from Alice to compute his feedback, it turns out that Bob only needs to send 1 bit saying whether he is sure of Alice's input or not.

Interleaved RR-rounds. With the feedback mechanism described above, one can already construct a protocol for message exchange with error resilience $\frac{4}{13}$, the best possible for protocols without RR-rounds. We omit all details about this protocol but mention that it has $T-3f$ rounds of the types described in item 1 and item 3 respectively, but no RR-rounds.

We now add RR-rounds to the protocol. More precisely, we add rounds to the protocol that will behave as RR-rounds if the adversary corrupts the parties in the way specified by our new attack. To get error resilience $\frac{5}{16}$, we need to ensure that, when this happens, then by corrupting f messages, the adversary can create $T - 3f$ RR-rounds.

It would be ideal if all the f corruptions are needed to create these RR-rounds, and it is not the case that these can be created with significantly smaller number of corruptions. This is owing to the fact that if $T - 3f$ RR-rounds can be created by a small number of corruptions, then the adversary has some corruptions left even after these RR-rounds, that he can use to derail the protocol, *e.g.*, create even more RR-rounds. As our protocol becomes very vulnerable after $T - 3f$ RR-rounds have taken place, we cannot even afford a small number of corruptions after these RR-rounds.

An extreme solution would be to somehow ensure that there are no RR-rounds if the adversary invests only $f - 1$ corruptions, but somehow there are $T - 3f$ RR-rounds if the adversary invests just 1 more corruption. However, this seems to be unimplementable as the adversary can create such a radical change with just his last corruption. We take a more moderate approach, ensuring that if the adversary has invested $f - k$ corruptions, for some k, then he can create $T - 3f - \Theta(k)$ RR-rounds. This approach prevents both problems: Neither does it give the last corruption by the adversary a lot of power nor does it leave the protocol that vulnerable if the adversary only spends $f - k$ corruptions. In particular, the protocol can still afford $\Theta(k)$ more RR-rounds.

We implement our moderate approach by interleaving rounds that can be potentially RR-rounds with rounds where Bob is sending messages to Alice. Thus, after every RR-round, Alice has another chance to hear from Bob that he is still unsure and she needs to speak more. Either the adversary will corrupt this message from Bob and earn a fresh RR-round or not corrupt this message in which case Alice knows that Bob is unsure and can transmit more.

3 Formal Problem Definition

3.1 The Adaptive Model

Adaptive protocols. We describe the two party adaptive model used in the paper. The model was suggested and studied by [GHS14].

Let Γ be a non-empty set that does not contain the special symbol λ[7]. Throughout, we will use Γ_+ to denote the set $\Gamma \cup \{\lambda\}$. Also, fix sets $\mathcal{X}^A, \mathcal{X}^B$ from which Alice and Bob (respectively) draw their input. A deterministic adaptive protocol Π over the alphabet Γ_+ in the adaptive model is defined by a tuple $\langle T, f^A, f^B \rangle$. Here, T is a parameter that denotes the length of the protocol, while f^A and f^B are *transmission functions* of the type:

$$f^A : \mathcal{X}^A \times \Gamma_+^* \to \Gamma_+ \qquad\qquad f^B : \mathcal{X}^B \times \Gamma_+^* \to \Gamma_+.$$

[7] It may be helpful to think of λ as silence, *i.e.*, if a party sends λ in a given round, then they choose to receive in this round, and if the party receives λ in a given round, then either the other party was receiving in this round or the adversary corrupted the symbol sent by the other party to λ.

Adversaries. When a length T protocol is executed in the adaptive model, some of the messages transmitted may be adversarially corrupted. An adversary Adv for a protocol $\Pi = \langle T, f^A, f^B \rangle$ in the adaptive model is defined by the tuple $\langle \{g^A_m\}_{m \in [T]}, \{g^B_m\}_{m \in [T]} \rangle$ of functions where for all $m \in [T]$, we have the types:

$$g^A_m, g^B_m : \mathcal{X}^A \times \mathcal{X}^B \to \Gamma_+.$$

Intuitively, the function $f^A(\cdot, \cdot)$ computes the symbols sent by Alice and the function $g^A_m(\cdot, \cdot)$ is the symbol received by Alice in round m (which may be different from the symbol sent by Bob in round m due to a corruption), and likewise for Bob. Note that since the adversary is assumed to know the inputs of both parties, he also knows the (uncorrupted) transcripts.

Let $m \in [T]$. The functions g^A_m, g^B_m must satisfy: $g^A_m(x^A, x^B) = \lambda$ if $f^A(x^A, g^A_{<m}(x^A, x^B)) \neq \lambda$, and, similarly, $g^B_m(x^A, x^B) = \lambda$ if $f^B(x^B, g^B_{<m}(x^A, x^B)) \neq \lambda$. Intuitively, the condition $f^A(x^A, g^A_{<m}(x^A, x^B)) \neq \lambda$ corresponds to Alice transmitting (instead of receiving) in round m and when this happens, we require that the adversary sends her λ, *i.e.* $g^A_m(x^A, x^B) = \lambda$, and likewise for Bob.

Define, for $m \in [T]$, the function $g^A_{\leq m} : \mathcal{X}^A \times \mathcal{X}^B \to \Gamma^m_+$ to be concatenation of the m values $\{g^A_{m'}\}_{m' \in [m]}$, and likewise, define $g^B_{\leq m}$. We often omit the subscript when $m = T$, *i.e.*, g^A is the same as $g^A_{\leq T}$ which is the same as $\{g^A_m\}_{m \in [T]}$.

Protocol execution. Let $\Pi = \langle T, f^A, f^B \rangle$ be a protocol and let $\mathsf{Adv} = \langle \{g^A_m\}_{m \in [T]}, \{g^B_m\}_{m \in [T]} \rangle$ be an adversary for Π. Let $x^A \in \mathcal{X}^A$ and $x^B \in \mathcal{X}^B$ be inputs. Define $\mathfrak{E}$ to be the tuple $\langle \Pi, x^A, x^B, \mathsf{Adv} \rangle$.

We think of $\mathfrak{E} = \langle \Pi, x^A, x^B, \mathsf{Adv} \rangle$ as inducing a (noisy) execution of the protocol Π, in the sense that given this tuple, one can generate the view of both parties (or, more generally, compute any value known to the parties) at every point in the execution. Specifically, for $m \in [T]$, let $\alpha_m = f^A(x^A, g^A_{<m}(x^A, x^B))$ be the symbol sent by Alice in round m and $\beta_m = f^B(x^B, g^B_{<m}(x^A, x^B))$ be the symbol sent by Bob in round m. If $\alpha_m = \lambda$, we say that Alice *received* in this round, otherwise, we say that Alice *transmitted* in this round. Similarly, if $\beta_m = \lambda$, we say that Bob *received* in this round, otherwise, we say that Bob *transmitted* in this round.

Types of rounds. For $m \in [T]$, if $\alpha_m \neq \lambda$ and $\beta_m = \lambda$, we say that $\mathsf{type}(\mathfrak{E}, m) = \mathsf{TR}$. Similarly, if $\alpha_m = \beta_m = \lambda$, we say that $\mathsf{type}(\mathfrak{E}, m) = \mathsf{RR}$. We define TT and RT analogously.

To count the number of rounds with type TT amongst the rounds $p, p+1, \cdots, q$ where $p, q \in [T]$, we use the function

$$\#\mathsf{TT}(\mathfrak{E}, [p, q]) = |\{p \leq m \leq q \mid \mathsf{type}(\mathfrak{E}, m) = \mathsf{TT}\}|.$$

Similarly, we define $\#\mathsf{TR}, \#\mathsf{RT}$, and $\#\mathsf{RR}$. When we use an expression like $\#\mathsf{TT}(\mathfrak{E}, (p, q])$, we mean that the inequality $p \leq m$ in the equation above is strict, *i.e.*, we only consider the rounds $p + 1, \cdots, q$.

Corruptions. We say that the adversary corrupted Alice in round m if Bob is transmitting and Alice is receiving in round m and the symbol transmitted by Bob is different from the symbol received by Alice. More precisely, using the same notation as above, we have

$$\begin{aligned} \mathsf{corr}^A_{\leq m}(\mathfrak{E}) &= |\{m' \in [m] \mid \mathsf{type}(\mathfrak{E}, m') = \mathsf{RT} \text{ and } f^B(x^B, g^B_{<m'}(x^A, x^B)) \neq g^A_{m'}(x^A, x^B)\}|. \\ \mathsf{corr}^B_{\leq m}(\mathfrak{E}) &= |\{m' \in [m] \mid \mathsf{type}(\mathfrak{E}, m') = \mathsf{TR} \text{ and } f^A(x^A, g^A_{<m'}(x^A, x^B)) \neq g^B_{m'}(x^A, x^B)\}|. \end{aligned} \tag{1}$$

Finally, define $\mathsf{corr}_{\leq m}(\mathfrak{E}) = \mathsf{corr}^A_{\leq m}(\mathfrak{E}) + \mathsf{corr}^B_{\leq m}(\mathfrak{E})$. As before, we omit the subscript when $m = T$.

3.2 The Message Exchange Problem

Informally, the *message exchange problem* requires each party to output the input of the other party. More formally, let Γ be a set that does not contain the symbol λ. We say that Π *solves the n-length message exchange problem with error tolerance θ over* Γ if Π is an adaptive protocol of length T with input sets $\mathcal{X}^A, \mathcal{X}^B = \{0,1\}^n$, and there exist functions $out^A : \mathcal{X}^A \times \Gamma_+^T \to \{0,1\}^n, out^B : \mathcal{X}^B \times \Gamma_+^T \to \{0,1\}^n$ such that for all adversaries $\mathsf{Adv} = \langle g^A, g^B \rangle$ and $x^A \in \mathcal{X}^A, x^B \in \mathcal{X}^B$, we have:

$$\mathsf{corr}(\langle \Pi, x^A, x^B, \mathsf{Adv} \rangle) \leq \lceil \theta T \rceil \implies out^A(x^A, g^A(x^A, x^B)) = x^B \wedge out^B(x^B, g^B(x^A, x^B)) = x^A.$$

4 The Lower Bound Part of Theorem 1.1

We are now ready to formally state our "lower-bound" part of Theorem 1.1.

Theorem 4.1. *Let $\theta = \frac{5}{16}$. Fix an adaptive protocol $\Pi = \langle T, f^A, f^B \rangle$ where $f^A : \mathcal{X}^A \times \Gamma_+^* \to \Gamma_+$ and $f^B : \mathcal{X}^B \times \Gamma_+^* \to \Gamma_+$ and $|\mathcal{X}^A|, |\mathcal{X}^B| \geq 2$. Also, fix any $x_1^A \neq x_2^A \in \mathcal{X}^A$ and $x_1^B \neq x_2^B \in \mathcal{X}^B$. There exists an adversary $\mathsf{Adv} = \langle \{g^A_m\}_{m \in [T]}, \{g^B_m\}_{m \in [T]} \rangle$ with $g^A_m, g^B_m : \mathcal{X}^A \times \mathcal{X}^B \to \Gamma_+$ such that:*

- *We have $\mathsf{corr}(\mathfrak{E}_{ij}) \leq \lceil \theta T \rceil$ for all $i, j \in [2]$, where $\mathfrak{E}_{ij} = \langle \Pi, x_i^A, x_j^B, \mathsf{Adv} \rangle$.*
- *Either $g^A(x_1^A, x_1^B) = g^A(x_1^A, x_2^B)$ or $g^B(x_1^A, x_1^B) = g^B(x_2^A, x_1^B)$.*

Informally, the above theorem shows that for every protocol there is an adversary that only corrupts θ fraction of the rounds and ensures that either the corrupted transcript for Alice on inputs (x_1^A, x_1^B) is identical to the corrupted transcript for Alice on inputs (x_1^A, x_2^B), or the corrupted transcript for Bob on inputs (x_1^A, x_1^B) is identical to the corrupted transcript for Bob on inputs (x_2^A, x_1^B). Therefore, with noise of rate θ, the adversary can either make Alice give the same output on inputs (x_1^A, x_1^B) and (x_1^A, x_2^B), or make Bob give the same output on inputs (x_1^A, x_1^B) and (x_2^A, x_1^B). In particular, if in the original protocol both players give different values on both of these pairs, no protocol can simulate the original protocol in the presence of noise of rate θ.

We note that Theorem 4.1 shows that even protocols for bit exchange cannot be simulated in the presence of noise of rate θ. We also note that our result holds when the adversary does not know the inputs of the parties (but rather only knows $\Pi = \langle T, f^A, f^B \rangle$ and the transcripts). Indeed, without loss of generality, the first message sent by each party is a non-constant function of its bit input and such functions are invertible. Thus, the adversary can figure out the inputs after the first message from each party.

4.1 Proof of Theorem 4.1

This section lays the groundwork for the proof of Theorem 4.1. We break the proof into several cases, which are dealt with in subsequent sections. The proofs of all lemmas, corollaries, and theorems formulated in this section are deferred to later sections.

We begin by defining some notation. We let $\Pi = \langle T, f^A, f^B \rangle$ be fixed for this proof and assume without loss of generality that θT is an integer. We can also assume that $x_1^A = x_1^B = 0$ and $x_2^A = x_2^B = 1$. For all adversaries Adv that we refer to in this proof and $i, j \in \{0, 1\}$, we will use $\mathfrak{E}_{\mathsf{Adv},i,j}$ to denote $\langle \Pi, i, j, \mathsf{Adv} \rangle$. Sometimes, we use the shorthand $\mathfrak{E}_{\mathsf{Adv}}$ to denote $\mathfrak{E}_{\mathsf{Adv},0,0}$.

Observe that the statement of Theorem 4.1 only deals with inputs in the set $\mathcal{I} = \{(0, 0), (0, 1), (1, 0)\}$ and throughout this proof, we will only define all our adversaries for inputs in $\mathcal{I}$. When the inputs to Alice and Bob are $(1, 1)$, none of the adversaries that we define will cause any corruptions.

The adversary Basic. We begin by defining an adversary $\mathsf{Basic} = \langle \alpha^A, \alpha^B \rangle$. The adversary Basic is defined in a way so that $\alpha^A(0, 0) = \alpha^A(0, 1)$ and $\alpha^B(0, 0) = \alpha^B(1, 0)$. Thus, the adversary Basic satisfies the second property of Theorem 4.1. However, Basic may not satisfy the first property. The rest and the core of the proof lies in using Basic to construct adversaries that satisfy the first property (while keeping the second property intact).

We define Basic inductively. Suppose that for $m \in [T]$, the values $\alpha^A_{<m}(i, j)$ and $\alpha^B_{<m}(i, j)$ have been defined for $(i, j) \in \mathcal{I}$. Observe that this partial definition fixes the value of $\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},i,j}, m)$ for all $(i, j) \in \mathcal{I}$. We define:

$$\alpha^A_m(0,1) = \alpha^A_m(0,0) = \begin{cases} \lambda & , \mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m) \in \{\mathsf{TR}, \mathsf{TT}\} \\ f^B(0, \alpha^B_{<m}(0,0)) & , \mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m) = \mathsf{RT} \\ f^B(1, \alpha^B_{<m}(0,1)) & , \mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m) = \mathsf{RR} \end{cases}.$$

$$\alpha^B_m(1,0) = \alpha^B_m(0,0) = \begin{cases} \lambda & , \mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m) \in \{\mathsf{RT}, \mathsf{TT}\} \\ f^A(0, \alpha^A_{<m}(0,0)) & , \mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m) = \mathsf{TR} \\ f^A(1, \alpha^A_{<m}(1,0)) & , \mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m) = \mathsf{RR} \end{cases}.$$

$$\alpha^A_m(1,0) = \begin{cases} \lambda & , \mathsf{type}(\mathfrak{E}_{\mathsf{Basic},1,0}, m) \in \{\mathsf{TR}, \mathsf{TT}, \mathsf{RR}\} \\ f^B(0, \alpha^B_{<m}(1,0)) & , \mathsf{type}(\mathfrak{E}_{\mathsf{Basic},1,0}, m) = \mathsf{RT} \end{cases}.$$

$$\alpha^B_m(0,1) = \begin{cases} \lambda & ,\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,1}, m) \in \{\mathsf{RT}, \mathsf{TT}, \mathsf{RR}\} \\ f^A(0, \alpha^A_{<m}(0,1)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,1}, m) = \mathsf{TR} \end{cases}.$$

Our definition of the adversary Basic satisfies the following lemma.

Lemma 4.2. *It holds that:*

(a) $\mathsf{corr}(\mathfrak{E}_{\mathsf{Basic},0,0}) = \mathsf{corr}^B(\mathfrak{E}_{\mathsf{Basic},0,1}) = \mathsf{corr}^A(\mathfrak{E}_{\mathsf{Basic},1,0}) = 0$.

(b) For all $m \in [T]$, $\mathsf{corr}^A_{\le m}(\mathfrak{E}_{\mathsf{Basic},0,1}) \le \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,m])$.

(c) For all $m \in [T]$, $\mathsf{corr}^B_{\le m}(\mathfrak{E}_{\mathsf{Basic},1,0}) \le \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,m])$.

We prove the following corollary of the above lemma:

Corollary 4.3. *If* $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,T]) \le \theta T$ *or* $\#\mathsf{TR}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,T]) \le \theta T$*, then, Theorem 4.1 holds.*

Due to Corollary 4.3, we assume that $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,T]), \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,T]) > \theta T$ for the rest of this proof. Define p^A to be the smallest such that $\#\mathsf{TR}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p^A]) \ge \theta T$ and p^B to be the smallest such that $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p^B]) \ge \theta T$. Due to our assumption above that $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,T]), \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,T]) > \theta T$, both p^A and p^B are well defined. Furthermore, as $\#\mathsf{TR}$ and $\#\mathsf{RT}$ increase by at most 1 in every round, we have that

$$\#\mathsf{TR}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p^A]) = \theta T \qquad\qquad \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p^B]) = \theta T. \tag{2}$$

Define $p = \min(p^A, p^B)$.

The adversaries $\mathsf{A\text{-}only}$ and $\mathsf{B\text{-}only}$. We next define the two additional adversaries, $\mathsf{A\text{-}only} = \langle \beta^A, \beta^B \rangle$ and $\mathsf{B\text{-}only} = \langle \gamma^A, \gamma^B \rangle$. In what follows, we only state the definition of $\mathsf{A\text{-}only}$. The definition of $\mathsf{B\text{-}only}$ is completely analogous with the roles of Alice and Bob reversed.

We define $\mathsf{A\text{-}only}$ to be the same as Basic in the first p rounds, *i.e.*, for all $(i,j) \in \mathcal{I}$,

$$\beta^A_{\le p}(i,j) = \alpha^A_{\le p}(i,j) \qquad\qquad \beta^B_{\le p}(i,j) = \alpha^B_{\le p}(i,j).$$

It remains to define $\beta^A_m(i,j)$ and $\beta^B_m(i,j)$ for $m > p$. We do this inductively. Suppose that for some $m > p$, the values $\beta^A_{<m}(i,j)$ and $\beta^B_{<m}(i,j)$ have been defined for all $(i,j) \in \mathcal{I}$. Observe that this partial definition fixes the value of $\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},i,j}, m)$ for all $(i,j) \in \mathcal{I}$. We have:

$$\beta^A_m(0,1) = \beta^A_m(0,0) = \begin{cases} \lambda & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}, m) \in \{\mathsf{TR}, \mathsf{TT}\} \\ f^B(1, \beta^B_{<m}(0,1)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}, m) = \mathsf{RT} \\ f^B(0, \beta^B_{<m}(0,0)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}, m) = \mathsf{RR} \end{cases}.$$

$$\beta^B_m(1,0) = \beta^B_m(0,0) = \begin{cases} \lambda & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}, m) \in \{\mathsf{RT}, \mathsf{TT}\} \\ f^A(0, \beta^A_{<m}(0,0)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}, m) = \mathsf{TR} \\ f^A(1, \beta^A_{<m}(1,0)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}, m) = \mathsf{RR} \end{cases}.$$

$$\beta^A_m(1,0) = \begin{cases} \lambda & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},1,0}, m) \in \{\mathsf{TR}, \mathsf{TT}, \mathsf{RR}\} \\ f^B(0, \beta^B_{<m}(1,0)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},1,0}, m) = \mathsf{RT} \end{cases}.$$

$$\beta^B_m(0,1) = \begin{cases} \lambda & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}, m) \in \{\mathsf{RT}, \mathsf{TT}, \mathsf{RR}\} \\ f^A(0, \beta^A_{<m}(0,1)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}, m) = \mathsf{TR} \end{cases}.$$

The adversaries A-only and B-only satisfy:

Lemma 4.4. *We have:*

(a) $\mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) = \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{Basic},0,1})$ *and* $\mathsf{corr}(\mathfrak{E}_{\mathsf{B\text{-}only},1,0}) = \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{Basic},1,0})$.

(b) $\mathsf{corr}^B(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}) = \mathsf{corr}^A(\mathfrak{E}_{\mathsf{B\text{-}only},0,0}) = 0$.

(c) For all $m \in [T]$, $\mathsf{corr}_{\leq m}(\mathfrak{E}_{\mathsf{A\text{-}only},1,0}) \leq \#\mathsf{TR}(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}, (0,m])$ *and* $\mathsf{corr}_{\leq m}(\mathfrak{E}_{\mathsf{B\text{-}only},0,1}) \leq \#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}only},0,0}, (0,m])$.

The adversary 2-Sided. Next, define the adversary 2-Sided $= \langle \delta^A, \delta^B \rangle$ so that

$$\delta^A(0,0) = \beta^A(0,0) \qquad\qquad \delta^B(0,0) = \gamma^B(0,0).$$

We leave the adversary 2-Sided undefined for the inputs $(0,1)$ and $(1,0)$ as we will never need those values. Using the adversary 2-Sided, we define q to be the smallest such that $\#\mathsf{TR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) \geq \theta T$. If no such value q exists, we define it to be $T+1$. Observe that since the sets of TR and RT rounds in an execution are disjoint, it holds that $\#\mathsf{TR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) \leq \theta T$.

For the rest of this proof, we assume without loss of generality that $p = p^A < p^B$. The argument when $p^A > p^B$ is analogous. This assumption implies that (from Equation 2):

$$\#\mathsf{TR}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p]) = \theta T \qquad\qquad \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p]) < \theta T. \tag{3}$$

Next, define the numbers:

$$\Delta = \#\mathsf{TR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) \qquad\qquad L = \#\mathsf{RR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]). \tag{4}$$

We can now show:

Theorem 4.5. *If* $\max(L, \Delta) \geq (1 - 3\theta)T$, *then Theorem 4.1 holds.*

Owing to Theorem 4.5, we assume for the rest of the proof that $\max(L, \Delta) < (1 - 3\theta)T$. We define q' to be q if $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}only}}, (0,q]) < \theta T$. Otherwise, we let q' denote the smallest value such that $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}only}}, (0,q']) \geq \theta T$. Observe that in either case, we have $q' \leq q$ and

$$\#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}only}}, (0,q']) \leq \theta T. \tag{5}$$

The adversary $\mathsf{B\text{-}then\text{-}A}$. Next, we define an adversary $\mathsf{B\text{-}then\text{-}A} = \langle \zeta^A, \zeta^B \rangle$. The adversary $\mathsf{B\text{-}then\text{-}A}$ does not corrupt any of the parties when the inputs are $(1, 0)$. When the inputs are $(0, 0)$ and $(0, 1)$, the first q' rounds, we define the adversary $\mathsf{B\text{-}then\text{-}A}$ to be the same as $\mathsf{B\text{-}only}$, *i.e.* for $j \in \{0, 1\}$,

$$\zeta^A_{\le q'}(0, j) = \gamma^A_{\le q'}(0, j) \qquad\qquad \zeta^B_{\le q'}(0, j) = \gamma^B_{\le q'}(0, j).$$

After round q', we define the adversary $\mathsf{B\text{-}then\text{-}A}$ inductively. Suppose that, for $m > q'$, $j \in \{0, 1\}$, the values $\zeta^A_{<m}(0, j)$ and $\zeta^B_{<m}(0, j)$ have been defined. This partial definition fixes the value of $\mathsf{type}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,j}, m)$ for $j \in \{0, 1\}$ and the value $k(m) = \#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, (0, m]) + \#\mathsf{RR}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, (q', m])$. We define:

$$\zeta^A_m(0,1) = \zeta^A_m(0,0) = \begin{cases} \lambda & ,\mathsf{type}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, m) \in \{\mathsf{TR}, \mathsf{TT}\} \\ f^B(0, \zeta^B_{<m}(0,0)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, m) \in \{\mathsf{RT}, \mathsf{RR}\} \text{ and } k(m) \le \theta T \\ f^B(1, \zeta^B_{<m}(0,1)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, m) \in \{\mathsf{RT}, \mathsf{RR}\} \text{ and } k(m) > \theta T \end{cases}.$$

$$\zeta^B_m(0,0) = \begin{cases} \lambda & ,\mathsf{type}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, m) \in \{\mathsf{RT}, \mathsf{TT}\} \\ f^A(0, \zeta^A_{<m}(0,0)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, m) \in \{\mathsf{TR}, \mathsf{RR}\} \end{cases}.$$

$$\zeta^B_m(0,1) = \begin{cases} \lambda & ,\mathsf{type}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,1}, m) \in \{\mathsf{RT}, \mathsf{TT}\} \\ f^A(0, \zeta^A_{<m}(0,1)) & ,\mathsf{type}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,1}, m) \in \{\mathsf{TR}, \mathsf{RR}\} \end{cases}.$$

We will denote using r the smallest value such that $k(r) \ge \theta T$. If no such value exists, we define $r = T + 1$. Observe that our definition of r satisfies $r \ge q'$: if $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}only}}, (0, q]) < \theta T$ then, by the definition of q', it holds that $q' = q$. In this case, since in the first q' rounds, $\mathsf{B\text{-}then\text{-}A}$ is the same as $\mathsf{B\text{-}only}$, we get $k(q') = \#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, (0, q'])+ \#\mathsf{RR}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}, (q', q']) < \theta T$, and therefore $r > q'$. Otherwise, we defined q' to be the smallest value such that $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}only}}, (0, q']) \ge \theta T$, and thus $r = q'$.

We have:

Lemma 4.6. *We have:*

(a) $\mathsf{corr}^A_{\le r}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0}) = \mathsf{corr}^A_{\le q'}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,0})$ *and* $\mathsf{corr}^A(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,1}) = \mathsf{corr}^A_{\le r}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,1})$.

(b) For $j \in \{0, 1\}$, *we have* $\mathsf{corr}^B(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,j}) = \mathsf{corr}^B_{\le q'}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A},0,j})$.

The adversary $\mathsf{Combine}$. Using $\mathsf{B\text{-}then\text{-}A}$, we define an adversary $\mathsf{Combine} = \langle \eta^A, \eta^B \rangle$ as follows:

$$\eta^A(0,0) = \zeta^A(0,0) \qquad\qquad \eta^B(0,0) = \gamma^B(0,0).$$

Also, define:

$$\begin{aligned} l^A &= \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) + \#\mathsf{RR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]). \\ l^B &= \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) + \#\mathsf{RR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]). \end{aligned} \tag{6}$$

We finish the proof by showing that Theorem 4.1 holds in all of the following exhaustive set of cases. We note that the only place where we use $\theta = \frac{5}{16}$ in this proof is in Equation 10 in the proof of item (c). All the other parts would work for any $\theta \geq \frac{2}{7}$.

Theorem 4.7. *We have:*

(a) If $r = T + 1$ or $l^A \leq 2\theta T - \#\mathsf{TR}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) - \#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A}}, (0, q'])$, then Theorem 4.1 holds.

(b) If $l^B \leq \theta T - L - \Delta$, then Theorem 4.1 holds.

(c) If $r \in [T]$ and $l^A + l^B \geq 3\theta T - L - \Delta - \#\mathsf{TR}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) - \#\mathsf{RT}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A}}, (0, q'])$, then Theorem 4.1 holds.

4.2 Proofs of the Lemmas in Theorem 4.1

In this section, we prove all the lemmas stated in the proof of Theorem 4.1. We use the same notation as subsection 4.1. We start with Lemma 4.2 that captures some observations about the adversary Basic.

Proof of Lemma 4.2. For all the parts, we upper bound the number of corruptions by upper bounding corr^A and corr^B using Equation 1.

(a) Let us start by showing that $\mathsf{corr}^A(\mathfrak{E}_{\mathsf{Basic},0,0}) = 0$. For this, consider any round m such that $\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m) = \mathsf{RT}$. For all such rounds m, the definition of Basic says that $\alpha^A_m(0,0) = f^B(0, \alpha^B_{<m}(0,0))$ implying that $\mathsf{corr}^A(\mathfrak{E}_{\mathsf{Basic},0,0}) = 0$.

To show that $\mathsf{corr}^B(\mathfrak{E}_{\mathsf{Basic},0,0}) = 0$, consider any round m such that $\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m) = \mathsf{TR}$. For all such rounds m, the definition of Basic says that $\alpha^B_m(0,0) = f^A(0, \alpha^A_{<m}(0,0))$ implying that $\mathsf{corr}^B(\mathfrak{E}_{\mathsf{Basic},0,0}) = 0$.

Analogous arguments show that $\mathsf{corr}^B(\mathfrak{E}_{\mathsf{Basic},0,1}) = \mathsf{corr}^A(\mathfrak{E}_{\mathsf{Basic},1,0}) = 0$.

(b) In order to upper bound $\mathsf{corr}^A_{\leq m}(\mathfrak{E}_{\mathsf{Basic},0,1})$ for $m \in [T]$, we consider any round $m' \leq m$ such that $\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,1}, m') = \mathsf{RT}$. By the definition of types, this means that $f^A(0, \alpha^A_{<m'}(0,1)) = \lambda$. We use the definition of Basic, saying that $\alpha^A_m(0,0) = \alpha^A_m(0,1)$ for all $m \in [T]$, to conclude that $f^A(0, \alpha^A_{<m'}(0,0)) = \lambda$. This implies $\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m') \in \{\mathsf{RT}, \mathsf{RR}\}$. If m' is such that $\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m') = \mathsf{RR}$, then $\alpha^A_m(0,1) = f^B(1, \alpha^B_{<m}(0,1))$ and the round m' does not count towards the corruptions. This means that the number of corruptions is upper bounded by the number of rounds m' such that $\mathsf{type}(\mathfrak{E}_{\mathsf{Basic},0,0}, m') = \mathsf{RT}$ implying $\mathsf{corr}^A_{\leq m}(\mathfrak{E}_{\mathsf{Basic},0,1}) \leq \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0, m])$.

(c) Proof of this part is similar to item (b) and is omitted.

□

Proof of Corollary 4.3. We prove assuming that $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0},(0,T]) \leq \theta T$. A similar argument shows the corollary assuming $\#\mathsf{TR}(\mathfrak{E}_{\mathsf{Basic},0,0},(0,T]) \leq \theta T$.

Let $\mathsf{Adv} = \langle g^A, g^B \rangle$ be an adversary that does not corrupt any of the parties when the inputs are $(1,0)$. When the inputs are $(0,0)$ or $(0,1)$, the adversary Adv behaves exactly like Basic. By construction we have

$$g^A(0,0) = \alpha^A(0,0) = \alpha^A(0,1) = g^A(0,1),$$

and the second property of Theorem 4.1 holds. It remains to show the first property. Observe that $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},1,0}) = 0$ by definition. Next, we have $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,0}) = \mathsf{corr}(\mathfrak{E}_{\mathsf{Basic},0,0}) = 0$ by Lemma 4.2. Finally, we have $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1}) = \mathsf{corr}(\mathfrak{E}_{\mathsf{Basic},0,1}) \leq \theta T$ due to Lemma 4.2 and our assumption that $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0},(0,T]) \leq \theta T$. □

Next, we show Lemma 4.4. We will make use of the following observation:

Observation 4.8. *For any adversaries $\mathsf{Adv} = \langle g^A, g^B \rangle, \mathsf{Adv}' = \langle g'^A, g'^B \rangle$, inputs $i, j, j' \in \{0,1\}$ and $m \in [T]$, if $g^A_{<m}(i,j) = g'^A_{<m}(i,j')$, then*

$$\mathsf{type}(\mathfrak{E}_{\mathsf{Adv},i,j}, m) \in \{\mathsf{TT}, \mathsf{TR}\} \iff \mathsf{type}(\mathfrak{E}_{\mathsf{Adv}',i,j'}, m) \in \{\mathsf{TT}, \mathsf{TR}\}.$$

An analogous result holds with B instead of A.

Proof of Lemma 4.4. We prove each part in turn.

(a) We only show the first claim as the second one is symmetric. Observe that for any round $m > p$ such that $\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}, m) = \mathsf{RT}$, we have that $f^B(1, \beta^B_{<m}(0,1)) = \beta^A_m(0,1)$. Also, for any round $m > p$ such that $\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}, m) = \mathsf{TR}$, we have that $f^A(0, \beta^A_{<m}(0,1)) = \beta^B_m(0,1)$. Together, we have that $\mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) = \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) = \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{Basic},0,1})$.

(b) We only show why $\mathsf{corr}^B(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}) = 0$ as the proof that $\mathsf{corr}^A(\mathfrak{E}_{\mathsf{B\text{-}only},0,0}) = 0$ is symmetric. Consider a round $m \in [T]$ such that $\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}, m) = \mathsf{TR}$. Using the definition of Basic if $m \leq p$ and the definition of $\mathsf{A\text{-}only}$ if $m > p$, we have that

$$f^A(0, \beta^A_{<m}(0,0)) = \beta^B_m(0,0),$$

implying that $\mathsf{corr}^B(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}) = 0$.

(c) We only show the first claim as the second one is similar. For any round $m \in [T]$ such that $\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},1,0}, m) = \mathsf{RT}$, using the definition of Basic if $m \leq p$ and the definition of $\mathsf{A\text{-}only}$ if $m > p$,

$$f^B(0, \beta^B_{<m}(1,0)) = \beta^A_m(1,0).$$

Thus, this round will not be counted as a corruption.

For any round $m \in [T]$ such that $\mathsf{type}(\mathfrak{E}_{\mathsf{A\text{-}only},1,0}, m) = \mathsf{TR}$, since $\beta^B_m(1,0) = \beta^B_m(0,0)$ for all $m \in [T]$, and by Observation 4.8 (used with $\mathsf{Adv}' = \mathsf{Adv}$), we have that

$\mathsf{type}(\mathfrak{E}_{\text{A-only},0,0}, m) \in \{\mathsf{TR}, \mathsf{RR}\}$. If $\mathsf{type}(\mathfrak{E}_{\text{A-only},0,0}, m) = \mathsf{RR}$, we have

$$f^A(1, \beta^A_{<m}(1,0)) = \beta^B_m(1,0).$$

We conclude a round m can only count to the number of corruptions if $\mathsf{type}(\mathfrak{E}_{\text{A-only},0,0}, m) = \mathsf{TR}$ and the claim follows.

□

Now, we show Lemma 4.6.

Proof of Lemma 4.6. We prove each part in turn.

(a) To show $\mathsf{corr}^A_{\leq r}(\mathfrak{E}_{\text{B-then-A},0,0}) = \mathsf{corr}^A_{\leq q'}(\mathfrak{E}_{\text{B-only},0,0})$, we simply observe that for all $m \in (q', r]$ such that $\mathsf{type}(\mathfrak{E}_{\text{B-then-A},0,0}, m) = \mathsf{RT}$, we have

$$f^B(0, \zeta^B_{<m}(0,0)) = \zeta^A_m(0,0).$$

Similarly to show that $\mathsf{corr}^A(\mathfrak{E}_{\text{B-then-A},0,1}) = \mathsf{corr}^A_{\leq r}(\mathfrak{E}_{\text{B-then-A},0,1})$, we observe that for all $m > r$ such that $\mathsf{type}(\mathfrak{E}_{\text{B-then-A},0,1}, m) = \mathsf{RT}$, since $\zeta^A_m(0,1) = \zeta^A_m(0,0)$ for all $m > r$, and by Observation 4.8 (used with $\mathsf{Adv}' = \mathsf{Adv}$), we have $\mathsf{type}(\mathfrak{E}_{\text{B-then-A},0,0}, m) = \{\mathsf{RT}, \mathsf{RR}\}$, and we get:

$$f^B(1, \zeta^B_{<m}(0,1)) = \zeta^A_m(0,1).$$

(b) To see why $\mathsf{corr}^B(\mathfrak{E}_{\text{B-then-A},0,j}) = \mathsf{corr}^B_{\leq q'}(\mathfrak{E}_{\text{B-then-A},0,j})$ for $j \in \{0,1\}$, note that for all $j \in \{0,1\}$, $m > q'$ such that $\mathsf{type}(\mathfrak{E}_{\text{B-then-A},0,j}, m) = \mathsf{TR}$, we have

$$f^A(0, \zeta^A_{<m}(0,j)) = \zeta^B_m(0,j).$$

□

4.3 Proof of Theorem 4.5

In this section, we prove Theorem 4.5. We use the same notation as subsection 4.1.

Proof. Our proof of Theorem 4.5 is roughly divided into two parts. We first show Theorem 4.1 assuming $L \geq (1-3\theta)T$. We then show that Theorem 4.1 also holds assuming $\Delta \geq (1-3\theta)T > L$.

Showing Theorem 4.1 when $L \geq (1-3\theta)T$. Let $\mathsf{Adv} = \langle g^A, g^B \rangle$ be an adversary that does not corrupt any of the parties when the inputs are $(1,0)$. When the inputs are $(0,0)$, the adversary Adv behaves like $\mathsf{2\text{-}Sided}$ till round q and does not corrupt any of the parties after that. Finally, when the inputs are $(0,1)$, the adversary Adv behaves like $\mathsf{A\text{-}only}$ till round q. Note that this means that

$$g^A_{\leq q}(0,0) = \delta^A_{\leq q}(0,0) = \beta^A_{\leq q}(0,0) = \beta^A_{\leq q}(0,1) = g^A_{\leq q}(0,1).$$

The adversary Adv then ensures that $g^A_{>q}(0,0) = g^A_{>q}(0,1)$ without corrupting Bob (only corrupting Alice) after round q. Since $g^A_{\leq q}(0,0) = g^A_{\leq q}(0,1)$ and $g^A_{>q}(0,0) = g^A_{>q}(0,1)$, the second property of Theorem 4.1 is satisfied.

For the first property, we have that $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},1,0}) = 0$ by definition. We also have:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,0}) = \mathsf{corr}_{\leq q}(\mathfrak{E}_{\mathsf{Adv},0,0}) &= \mathsf{corr}_{\leq q}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}) \\
&\leq \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) \\
&\leq \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{Basic}}) + \theta T \qquad \text{(Definitions of } \mathsf{2\text{-}Sided} \text{ and } q\text{)} \\
&= \theta T. \qquad \text{(Lemma 4.2)}
\end{aligned}$$

It remains to analyze $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1})$. If $q = T+1$, then we simply have

$$\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1}) = \mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) = \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{Basic},0,1}) \leq \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p]) \leq \theta T,$$

by Lemma 4.4, Lemma 4.2 and Equation 3. On the other hand, if $q \in [T]$, by our choice of q and L, we have

$$q - p \geq \#\mathsf{RR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) = L + \theta T. \tag{7}$$

We get:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1}) &\leq \mathsf{corr}_{\leq q}(\mathfrak{E}_{\mathsf{Adv},0,1}) + T - q \\
&\leq T + \mathsf{corr}_{\leq q}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) - p - (q-p) \\
&\leq T + \mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) - p - (L + \theta T) \qquad \text{(Equation 7)} \\
&\leq T + \mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) - (\theta T + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p])) - (L + \theta T) \\
&\qquad \text{(Equation 3)} \\
&\leq \theta T + \mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) - \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p]) \qquad \text{(Assumption } L \geq (1-3\theta)\,T\text{)} \\
&\leq \theta T. \qquad \text{(Lemma 4.4 and Lemma 4.2)}
\end{aligned}$$

Showing Theorem 4.1 when $\Delta \geq (1-3\theta)\,T > L$. For this part of the proof, we define z to be the smallest such that $\#\mathsf{RT}(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}, (p,z]) \geq \theta T$. If no such value exists, define $z = T+1$. We start by showing that $z \geq q$ (also recall that $q \geq p$). For this it is enough to show that

$$\begin{aligned}
\#\mathsf{RT}(\mathfrak{E}_{\mathsf{A\text{-}only},0,0}, (p,q]) &\leq \#\mathsf{RT}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) + \#\mathsf{RR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) \qquad \text{(Observation 4.8)} \\
&< \#\mathsf{RT}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,q]) \qquad \text{(As } L < \Delta\text{)} \\
&\leq \theta T. \qquad \text{(Definition of } q\text{)}
\end{aligned}$$

Now, let $\mathsf{Adv} = \langle g^A, g^B \rangle$ be an adversary that does not corrupt any of the parties when the inputs are $(1,0)$. When the inputs are $(0,0)$, the adversary Adv behaves like $\mathsf{A\text{-}only}$ till round z and does not corrupt any of the parties after that. Finally, when the inputs are

$(0,1)$, the adversary Adv behaves like $\mathsf{A\text{-}only}$ till round z. Note that this means that

$$g^A_{\leq z}(0,0) = \beta^A_{\leq z}(0,0) = \beta^A_{\leq z}(0,1) = g^A_{\leq z}(0,1).$$

The adversary Adv then ensures that $g^A_{>z}(0,0) = g^A_{>z}(0,1)$ without corrupting Bob (only corrupting Alice) after round z. Since $g^A_{\leq z}(0,0) = g^A_{\leq z}(0,1)$ and $g^A_{>z}(0,0) = g^A_{>z}(0,1)$, the second property of Theorem 4.1 is satisfied.

For the first property, we have that $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},1,0}) = 0$ by definition. We also have:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,0}) = \mathsf{corr}_{\leq z}(\mathfrak{E}_{\mathsf{Adv},0,0}) &= \mathsf{corr}_{\leq z}(\mathfrak{E}_{\mathsf{A\text{-}only}}) \\
&\leq \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{A\text{-}only}}) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{A\text{-}only}}, (p,z]) && \text{(Lemma 4.4)} \\
&\leq \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{Basic}}) + \theta T && \text{(Definitions of } \mathsf{A\text{-}only} \text{ and } z) \\
&= \theta T. && \text{(Lemma 4.2)}
\end{aligned}$$

It remains to analyze $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1})$. If $z = T+1$, then we simply have

$$\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1}) = \mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) = \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{Basic},0,1}) \leq \theta T,$$

by Lemma 4.4, Lemma 4.2 and Equation 3. On the other hand, if $z \in [T]$, we have

$$\begin{aligned}
z - p &\geq \#\mathsf{TT}(\mathfrak{E}_{\mathsf{A\text{-}only}}, (p,z]) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{A\text{-}only}}, (p,z]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{A\text{-}only}}, (p,z]) \\
&\geq \#\mathsf{TR}(\mathfrak{E}_{\mathsf{2\text{-}Sided}}, (p,z]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{A\text{-}only}}, (p,z]) && \text{(Observation 4.8)} \\
&\geq \Delta + \theta T. && \text{(Definitions of } \Delta \text{ and } z\text{, and } z \geq q)
\end{aligned}$$

Using this, we get:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1}) &\leq \mathsf{corr}_{\leq z}(\mathfrak{E}_{\mathsf{Adv},0,1}) + T - z \\
&\leq T + \mathsf{corr}_{\leq z}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) - p - (z - p) \\
&\leq T + \mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) - p - (\Delta + \theta T) \\
&\leq T + \mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) - (\theta T + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p])) - (\Delta + \theta T) \\
& && \text{(Equation 3)} \\
&\leq \theta T + \mathsf{corr}(\mathfrak{E}_{\mathsf{A\text{-}only},0,1}) - \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Basic},0,0}, (0,p]) && \text{(Assumption } \Delta \geq (1-3\theta)\,T) \\
&\leq \theta T. && \text{(Lemma 4.4 and Lemma 4.2)}
\end{aligned}$$

□

4.4 Proof of Theorem 4.7

In this section, we prove Theorem 4.7. We prove each part separately and use the same notation as subsection 4.1.

4.4.1 Proving item (a)

Proof of item (a) of Theorem 4.7. Let $\mathsf{Adv} = \mathsf{B\text{-}then\text{-}A}$. The second property of Theorem 4.1 holds by construction.

For the first property, we observe that $\mathsf{corr}(\mathfrak{C}_{\mathsf{Adv},1,0}) = 0$ by definition. By Theorem 4.5, if $\max(L, \Delta) \geq (1-3\theta)T$, then Theorem 4.1 holds, and we are done. Thus, we assume $L, \Delta < (1-3\theta)T$. We have:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}) &\leq \mathsf{corr}^{B}_{\leq q'}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}) + \mathsf{corr}^{A}_{\leq q'}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}, (r, T]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Lemma 4.6)} \\
&\leq \mathsf{corr}^{B}_{\leq q'}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}) + \mathsf{corr}^{A}_{\leq q'}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}, (r, T]) \\
&\leq \mathsf{corr}^{B}_{\leq q'}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}, (r, T]) && \text{(Lemma 4.4)} \\
&\leq \mathsf{corr}^{B}_{\leq p}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}) + \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}, (p, q']) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}, (r, T]) \\
&\leq \mathsf{corr}^{B}_{\leq p}(\mathfrak{C}_{\mathsf{Basic},0,0}) + \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}, (p, q']) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}, (r, T]) \\
&\leq \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}, (p, q']) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}, (r, T]). && \text{(Lemma 4.2)}
\end{aligned}$$

If $r = T + 1$, we continue as follows:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}) &\leq \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}, (p, q']) \\
&\leq \#\mathsf{TR}(\mathfrak{C}_{\mathsf{2\text{-}Sided},0,0}, (p, q']) + \#\mathsf{RR}(\mathfrak{C}_{\mathsf{2\text{-}Sided},0,0}, (p, q']) && \text{(Observation 4.8)} \\
&\leq \Delta + L && \text{(As } q' \leq q \text{, Equation 4)} \\
&\leq 2T(1-3\theta) && (L, \Delta < (1-3\theta)T) \\
&\leq \theta T. && (\theta \geq 2/7)
\end{aligned}$$

If $r \in [T]$, we continue as follows:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}) &\leq \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}only},0,0}, (p, q']) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,0}, (r, T]) \\
&\leq \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{Combine}}, (r, T]) + \#\mathsf{RR}(\mathfrak{C}_{\mathsf{Combine}}, (r, T]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Observation 4.8)} \\
&\leq l^{A} + \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) - \#\mathsf{RT}(\mathfrak{C}_{\mathsf{Combine}}, (q', r]) - \#\mathsf{RR}(\mathfrak{C}_{\mathsf{Combine}}, (q', r]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Equation 6)} \\
&\leq l^{A} + \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) - \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A}}, (q', r]) - \#\mathsf{RR}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A}}, (q', r]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(Observation 4.8)} \\
&\leq l^{A} + \#\mathsf{TR}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A}}, (0, q']) - \theta T && \text{(As } r \in [T]) \\
&\leq \theta T,
\end{aligned}$$

by our assumption on l^{A}. Finally, we analyze $\mathsf{corr}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,1})$.

$$\begin{aligned}
\mathsf{corr}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,1}) &\leq \mathsf{corr}^{A}_{\leq r}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,1}) + \mathsf{corr}^{B}_{\leq q'}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,1}) && \text{(Lemma 4.6)} \\
&\leq \mathsf{corr}_{\leq q'}(\mathfrak{C}_{\mathsf{B\text{-}only},0,1}) + \#\mathsf{RT}(\mathfrak{C}_{\mathsf{B\text{-}then\text{-}A},0,1}, (q', r])
\end{aligned}$$

$$\begin{aligned}
&\leq \mathsf{corr}_{\leq q'}(\mathfrak{E}_{\textsf{B-only},0,1}) + \#\mathsf{RT}(\mathfrak{E}_{\textsf{B-then-A},0,0}, (q', r]) + \#\mathsf{RR}(\mathfrak{E}_{\textsf{B-then-A},0,0}, (q', r]) \\
&\hfill \text{(Observation 4.8)} \\
&\leq \#\mathsf{RT}(\mathfrak{E}_{\textsf{B-only},0,0}, (0, q']) + \#\mathsf{RT}(\mathfrak{E}_{\textsf{B-then-A},0,0}, (q', r]) + \#\mathsf{RR}(\mathfrak{E}_{\textsf{B-then-A},0,0}, (q', r]) \\
&\hfill \text{(Lemma 4.4)} \\
&\leq \#\mathsf{RT}(\mathfrak{E}_{\textsf{B-then-A},0,0}, (0, r]) + \#\mathsf{RR}(\mathfrak{E}_{\textsf{B-then-A},0,0}, (q', r]) \leq \theta T,
\end{aligned}$$

by definition of r.

□

4.4.2 Proving item (b)

Proof of item (b) of Theorem 4.7. Let $\mathsf{Adv} = \langle g^A, g^B \rangle$ be an adversary that does not corrupt any of the parties when the inputs are $(0,1)$. When the inputs are $(0,0)$ or $(1,0)$, the adversary Adv behaves the same as $\textsf{B-only}$. By the definition of $\textsf{B-only}$, we have $g^B(0,0) = g^B(1,0)$ and the second property of Theorem 4.1 holds. It remains to show the first property.

For this property, we have $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1}) = 0$ by definition. We also have:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,0}) &= \mathsf{corr}(\mathfrak{E}_{\textsf{B-only},0,0}) \\
&= \mathsf{corr}^B(\mathfrak{E}_{\textsf{B-only},0,0}) && \text{(Lemma 4.4)} \\
&\leq \mathsf{corr}^B_{\leq p}(\mathfrak{E}_{\textsf{B-only},0,0}) + \#\mathsf{TR}(\mathfrak{E}_{\textsf{B-only},0,0}, (p, q]) + \#\mathsf{TR}(\mathfrak{E}_{\textsf{B-only},0,0}, (q, T]) \\
&= \#\mathsf{TR}(\mathfrak{E}_{\textsf{B-only},0,0}, (p, q]) + \#\mathsf{TR}(\mathfrak{E}_{\textsf{B-only},0,0}, (q, T]) && \text{(Lemma 4.2)} \\
&\leq \#\mathsf{TR}(\mathfrak{E}_{\textsf{2-Sided}}, (p, q]) + \#\mathsf{RR}(\mathfrak{E}_{\textsf{2-Sided}}, (p, q]) \\
&\qquad + \#\mathsf{TR}(\mathfrak{E}_{\textsf{Combine}}, (q, T]) + \#\mathsf{RR}(\mathfrak{E}_{\textsf{Combine}}, (q, T]) && \text{(Observation 4.8)} \\
&\leq \Delta + L + l^B && \text{(Equation 4, Equation 6 and } q' \leq q\text{)} \\
&\leq \theta T. && \text{(Assumption } l^B \leq \theta T - L - \Delta\text{)}
\end{aligned}$$

Finally, we analyze $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},1,0})$. We have:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},1,0}) &= \mathsf{corr}(\mathfrak{E}_{\textsf{B-only},1,0}) \\
&= \mathsf{corr}_{\leq p}(\mathfrak{E}_{\textsf{Basic},1,0}) && \text{(Lemma 4.4)} \\
&\leq \theta T. && \text{(Lemma 4.2 and Equation 3)}
\end{aligned}$$

□

4.4.3 Proving item (c)

We prove of item (c) of Theorem 4.7. The proof uses the following lemma.

Lemma 4.9. *If $r \in [T]$ and $l^A + l^B \geq 3\theta T - L - \Delta - \#\mathsf{TR}(\mathfrak{E}_{\textsf{B-then-A}}, (p, q']) -$*

$\#\mathsf{RT}(\mathfrak{E}_{\text{B-then-A}},(0,q'])$, *we have*

$$2T \geq \#\mathsf{RT}(\mathfrak{E}_{\text{Combine}},(q',T]) + \#\mathsf{TR}(\mathfrak{E}_{\text{Combine}},(q',T]) + \#\mathsf{TR}(\mathfrak{E}_{\text{B-then-A}},(p,q']) + 6\theta T - L - 2\Delta.$$

Proof. We use the following inequalities:

$$\begin{aligned}
p &\geq \#\mathsf{RT}(\mathfrak{E}_{\text{B-then-A}},(0,p]) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-then-A}},(0,p]) + \#\mathsf{TR}(\mathfrak{E}_{\text{B-then-A}},(0,p]) \\
&= \#\mathsf{RT}(\mathfrak{E}_{\text{B-then-A}},(0,p]) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-then-A}},(0,p]) + \#\mathsf{TR}(\mathfrak{E}_{\text{Basic}},(0,p]) \\
&= \#\mathsf{RT}(\mathfrak{E}_{\text{B-then-A}},(0,p]) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-then-A}},(0,p]) + \theta T. && \text{(Equation 3)} \\
q'-p &\geq \#\mathsf{RT}(\mathfrak{E}_{\text{B-then-A}},(p,q']) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-then-A}},(p,q']) + \#\mathsf{TR}(\mathfrak{E}_{\text{B-then-A}},(p,q']). \\
T-q' &\geq \#\mathsf{RT}(\mathfrak{E}_{\text{Combine}},(q',T]) + \#\mathsf{TR}(\mathfrak{E}_{\text{Combine}},(q',T]) + \#\mathsf{RR}(\mathfrak{E}_{\text{Combine}},(q',T]).
\end{aligned}$$

Multiplying the last inequality by 2 and using Equation 6, we get:

$$2T - 2q' \geq \#\mathsf{RT}(\mathfrak{E}_{\text{Combine}},(q',T]) + \#\mathsf{TR}(\mathfrak{E}_{\text{Combine}},(q',T]) + l^A + l^B. \tag{8}$$

Adding the lower bounds on $p, q'-p$, we get:

$$q' \geq \#\mathsf{RT}(\mathfrak{E}_{\text{B-then-A}},(0,q']) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-then-A}},(0,q']) + \#\mathsf{TR}(\mathfrak{E}_{\text{B-then-A}},(p,q']) + \theta T.$$

We use this to continue Equation 8 as follows:

$$\begin{aligned}
2T &\geq \#\mathsf{RT}(\mathfrak{E}_{\text{Combine}},(q',T]) + \#\mathsf{TR}(\mathfrak{E}_{\text{Combine}},(q',T]) + l^A + l^B + 2\theta T \\
&\quad + 2\cdot\#\mathsf{RT}(\mathfrak{E}_{\text{B-then-A}},(0,q']) + 2\cdot\#\mathsf{TT}(\mathfrak{E}_{\text{B-then-A}},(0,q']) + 2\cdot\#\mathsf{TR}(\mathfrak{E}_{\text{B-then-A}},(p,q']) \\
&\geq \#\mathsf{RT}(\mathfrak{E}_{\text{Combine}},(q',T]) + \#\mathsf{TR}(\mathfrak{E}_{\text{Combine}},(q',T]) + 5\theta T - L - \Delta \\
&\quad + \#\mathsf{RT}(\mathfrak{E}_{\text{B-then-A}},(0,q']) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-then-A}},(0,q']) + \#\mathsf{TR}(\mathfrak{E}_{\text{B-then-A}},(p,q']) \\
&= \#\mathsf{RT}(\mathfrak{E}_{\text{Combine}},(q',T]) + \#\mathsf{TR}(\mathfrak{E}_{\text{Combine}},(q',T]) + 5\theta T - L - \Delta \\
&\quad + \#\mathsf{RT}(\mathfrak{E}_{\text{B-only}},(0,q']) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-only}},(0,q']) + \#\mathsf{TR}(\mathfrak{E}_{\text{B-then-A}},(p,q']).
\end{aligned} \tag{9}$$

We now consider two cases and analyze the term $\#\mathsf{RT}(\mathfrak{E}_{\text{B-only}},(0,q'])+\#\mathsf{TT}(\mathfrak{E}_{\text{B-only}},(0,q'])$ in each case. If $\#\mathsf{RT}(\mathfrak{E}_{\text{B-only}},(0,q]) < \theta T$, then we have $q' = q \leq r \leq T$ and:

$$\begin{aligned}
&\#\mathsf{RT}(\mathfrak{E}_{\text{B-only}},(0,q']) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-only}},(0,q']) \\
&\qquad = \#\mathsf{RT}(\mathfrak{E}_{\text{B-only}},(0,q]) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-only}},(0,q]) \\
&\qquad = \#\mathsf{RT}(\mathfrak{E}_{\text{2-Sided}},(0,q]) + \#\mathsf{TT}(\mathfrak{E}_{\text{2-Sided}},(0,q]) && \text{(Observation 4.8)} \\
&\qquad \geq \#\mathsf{RT}(\mathfrak{E}_{\text{2-Sided}},(p,q]) \\
&\qquad \geq \theta T - \Delta. && \text{(As } q \in [T] \text{ and Equation 4)}
\end{aligned}$$

Otherwise, we have

$$\#\mathsf{RT}(\mathfrak{E}_{\text{B-only}},(0,q']) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-only}},(0,q']) \geq \#\mathsf{RT}(\mathfrak{E}_{\text{B-only}},(0,q']) = \theta T \geq \theta T - \Delta.$$

Thus, in either case, we have $\#\mathsf{RT}(\mathfrak{E}_{\text{B-only}},(0,q']) + \#\mathsf{TT}(\mathfrak{E}_{\text{B-only}},(0,q']) \geq \theta T - \Delta$. Plugging into Equation 9, we get:

$$2T \geq \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) + 6\theta T - L - 2\Delta.$$

□

Proof of item (c) of Theorem 4.7. Let the $\mathsf{Adv} = \langle g^A, g^B \rangle$ be such that there are no corruptions when the inputs are $(0, 1)$. When the inputs are $(0, 0)$, the adversary Adv behaves like as $\mathsf{Combine}$. When the inputs are $(1, 0)$, the adversary Adv behaves like as $\mathsf{B\text{-}only}$. By the definition of $\mathsf{Combine}$, we have $g^B(0, 0) = g^B(1, 0)$ and the second property of Theorem 4.1 is satisfied.

For the first property, we start by observing that $\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,1}) = 0$ by definition. Also

$$\begin{aligned}
\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,0}) &= \mathsf{corr}(\mathfrak{E}_{\mathsf{Combine}}) \\
&\leq \mathsf{corr}_{\leq q'}(\mathfrak{E}_{\mathsf{Combine}}) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) \\
&= \mathsf{corr}_{\leq q'}(\mathfrak{E}_{\mathsf{B\text{-}only}}) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) \\
&= \mathsf{corr}^B_{\leq q'}(\mathfrak{E}_{\mathsf{B\text{-}only}}) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{Lemma 4.4}) \\
&\leq \mathsf{corr}^B_{\leq p}(\mathfrak{E}_{\mathsf{B\text{-}only}}) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{B\text{-}only}}, (p, q']) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) \\
&\qquad + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) \\
&\leq \mathsf{corr}^B_{\leq p}(\mathfrak{E}_{\mathsf{Basic}}) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) \\
&\qquad + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) \\
&\leq \#\mathsf{TR}(\mathfrak{E}_{\mathsf{B\text{-}then\text{-}A}}, (p, q']) + \#\mathsf{TR}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) + \#\mathsf{RT}(\mathfrak{E}_{\mathsf{Combine}}, (q', T]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{Lemma 4.2}) \\
&\leq 2T(1 - 3\theta) + L + 2\Delta. \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\text{Lemma 4.9})
\end{aligned}$$

By Theorem 4.5, if $\max(L, \Delta) \geq (1 - 3\theta)\, T$, then Theorem 4.1 holds, and we are done. Thus, we assume $L, \Delta < (1 - 3\theta)\, T$. We get

$$\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,0}) \leq 2T(1 - 3\theta) + L + 2\Delta \leq 5T(1 - 3\theta).$$

To finish, we use $\theta = \frac{5}{16}$ to get

$$\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},0,0}) \leq 5T(1 - 3\theta) \leq \theta T. \tag{10}$$

Finally, we have:

$$\begin{aligned}
\mathsf{corr}(\mathfrak{E}_{\mathsf{Adv},1,0}) &= \mathsf{corr}(\mathfrak{E}_{\mathsf{B\text{-}only},1,0}) \\
&= \mathsf{corr}_{\leq p}(\mathfrak{E}_{\mathsf{Basic},1,0}) \qquad\qquad\qquad\qquad\qquad (\text{Lemma 4.4}) \\
&\leq \theta T. \qquad\qquad\qquad\qquad\qquad (\text{Lemma 4.2 and Equation 3})
\end{aligned}$$

□

5 The $\frac{5}{16}$ Error Resilient Protocol

We now show the "upper-bound" part of Theorem 1.1. This is formalized in Theorem 5.1 below:

Theorem 5.1. *Let $n \in \mathbb{N}$ and $\epsilon > 0$. There exists a set $\Gamma, |\Gamma| = 2^{n+1}$ and a deterministic, adaptive protocol Π of length $T = \mathcal{O}\left(\frac{1}{\epsilon}\right)$ that solves the n-length message exchange problem with error tolerance $\theta = \frac{5}{16} - \epsilon$ over Γ.*

The proof of Theorem 5.1 spans the remainder of this section. Fix $n \in \mathbb{N}, \epsilon > 0$ and let $\Gamma = \{0,1\}^{n+1}$. We assume without loss of generality that $\frac{1}{\epsilon}$ is an integer and a multiple of 24. We define a protocol Π for Alice and Bob in Algorithm 1 and Algorithm 2 respectively and show that this protocol satisfies Theorem 5.1.

5.1 Our Protocols

We begin with some notation. We will use $x \in \{0,1\}^n$ to denote the input of Alice and $y \in \{0,1\}^n$ to denote the input of Bob. Define $N = \frac{1}{\epsilon}$. The length of our protocol is $T = 16N = \frac{16}{\epsilon}$. We divide the $16N$ rounds in our protocol into 5 stages. We define $\mathsf{stageA} = [6N]$, $\mathsf{stageB}(0) = (6N, 8N]$, $\mathsf{stageB}(1) = (8N, 11N]$, $\mathsf{stageB}(2) = (11N, 15N]$, and $\mathsf{stageC} = (15N, 16N]$. Define $\mathsf{NA\text{-}Bob} = (6N, 8N] \cup \{8N+1, 8N+3, 8N+4, 8N+6, \cdots, 11N-2, 11N\} \cup \{11N+2, 11N+4, 11N+6, \cdots, 15N\}$. Observe that $|\mathsf{NA\text{-}Bob}| = 6N$. We break ties in all the $\arg\max$ in our protocols arbitrarily.

5.2 Protocol Analysis

This section shows that the protocol, Π, given in Algorithm 1 and Algorithm 2 solves the n-length message exchange problem with error tolerance $\theta = \frac{5}{16} - \epsilon$ over Γ, thereby proving Theorem 5.1. In order to show this, we show that for all adversaries $\mathsf{Adv} = \langle g^A, g^B \rangle$ and $x, y \in \{0,1\}^n$, we have:

$$\mathsf{corr}(\langle \Pi, x, y, \mathsf{Adv} \rangle) \leq \lceil \theta T \rceil \implies \tilde{y} = y \wedge \tilde{x} = x.$$

For the rest of the text, fix inputs $x, y \in \{0,1\}^n$ and an adversary $\mathsf{Adv} = \langle g^A, g^B \rangle$ for our protocol with $\mathsf{corr}(\mathfrak{E}) < 5N - 5$, where $\mathfrak{E} = \langle \Pi, x, y, \mathsf{Adv} \rangle$. As explained in subsection 3.1, fixing $\mathfrak{E}$ describes an execution of the protocol completely, and fixing $\mathfrak{E}$ also fixes the types of the rounds and the values of all the variables used by Algorithm 1 and Algorithm 2 at any point in this execution. From now on, we omit the parameter $\mathfrak{E}$ and write, for example, $\mathsf{corr}_{\leq T}$ instead of $\mathsf{corr}_{\leq T}(\mathfrak{E})$, *etc.* We use RR to denote the set of rounds where both parties are receiving, *i.e.* all rounds $m \in [T]$ such that $\mathsf{type}(\mathfrak{E}, m) = \mathsf{RR}$, and RT, TT, TR, are defined analogously.

Note that both Algorithm 1 and Algorithm 2 loop over $i \in [16N]$. We use var_i to denote the value of a variable var at the end of iteration i (here var may be any of the variables

Algorithm 1 Alice's side of our protocol

```
Input: String $x \in \{0,1\}^n$.
Output: String $\tilde{y} \in \{0,1\}^n$.
$\forall s \in \{0,1\}^n : \mathsf{sv}(s), \mathsf{uv}(s) \leftarrow 0$.
$\mathsf{buf} \leftarrow 6N$.
$isBobSure \leftarrow \mathsf{False}$.
for all $i \in [16N]$ do
    if $i \in \mathsf{NA\text{-}Bob}$ or $isBobSure$ or $\mathsf{buf} = 0$ then
        Receive $(\hat{y}, sure)$ from Bob.
        if $sure$ or $isBobSure$ or $i \notin \mathsf{NA\text{-}Bob}$ then
            $\mathsf{sv}(\hat{y}) \leftarrow \mathsf{sv}(\hat{y}) + 1$.
        else
            if $\mathsf{uv}(\hat{y}) = \max_{t \in \{0,1\}^n} \mathsf{uv}(t)$ then
                $\mathsf{buf} \leftarrow \min(N, \mathsf{buf} + 1)$.
            end if
            $\mathsf{uv}(\hat{y}) \leftarrow \mathsf{uv}(\hat{y}) + 1$.
        end if
    else
        Send $x$ to Bob.
        $\mathsf{buf} \leftarrow \mathsf{buf} - 1$.
    end if
    if $i + |\mathsf{NA\text{-}Bob} \cap [i]| - \max_{t \in \{0,1\}^n} \mathsf{uv}(t) - \sum_{t \in \{0,1\}^n} \mathsf{sv}(t) + \mathsf{uv}(t) \geq 10N$ then
        $isBobSure \leftarrow \mathsf{True}$.
    end if
end for
$\forall s \in \{0,1\}^n : \mathsf{tv}(s) \leftarrow \mathsf{sv}(s) + \mathsf{uv}(s) \cdot \mathbb{1}\left(\mathsf{uv}(s) < \max_{t \in \{0,1\}^n} \mathsf{uv}(t)\right)$.
if $\max_{t \in \{0,1\}^n} \mathsf{tv}(t) \geq \sum_{t \in \{0,1\}^n} \mathsf{sv}(t) + \mathsf{uv}(t) - 5N$ then
    Output $\tilde{y} \leftarrow \arg\max_{t \in \{0,1\}^n} \mathsf{tv}(t)$.
else
    Output $\tilde{y} \leftarrow \arg\max_{t \in \{0,1\}^n} \mathsf{sv}(t) + \mathsf{uv}(t)$.
end if
```

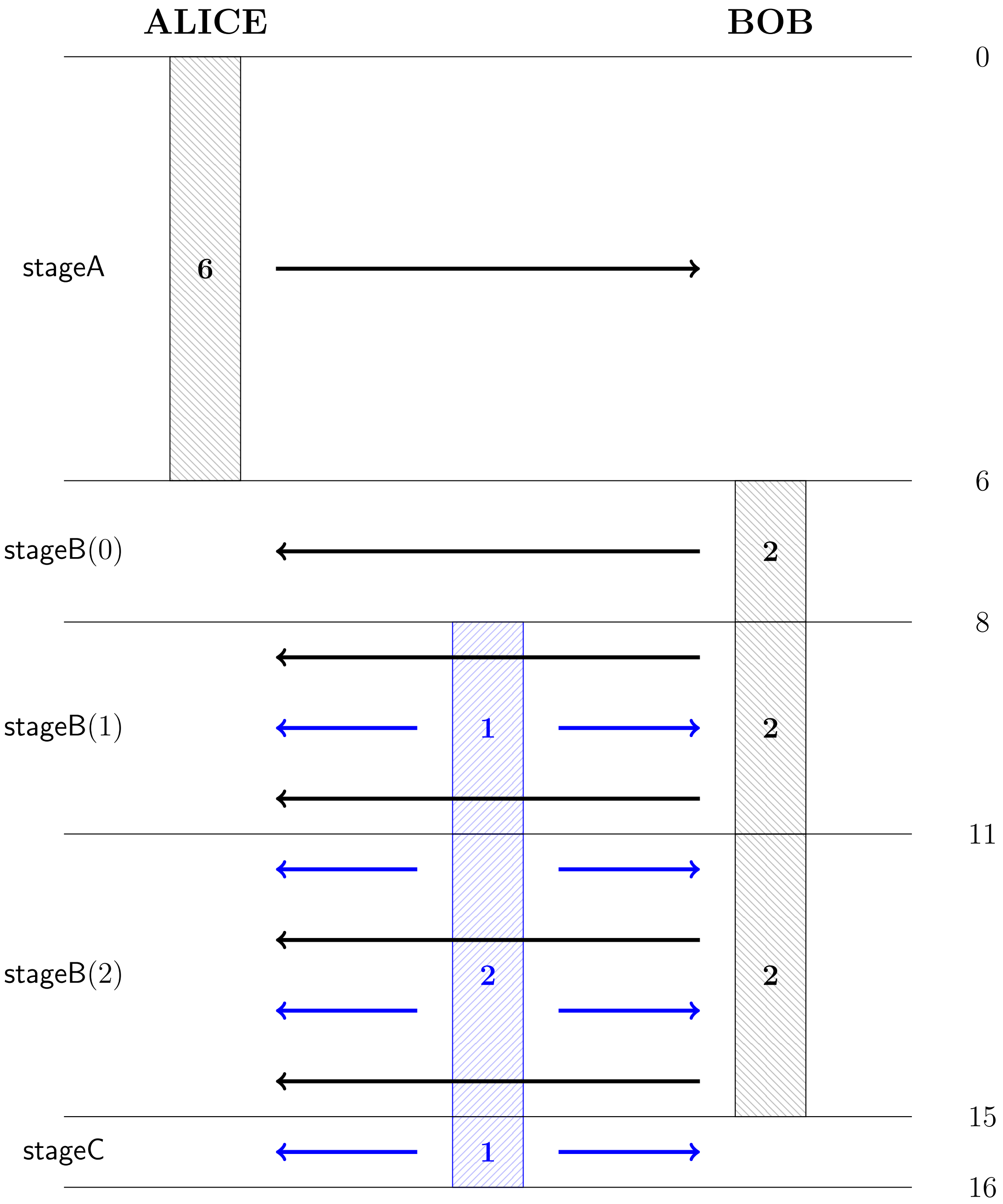

Figure 2: A depiction of the 5 stages in our protocol in section 5 with their relative lengths.

Algorithm 2 Bob's side of our protocol

```
Input: String $y \in \{0,1\}^n$.
Output: String $\tilde{x} \in \{0,1\}^n$.
29: $\forall s \in \{0,1\}^n : \mathsf{v}(s) \leftarrow 0$.
30: $isSure \leftarrow \mathsf{False}$.
31: for all $i \in [16N]$ do
32:     if $isSure$ or $i \in \mathsf{NA\text{-}Bob}$ then
33:         Send $(y, isSure)$ to Alice.
34:     else
35:         Receive $\hat{x}$ from Alice.
36:         $\mathsf{v}(\hat{x}) \leftarrow \mathsf{v}(\hat{x}) + 1$.
37:         if $\mathsf{v}(\hat{x}) \geq 5N$ then
38:             $isSure \leftarrow \mathsf{True}$.
39:         end if
40:     end if
41: end for
42: Output $\tilde{x} \leftarrow \arg\max_{t \in \{0,1\}^n} \mathsf{v}(t)$.
```

used by the protocols or one of the previously defined values *e.g.*, corr_i will denote $\mathsf{corr}_{\leq i}$, *etc.*). The notation var_0 will denote the value of var at the beginning of the protocol. We omit the subscript when we refer to the value of var at the end of the protocol, *i.e.* var_{16N}. We also omit the subscript when making claims like, *"the value of the variable var only increases"*. These two cases can be differentiated from context.

As we chose the variables in Algorithm 1 and Algorithm 2 to be disjoint, we will leave implicit which protocol a particular variable belongs to. We also use the convention that $\mathsf{True} = 1$ and $\mathsf{False} = 0$, and treat boolean values as numeric (*e.g.*, we can write $\mathsf{True} > \mathsf{False}$).

5.2.1 Structural Lemmas About Our Protocol

We start with some simple observations about our protocol.

Observation 5.2. *We have:*

1. *In every iteration, the value of each of the numeric (and boolean) variables, except* buf*, used by Algorithm 1 and Algorithm 2, can either increase by* 1 *or stay unchanged. The same holds for the value of* $\sum_{t \in \{0,1\}^n} \mathsf{sv}(t) + \mathsf{uv}(t)$ *and the value in Line 20,* i.e.

$$i + |\mathsf{NA\text{-}Bob} \cap [i]| - \max_{t \in \{0,1\}^n} \mathsf{uv}(t) - \sum_{t \in \{0,1\}^n} \mathsf{sv}(t) + \mathsf{uv}(t).$$

The value of buf *can either increase by 1, stay unchanged, or decrease by* 1.

2. *For all* $i \in [16N]$*, we have* $|(\mathsf{RR} \cup \mathsf{RT}) \cap [i]| = \sum_{t \in \{0,1\}^n} \mathsf{sv}_i(t) + \mathsf{uv}_i(t)$.

3. $\mathsf{NA\text{-}Bob} \subseteq \mathsf{RT}$.

4. *For all $i \in [6N]$, we have $\mathsf{buf}_i = 6N - i$ and $i \in \mathsf{TR} \cup \mathsf{TT}$.*

Bounding the number of times Alice transmits. The following lemma contains what we show about the set $\mathsf{TT} \cup \mathsf{TR}$ of all the iterations where Alice transmits.

Lemma 5.3. *We have $[6N] \subseteq \mathsf{TT} \cup \mathsf{TR}$ and for all $6N \leq i \leq i'$*

$$-2N \leq |(\mathsf{TR} \cup \mathsf{TT}) \cap (i, i']| + \mathsf{buf}_{i'} - \mathsf{buf}_i - \left(\max_{t \in \{0,1\}^n} \mathsf{uv}_{i'}(t) - \max_{t \in \{0,1\}^n} \mathsf{uv}_i(t) \right) \leq 0.$$

Furthermore, if $\mathsf{buf}_{i''-1} < N$ for all $i'' \in (i, i'] \cap (\mathsf{RT} \cup \mathsf{RR})$, we have:

$$|(\mathsf{TR} \cup \mathsf{TT}) \cap (i, i']| + \mathsf{buf}_{i'} - \mathsf{buf}_i - \left(\max_{t \in \{0,1\}^n} \mathsf{uv}_{i'}(t) - \max_{t \in \{0,1\}^n} \mathsf{uv}_i(t) \right) = 0.$$

Proof. The claim $6N \subseteq \mathsf{TT} \cup \mathsf{TR}$ follows from item 4 in Observation 5.2. For the other claim, we observe that:

$$\begin{aligned}
\mathsf{buf}_{i'} - \mathsf{buf}_i &= \sum_{i'' \in (i, i']} \mathsf{buf}_{i''} - \mathsf{buf}_{i''-1} \\
&= \sum_{i'' \in (i, i'] \cap (\mathsf{TR} \cap \mathsf{TT})} \mathsf{buf}_{i''} - \mathsf{buf}_{i''-1} + \sum_{i'' \in (i, i'] \cap (\mathsf{RT} \cup \mathsf{RR})} \mathsf{buf}_{i''} - \mathsf{buf}_{i''-1} \\
&= -|(\mathsf{TR} \cup \mathsf{TT}) \cap (i, i']| + \sum_{i'' \in (i, i'] \cap (\mathsf{RT} \cup \mathsf{RR})} \mathbb{1}\left(\mathsf{buf}_{i''} - \mathsf{buf}_{i''-1} = 1\right).
\end{aligned}$$

Next, we observe that, for all $i'' \in (i, i'] \cap (\mathsf{RT} \cup \mathsf{RR})$, we have:

$$\mathbb{1}\left(\mathsf{buf}_{i''} - \mathsf{buf}_{i''-1} = 1\right) = \mathbb{1}\left(\max_{t \in \{0,1\}^n} \mathsf{uv}_{i''}(t) - \max_{t \in \{0,1\}^n} \mathsf{uv}_{i''-1}(t) = 1 \right) \cdot \mathbb{1}\left(\mathsf{buf}_{i''-1} < N\right).$$

This immediately gives:

$$\begin{aligned}
\mathsf{buf}_{i'} - \mathsf{buf}_i &\leq -|(\mathsf{TR} \cup \mathsf{TT}) \cap (i, i']| + \sum_{i'' \in (i, i'] \cap (\mathsf{RT} \cup \mathsf{RR})} \mathbb{1}\left(\max_{t \in \{0,1\}^n} \mathsf{uv}_{i''}(t) - \max_{t \in \{0,1\}^n} \mathsf{uv}_{i''-1}(t) = 1 \right) \\
&= -|(\mathsf{TR} \cup \mathsf{TT}) \cap (i, i']| + \max_{t \in \{0,1\}^n} \mathsf{uv}_{i'}(t) - \max_{t \in \{0,1\}^n} \mathsf{uv}_i(t).
\end{aligned}$$

We also have:

$$\begin{aligned}
\mathsf{buf}_{i'} - \mathsf{buf}_i &\geq -|(\mathsf{TR} \cup \mathsf{TT}) \cap (i, i']| + \sum_{i'' \in (i, i'] \cap (\mathsf{RT} \cup \mathsf{RR})} \mathbb{1}\left(\max_{t \in \{0,1\}^n} \mathsf{uv}_{i''}(t) - \max_{t \in \{0,1\}^n} \mathsf{uv}_{i''-1}(t) = 1 \right) \\
&\quad - \sum_{i'' \in (i, i'] \cap (\mathsf{RT} \cup \mathsf{RR})} \mathbb{1}\left(\mathsf{buf}_{i''-1} = N\right) \cdot \mathbb{1}\left(i'' \in \mathsf{NA\text{-}Bob}\right) \cdot \mathbb{1}\left(isBobSure_{i''-1} = \mathsf{False}\right) \\
&\geq -|(\mathsf{TR} \cup \mathsf{TT}) \cap (i, i']| + \max_{t \in \{0,1\}^n} \mathsf{uv}_{i'}(t) - \max_{t \in \{0,1\}^n} \mathsf{uv}_i(t) \\
&\quad - \sum_{i'' \in (i, i'] \cap (\mathsf{RT} \cup \mathsf{RR})} \mathbb{1}\left(\mathsf{buf}_{i''-1} = N\right) \cdot \mathbb{1}\left(i'' - 1, i'' \in \mathsf{NA\text{-}Bob}\right)
\end{aligned}$$

$$\geq -|(\mathsf{TR} \cup \mathsf{TT}) \cap (i, i']| + \max_{t \in \{0,1\}^n} \mathsf{uv}_{i'}(t) - \max_{t \in \{0,1\}^n} \mathsf{uv}_i(t) - 2N.$$

The furthermore part is straightforward from our derivation.

□

The variable $\mathit{isBobSure}$. We now establish some properties of the variable $\mathit{isBobSure}$ of Alice.

Lemma 5.4. *For all $i \in [16N]$, we have $\mathit{isBobSure}_i = \mathsf{True} \implies \mathit{isSure}_i = \mathsf{True}$.*

Proof. Proof by contradiction. Suppose there is an i' such that $\mathit{isBobSure}_{i'} = \mathsf{True}$ and $\mathit{isSure}_{i'} = \mathsf{False}$. We let i denote the smallest such i'. First, by our choice of i, we bound corr^A as:

$$\begin{aligned} \mathsf{corr}^A &\geq |\mathsf{NA\text{-}Bob} \cap [i]| - |\{j \in \mathsf{NA\text{-}Bob} \cap [i] \mid (\hat{y}_j, \mathit{sure}_j) = (y, \mathsf{False})\}| \\ &\geq |\mathsf{NA\text{-}Bob} \cap [i]| - \mathsf{uv}_i(y) \\ &\geq |\mathsf{NA\text{-}Bob} \cap [i]| - \max_{t \in \{0,1\}^n} \mathsf{uv}_i(t). \end{aligned} \tag{11}$$

Also, as $\mathit{isSure}_i = \mathsf{False}$, by Observation 5.2, we have that $\mathsf{TT} \cap [i] = \emptyset$. We get that:

$$\begin{aligned} \mathsf{corr}^B &\geq |(\mathsf{TT} \cup \mathsf{TR}) \cap [i]| - |\{j \in (\mathsf{TT} \cup \mathsf{TR}) \cap [i] \mid \hat{x}_j = x\}| \\ &\geq |(\mathsf{TT} \cup \mathsf{TR}) \cap [i]| - \mathsf{v}_i(x) \\ &\geq |(\mathsf{TT} \cup \mathsf{TR}) \cap [i]| - 5N. \end{aligned} \tag{12}$$

Combining, we have:

$$\begin{aligned} 10N &= |(\mathsf{NA\text{-}Bob} \cup \mathsf{TR} \cup \mathsf{TT}) \cap [i]| - \max_{t \in \{0,1\}^n} \mathsf{uv}_i(t) && \text{(Observation 5.2)} \\ &\leq \mathsf{corr} + 5N && \text{(Equation 11 and Equation 12)} \\ &< 10N, \end{aligned}$$

a contradiction.

□

Lemma 5.5. $\mathit{isBobSure}_{15N+\mathsf{buf}_{15N}} = \mathsf{True}$ *and* $\mathit{isBobSure}_{11N-1} = \mathsf{False}$.

Proof. We prove both claims by contradiction.

For the first claim, observe from our protocol that, if $\mathit{isBobSure}_{15N+\mathsf{buf}_{15N}} = \mathsf{False}$, then Alice transmits in iterations $(15N, 15N+\mathsf{buf}_{15N}]$ and thus, $\mathsf{buf}_{15N+\mathsf{buf}_{15N}} = 0$. By Lemma 5.3, we get that (define $i_* = 15N + \mathsf{buf}_{15N}$):

$$\begin{aligned} 10N &\leq 12N + |(\mathsf{TR} \cup \mathsf{TT}) \cap (6N, i_*]| - \max_{t \in \{0,1\}^n} \mathsf{uv}_{i_*}(t) \\ &\leq |(\mathsf{NA\text{-}Bob} \cup \mathsf{TR} \cup \mathsf{TT}) \cap [i_*]| - \max_{t \in \{0,1\}^n} \mathsf{uv}_{i_*}(t). \end{aligned}$$

implying that $isBobSure_{i_*} = \mathsf{True}$, a contradiction.

For the second claim, if $\max_{t\in\{0,1\}^n} \mathsf{uv}_{11N-1}(t) \geq N$, then, we have a contradiction as by, Observation 5.2,

$$\begin{aligned} 10N &\leq |(\mathsf{NA\text{-}Bob} \cup \mathsf{TR} \cup \mathsf{TT}) \cap [11N-1]| - \max_{t\in\{0,1\}^n} \mathsf{uv}_{11N-1}(t) \\ &\leq 10N - 1. \end{aligned}$$

Otherwise, as buf only increases when $\max_{t\in\{0,1\}^n} \mathsf{uv}(t)$ does, we get that $\mathsf{buf}_{i'-1} < N$ for all $i' \in (6N, 11N]$. We have

$$\begin{aligned} 10N &\leq |(\mathsf{NA\text{-}Bob} \cup \mathsf{TR} \cup \mathsf{TT}) \cap [11N-1]| - \max_{t\in\{0,1\}^n} \mathsf{uv}_{11N-1}(t) \\ &\leq |\mathsf{NA\text{-}Bob} \cap [11N-1]| + |(\mathsf{TR} \cup \mathsf{TT}) \cap [11N-1]| - \max_{t\in\{0,1\}^n} \mathsf{uv}_{11N-1}(t) \\ &< 10N + |(\mathsf{TR} \cup \mathsf{TT}) \cap (6N, 11N-1]| - \max_{t\in\{0,1\}^n} \mathsf{uv}_{11N-1}(t) \\ &\leq 10N, && \text{(Lemma 5.3)} \end{aligned}$$

a contradiction.

□

Defining i^A and i^B. We define $i^B \in [16N]$ to be the smallest such that $isSure_{i^B} = \mathsf{True}$. Similarly, define $i^A \in [16N]$ to be the smallest such that $isBobSure_{i^A} = \mathsf{True}$. Owing to Lemma 5.4 and Lemma 5.5, we have that $isSure = isBobSure = \mathsf{True}$. and therefore, both i^A and i^B are well defined.

Furthermore, from Lemma 5.4 and Lemma 5.5, we conclude that $11N, i^B \leq i^A$ and from Algorithm 2 that $5N \leq i^B \notin \mathsf{NA\text{-}Bob}$. We have:

Lemma 5.6. *We have for all $i \leq i^B$ that* $\mathsf{corr}_i^B \geq |[i] \setminus \mathsf{NA\text{-}Bob}| - 5N - |\mathsf{RR} \cap [i]|$.

Proof. Observe that $[i] \setminus \mathsf{NA\text{-}Bob} \subseteq \mathsf{TR} \cup \mathsf{RR} \implies |\mathsf{TR} \cap [i]| \geq |[i] \setminus \mathsf{NA\text{-}Bob}| - |\mathsf{RR} \cap [i]|$. We know that Alice sends x in iteration i' for all $i' \in \mathsf{TR}$. Therefore,

$$\mathsf{corr}_i^B \geq |\mathsf{TR} \cap [i]| - \mathsf{v}(x) \geq |[i] \setminus \mathsf{NA\text{-}Bob}| - |\mathsf{RR} \cap [i]| - 5N.$$

□

Lemma 5.7. $(\mathsf{TR} \cup \mathsf{RR}) \cap (i^B, 16N] = \emptyset$ *and* $\mathsf{TT} \subseteq (i^B, i^A] \subseteq \mathsf{RT} \cup \mathsf{TT}$.

Proof. Bob transmits in all iterations $> i^B$. It follows that $(\mathsf{TR} \cup \mathsf{RR}) \cap (i^B, 16N] = \emptyset$ and $(i^B, i^A] \subseteq \mathsf{RT} \cup \mathsf{TT}$. To see why $\mathsf{TT} \subseteq (i^B, i^A]$, observe that Alice receives in all iterations $> i^A$ and in iterations $i \leq i^B$, Bob transmits only if $i \in \mathsf{NA\text{-}Bob}$ when Alice is receiving. □

The set RR. We finish this section with lemmas concerning the set RR. Throughout, we use that $i \in \mathsf{RR} \implies i \leq i^B \leq i^A \implies \mathsf{buf}_{i-1} = \mathsf{buf}_i = 0$. This is due to Lemma 5.7.

Lemma 5.8. *If, for some $i > 8N$, we have $i \notin \mathsf{NA\text{-}Bob}$, $\mathsf{buf}_i = 0$, then, for $i \le i' \le i^A$, we have*

$$0 \le \mathsf{buf}_{i'} \le |(i, i'] \cap \mathsf{NA\text{-}Bob}| - |(i, i'] \setminus \mathsf{NA\text{-}Bob}|.$$

Proof. We start with the following simple claims:

Claim 5.9. *For $i'' \ge 15N$ satisfying $\mathsf{buf}_{i''} = 0$, we have $i'' \ge i^A$.*

Proof. Observation 5.2 says that buf_i decreases by at most 1 in any iteration. Thus, we have $i'' \ge 15N + \mathsf{buf}_{15N} \ge i^A$ by Lemma 5.5. □

Claim 5.10. *If $15N < i' \le i^A$, then $\mathsf{buf}_{i'} = \mathsf{buf}_{i'-1} - 1$.*

Proof. From the contrapositive of Claim 5.9, we have that $\mathsf{buf}_{i'-1} > 0$. This together with $15N < i' \le i^A$ implies that Alice transmits in iteration i' and the claim follows. □

The claim is trivial if $i = i^A$, so assume that $i < i^A$. We have from Claim 5.9 that $i < 15N$. We focus on showing $\mathsf{buf}_{i'} \le |(i, i'] \cap \mathsf{NA\text{-}Bob}| - |(i, i'] \setminus \mathsf{NA\text{-}Bob}|$ as the other inequality is trivial. Due to Claim 5.10, we can assume without loss of generality that $i' \le 15N$. Moreover, as our definition of $\mathsf{NA\text{-}Bob}$ implies that the right hand side decreases with i (for values $i \notin \mathsf{NA\text{-}Bob}$), we can assume without loss of generality that $i \le i'$ is the largest such that $i \notin \mathsf{NA\text{-}Bob}$, $\mathsf{buf}_i = 0$. We have:

$$\mathsf{buf}_{i'} = \sum_{i'' \in (i,i']} \mathsf{buf}_{i''} - \mathsf{buf}_{i''-1} = \sum_{i'' \in (i,i'] \cap \mathsf{NA\text{-}Bob}} (\mathsf{buf}_{i''} - \mathsf{buf}_{i''-1}) + \sum_{i'' \in (i,i'] \setminus \mathsf{NA\text{-}Bob}} (\mathsf{buf}_{i''} - \mathsf{buf}_{i''-1}).$$

Now, as $i \le i'$ is the largest such that $i \notin \mathsf{NA\text{-}Bob}$, $\mathsf{buf}_i = 0$, we get that for all $i'' \in (i, i'] \setminus \mathsf{NA\text{-}Bob}$, we have $\mathsf{buf}_{i''} > 0 \implies \mathsf{buf}_{i''} = \mathsf{buf}_{i''-1} - 1$. This gives:

$$\begin{aligned}\mathsf{buf}_i &= \sum_{i'' \in (i,i'] \cap \mathsf{NA\text{-}Bob}} (\mathsf{buf}_{i''} - \mathsf{buf}_{i''-1}) - |(i, i'] \setminus \mathsf{NA\text{-}Bob}| \\ &\le |(i, i'] \cap \mathsf{NA\text{-}Bob}| - |(i, i'] \setminus \mathsf{NA\text{-}Bob}|.\end{aligned}$$

□

Lemma 5.11. *It holds that:*

1. *If $\mathsf{RR} \cap [11N] \ne \emptyset$, then $\mathsf{corr}^B_{i^B} \ge N$, $\mathsf{corr}^A_{i^B} \ge 2 \cdot (N + |\mathsf{RR}|) - 1$, and $\mathsf{RR} \cap (11N, 16N] = \emptyset$.*
2. *If $\mathsf{RR} \cap (11N, 15N] \ne \emptyset$, then $\mathsf{corr}^B_{i^B} \ge 2N$, $\mathsf{corr}^A_{i^B} \ge N$ and $\mathsf{corr}_{i^B} \ge 4N + |\mathsf{RR}| - 2$, and $\mathsf{RR} \cap (15N, 16N] = \emptyset$.*
3. *$\mathsf{RR} \cap (15N, 16N] = \emptyset$.*

It follows that $|\mathsf{RR}| \le \min(N, \mathsf{corr}^A, \mathsf{corr}^B)$.

Proof. We prove each part separately.

1. If $\mathsf{RR} \cap [11N] \neq \emptyset$, then, let r be the largest element in $\mathsf{RR} \cap [11N]$. Due to Lemma 5.7 and Observation 5.2, we have that $i^B \geq 6N$ and $[6N] \in \mathsf{TR}$. The claim about $\mathsf{corr}^B_{i^B}$ then follows from Lemma 5.6 and $i^B \geq 6N$.

   Next, we argue that $\mathsf{RR} \cap (11N, 16N] = \emptyset$. For this, we first show:

   Claim 5.12. *For all $i' \in (6N, 11N)$, we have $\mathsf{buf}_{i'} < N$.*

   Proof. For $i' \geq r$, we use Lemma 5.8 to conclude that $\mathsf{buf}_{i'} \leq |(r, i'] \cap \mathsf{NA\text{-}Bob}| - |(r, i'] \setminus \mathsf{NA\text{-}Bob}| < N$ for all $i' < 11N$ by definition of $\mathsf{NA\text{-}Bob}$. For $i' < r$, we proceed via contradiction. If $\mathsf{buf}_{i'} = N$ for some $i' > 6N$, then as buf decreases by at most 1 in every iteration and decreases only when Alice transmits, we get from the definition of $\mathsf{NA\text{-}Bob}$ and the fact that Alice does not transmit in iterations in $\mathsf{NA\text{-}Bob}$ that $\mathsf{buf}_{r-1} > 0$, a contradiction. □

   Suppose that $r' \in \mathsf{RR} \cap (11N, 16N]$ for the sake of contradiction. We get:

   $$\begin{aligned}
   \mathsf{corr} &\geq \mathsf{corr}^B_{r'-1} + \mathsf{corr}^A_{11N} \\
   &\geq |[r'-1] \setminus \mathsf{NA\text{-}Bob}| - 5N - |\mathsf{RR} \cap [r'-1]| + \mathsf{corr}^A_{11N} && \text{(Lemma 5.6)} \\
   &\geq N + |\mathsf{TR} \cap (6N, r')| + \mathsf{corr}^A_{11N} \\
   &\geq N + |\mathsf{TR} \cap (6N, 11N]| + \mathsf{buf}_{11N} + \mathsf{corr}^A_{11N} \\
   &\geq 5N + |\mathsf{TR} \cap (6N, 11N]| + \mathsf{buf}_{11N} - \max_{t \in \{0,1\}^n} \mathsf{uv}_{11N}(t) \\
   &\geq 5N, && \text{(Lemma 5.3 and Lemma 5.7)}
   \end{aligned}$$

   a contradiction.

   Finally, we argue about $\mathsf{corr}^A_{i^B}$. We have:

   $$\begin{aligned}
   \mathsf{corr}^A_{i^B} &\geq |\mathsf{NA\text{-}Bob} \cap [r]| - \mathsf{uv}_r(y) \\
   &\geq |\mathsf{NA\text{-}Bob} \cap [r]| - \max_{t \in \{0,1\}^n} \mathsf{uv}_r(t) \\
   &\geq |\mathsf{NA\text{-}Bob} \cap [r]| - |\mathsf{TR} \cap (6N, r]| && \text{(Lemma 5.3 and Lemma 5.7)} \\
   &\geq 2N + |\mathsf{TR} \cap (6N, r]| + 2 \cdot |\mathsf{RR} \cap [r]| - 1 \\
   &= 2N + |\mathsf{TR} \cap (6N, r]| + 2 \cdot |\mathsf{RR}| - 1.
   \end{aligned}$$

2. If $\mathsf{RR} \cap (11N, 15N] \neq \emptyset$, then, by the previous part, we have $\mathsf{RR} \cap [11N] = \emptyset$. Let $\underline{r}$ and $\overline{r}$ be the smallest and the largest elements in $\mathsf{RR} \cap (11N, 15N]$ respectively. Observe that $11N < \underline{r} \leq \overline{r} \leq i^B$ and $[\underline{r} - 1] \setminus \mathsf{NA\text{-}Bob} \subseteq \mathsf{TR}$. The claim about $\mathsf{corr}^B_{i^B}$ then follows from Lemma 5.6 and $i^B \geq 11N$.

   Next, we argue that $\mathsf{RR} \cap (15N, 16N] = \emptyset$. Suppose that $r' \in \mathsf{RR} \cap (15N, 16N]$ for the sake of contradiction. Observe that:

   $$\mathsf{corr} \geq \mathsf{corr}^B_{r'-1} + \mathsf{corr}^A_{15N}$$

$$\begin{aligned}
&\geq |[r'-1] \setminus \mathsf{NA\text{-}Bob}| - 5N - |\mathsf{RR} \cap [r'-1]| + \mathsf{corr}^A_{15N} && \text{(Lemma 5.6)} \\
&\geq N + |\mathsf{TR} \cap (6N, r')| + \mathsf{corr}^A_{15N} \\
&\geq N + |\mathsf{TR} \cap (6N, 15N]| + \mathsf{buf}_{15N} + \mathsf{corr}^A_{15N} \\
&\geq 7N + |\mathsf{TR} \cap (6N, 15N]| + \mathsf{buf}_{15N} - \max_{t \in \{0,1\}^n} \mathsf{uv}_{15N}(t) \\
&\geq 5N, && \text{(Lemma 5.3 and Lemma 5.7)}
\end{aligned}$$

a contradiction.

Define $r_* > 6N$ to be the largest such that $\mathsf{buf}_{r_*-1} = N$. If no such value exists, define $r_* = 6N$. Also observe that $r_* < \underline{r} \leq \overline{r}$ by Lemma 5.8. We have:

$$\begin{aligned}
\mathsf{corr}^A_{i^B} &\geq |\mathsf{NA\text{-}Bob} \cap [\overline{r}]| - \max_{t \in \{0,1\}^n} \mathsf{uv}_{\overline{r}}(t) \\
&\geq |\mathsf{NA\text{-}Bob} \cap (r_*, \overline{r}]| - \max_{t \in \{0,1\}^n} \mathsf{uv}_{\overline{r}}(t) + \max_{t \in \{0,1\}^n} \mathsf{uv}_{r_*}(t) \\
&\geq |\mathsf{NA\text{-}Bob} \cap (r_*, \overline{r}]| + (N-1) \cdot \mathbb{1}(r_* \neq 6N) - |\mathsf{TR} \cap (r_*, \overline{r}]| \\
& && \text{(Lemma 5.3 and Lemma 5.7)}
\end{aligned}$$

Observe that $\mathsf{corr}^A_{i^B} \geq N$ follows. We also get that

$$\begin{aligned}
\mathsf{corr}_{i^B} &\geq |\mathsf{NA\text{-}Bob} \cap (r_*, \overline{r}]| + (N-1) \cdot \mathbb{1}(r_* \neq 6N) - |\mathsf{TR} \cap (r_*, \overline{r}]| + \mathsf{corr}^B_{i^B} \\
&\geq |\mathsf{NA\text{-}Bob} \cap (r_*, \overline{r}]| + 2N + (N-1) \cdot \mathbb{1}(r_* \neq 6N) - |\mathsf{TR} \cap (r_*, \overline{r}]| + |\mathsf{TR} \cap (11N, \overline{r}]|. \\
& && \text{(Lemma 5.6)}
\end{aligned}$$

If $r_* > 11N$, we continue as follows:

$$\begin{aligned}
\mathsf{corr}_{i^B} &\geq |\mathsf{NA\text{-}Bob} \cap (r_*, \overline{r}]| + 3N \\
&\geq 4N + |\mathsf{TR} \cap (\underline{r}, \overline{r}]| + |\mathsf{RR}| - 1.
\end{aligned}$$

Observe that $r_* = 11N$ is not possible as $r_* \notin \mathsf{NA\text{-}Bob}$. If $r_* < 11N$, we continue as follows:

$$\begin{aligned}
\mathsf{corr}_{i^B} &\geq |\mathsf{NA\text{-}Bob} \cap (r_*, \overline{r}]| + 2N + (N-1) \cdot \mathbb{1}(r_* \neq 6N) - |\mathsf{TR} \cap (r_*, 11N]| \\
&\geq 4N + |\mathsf{TR} \cap (\underline{r}, \overline{r}]| + |\mathsf{RR}| - 2.
\end{aligned}$$

3. If $\mathsf{RR} \cap [15N] \neq \emptyset$, then we are done by the previous parts. Otherwise, suppose that r is the smallest $\in \mathsf{RR} \cap (15N, 16N]$. This means that $i^B > 15N$, which when combined with $\mathsf{RR} \cap [15N] = \emptyset$ implies that $\mathsf{TR} \cap [15N] = 9N$. Observe that:

$$\begin{aligned}
\mathsf{corr} &\geq \mathsf{corr}^B_{r-1} + \mathsf{corr}^A_{15N} \\
&\geq |[r-1] \setminus \mathsf{NA\text{-}Bob}| - 5N + \mathsf{corr}^A_{15N} && \text{(Lemma 5.6)} \\
&\geq N + |\mathsf{TR} \cap (6N, r)| + \mathsf{corr}^A_{15N} \\
&\geq N + |\mathsf{TR} \cap (6N, 15N]| + \mathsf{buf}_{15N} + \mathsf{corr}^A_{15N}
\end{aligned}$$

$$\begin{aligned}&\geq 7N + |\mathsf{TR} \cap (6N, 15N]| + \mathsf{buf}_{15N} - \max_{t \in \{0,1\}^n} \mathsf{uv}_{15N}(t) \\ &\geq 5N, && \text{(Lemma 5.3 and Lemma 5.7)}\end{aligned}$$

a contradiction.

□

Lemma 5.13. *If* $\mathsf{RR} \neq \emptyset$*, then it holds that* $|\mathsf{TT}| \leq 2N - 2 \cdot |\mathsf{RR}|$.

Proof. We break the proof into two cases that are exhaustive by Lemma 5.11. First, assume that $\mathsf{RR} \subseteq [11N]$. Let r be the largest element in RR. In this case, we have

$$\begin{aligned}\mathsf{corr}_{i^B} &\geq \mathsf{corr}^A_{i^B} + \mathsf{corr}^B_{i^B} \\ &\geq 2N + 2 \cdot |\mathsf{RR}| + \mathsf{corr}^B_{i^B} - 1 && \text{(Lemma 5.11)} \\ &\geq 3N + 2 \cdot |\mathsf{RR}| + |(r, i^B] \setminus \mathsf{NA\text{-}Bob}| - 1 && \text{(Lemma 5.6)} \\ &\geq 3N + 2 \cdot |\mathsf{RR}| + \mathsf{buf}_{i^B} - 1. && \text{(Lemma 5.8)}\end{aligned}$$

Using this inequality, we get:

$$\begin{aligned}\mathsf{buf}_{i^B} &\geq \sum_{i' \in (i^B, 16N]} \mathsf{buf}_{i'-1} - \mathsf{buf}_{i'} \\ &\geq |\mathsf{TT}| + \sum_{i' \in (i^B, 16N] \cap \mathsf{RT}} \mathsf{buf}_{i'-1} - \mathsf{buf}_{i'} && \text{(Lemma 5.7)} \\ &\geq |\mathsf{TT}| + \mathsf{corr}_{i^B} - \mathsf{corr} \\ &\geq |\mathsf{TT}| - 2N + 2 \cdot |\mathsf{RR}| + \mathsf{buf}_{i^B}.\end{aligned}$$

The result follows. Next, assume that $\mathsf{RR} \subseteq (11N, 15N]$. In this case, by Lemma 5.11, we have $\mathsf{corr}_{i^B} \geq 4N + |\mathsf{RR}| - 2$. Using this inequality and Lemma 5.8, we get:

$$\begin{aligned}1 \geq \mathsf{buf}_{i^B} &\geq \sum_{i' \in (i^B, 16N]} \mathsf{buf}_{i'-1} - \mathsf{buf}_{i'} \\ &\geq |\mathsf{TT}| + \sum_{i' \in (i^B, 16N] \cap \mathsf{RT}} \mathsf{buf}_{i'-1} - \mathsf{buf}_{i'} && \text{(Lemma 5.7)} \\ &\geq |\mathsf{TT}| + \mathsf{corr}_{i^B} - \mathsf{corr} \\ &\geq |\mathsf{TT}| + 1 - N + |\mathsf{RR}| \\ &\geq |\mathsf{TT}| + 1 - 2N + 2 \cdot |\mathsf{RR}|. && \text{(Lemma 5.11)}\end{aligned}$$

The result follows.

□

5.2.2 Bob's Output is Correct

Lemma 5.14. $\tilde{x} = x$.

Proof. Due to Lemma 5.4 and Lemma 5.5, there exists t such that $\mathsf{v}(t) \geq 5N$, it also holds that $\mathsf{v}(\tilde{x}) \geq 5N$. Thus, there exists a set I of size $|I| \geq 5N$ such that Bob receives $\tilde{x}$ for all iterations $i \in I$. Since Alice transmits x for all $i \in I \setminus \mathsf{RR}$ and since $\mathsf{corr}^B \leq \mathsf{corr} - \mathsf{corr}^A < |I| - |\mathsf{RR}|$ due to Lemma 5.11, we have $\tilde{x} = x$. □

5.2.3 Alice's Output is Correct

This section is dedicated to proving the following lemma.

Lemma 5.15. $\tilde{y} = y$.

We divide the proof into two parts based on the two cases in Line 24.

When Line 24 evaluates to true. For this part of the proof, we assume that $\max_{t\in\{0,1\}^n} \mathsf{tv}(t) \geq \sum_{t\in\{0,1\}^n} \mathsf{sv}(t) + \mathsf{uv}(t) - 5N$. In particular, we have that:

$$\mathsf{tv}(\tilde{y}) \geq \sum_{t\in\{0,1\}^n} \mathsf{sv}(t) + \mathsf{uv}(t) - 5N. \tag{13}$$

All the results stated in this section assume that Line 24 evaluates to true.

Lemma 5.16. $\mathsf{tv}(\tilde{y}) - \mathsf{sv}(\tilde{y}) + \max_{t\in\{0,1\}^n} \mathsf{uv}(t) \leq \sum_{t\in\{0,1\}^n} \mathsf{uv}(t)$.

Proof. If $\mathsf{tv}(\tilde{y}) = \mathsf{sv}(\tilde{y})$, then there is nothing to show. So, we assume that $\mathsf{tv}(\tilde{y}) > \mathsf{sv}(\tilde{y})$ implying that $\mathsf{uv}(\tilde{y}) < \max_{t\in\{0,1\}^n} \mathsf{uv}(t)$. In this case, we have

$$\sum_{t\in\{0,1\}^n} \mathsf{uv}(t) \geq \mathsf{uv}(\tilde{y}) + \max_{t\in\{0,1\}^n} \mathsf{uv}(t) = \mathsf{tv}(\tilde{y}) - \mathsf{sv}(\tilde{y}) + \max_{t\in\{0,1\}^n} \mathsf{uv}(t).$$

□

We define a potential function $\Phi_i(s)$ for all $i \in [0, 16N]$ and $s \in \{0,1\}^n$:

$$\Phi_i(s) = \mathsf{sv}_i(s) - \sum_{t\in\{0,1\}^n} \mathsf{sv}_{\min(i,i^A)}(t) - \mathsf{corr}_i - |\mathsf{RR} \cap [i]|. \tag{14}$$

We also define $\Phi_0(s) = 0$ and $\Phi(s) = \Phi_{16N}(s)$ for all $s \in \{0,1\}^n$. The main property that our potential function satisfies is:

Lemma 5.17. *For all $s \neq y$ and $i \in [16N]$, we have*

$$\Phi_i(s) \leq \Phi_{i-1}(s).$$

Furthermore, the inequality is strict if $i \in \mathsf{RT} \cap (i^B, i^A]$.

Proof. If Alice is transmitting in iteration i, then, for all $s \in \{0,1\}^n$, we simply have $\Phi_i(s) - \Phi_{i-1}(s) = \mathsf{corr}_{i-1} - \mathsf{corr}_i \leq 0$ and we are done. Otherwise, Alice is receiving in iteration i. If $i > i^A$, we have:

$$\Phi_i(s) - \Phi_{i-1}(s) = \mathsf{sv}_i(s) - \mathsf{sv}_{i-1}(s) - \mathbb{1}(i \in \mathsf{RT} \wedge (\hat{y}_i, sure_i) \neq (y, isSure_{i-1})) - \mathbb{1}(i \in \mathsf{RR})$$

$$
\begin{aligned}
&= \mathbb{1}(\hat{y}_i = s) - \mathbb{1}(i \in \mathsf{RT} \wedge (\hat{y}_i, sure_i) \neq (y, isSure_{i-1})) - \mathbb{1}(i \in \mathsf{RR}) \\
&\hfill \text{(Alice is receiving in iteration } i > i^A) \\
&\leq \mathbb{1}(\hat{y}_i \neq y) - \mathbb{1}(i \in \mathsf{RT} \wedge (\hat{y}_i, sure_i) \neq (y, isSure_{i-1})) - \mathbb{1}(i \in \mathsf{RR}) \\
&\hfill \text{(As } s \neq y) \\
&\leq 0.
\end{aligned}
$$

Assume henceforth that $i \leq i^A$. We have:

$$
\begin{aligned}
\Phi_i(s) - \Phi_{i-1}(s) = \sum_{t \neq s \in \{0,1\}^n} \mathsf{sv}_{i-1}(t) - \sum_{t \neq s \in \{0,1\}^n} \mathsf{sv}_i(t) \\
- \mathbb{1}(i \in \mathsf{RT} \wedge (\hat{y}_i, sure_i) \neq (y, isSure_{i-1})) - \mathbb{1}(i \in \mathsf{RR}),
\end{aligned}
$$

which is non-positive by Observation 5.2, and all that remains is to show that "furthermore" part. If $i \in \mathsf{RT} \cap (i^B, i^A]$, we simplify as:

$$
\begin{aligned}
\Phi_i(s) - \Phi_{i-1}(s) &= \sum_{t \neq s \in \{0,1\}^n} (\mathsf{sv}_{i-1}(t) - \mathsf{sv}_i(t)) - \mathbb{1}((\hat{y}_i, sure_i) \neq (y, \mathsf{True})) \\
&\leq - \sum_{t \neq s \in \{0,1\}^n} \mathbb{1}((\hat{y}_i, sure_i) = (t, \mathsf{True})) - \mathbb{1}((\hat{y}_i, sure_i) \neq (y, \mathsf{True})) \\
&\leq -\mathbb{1}((\hat{y}_i, sure_i) = (y, \mathsf{True})) - \mathbb{1}((\hat{y}_i, sure_i) \neq (y, \mathsf{True})) \qquad \text{(As } s \neq y) \\
&\leq -1.
\end{aligned}
$$

□

Lemma 5.18. *For all $s \neq y$, we have*

$$
\Phi(s) \leq -4N + |\mathsf{NA\text{-}Bob} \cap [i^A]| - \sum_{t \in \{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) - |\mathsf{RR}|.
$$

Proof. We argue using Lemma 5.17.

$$
\begin{aligned}
\Phi(s) \leq \Phi_{i^A}(s) \leq \Phi_{i^B}(s) &- |\mathsf{RT} \cap (i^B, i^A]| \\
&\leq -\mathsf{corr}_{i^B} - |\mathsf{RR} \cap [i^B]| - |\mathsf{RT} \cap (i^B, i^A]| && \text{(Equation 14)} \\
&\leq -\mathsf{corr}_{i^B} - |\mathsf{RR}| - |\mathsf{RT} \cap (i^B, i^A]| && \text{(Lemma 5.7)} \\
&\leq -\mathsf{corr}^A_{i^B} - \mathsf{corr}^B_{i^B} - |\mathsf{RR}| - |\mathsf{RT} \cap (i^B, i^A]| \\
&\leq 5N - \mathsf{corr}^A_{i^B} - |[i^B] \setminus \mathsf{NA\text{-}Bob}| - |\mathsf{RT} \cap (i^B, i^A]|. && \text{(Lemma 5.6)}
\end{aligned}
$$

We now consider two cases:

- $\boldsymbol{i^B \in [6N]}$**:** In this case, we have $\mathsf{RR} = \emptyset$ and we get:

$$
\begin{aligned}
\Phi(s) &\leq 5N - \mathsf{corr}^A_{i^B} - |[i^B] \setminus \mathsf{NA\text{-}Bob}| - |\mathsf{RT} \cap (i^B, i^A]| \\
&\leq -|\mathsf{RT} \cap (i^B, i^A]|
\end{aligned}
$$

$$\leq -4N + |\mathsf{NA\text{-}Bob} \cap [i^A]| - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) - |\mathsf{RR}|,$$

as $i^A \geq 11N$ (Lemma 5.5) and $\mathsf{RR} = \emptyset$.

- $\boldsymbol{i^B > 6N}$**:** We derive:

$$\begin{aligned}10N = i^A &- \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) + |\mathsf{NA\text{-}Bob} \cap [i^A]| - \max_{t\in\{0,1\}^n} \mathsf{uv}_{i^A}(t)\\ &\leq \mathsf{corr}^A_{i^B} - \left(|\mathsf{NA\text{-}Bob} \cap [i^B]| - \max_{t\in\{0,1\}^n} \mathsf{uv}_{i^B}(t)\right) + i^A\\ &\quad - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) + |\mathsf{NA\text{-}Bob} \cap [i^A]| - \max_{t\in\{0,1\}^n} \mathsf{uv}_{i^A}(t).\end{aligned}$$

This gives using Lemma 5.7:

$$\begin{aligned}\Phi(s) &\leq 5N - \mathsf{corr}^A_{i^B} - |[i^B] \setminus \mathsf{NA\text{-}Bob}| - |\mathsf{RT} \cap (i^B, i^A]|\\ &\leq -5N + i^A - i^B - \left(\max_{t\in\{0,1\}^n} \mathsf{uv}_{i^A}(t) - \max_{t\in\{0,1\}^n} \mathsf{uv}_{i^B}(t)\right)\\ &\quad - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) + |\mathsf{NA\text{-}Bob} \cap [i^A]| - |\mathsf{RT} \cap (i^B, i^A]|\\ &\leq -5N + i^A - i^B + \mathsf{buf}_{i^B} - |(\mathsf{TR} \cup \mathsf{TT}) \cap (i^B, i^A]|\\ &\quad - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) + |\mathsf{NA\text{-}Bob} \cap [i^A]| - |\mathsf{RT} \cap (i^B, i^A]| && \text{(Lemma 5.3)}\\ &\leq -5N + \mathsf{buf}_{i^B} - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) + |\mathsf{NA\text{-}Bob} \cap [i^A]|\\ &\leq -4N - |\mathsf{RR}| - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) + |\mathsf{NA\text{-}Bob} \cap [i^A]|. && \text{(Lemma 5.7, Lemma 5.8)}\end{aligned}$$

□

Lemma 5.19. *We have:*

$$\Phi(\tilde{y}) > -4N + |\mathsf{NA\text{-}Bob} \cap [i^A]| - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) - |\mathsf{RR}|.$$

Proof. We derive:

$$\begin{aligned}\Phi(\tilde{y}) &= \mathsf{sv}(\tilde{y}) - \sum_{t\in\{0,1\}^n} \mathsf{sv}_{i^A}(t) - \mathsf{corr} - |\mathsf{RR}| && \text{(Equation 14)}\\ &> \mathsf{tv}(\tilde{y}) + \max_{t\in\{0,1\}^n} \mathsf{uv}(t) - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}(t)) - 5N - |\mathsf{RR}| && \text{(Lemma 5.16)}\end{aligned}$$

$$\begin{aligned}
&\geq \mathsf{tv}(\tilde{y}) + \max_{t\in\{0,1\}^n} \mathsf{uv}_{i^A}(t) - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) - 5N - |\mathsf{RR}| \\
&\geq \mathsf{tv}(\tilde{y}) + |(\mathsf{NA\text{-}Bob} \cup \mathsf{TR} \cup \mathsf{TT}) \cap [i^A]| - 15N - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) - |\mathsf{RR}| \\
&\hspace{20em} \text{(Observation 5.2)} \\
&\geq \mathsf{tv}(\tilde{y}) + |\mathsf{TR} \cup \mathsf{TT}| + |\mathsf{NA\text{-}Bob} \cap [i^A]| - 15N - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) - |\mathsf{RR}| \\
&\geq -4N + |\mathsf{NA\text{-}Bob} \cap [i^A]| - \sum_{t\in\{0,1\}^n} (\mathsf{sv}_{i^A}(t) + \mathsf{uv}_{i^A}(t)) - |\mathsf{RR}|. \qquad \text{(Equation 13)}
\end{aligned}$$

□

Lemma 5.18 and Lemma 5.19 show Lemma 5.15 assuming that Line 24 evaluates to true.

When Line 24 evaluates to false. We now consider the case when Line 24 evaluates to False. Henceforth, we assume without saying in all our lemmas that (see Observation 5.2)

$$\max_{t\in\{0,1\}^n} \mathsf{tv}(t) < |\mathsf{RR} \cup \mathsf{RT}| - 5N \tag{15}$$

Lemma 5.20. $i^B > 6N$.

Proof. Suppose for the sake of contradiction that $i^B \leq 6N$. This means that $\mathsf{RR} = \emptyset$ and Bob transmits (y, True) in all iterations $> i^B$. In particular, in every round where Alice receives, Bob transmits (y, True). Therefore, we have:

$$\mathsf{tv}(y) \geq \mathsf{sv}(y) \geq |\mathsf{RT} \cup \mathsf{RR}| - \mathsf{corr} > |\mathsf{RT} \cup \mathsf{RR}| - 5N,$$

a contradiction to Equation 15. □

Lemma 5.21. *If* $\mathsf{RR} \neq \emptyset$*, then* $\tilde{y} = y$*.*

Proof. If $\mathsf{RR} \neq \emptyset$, we use Lemma 5.13 to conclude that $|\mathsf{TT}| \leq 2N - 2 \cdot |\mathsf{RR}|$ implying that $|\mathsf{RR}| + |\mathsf{RT}| + |\mathsf{TR}| \geq 14N + 2 \cdot |\mathsf{RR}|$. We also have from Lemma 5.6 and Lemma 5.7 that $\mathsf{corr}^B \geq \mathsf{corr}^B_{i^B} \geq |\mathsf{TR}| - 5N \geq N \implies \mathsf{corr}^A < 5N - \mathsf{corr}^B \leq 10N - |\mathsf{TR}|$.

Combining, and using Lemma 5.20, we get that

$$|\mathsf{RT}| + |\mathsf{RR}| \geq 14N + 2 \cdot |\mathsf{RR}| - |\mathsf{TR}| > 4N + 2 \cdot |\mathsf{RR}| + \mathsf{corr}^A \geq 2 \cdot \left(|\mathsf{RR}| + \mathsf{corr}^A\right).$$

Now, $\hat{y}_i = y$ for all $i \in \mathsf{RT}$ that are not corrupted. This means that

$$\begin{aligned}
\mathsf{sv}(y) + \mathsf{uv}(y) &\geq |\mathsf{RT}| + |\mathsf{RR}| - \left(\mathsf{corr}^A + |\mathsf{RR}|\right) \\
&> \frac{1}{2} \cdot (|\mathsf{RT}| + |\mathsf{RR}|) = \frac{1}{2} \cdot \sum_{t\in\{0,1\}^n} (\mathsf{sv}(t) + \mathsf{uv}(t)).
\end{aligned}$$

It follows from our choice of $\tilde{y}$ that $\tilde{y} = y$.

□

Lemma 5.22. *If* $\mathsf{RR} = \emptyset$, *then* $\tilde{y} = y$.

Proof. We first claim that $\max_{t \in \{0,1\}^n} \mathsf{uv}(t) = \mathsf{uv}(y)$. Suppose not. Then, as Bob transmits either (y, True) or (y, False) in all rounds in RT, we get.

$$\mathsf{tv}(y) = \mathsf{sv}(y) + \mathsf{uv}(y) \geq |\mathsf{RT}| - \mathsf{corr}^A \geq |\mathsf{RT}| - 5N,$$

contradicting Equation 15. Next, by Lemma 5.20, we have that $i^B > 6N$, implying, due to Lemma 5.6, that $\mathsf{corr}^A < 5N - \mathsf{corr}^B \leq 4N$.

Assume for now that $|\mathsf{TR} \cup \mathsf{TT}| \leq 16N - 2 \cdot \mathsf{corr}^A$. This means that $|\mathsf{RT}| \geq 2 \cdot \mathsf{corr}^A$. We get that $\mathsf{sv}(y) + \mathsf{uv}(y) \geq |\mathsf{RT}| - \mathsf{corr}^A \geq \frac{1}{2}|\mathsf{RT}| \geq \frac{1}{2}\left(\sum_{t \in \{0,1\}^n} \mathsf{sv}(t) + \mathsf{uv}(t)\right)$, implying that $\tilde{y} = y$ by our choice of $\tilde{y}$. For the rest of the proof, we assume that $|\mathsf{TR} \cup \mathsf{TT}| > 16N - 2 \cdot \mathsf{corr}^A > 8N \implies i^A > 13N$.

Using $i^A > 13N$ and the definition of i^A and $\mathsf{NA\text{-}Bob}$, we get:

$$\begin{aligned}
32N - 4 \cdot \mathsf{corr}^A &< 2 \cdot |\mathsf{TR} \cup \mathsf{TT}| - 1 \\
&= 2 \cdot |(\mathsf{TR} \cup \mathsf{TT}) \cap [i^A]| - 1 \\
&\leq 3N + |(\mathsf{TR} \cup \mathsf{TT} \cup \mathsf{NA\text{-}Bob}) \cap [i^A]| && (\text{As } i^A > 13N) \\
&= 13N + \max_{t \in \{0,1\}^n} \mathsf{uv}_{i^A}(t) \\
&= 13N + \max_{t \in \{0,1\}^n} \mathsf{uv}(t) \\
&= 13N + \mathsf{uv}(y). && (\text{As } \max_{t \in \{0,1\}^n} \mathsf{uv}(t) = \mathsf{uv}(y))
\end{aligned}$$

Now, as $\mathsf{corr}^A < 4N$, we get that $\mathsf{uv}(y) > 3N$. If $\mathsf{uv}(y) \geq 4N$, then by our choice of $\tilde{y}$, we have that $\mathsf{sv}(\tilde{y}) + \mathsf{uv}(\tilde{y}) \geq 4N$. This means that there exists a set I, $|I| \geq 4N$, of iterations such that $\hat{y}_i = \tilde{y}$, for all $i \in I$. As we assume that $\mathsf{RR} = \emptyset$ and $\mathsf{corr}^A < 4N \leq |I|$, we have that there $\tilde{y} = y$.

Thus, we can assume that $\mathsf{uv}(y) < 4N$ implying that $\mathsf{corr}^A > \frac{15}{4}N$ and $\mathsf{corr}^B < \frac{5}{4}N$ and therefore $i^B \leq \frac{35}{4}N$ by Lemma 5.6. As Bob sends (y, False), whenever he transmits before i^B and (y, True) whenever he transmits after i^B, we get that

$$\begin{aligned}
4N > \mathsf{corr}^A &\geq |\mathsf{RT}| - \mathsf{sv}(y) - \mathsf{uv}_{\frac{35}{4}N}(y) \\
&\geq |\mathsf{RT}| - \mathsf{sv}(y) + 3N - \mathsf{uv}(y) - \mathsf{uv}_{\frac{35}{4}N}(y) && (\text{As } \mathsf{uv}(y) > 3N) \\
&\geq |\mathsf{RT}| - \mathsf{sv}(y) + \frac{1}{2}N - \mathsf{uv}(y) \\
&\geq 8N - \mathsf{sv}(y) - \mathsf{uv}(y) && (\text{As } 2 \cdot |\mathsf{TR} \cup \mathsf{TT}| - 1 \leq 13N + \mathsf{uv}(y) \leq 17N - 1) \\
&\geq 8N - \mathsf{sv}(\tilde{y}) - \mathsf{uv}(\tilde{y}).
\end{aligned}$$

Rearranging gives $\mathsf{sv}(\tilde{y}) + \mathsf{uv}(\tilde{y}) \geq 4N$ which implies $\tilde{y} = y$ just like before.

□

Observe that Lemma 5.21 and Lemma 5.22 imply Lemma 5.15 assuming that Line 24 evaluates to false. This together with the arguments in the foregoing section finishes the proof of Theorem 5.1.

References

[AGS16] Shweta Agrawal, Ran Gelles, and Amit Sahai. Adaptive protocols for interactive communication. In *Information Theory (ISIT)*, pages 595–599. IEEE, 2016. 5

[BE17] Mark Braverman and Klim Efremenko. List and unique coding for interactive communication in the presence of adversarial noise. *SIAM Journal on Computing*, 46(1):388–428, 2017. 5

[Ber64] Elwyn R. Berlekamp. *Block Coding with Noiseless Feedback.* PhD thesis, Massachusetts Institute of Technology (MIT), 1964. 5

[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. 5

[BKN14] Zvika Brakerski, Yael Tauman Kalai, and Moni Naor. Fast interactive coding against adversarial noise. *Journal of the ACM (JACM)*, 61(6):35, 2014. 5

[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. 1, 2, 5, 6

[Bra12] Mark Braverman. Towards deterministic tree code constructions. In *Innovations in Theoretical Computer Science (ITCS)*, pages 161–167. ACM, 2012. 5

[CK85] Imrich Chlamtac and Shay Kutten. On broadcasting in radio networks-problem analysis and protocol design. *IEEE Trans. Communications*, 33(12):1240–1246, 1985. 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. 3, 5

[EKS18] Klim Efremenko, Gillat Kol, and Raghuvansh Saxena. Interactive coding over the noisy broadcast channel. In *Symposium on Theory of Computing (STOC)*, pages 507–520. ACM, 2018. 5

[EKS20] Klim Efremenko, Gillat Kol, and Raghuvansh Saxena. Interactive error resilience beyond 2/7. In *Symposium on Theory of Computing (STOC)*. ACM, 2020. 1, 2, 3, 5, 7, 10, 11

[FGOS15] Matthew Franklin, Ran Gelles, Rafail Ostrovsky, and Leonard J. Schulman. Optimal coding for streaming authentication and interactive communication. *IEEE Transactions on Information Theory*, 61(1):133–145, 2015. 5

[Gel17] Ran Gelles. Coding for interactive communication: A survey. *Foundations and Trends® in Theoretical Computer Science*, 13(1–2):1–157, 2017. 5

[GH14] Mohsen Ghaffari and Bernhard Haeupler. Optimal Error Rates for Interactive Coding II: Efficiency and List Decoding. In *Foundations of Computer Science (FOCS)*, pages 394–403, 2014. 5

[GH17] Ran Gelles and Bernhard Haeupler. Capacity of interactive communication over erasure channels and channels with feedback. *SIAM Journal on Computing*, 46(4):1449–1472, 2017. 5

[GHK+18] Ran Gelles, Bernhard Haeupler, Gillat Kol, Noga Ron-Zewi, and Avi Wigderson. Explicit capacity approaching coding for interactive communication. *IEEE Transactions on Information Theory*, 64(10):6546–6560, 2018. 5

[GHS14] Mohsen Ghaffari, Bernhard Haeupler, and Madhu Sudan. Optimal error rates for interactive coding i: Adaptivity and other settings. In *Symposium on Theory of computing (STOC)*, pages 794–803, 2014. 1, 2, 3, 4, 5, 6, 7, 8, 10, 12

[GMS11] Ran Gelles, Ankur Moitra, and Amit Sahai. Efficient and explicit coding for interactive communication. In *Foundations of Computer Science (FOCS)*, pages 768–777. IEEE, 2011. 5

[GMS14] Ran Gelles, Ankur Moitra, and Amit Sahai. Efficient coding for interactive communication. *IEEE Transactions on Information Theory*, 60(3):1899–1913, 2014. 5

[Hae14] Bernhard Haeupler. Interactive channel capacity revisited. In *Foundations of Computer Science (FOCS)*, pages 226–235. IEEE, 2014. 4, 5

[HKV15] Bernhard Haeupler, Pritish Kamath, and Ameya Velingker. Communication with partial noiseless feedback. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*, 2015. 5

[HSV18] Bernhard Haeupler, Amirbehshad Shahrasbi, and Ellen Vitercik. Synchronization strings: Channel simulations and interactive coding for insertions and deletions. In *International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 75:1–75:14, 2018. 5

[HV17] Bernhard Haeupler and Ameya Velingker. Bridging the capacity gap between interactive and one-way communication. In *Symposium on Discrete Algorithms (SODA)*, pages 2123–2142, 2017. 5

[Kas85] Amiram Kaspi. Two-way source coding with a fidelity criterion. *IEEE Transactions on Information Theory*, 31(6):735–740, 1985. 5

[KR13] Gillat Kol and Ran Raz. Interactive channel capacity. In *Symposium on Theory of computing (STOC)*, pages 715–724, 2013. 5

[MI13] Nan Ma and Prakash Ishwar. The infinite-message limit of two-terminal interactive source coding. *IEEE transactions on information theory*, 59(7):4071–4094, 2013. 5

[Pan13] Denis Pankratov. On the power of feedback in interactive channels. Manuscript, 2013. 5

[Sch92] Leonard J Schulman. Communication on noisy channels: A coding theorem for computation. In *Foundations of Computer Science (FOCS)*, pages 724–733. IEEE, 1992. 5

[Sch93] Leonard J Schulman. Deterministic coding for interactive communication. In *Symposium on Theory of computing (STOC)*, pages 747–756. ACM, 1993. 5

[Sch96] Leonard J. Schulman. Coding for interactive communication. *IEEE Transactions on Information Theory*, 42(6):1745–1756, 1996. 2, 5

[SW17] Alexander A. Sherstov and Pei Wu. Optimal interactive coding for insertions, deletions, and substitutions. In *Foundations of Computer Science (FOCS)*, pages 240–251, 2017. 5

[WQC17] Gang Wang, Yanyuan Qin, and Chengjuan Chang. Communication with partial noisy feedback. In *IEEE Symposium on Computers and Communications (ISCC)*, pages 602–607, 2017. 5