

The zero-rate threshold for adversarial bit-deletions is less than $\frac{1}{2}$

Venkatesan Guruswami*

Xiaoyu He[†]Ray Li[‡]

Abstract

We prove that there exists an absolute constant $\delta > 0$ such any binary code $C \subset \{0, 1\}^N$ tolerating $(1/2 - \delta)N$ adversarial deletions must satisfy $|C| \leq 2^{\text{poly log } N}$ and thus have rate asymptotically approaching 0. This is the first constant fraction improvement over the trivial bound that codes tolerating $N/2$ adversarial deletions must have rate going to 0 asymptotically. Equivalently, we show that there exists absolute constants A and $\delta > 0$ such that any set $C \subset \{0, 1\}^N$ of $2^{\log^A N}$ binary strings must contain two strings c and c' whose longest common subsequence has length at least $(1/2 + \delta)N$. As an immediate corollary, we show that q -ary codes tolerating a fraction $1 - (1 + 2\delta)/q$ of adversarial deletions must also have rate approaching 0.

Our techniques include string regularity arguments and a structural lemma that classifies binary strings by their oscillation patterns. Leveraging these tools, we find in any large code two strings with similar oscillation patterns, which is exploited to find a long common subsequence.

Contents

| | | |
|----------|--|-----------|
| 1 | Introduction | 1 |
| 1.1 | Our results | 2 |
| 1.2 | Related works | 2 |
| 1.3 | Deletion correction in related models | 3 |
| 2 | Proof overview | 5 |
| 3 | Preliminaries and Notation | 8 |
| 4 | The structure lemma and definition of types | 11 |
| 4.1 | The structure lemma | 11 |
| 4.2 | Definition of types | 15 |
| 5 | The entropy regularity argument | 15 |
| 5.1 | Flag balance | 16 |
| 5.2 | Flag balance of intervals | 16 |
| 5.3 | Flag balance of substrings | 17 |
| 6 | Green case | 19 |
| 7 | Blue-Yellow case | 21 |
| 8 | Putting it all together | 26 |
| 8.1 | Statistics | 26 |
| 8.2 | The Imbalanced case | 27 |
| 8.3 | Combining the arguments for the Imbalanced, Green, and Blue-Yellow cases | 28 |
| 8.4 | Finishing the proof | 30 |
| 9 | Conclusion and open questions | 31 |

*Computer Science Department, Carnegie Mellon University. venkatg@cs.cmu.edu. Research supported in part by NSF grants CCF-1814603 and a Simons Investigator Award.

[†]Department of Mathematics, Stanford University. alkjash@stanford.edu. Research supported by NSF GRFP Grant DGE-1656518.

[‡]Department of Computer Science, Stanford University. rayyli@cs.stanford.edu. Research supported by NSF Grants DGE-1656518, CCF-1814629, and by Jacob Fox's Packard Fellowship.

1 Introduction

This work considers the limits of reliable communication against an adversarial deletion channel. Suppose we are to transmit N bits on a channel that can adversarially delete a fraction p of the bits, leaving the receiver with a subsequence of length $(1-p)N$. Crucially, the receiver does not know the location of the deleted bits. We would like to achieve zero-error communication over such an adversarial deletion channel. To do so, we restrict the sequence of transmitted bits to a subset $C \subset \{0,1\}^N$ so that every $x \in C$ can be unambiguously identified from an arbitrary subsequence of x of length $(1-p)N$. It is easy to see that this property is equivalent to the property that for every two distinct codewords $x, y \in C$, the length of their longest common subsequence, denoted $\text{LCS}(x, y)$, is less than $(1-p)N$.

Defining $\text{LCS}(C)$ to be the largest value of $\text{LCS}(x, y)$ over all distinct pairs $x, y \in C$, we therefore call a subset $C \subseteq \{0,1\}^N$ a *p-deletion correcting code* if $\text{LCS}(C) < (1-p)N$. The rate of such a code, defined as $R(C) = (\log_2 |C|)/N$, measures the average number of information bits communicated per transmitted codeword bit. If there exists a family of such codes C whose rates are bounded away from zero as $N \rightarrow \infty$, we say it is possible to achieve a non-vanishing rate of information communication.

For any noise model of interest, one of the basic goals is to understand the threshold noise level below which it is possible to communicate with non-vanishing rate. For example, it is well-known that for a channel that flips an adversarially chosen set of at most pN bits, the threshold value for the error-fraction p equals $1/4$. On the other hand, for the adversarial deletions channel, this fundamental question remains unsolved:

What is the largest fraction of deletions $p \in (0, 1)$ for which it is possible to achieve zero-error communication with non-vanishing information rate?

Formally, define the *zero-rate threshold* of adversarial bit-deletions to be

$$p_{\text{del}}^{\text{thr}} := \sup\{p \mid \exists \alpha_p > 0 \text{ s.t for infinitely many } N \text{ there is a subset } C \subset \{0, 1\}^N \text{ with } \text{LCS}(C) < (1-p)N \text{ and } |C| \geq 2^{\alpha_p N}\}. \quad (1)$$

The above question is then: What is the value of $p_{\text{del}}^{\text{thr}}$? We have a trivial upper bound $p_{\text{del}}^{\text{thr}} \leq 1/2$. Indeed, among any three strings $x, y, z \in \{0, 1\}^N$, there must be two with the same majority bit, and thus a common subsequence (of all 0's or all 1's) of length at least $N/2$. Thus any $1/2$ -deletion correcting code $C \subset \{0, 1\}^N$ satisfies $|C| \leq 2$.

The value of $p_{\text{del}}^{\text{thr}}$ remains unknown. Even more starkly, as simplistic as the above argument is, it was not previously known if $p_{\text{del}}^{\text{thr}}$ is strictly bounded away from $1/2$, or whether there are in fact codes of non-vanishing rate for correcting a $(1/2 - \delta)$ fraction of deletions for any desired $\delta > 0$. This tantalizing question was implicit in early works on deletion codes, particularly in [Ull67], which gave bounds on the achievable tradeoffs between rate and deletion fraction, and was explicitly raised in [KMTU11]. Since then, this question has been mentioned in several works, including the work of Bukh and Ma [BM14] which showed that an upper bound of $\frac{1}{2} - \frac{1}{\text{poly} \log N}$ on the correctable deletion fraction, and many recent works on deletion code constructions such as [Wan15, GL16, GW17, BGH17, GL20, GHS20], other works on coding theory [ZBJ20], as well as the recent surveys [CR21, HS21]. In the other direction, the best known lower bound $p_{\text{del}}^{\text{thr}} > \sqrt{2} - 1$ is due to [BGH17], who constructed explicit binary codes of non-vanishing rate to correct a fraction of deletions approaching $\sqrt{2} - 1$ (see [SZ99, KMTU11] for prior constructions).

1.1 Our results

In this work, we prove the first nontrivial upper bound on $p_{\text{del}}^{\text{thr}}$.

Theorem 1.1. *There exists an absolute constant $\delta_0 > 0$ such that $p_{\text{del}}^{\text{thr}} \leq \frac{1}{2} - \delta_0$. More concretely, there exists absolute constants $A, \delta_0 > 0$ such that for all large enough N , any binary code $C \subset \{0, 1\}^N$ tolerating $(\frac{1}{2} - \delta_0)N$ adversarial deletions must satisfy $|C| \leq 2^{(\log N)^A}$.*

We show the above in the contrapositive form—in any code $C \subset \{0, 1\}^N$ of quasi-polynomial size, we find two codewords $s, t \in C$ with $\text{LCS}(s, t) > (1/2 + \delta_0)N$. We made no attempts to optimize the value of δ_0 but regardless it is very small for our argument. In Section 2, we give an overview of the proof and an outline of this paper. In the remainder of this introduction we survey some generalizations of Theorem 1.1 and connections to other problems in coding theory.

Non-binary alphabets. We generalize Theorem 1.1 to alphabets of larger size. Let us denote the quantity analogous to (1) for any fixed alphabet size $q \geq 2$, namely the zero-rate threshold for q -ary deletion codes, by $p_{\text{del}}^{\text{thr}}(q)$. The trivial upper bound is $p_{\text{del}}^{\text{thr}}(q) \leq 1 - 1/q$; this corresponds to finding a common sequence of at least N/q repeated i 's between two strings that share the same most frequent symbol $i \in \{0, 1, \dots, q-1\}$, in any code of size bigger than q . Just as in the binary case, no improvement over this trivial bound was previously known.

For any code $C \subseteq \{0, 1, \dots, q-1\}^N$ over an alphabet of size $q > 2$, we may pick some two symbols i, j and a set $C_{i,j} \subseteq C$ of at least $|C|/q^2$ strings whose two most frequent symbols are i and j . We can then obtain a binary code $C' \subseteq \{i, j\}^{2N/q}$ by restricting each element of $C_{i,j}$ to a substring of length $2N/q$ consisting only of i 's and j 's. Applying Theorem 1.1 to C' , we see that some two strings in C' have a common subsequence with length at least $(\frac{1}{2} + \delta_0)\frac{2N}{q}$. We have thus shown the following theorem as an immediate corollary of Theorem 1.1.

Theorem 1.2. *Fix an integer $q \geq 2$. Then*

$$p_{\text{del}}^{\text{thr}}(q) \leq 1 - \frac{1+2\delta_0}{q} < 1 - \frac{1}{q},$$

where $\delta_0 > 0$ is the positive constant promised in Theorem 1.1.

We note that for the simpler model of erasures where the location of missing symbols are known to the decoder, the zero-rate threshold equals $1 - 1/q$.¹ Thus our results also show a formal separation between the zero-rate threshold for the models of erasures and deletions, for any fixed alphabet.

In the list-decoding model with list-size L for deletion fraction p , there can be up to L codewords that contain the (arbitrary) input sequence $y \in \{0, 1\}^{(1-p)N}$. The zero-rate threshold for *list-decoding* from deletions, as the list-size $L \rightarrow \infty$, is known to equal $1 - 1/q$ [GW17]. Thus our result also demonstrates that list-decoding is provably more powerful in terms of the deletion fractions that can be handled with non-vanishing rate.

1.2 Related works

Performance of random codes. An ubiquitous approach to establish strong, and in many cases the best known, *possibility* results in coding theory is to analyze random codes of certain rates. These results typically

¹The erasure fraction correctable by a code is exactly governed by its relative (Hamming) distance. The Plotkin bound shows that the rate must be vanishing for relative Hamming distance $1 - 1/q$. We know the existence and even explicit constructions of codes of non-vanishing rate and relative Hamming distance $1 - 1/q - \epsilon$ for any $\epsilon > 0$.

also identify the precise performance threshold of random codes [GMR⁺21]. For the case of binary deletion codes, however, the performance of random codes itself is hard to analyze, as we do not rigorously know a tight estimate of the expected length γn of the longest common subsequence of two random n -bit strings (γ is called the Chvátal-Sankoff constant [CS75]). The known bounds on this expectation γn [Lue09], together with standard probabilistic arguments, imply that with high probability, random codes can tolerate a deletion fraction at least 0.17, but also at most 0.22 [KMTU11]. For codes over alphabet size q , random codes can correct a deletion fraction approaching $1 - 2/\sqrt{q}$ for large q [KLM04].

As mentioned earlier, we now have constructions of binary codes that can correct a deletion fraction 0.414 [BGH17], which is substantially better than random codes. This raised the possibility that perhaps there might be binary codes of non-vanishing rate capable of correcting a deletion fraction all the way up to the trivial limit of $1/2$, which we refute in this work.

Trade-offs for correcting $N/2 - N^{1-\theta}$ deletions. In terms of previously known limitations of deletion codes, Bukh and Ma [BM14] showed that for each fixed r and large enough N (specifically, at least $r^{O(r)}$), every set $C \subseteq \{0, 1\}^N$ of size $r + 4$ satisfies

$$\text{LCS}(C) \geq \frac{N}{2} + \Omega(r^{-9})N^{1-1/r}. \quad (2)$$

Choosing r appropriately, the result (2) implies that there exist absolute constants b, c such that every code $C \subseteq \{0, 1\}^N$ with $\text{LCS}(C) < \frac{N}{2} + \frac{N}{(\log N)^b}$ has size $|C| \leq c \frac{\log N}{\log \log N}$. Bukh and Ma demonstrated that this $N^{1-1/r}$ advantage in (2) is asymptotically sharp for each fixed r , by exhibiting a set \mathcal{W} of $(r + 4)$ N -bit strings with $\text{LCS}(\mathcal{W}) \leq \frac{N}{2} + O(N^{1-1/r})$. Interestingly, this set \mathcal{W} played a crucial role in the developments on *constructions* of codes to correct a large fraction of deletions in [BGH17, GL20], as well as codes achieving the zero-rate threshold for list decoding from insertions and deletions in [GHS20]. A suitable modification of this Bukh-Ma code \mathcal{W} also drives the best known 0.414-deletion correcting codes of [BGH17].

Twins and regularity techniques. One of the ideas used in this work is a new regularity-type result about strings. Szemerédi’s regularity lemma and its variants are ubiquitous in extremal and additive combinatorics, but applying these ideas to coding theory is a relatively recent development. The first example of such a result was proved by [APP13], and their regularity lemma roughly shows that every long string can be partitioned into a constant number of consecutive substrings, each of which is regular (a regular string is one in which the one-density in any long consecutive substring is close to the one-density in the whole string). They used this regularity lemma to prove that every string of length N contains two disjoint copies of some length $(1/2 - o(1))N$ subsequence (so-called “twins”). Given the similarity between finding twins in a single string and finding long common sequences between different strings, it should not come as a surprise that these techniques are useful here as well. The main difference in our approach is that we require a stronger regularity condition, which is that every substring not only has the same one-density but has similar “oscillation statistics” at many scales with the parent string.

1.3 Deletion correction in related models

To offer some wider context, we now discuss some results related to the broader study of codes for deletions and synchronization errors under various channel assumptions.

Non-adversarial models. Our work focuses on the adversarial model, where an arbitrary subset of p fraction of the codeword bits, can be deleted. There is a rich body of work on the binary deletion channel where each codeword bit is deleted i.i.d with probability p . In this case, it is known that one can have positive

rate codes that ensure vanishing miscommunication probability even for p approaching 1 (so the zero-rate threshold equals 1). The interested reader can find more information about codes for the deletion channel in the surveys [Mit09, CR21].

One can consider models that are intermediate in power between i.i.d random and adversarial channels. For instance, in the *oblivious* model the deletion pattern can be chosen arbitrarily, but without knowledge of the codeword. In this case, too, the zero-rate threshold is 1, as for any $p < 1$, Guruswami and Li [GL20] showed the existence of codes that ensured that for every pattern of p -fraction deletions *most* codewords are communicated correctly.² Their work also considered the *online* model, where the decision to delete the i -th bit must be made based only on the first i bits of the codeword. They showed that the zero-rate threshold for this model (again, for the average-error criterion of ensuring most codewords are communicated correctly for any deletion pattern) equals $1/2$ if and only if $p_{\text{del}}^{\text{thr}} = 1/2$. By virtue of Theorem 1.1, this implies that the zero-rate threshold for the online model is also bounded away from $1/2$.

Large alphabets. We focused on codes over the binary and fixed small alphabets in this work. This is in fact the most challenging setting for deletion codes. Indeed, if the code alphabet is allowed to grow with N , then one can include the index i along with the i -th codeword symbol, effectively reducing the deletion model to the much simpler erasure model, where Reed-Solomon codes give a simple, optimal solution. For alphabets that are large, but still independent of N , a natural greedy strategy shows the existence of codes of rate $(1 - p - \epsilon)$ capable of correcting a fraction p of deletions, over an alphabet of size $\exp(O(1/\epsilon))$ [GW17]. In particular, the zero-rate threshold approaches 1. Also, $1 - p$ is a trivial upper bound on the possible rate, even for the simpler model of p fraction of erasures. Explicit constructions of p -deletion correcting of rate approaching $1 - p$ over an alphabet size independent of N were given in [HS18] based on synchronization strings, which is a very elegant tool that has since found several other applications (see the survey [HS21]).

Insertions and deletions. Another form of errors that affect the synchronization between sender and receiver are insertions of symbols. It is well known (since [Lev66]) that a code C with $\text{LCS}(C) < (1 - p)N$ can tolerate any combination of a total of pN insertions and deletions (insdel errors). Thus allowing insertions as well does not change the combinatorial aspects of the underlying coding problem, as it is governed by the LCS. However, for efficient algorithms for insdel errors are not implied by deletion correction algorithms, and have to be reworked [GL16].

In the model of list-decoding, even the combinatorial aspects are more nuanced in the presence of insertions. The trade-off between the combinations of fractions of insertions and deletions that governs the zero-rate region exhibits an interesting piece-wise linear behavior [GHS20]. (As mentioned earlier, the zero-rate threshold for list-decoding q -ary codes from deletions alone equals $1 - 1/q$.)

Low-deletions regime. This work focused on the largest deletion fraction that can be corrected with non-vanishing rate. At the opposite end of the spectrum are codes to correct a deletion fraction $p \rightarrow 0$. In this case, the optimal rate behaves as $1 - O(p \log(1/p))$ and we also know explicit codes with such rate $1 - O(p \log^2(1/p))$ and efficient deletion-correction algorithms [CJLW18, Hae19]. There has also been an active line of recent code constructions, triggered by [BGZ18], for correction of a fixed *number* k of deletions with redundancy at most $c_k \log N$. We now have codes with the optimal (up to constant factors) redundancy of $O(k \log N)$ [CJLW18, Hae19, SB21, SGB20].

²This average-case criterion to achieve decoding success for most, as opposed to all, codewords is necessary, as otherwise tackling the oblivious model becomes as hard as tackling the adversarial model. Alternatively, one can allow a stochastic encoder, and ensure high probability of successful transmission of each message when averaged over the choice of its random encoding.

2 Proof overview

In this section, we give a high-level overview of the proof of Theorem 1.1, as well as the organization of the rest of this paper. Let $C \subseteq \{0, 1\}^N$ be a binary code of size $2^{(\log N)^A}$ for some large constant A , and our goal will be to find two elements $s, t \in C$ for which $\text{LCS}(s, t) \geq (1/2 + \delta_0)N$. The proof breaks down into five conceptually independent parts that roughly correspond to the Sections 4 through 8. It will be natural to explain these parts here in roughly reverse order, starting with Section 8.

Pigeonholing by “statistics”. The only place where we use the size of C is in the final Section 8, which wraps up the proof of Theorem 1.1. We need C to be large enough to find by the pigeonhole principle two elements $s, t \in C$ with similar “macroscopic statistics.” That is, we pick s and t to have the same number of ones in every long subinterval of length $N/\text{poly log } N$, and also to share some other statistics that characterize the “frequencies at which they oscillate.” As there are only $O(\text{poly log } N)$ long intervals and the statistics in question take on only $2^{\text{poly log } N}$ possible values on each interval, C is large enough to guarantee the existence of two s and t sharing identical statistics on all such intervals. The remaining sections explain how to define the statistics we care about and show that if s and t have identical statistics, then they must have a long LCS.

We now describe the three different high-level strategies we use for finding long common subsequences between s and t .

Strategy 1: Globally imbalanced strings. The first strategy is extremely simple: match corresponding ones (or zeros if there are more zeros) in s and t . In the case that s and t are significantly imbalanced, this strategy immediately finds an LCS of length noticeably more than $N/2$. This naive strategy is illustrated in Figure 1. It may be helpful to visualize the strategy as sending two runners, one down the length of each string, who must advance simultaneously while holding hands and only step on the ones in their respective strings.

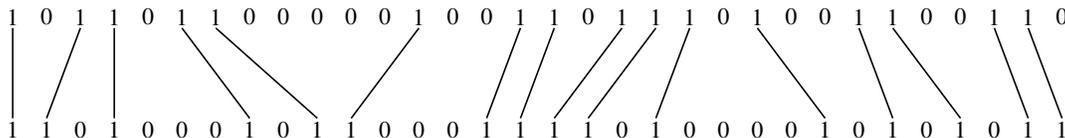


Figure 1: In the naive strategy, we match ones greedily between s and t . In this example, the strings are balanced so the naive strategy finds a common subsequence of length exactly 16 between s and t of length 32.

Strategy 2: Green strategy. The other two strategies, which we call the Green strategy and the Blue-Yellow strategy, are both modifications of the naive strategy. We first describe the Green Strategy, which is carried out in Section 6, as it is simpler. The naive strategy above can be thought of as a scanning process, where two runners move along the ones in s and t simultaneously, matching bits together to find a common subsequence composed entirely of ones. In the Green strategy, we fix an “oscillation period” $\ell \geq 1$ and preprocess s by counting, for every index i of a one-bit in s , the number of zeros between the i -th one and the $(i + \ell)$ -th one. For each such i , we plant a marker there, which we call a *Green ℓ -flag*, if there are more than $(1 + \varepsilon)(\ell - 1)$ zeros in this interval. Since there are exactly $\ell - 1$ ones in this same interval, the Green ℓ -flags are meant to signal to the runners that they are entering a zero-rich patch within s . The same preprocessing is also done in t .

In the Green strategy, the two runners proceed in the same way as the naive strategy except that each time the runners reach Green flags simultaneously, they switch to stepping only on zeros for the duration of the flagged regions. As there are more zeros than ones in the flagged regions, they pick up an advantage over the naive strategy for every single pair of Green flags they simultaneously match. The Green strategy is pictured in Figure 2.

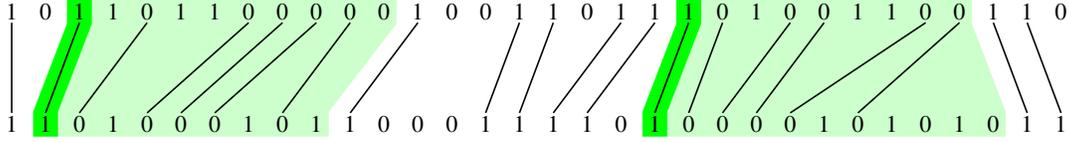


Figure 2: In the Green strategy, we find a long common subsequence by matching zeros instead of ones in the zero-rich patches immediately following Green ℓ -flags. In this example $\ell = 4$, the darker Green one-bits are Green ℓ -flags, and the light Green substrings following them are zero-rich patches. The Green strategy finds a common subsequence of length 20 between the s and t pictured above.

Our analysis of the success of the Green strategy is conditioned on the existence of a single oscillation period ℓ for which many of these zero-rich patches exist in both s and t . Indeed, suppose there exists ℓ for which a constant $g_\ell = \Omega(1)$ fraction of the ones in both s and t are Green ℓ -flags. Typically, we expect that the two runners hit Green flags simultaneously a constant g_ℓ^2 fraction of the time (this can be made rigorous by randomly shifting the starting position of one of the runners slightly). Thus, using the Green strategy one can find a common subsequence of length $(1/2 + g_\ell^2 \varepsilon)N$. The Green case finishes the proof of Theorem 1.1 if there exists any single oscillation period ℓ for which a constant fraction of ones in s and t are Green ℓ -flags.

Unfortunately, it is not always the case that a string s has a single oscillation period ℓ as above. Indeed, if

$$s_i \stackrel{\text{def}}{=} (1^i 0^{2^i})^{2^{k-i-1}},$$

then each s_i is a string of length 2^k which oscillates with period 2^i . It is not hard to check that the concatenation $s \stackrel{\text{def}}{=} s_0 s_1 \cdots s_{k-1}$ is a string of length $N = k \cdot 2^k$, such that there are at most $O(2^k)$ Green ℓ -flags in s for any given choice of ℓ . Thus, $g_\ell = O((\log N)^{-1}) = o(1)$ for every single ℓ , so the Green strategy is insufficient for this type of string. We remark that is essentially the worst case, and one can always find two strings s and t in C with $g_\ell = \Theta((\log N)^{-1})$ with the same ℓ , proving $\text{LCS}(s, t) \geq (1/2 + \Omega((\log N)^{-2}))N$ using the Green strategy alone. Already, this argument saves several factors of $\log N$ in the surplus term over the argument of Bukh and Ma [BM14].

Strategy 3: Blue-Yellow strategy. We give a third and final strategy which handles the cases in which $g_\ell = o(1)$ for all oscillation periods ℓ , which we call the Blue-Yellow strategy. This strategy, handled in Section 7, is the most involved of the three and we do not explain all of the technical complications here. However, the general picture is similar to the Green strategy: we send two runners along s and t matching ones, and find opportune moments to switch to matching zeros to gain an advantage.

In the Blue-Yellow strategy, we also mark certain one-bits in s and t by flags, but we use flags of two different colors Blue and Yellow. A Blue ℓ -flag is a relatively rare occurrence: it signals that there is an extremely zero-rich interval afterwards containing $\ell - 1$ ones and more than $\varepsilon^{-1}(\ell - 1)$ zeros. A Yellow ℓ -flag, on the other hand, is very common: it signals there is an interval afterwards containing $\ell - 1$ ones and more than $0.9(\ell - 1)$ zeros. Also, since there is no single oscillation period that captures the behavior of s and t (or else we would apply the Green strategy), we must pay attention to flags at many different scales

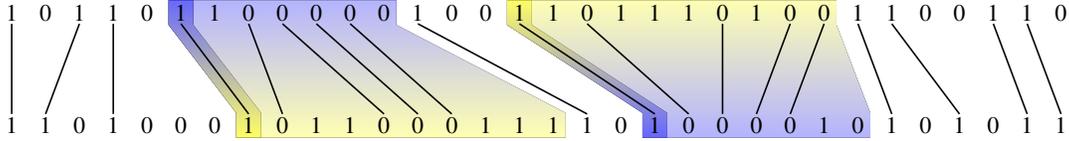


Figure 3: In the Blue case, we find a long common subsequence by matching zeros from extremely zero-rich patches (signalled by Blue flags) to longer relatively balanced patches (signalled by Yellow flags) and vice-versa. The Blue-Yellow strategy finds an LCS of length 18 between the s and t pictured above.

ℓ at the same time. The rough idea is then that the runners will switch to matching zeros when one of them reaches a Blue flag, and the other one simultaneously hits a Yellow flag of a similar scale, see Figure 3.

In the above diagram, the top runner reaches a Blue flag first, and the bottom runner happens upon a Yellow flag at the same time. This signals both of them to switch to matching zeros, which allows the top runner to gain a great advantage (since the patch past a Blue flag is so zero-rich). The bottom runner may lose out slightly in efficiency because Yellow intervals can have slightly fewer zeros than ones, but on net we see that more bits are used from the two patches together than would have been otherwise. In the long run, we expect Blue flags to appear approximately equally frequently in s and t , so the advantages and losses balance out to a net gain on both sides.

String regularity. In order to guarantee that the two runners remain relatively synchronized as the Blue-Yellow strategy proceeds, we need Blue flags to be somewhat consistently distributed within s and within t . We get this desired property by proving a string regularity lemma similar to that of [APP13] (see also [BZ16, ACK⁺19, HKPS21]). Our regularity lemma, proved in Section 5 differs from previous versions for words in that we use an *entropy increment* argument, rather than the usual density increment argument.

The structure lemma. The remainder of the paper is designed to set up the strings s and t so that one of the above three strategies can succeed in finding a long common subsequence. To do this, we prove a structure lemma in Section 4 about strings, which says each string falls in one of three cases (1) Globally imbalanced, (2) Green at some oscillation period ℓ , or (3) Blue-Yellow at some oscillation period ℓ . These types are defined such that, if two strings s and t have the same type and same oscillation period (if applicable), one can find a long common subsequence of s and t using the corresponding strategy.

With this structure lemma, we simply need to put all the pieces together (Section 8). We partition each codeword s into $\text{poly log } N$ substrings $s_1, \dots, s_{\text{poly log } N}$ and apply the structure lemma to each substring s_i . By pigeonhole, there exist two strings s and t such that, for each $i = 1, \dots, \text{poly log } N$, the substrings s_i and t_i are the same “type,” meaning that they are in the same case of the structure lemma and have the same oscillation period (if applicable). Then in each pair of substrings s_i and t_i one can find a long common subsequence using one of the three strategies, giving an overall large LCS.

It is important for two technical reasons to split into substrings s_i and t_i , rather than applying the structure lemma directly to the entire strings s and t . First, we need to randomly shift the starting position of one of the “runners” to get enough synchronized flags, incurring a loss of order up to $|s_1|$, so it is necessary that this loss is $o(N)$. Second, our regularity lemma guarantees Blue flags to have sufficient regularity at most, but not all, substrings lengths. Thus, we may not obtain the desired regularity until we consider substring lengths down to around $O(N/\text{poly log } N)$.

Organization. Section 3 collects the common notations, definitions, and preliminary lemmas we need for the rest of the paper. In Section 4, we prove a structure lemma which divides strings into three types, one

suitable to each of the three strategies above. In Section 5, we perform an additional technical argument to prove a “regularity-type” property of strings necessary for the runners to remain synchronized in the Blue-Yellow case (so that one does not race too far ahead of the other). These two sections together set the stage for Sections 6, 7, and 8 to handle the Green case, the Blue-Yellow case, and complete the proof, respectively. Finally, we collect some of the tantalizing open questions that remain in this area in Section 9.

3 Preliminaries and Notation

Constants. Throughout, fix $\varepsilon = 10^{-6}$ and $\gamma = 10^{-15} = 0.001\varepsilon^2$.

Subsequences and substrings. A *subsequence* in a string s is any string obtained from s by deleting zero or more symbols. In contrast, a *substring* is a subsequence consisting of consecutive symbols of s (substrings are also sometimes referred to as *subwords* elsewhere, but we do not use this terminology). Thus, if $s = 10001$, then 101 is a subsequence of s but not a substring.

Intervals and strings. Throughout, for real numbers x and y we define an *interval* $I = [x, y]$ to be the set of integers a such that $x \leq a \leq y$ (rather than the set of real numbers a). We let $[n]$ denote the interval $[1, n]$. We similarly define intervals $(x, y]$ and $[x, y)$ and (x, y) as subsets of the integers. The *size* of an interval is the number of integers in the interval. For $\alpha \in (0, 1)$ and real number x , let $(1 \pm \alpha)x$ denote the interval $[(1 - \alpha)x, (1 + \alpha)x]$.

Throughout the remainder of the paper, all strings are binary. Let $\{0, 1\}^*$ be the set of all binary strings of any nonnegative length. For integers $m \geq 0$ and $i \geq 1$, we let $I_{m,i} \stackrel{\text{def}}{=} [(i-1) \cdot 2^m + 1, i \cdot 2^m]$. We call such an $I_{m,i}$, where both the size is a power of two and the endpoints are aligned with the same power of two, a *dyadic interval*. For strings s_1 and s_2 , let s_1s_2 denote the string concatenation of s_1 with s_2 .

For a string s with L ones and an interval $I = [x, y]$, let s_I denote the contiguous substring of s between the x -th one of s (or the beginning of the string if $x \leq 0$) and the $(y+1)$ -st one of s (or until the end of the string if $y \geq L$), including the first but excluding the second. For example, if $w = 1001011$, we have $w_{[1,2]} = 10010$. For $m \geq 0$ and $i \geq 1$ write $s_{m,i}$ as shorthand for $s_{I_{m,i}}$. Informally, we refer to $s_{m,1}, s_{m,2}, s_{m,3}, \dots$ as the *substrings of s at scale m* . We note that leading zeros of a string are not included in any dyadic substring $s_{m,i}$, but this is negligible as we typically work with strings that start with a one.

We write $z(s)$ for the number of zeros in a string s .

Reversing strings that begin with a one. In the Blue-Yellow strategy on two strings s and t , we apply the Blue-Yellow matchings in pairs: (i) matching Blue flags in s with Yellow flags in t , and (ii) matching Blue flags in t with Yellow flags in s . Arguments (i) and (ii) can be seen as applying the same lemma (Lemma 7.1) when (ii) is viewed as applying the lemma on the reversals of s and t . However, since throughout we index our substrings s_I by the one-bits rather than all bits, it is helpful to slightly modify the definition of string reversal as follows. Given a string s starting with a one, let $\text{rev}(s)$ denote the string obtained by reversing the order of all the bits in s after the first bit. Thus, $\text{rev}(s)$ is only defined for strings starting with a one. It is easy to check the following properties of rev .

Lemma 3.1. *Let w be a string that begins with a one and has L ones in total.*

1. *The strings w and $\text{rev}(w)$ have the same length and number of ones.*
2. *For an interval $I = [x, y] \subset [L]$, we have $\text{rev}(w_I) = \text{rev}(w)_{[L+1-y, L+1-x]}$.*
3. *When w has $L = 2^n$ ones we have $\text{rev}(w_{m,i}) = \text{rev}(w)_{m, 2^{n-m} + 1 - i}$.*

Proof. The first item is obvious. For the second item, it suffices to consider when x and y are integers: indeed, for real numbers x and y , we have $\lceil x, y \rceil = [\lceil x \rceil, \lfloor y \rfloor]$ and $\lceil L+1-y, L+1-x \rceil = \lceil L+1-\lfloor y \rfloor, L+1-\lceil x \rceil \rceil$, so we may replace x and y with $\lceil x \rceil$ and $\lfloor y \rfloor$. The zeros between the i -th and $(i+1)$ -st one of w map to the zeros between the $(L+1-i)$ -th and $(L+2-i)$ -th one of $\text{rev}(s)$. Let z_i denote the number of zeros between the i -th and $(i+1)$ -st one of w . Then

$$\text{rev}(w_{\lceil x, y \rceil}) = \text{rev}(10^{z_x} 10^{z_{x+1}} 1 \cdots 10^{z_y}) = 10^{z_y} 10^{z_{y-1}} 1 \cdots 10^{z_x} = \text{rev}(w)_{\lceil L+1-y, L+1-x \rceil}.$$

The third item follows from the second:

$$\begin{aligned} \text{rev}(w_{m,i}) &= \text{rev}(w_{\lceil (i-1) \cdot 2^m + 1, i \cdot 2^m \rceil}) = \text{rev}(w)_{\lceil 2^{n+1} - i \cdot 2^m, 2^n - (i-1) \cdot 2^m \rceil} \\ &= \text{rev}(w)_{\lceil 2^m(2^{n-m-i} + 1), 2^m \cdot (2^{n-m-i} + 1) \rceil} = \text{rev}(w)_{m, 2^{n-m-i} + 1}. \quad \square \end{aligned}$$

Example 3.2. For $w = 1001011$, we have

$$\text{rev}(w_{\lceil 1, 2 \rceil}) = \text{rev}(10010) = 10100 = (1110100)_{\lceil 3, 4 \rceil} = \text{rev}(w)_{\lceil 3, 4 \rceil}.$$

Lemma 3.3. (*rev preserves LCS*) For strings s and t starting with a one, $\text{LCS}(s, t) = \text{LCS}(\text{rev}(s), \text{rev}(t))$.

Proof. The LCS always matches the first bits if they are equal, and reversing strings preserves the LCS. \square

Flags. We now define flags, a key notion that measures the oscillation frequencies within string.

Definition 3.4 (Flags). For a positive integer ℓ and a string w , define an index $i \in \mathbb{Z}$ to be an ℓ -flag of rate r in w if $(\ell-1)^{-1}z(w_{\lceil i, i+\ell \rceil}) = r$. Here $r \in [0, +\infty]$ (so it can take on the value $+\infty$) and we define $0^{-1} \cdot 0 = 0$ and $0^{-1} \cdot m = +\infty$ for any positive integer m . The rate of an ℓ -flag i in w is the ratio of zeros to ones (strictly) between the i -th one and the $(i+\ell)$ -th one of w , and we would like to find ℓ -flags with high rate in order to execute the zero-matching strategies described in the previous section. We say ℓ -flag i of rate r is

$$\begin{cases} \text{Blue} & \text{if } r > \varepsilon^{-1}, \\ \text{Green} & \text{if } r > 1 + 2\varepsilon, \\ \text{Yellow} & \text{if } r > 0.9, \\ \text{Red} & \text{if } r \leq 0.9. \end{cases}$$

Note that Blue flags are Green flags and Green flags are Yellow flags. For a string w with L ones, for each $i \in [L]$, define $b_w(i)$ to be the largest power of two $\ell \in [L]$ such that i is a Blue ℓ -flag in w , and 0 if no such ℓ exists. We say i is a Blue ℓ^+ -flag in w if $b_w(i) \geq \ell$.

Imbalanced strings. For $\delta \in (0, 1/2)$, we say a string w with L ones is δ -imbalanced if its number of zeros $z(w)$ is not in $(1 \pm \delta)L$. For convenience, we simply say that w is imbalanced if it is ε -imbalanced with $\varepsilon = 10^{-6}$ defined at the beginning of this section. We will reason about imbalanced substrings w_I of w at various scales, and exploit the existence of these imbalanced substrings.

Lemma 3.5. Let w be a string with L ones, and let $\ell \geq 2\varepsilon^{-1}$. Suppose that i is a Blue or Green ℓ -flag in w , or $i \leq L - \ell + 1$ is a Red ℓ -flag. On the interval $I = [i, \min(i + \ell - 1, L)]$, the substring w_I is imbalanced.

Proof. If i is a Green ℓ -flag, substring w_I has at least $(1 + 2\varepsilon)(\ell - 1) > (1 + \varepsilon)\ell \geq (1 + \varepsilon)|I|$ zeros. Since Blue flags are Green flags, w_I is also imbalanced if i is a Blue ℓ -flag. If i is a Red ℓ -flag, substring w_I has at most $0.9(\ell - 1) < (1 - \varepsilon)|I|$ zeros. In all three cases, w_I is imbalanced, as desired. \square

It is also easy to see that if two imbalanced strings have the same length n and the same number of ones, then their LCS is a constant fraction larger than $n/2$.

Lemma 3.6. *Let $\delta \in (0, 1/2)$. Let s and t be δ -imbalanced strings of the same length with the same number L of ones in each. Then $\text{LCS}(s, t) \geq (1/2 + \delta/5)|s|$.*

Proof. If the number of zeros is at most $(1 - \delta)L$, then the all-ones string is a common subsequence of length $L \geq \frac{1}{2-\delta}|s| \geq (1/2 + \delta/5)|s|$. If the number of zeros is at least $(1 + \delta)L$, then the all-zeros string is a common subsequence of length at least $\frac{1+\delta}{2+\delta}|s| \geq (1/2 + \delta/5)|s|$. \square

Prefixes and suffixes. For a string w with L ones, and $\Delta \in [-L, L]$, let $\text{Trim}_\Delta(w) \stackrel{\text{def}}{=} w_{[\max(1, 1-\Delta), \min(L, L-\Delta)]}$. Thus, $\text{Trim}_\Delta(w)$ is a prefix of w if $\Delta \geq 0$ and a suffix otherwise. The following lemma (see Figure 4) shows that finding long common subsequences across prefixes and suffixes of many subintervals of s and t implies that $\text{LCS}(s, t)$ is large overall.

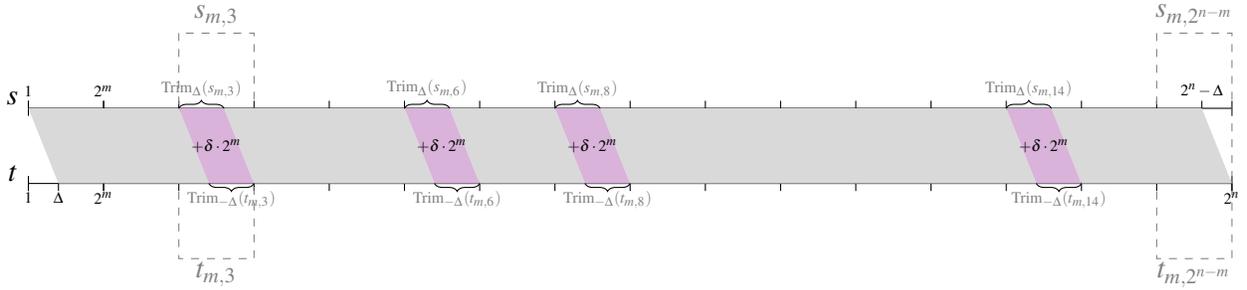


Figure 4: If, for some Δ , we find a large LCS between many (prefixes and suffixes of) dyadic substrings of s and t , then $\text{LCS}(s, t)$ is large overall. We note that Lemma 3.7 works as long as the subintervals (in purple) have LCS beating the trivial matching by $\delta \cdot 2^m$ on average, even though the figure depicts each subinterval having LCS advantage $\delta \cdot 2^m$. In the diagram, the set Z from Lemma 3.7 is $\{3, 6, 8, 14\}$.⁴

Lemma 3.7 (Prefix/Suffix LCS). *Let $\delta > 0$, let m and n be integers with $0 \leq m \leq n - 10 - \log \delta^{-1}$ and $L = 2^n$, and let $Z \subset [2^{n-m}]$ satisfy $|Z| \geq 2^{n-m}/10$. Suppose that s and t are strings with L ones each, and there exists $\Delta \in [-2^m, 2^m]$ and $\delta > 0$ such that*

$$\sum_{i \in Z} \text{LCS}(\text{Trim}_\Delta(s_{m,i}), \text{Trim}_{-\Delta}(t_{m,i})) \geq |Z| \cdot (2^m - |\Delta| + \delta \cdot 2^m).$$

Then we have

$$\text{LCS}(s, t) \geq \left(1 + \frac{\delta}{20}\right) L.$$

Proof. Finding a common sequence between s and t is equivalent to exhibiting a matching between the bits of s and the bits of t such that only equal bits are matched and such that the matching is “non-crossing,” meaning that earlier bits of s are matched with earlier bits of t .

Consider the matching where we match the i -th one in s with the $(i + \Delta)$ -th one in t . This matches $L - |\Delta|$ ones. In this matching, for each $i \in Z$, the $2^m - |\Delta|$ ones of $\text{Trim}_\Delta(s_{m,i})$ are exactly matched to the $2^m - |\Delta|$

⁴Technically, the figure is invalid because we need $m \leq n - 10 - \log \delta^{-1}$ and here $m = n - 4$, but we ignore this issue for illustration.

ones of $\text{Trim}_{-\Delta}(t_{m,i})$. For each $i \in Z$, replace the matching between the ones of $\text{Trim}_{\Delta}(s_{m,i})$ and $\text{Trim}_{-\Delta}(t_{m,i})$ with a matching for the LCS of $\text{Trim}_{\Delta}(s_{m,i})$ and $\text{Trim}_{-\Delta}(t_{m,i})$.

All of these replacements can be done simultaneously and independently while keeping the matching non-crossing. Each of the $|Z|$ replacement operations deletes $2^m - |\Delta|$ pairs, and in total the replacements add $|Z|(2^m - |\Delta| + \delta \cdot 2^m)$ pairs. Thus in total the replacements increase the number of matched pairs by at least $|Z| \cdot \delta \cdot 2^m$. Thus, the total length of this common subsequence is at least (recall $L = 2^n$)

$$L - |\Delta| + |Z| \cdot (\delta 2^m) \geq L - 2^m + \frac{2^{n-m}}{10} \cdot \delta \cdot 2^m \geq L - \frac{\delta}{2^{10}}L + \frac{\delta}{10}L \geq \left(1 + \frac{\delta}{20}\right)L.$$

In the second inequality, we used that $m \leq n - 10 - \log \delta^{-1}$. Thus $\text{LCS}(s, t) \geq \left(1 + \frac{\delta}{20}\right)L$, as desired. \square

4 The structure lemma and definition of types

4.1 The structure lemma

Throughout this section, we reason about a single string w with L ones, and assume w starts with a one. Recall that $\varepsilon = 10^{-6}$. Our main structure lemma is as follows.

Lemma 4.1 (Structure Lemma). *If $w \in \{0, 1\}^*$ is a string that starts with one and has exactly $L = 2^n$ ones, and n is sufficiently large (in terms of ε), then at least one of the following conditions hold.*

1. *There exists an interval $I \subseteq [L]$ of size $|I| \geq \varepsilon^2 L$ such that w_I is imbalanced.*
2. *There exists $1 \leq \ell \leq L$ such that the number of Green ℓ -flags in w is at least $\varepsilon^2 L$.*
3. *There exists $1 \leq m \leq n$ such that the number of Blue $(2^m)^+$ -flags in w is at least $\varepsilon^2 L$, and for every $\ell \geq 2^m$ the number of Red ℓ -flags in w is at most $600\varepsilon L$.*

The three cases of the Structure Lemma correspond exactly to the three matching strategies outlined in the Overview (Section 2). Case 1 is when w is imbalanced at a macroscopic scale, i.e., a linear-length subword with density far from $\frac{1}{2}$. Case 2, the ‘‘Green case’’, is when w ‘‘fluctuates on a single scale’’ and can be treated by studying that scale only, i.e., using the Green strategy described in the Overview. Case 3 is when w is ‘‘sporadic’’ and must be analyzed at many scales simultaneously, which is done with the Blue-Yellow strategy in the Overview. Before we prove Lemma 4.1, we need the following technical lemma, which gives part of Lemma 4.1 under the additional assumption that many of the zeros in w are concentrated at Blue flags.

Lemma 4.2. *Suppose $\alpha > 0$, n is sufficiently large, $L = 2^n$, $1 \leq \ell \leq L$, and $w \in \{0, 1\}^*$ is a string with L ones. If*

$$\frac{1}{\ell} \sum_{i \in B_\ell} z(w_{[i, i+\ell)}) \geq \alpha L,$$

where B_ℓ is the set of all Blue ℓ -flags of w , then at least one of the following conditions hold.

1. *There exists an interval $I \subseteq [L]$ of size $|I| \geq \varepsilon^2 L$ such that w_I is imbalanced.*
2. *The number of Blue ℓ -flags in w is at least $\varepsilon^2 L$.*

3. The number of Blue ℓ^+ -flags in w is at least $(\alpha - 22\varepsilon)\varepsilon L/16$.

Proof. We assume Conditions 1 and 2 do not hold and prove Condition 3. We first prove a slightly stronger lower bound (see (4)) on the number of Blue ℓ^+ flags than claimed in Condition 3 in the special case that ℓ is a power of 2, and will then handle the case of general ℓ .

Since $|B_\ell| < \varepsilon^2 L$, if we define $A_\ell \stackrel{\text{def}}{=} \{i \in B_\ell \mid z(w_{[i, i+\ell)}) > 2\varepsilon^{-1}\ell\}$ we find that

$$\frac{1}{\ell} \sum_{i \in B_\ell \setminus A_\ell} z(w_{[i, i+\ell)}) \leq \frac{1}{\ell} \cdot (2\varepsilon^{-1}\ell) \cdot |B_\ell \setminus A_\ell| \leq 2\varepsilon L, \quad \text{so} \quad \frac{1}{\ell} \sum_{i \in A_\ell} z(w_{[i, i+\ell)}) \geq (\alpha - 2\varepsilon)L.$$

By the pigeonhole principle, we can pick a residue class $r \in \{1, \dots, \ell\}$ such that the set $S \subseteq [L/\ell]$ defined by $S \stackrel{\text{def}}{=} \{j \mid (j-1)\ell + r \in A_\ell\}$ satisfies

$$\sum_{j \in S} z(w_{[(j-1)\ell+r, j\ell+r)}) \geq (\alpha - 2\varepsilon)L.$$

Write $b_j \stackrel{\text{def}}{=} z(w_{[(j-1)\ell+r, j\ell+r)})$. We have that for each $j \in S$, $b_j > 2\varepsilon^{-1}\ell$, and $b_S \geq (\alpha - 2\varepsilon)L$ (using the summation notation $b_S \stackrel{\text{def}}{=} \sum_{j \in S} b_j$).

Let $L' = L/\ell$. Since ℓ and L are powers of 2, L' is as well. We consider the family of all dyadic intervals $I_{m,i} \stackrel{\text{def}}{=} [(i-1) \cdot 2^m + 1, i \cdot 2^m]$ where $0 \leq m \leq \log_2(L')$ and $1 \leq i \leq L' \cdot 2^{-m}$. Let \mathcal{I} be the set of such intervals $I_{m,i}$ maximal under the property that $b_{I_{m,i}} > 2\varepsilon^{-1}\ell \cdot |I_{m,i}|$. By maximality of the $I_{m,i}$, the intervals of \mathcal{I} are pairwise disjoint. Furthermore, for $j \in S$, we have $b_{I_{0,j}} = b_j > 2\varepsilon^{-1}\ell$, so each $j \in S$ is in some interval of \mathcal{I} .

We claim that these intervals satisfy $b_{I_{m,i}} \leq 4\varepsilon^{-1}\ell \cdot |I_{m,i}|$. Suppose otherwise. Either $I_{m,i} = [L']$ or there is a dyadic interval $I_{m+1, [i/2]}$ in $[L']$ containing $I_{m,i}$ with twice the size of $I_{m,i}$. In the former case, $z(w_{[L]}) = b_{[L]} > 4\varepsilon^{-1}\ell L' > L + \varepsilon L$, which would imply condition 1. In the latter case, $I_{m+1, [i/2]}$ is an interval containing $I_{m,i}$ satisfying $b_{I_{m+1, [i/2]}} > 2\varepsilon^{-1}\ell \cdot |I_{m+1, [i/2]}|$, contradicting the maximality of $I_{m,i}$. This proves the claim.

Since every $i \in S$ lies in some element of \mathcal{I} , we have

$$4\varepsilon^{-1}\ell \cdot \sum_{I_{m,i} \in \mathcal{I}} |I_{m,i}| \geq \sum_{I_{m,i} \in \mathcal{I}} b_{I_{m,i}} \geq b_S \geq (\alpha - 2\varepsilon)L,$$

and so $\sum_{\mathcal{I}} |I_{m,i}| \geq \frac{1}{4}(\alpha - 2\varepsilon)\varepsilon L/\ell$.

Thus the dyadic intervals in \mathcal{I} have an abundance of zeroes in total. We need to convert this into an abundance of ℓ^+ -flags. To this end, let us define $J_{m,i} \stackrel{\text{def}}{=} [(i-1) \cdot 2^m \ell + r, i \cdot 2^m \ell + r)$, defined so that $b_{I_{m,i}} = z(w_{J_{m,i}})$. The key observation is that if $I_{m,i} \in \mathcal{I}$, then any $j \in J_{m,i-1}$ is a Blue ℓ^+ -flag. Indeed, for such a j we have $[j, j + 2^{m+1}\ell) \supseteq J_{m,i}$, so

$$z(w_{[j, j+2^{m+1}\ell)}) \geq z(w_{J_{m,i}}) = b_{I_{m,i}} > 2\varepsilon^{-1}\ell \cdot |I_{m,i}| = \varepsilon^{-1} \cdot 2^{m+1}\ell,$$

so j is a Blue $(2^{m+1}\ell)$ -flag, and thus an ℓ^+ -flag as desired since ℓ is a power of 2.

We conclude that all of the elements of

$$T \stackrel{\text{def}}{=} [L] \cap \bigcup_{I_{m,i} \in \mathcal{I}} J_{m,i-1} \tag{3}$$

are Blue ℓ^+ -flags of w .

Note that the union in (3) may not be a disjoint union. Indeed, although any two intervals $I_{m_1, i_1}, I_{m_2, i_2} \in \mathcal{I}$ must be disjoint, their predecessor intervals $I_{m_1, i_1-1}, I_{m_2, i_2-1}$ may not be disjoint if $m_1 \neq m_2$ (and the

corresponding $J_{m,i}$ may not be either). To address this issue, we pass to a subcollection $\mathcal{S}' \subseteq \mathcal{S}$ so that for any two $I_{m_1,i_1}, I_{m_2,i_2} \in \mathcal{S}'$, their respective shifts I_{m_1,i_1-1} and I_{m_2,i_2-1} are disjoint. Notice that for disjoint $I_{m_1,i_1}, I_{m_2,i_2} \in \mathcal{S}$ with $m_1 \leq m_2$, their shifts I_{m_1,i_1-1} and I_{m_2,i_2-1} intersect only if $I_{m_1,i_1} \subsetneq I_{m_2,i_2-1}$. Thus, it suffices to find a subcollection $\mathcal{S}' \subseteq \mathcal{S}$ so that no interval I_{m_1,i_1} lies in the shift I_{m_2,i_2-1} of another. Such a subcollection can be picked greedily by scanning from right to left through \mathcal{S} , skipping any I_{m_1,i_1} which appears in the shift I_{m_2,i_2-1} of an interval already picked, and breaking ties by preferring larger intervals. Any greedily chosen I_{m_2,i_2} removes at most $|I_{m_2,i_2}|$ in total interval size from \mathcal{S}' , so the total size of the intervals in \mathcal{S}' is at least half of the total size of intervals in \mathcal{S} .

Thus, $\sum_{\mathcal{S}'} |I_{m,i}| \geq \frac{1}{2} \sum_{\mathcal{S}} |I_{m,i}|$, and $\{J_{m,i-1} \mid I_{m,i} \in \mathcal{S}'\}$ is now a disjoint collection. Inside \mathcal{S}' , there can be at most one interval $I_{m,i}$ for which $J_{m,i-1}$ does not lie entirely inside $[L]$, and $J_{m,i-1}$ must have size at most $\varepsilon^2 L$ or else

$$z(w_{J_{m,i-1}}) > (1 + \varepsilon) \cdot 2^m,$$

for $2^m \geq \varepsilon^2 L$, implying condition 1. It follows that w has at least

$$|T| \geq \sum_{I_{m,i} \in \mathcal{S}'} |J_{m,i-1}| - \varepsilon^2 L \geq \frac{1}{2} \sum_{I_{m,i} \in \mathcal{S}} |J_{m,i-1}| - \varepsilon^2 L \geq \frac{(\alpha - 10\varepsilon)\varepsilon}{8} L, \quad (4)$$

Blue ℓ^+ -flags. This proves the lemma, in fact with a stronger lower bound on number of Blue ℓ^+ flags, when ℓ is a power of 2.

Now suppose ℓ is not a power of 2. If ℓ' is the smallest power of 2 greater than or equal to ℓ , then all Blue $(\ell')^+$ -flags are also Blue ℓ^+ -flags and $1 \leq \ell' \leq L$ since L is a power of 2. Furthermore, if $B_{\ell'}$ is the set of Blue ℓ' -flags, $z(w_{[i,i+\ell]}) \leq z(w_{[i,i+\ell']}) \leq \varepsilon^{-1}(\ell' - 1)$ if $i \notin B_{\ell'}$. Thus, since $|B_{\ell'}| < \varepsilon^2 L$ we get

$$\frac{1}{\ell'} \sum_{i \in B_{\ell'} \setminus B_{\ell}} z(w_{[i,i+\ell]}) \leq \varepsilon L,$$

which implies

$$\frac{1}{\ell'} \sum_{i \in B_{\ell'}} z(w_{[i,i+\ell]}) \geq \frac{1}{\ell'} \sum_{i \in B_{\ell'} \cap B_{\ell}} z(w_{[i,i+\ell]}) \geq \frac{1}{2\ell} \sum_{i \in B_{\ell}} z(w_{[i,i+\ell]}) - \varepsilon L \geq (\alpha/2 - \varepsilon)L,$$

and so the conditions of the lemma are true with modified parameters $\ell' \geq \ell$ a power of 2 and $\alpha' = \alpha/2 - \varepsilon$. It follows by applying (4) with these parameters instead that w must have at least

$$\frac{(\alpha' - 10\varepsilon)\varepsilon}{8} L \geq \frac{(\alpha - 22\varepsilon)\varepsilon}{16} L$$

Blue ℓ^+ -flags in the general case, thus completing the proof. \square

Now we are ready to prove Lemma 4.1.

Proof of Lemma 4.1. We assume conditions 1 and 2 do not hold for some w , and prove condition 3.

Pick $m \in [0, n]$ maximal such that w contains at least $\varepsilon^2 L$ Blue $(2^m)^+$ -flags. To see that such an m exists, let B_1 denote the set of Blue 1-flags in w , which is just the set of one-bits in w immediately followed by at least one zero. Then, we have

$$\sum_{i \in B_1} z(w_{[i,i+1]}) = z(w_{[L]}) \geq L - \varepsilon L,$$

assuming condition 1 does not hold. Furthermore, because Blue flags are Green flags, condition 2 being false implies there are fewer than $\varepsilon^2 L$ Blue 2^m -flags for any $0 \leq m \leq n$. In particular, $|B_1| < \varepsilon^2 L$. Thus, the conditions of Lemma 4.2 are satisfied with $\ell = 1$ and $\alpha = 1 - \varepsilon$, and we obtain that either w satisfies condition 1 or condition 2 (since Blue flags are Green flags) or the number of Blue 1^+ -flags in w is at least

$$(\alpha - 22\varepsilon)\varepsilon L/16 = (\varepsilon - 23\varepsilon^2)L/16 \geq 2\varepsilon^2 L.$$

Hence we used that ε is sufficiently small. Thus, some such $0 \leq m \leq n$ exists.

By the maximality of m and the fact that there are fewer than $\varepsilon^2 L$ Blue 2^m -flags for any particular $0 \leq m \leq n$, we see that in fact $m \geq 1$ and the number of Blue $(2^m)^+$ -flags is in $[\varepsilon^2 L, 2\varepsilon^2 L]$. It remains to check that the second half of condition 3 holds.

Suppose $\ell \geq 2^m$, and let B_ℓ, G_ℓ, Y_ℓ , and R_ℓ be the sets of ℓ -flags in w which are Blue, Green, Yellow, and Red (respectively). Note that by our definitions of the colors, $B_\ell \subseteq G_\ell \subseteq Y_\ell$ and $Y_\ell \sqcup R_\ell = [L]$. Suppose for the sake of contradiction that $|R_\ell| > 600\varepsilon L$. We may assume $\ell \leq \varepsilon^2 L$, as otherwise a single Red ℓ -flag would violate condition 1. We can express $z(w_{[L]})$ as

$$z(w_{[L]}) = \frac{1}{\ell} \sum_{i=-\ell}^L z(w_{[i, i+\ell)})$$

since each $z(w_{[i]})$ appears exactly ℓ times in the sum on the right. Setting aside the terms on the right with $i \leq 0$, we find by breaking up the sum in terms of the colors of the flags,

$$z(w_{[L]}) \leq \frac{1}{\ell} \left(\sum_{i=-\ell}^0 z(w_{[i, i+\ell)}) + \sum_{i \in B_\ell} z(w_{[i, i+\ell)}) + (\ell - 1)(\varepsilon^{-1}|G_\ell \setminus B_\ell| + (1 + 2\varepsilon)|Y_\ell \setminus G_\ell| + 0.9|R_\ell|) \right). \quad (5)$$

We can bound $\frac{1}{\ell} \sum_{i=-\ell}^0 z(w_{[i, i+\ell)}) \leq z(w_{[\ell]})$, $|G_\ell \setminus B_\ell| \leq |G_\ell| < \varepsilon^2 L$ (since condition 2 is false), and $|Y_\ell \setminus G_\ell| \leq |Y_\ell| = L - |R_\ell|$. Putting these together with (5), we obtain

$$z(w_{[L]}) \leq L + 3\varepsilon L + z(w_{[\ell]}) + \frac{1}{\ell} \sum_{i \in B_\ell} z(w_{[i, i+\ell)}) - 0.1|R_\ell|. \quad (6)$$

Since condition 1 is false, we have $z(w_{[L]}) \geq L - \varepsilon L$, so together with (6) and $|R_\ell| > 600\varepsilon L$ we get

$$z(w_{[\ell]}) + \frac{1}{\ell} \sum_{i \in B_\ell} z(w_{[i, i+\ell)}) \geq 56\varepsilon L.$$

Next, we claim that $z(w_{[\ell]}) \leq \varepsilon L$. This follows from the facts that $\ell \leq \varepsilon^2 L$ and $z(w_{[\varepsilon^2 L]}) \leq \varepsilon L$ (by the assumption that condition 1 does not hold). We get

$$\frac{1}{\ell} \sum_{i \in B_\ell} z(w_{[i, i+\ell)}) \geq 55\varepsilon L.$$

The conditions of Lemma 4.2 are satisfied with this ℓ and $\alpha = 55\varepsilon$. Applying the lemma, we find that either w satisfies one of condition 1 or 2, or the number of Blue ℓ^+ -flags in w is at least $(55\varepsilon - 22\varepsilon)\varepsilon L/16 > 2\varepsilon^2 L$. This contradicts the observation we made before that the number of Blue $(2^m)^+$ -flags is in $[\varepsilon^2 L, 2\varepsilon^2 L]$ and completes the proof. \square

4.2 Definition of types

Using the structure theorem, we define below the *type* of a string roughly based on the case that it satisfies in the structure theorem. These three definitions of types (Imbalanced, Green, Blue-Yellow) roughly align with the three cases of the structure theorem, though for Green and Blue-Yellow types, it helps to additionally have an upper bound on ℓ , the length of the flags. Because we only prove the Structure Lemma (Lemma 4.1) for strings whose number of ones is a power of two, we also only define types for strings whose number of ones is a power of two, which is enough for our application. Recall that $\gamma = 0.001\epsilon^2$.

Definition 4.3. Given a string w with $L = 2^n$ ones with n sufficiently large, we say the *type* of w is

1. **Imbalanced** if there exists some interval $I \subseteq [L]$ of size $|I| \geq \epsilon^5 L$ such that w_I is imbalanced.
2. **ℓ -Green** for some integer $1 \leq \ell \leq \epsilon^5 L$ if the number of Green ℓ -flags in w is at least $\epsilon^2 L$.
3. **m -Blue-Yellow** if there exists $1 \leq m \leq n$ such that the number of indices $i \in [L]$ with $2^m \leq b_w(i) \leq \gamma L$ is at least $(\epsilon^2 - \gamma)L$, and the number of Red ℓ -flags in w is at most $600\epsilon L$ for any $\ell \geq 2^m$.

If w could be more than one type, we assign w one of the types arbitrarily.

Note that there are at most $1 + L + \log L = O(|w|)$ possible types for a string w . As a corollary of Lemma 4.1, each string w has a type, assuming n is sufficiently large:

Lemma 4.4. *If n is sufficiently large, each string w with $L = 2^n$ ones has a type.*

Proof. If w satisfies Case 1 of Lemma 4.1, then w has type Imbalanced.

If w satisfies Case 2 of Lemma 4.1 with parameter ℓ , then w has at least $\epsilon^2 L$ Green ℓ -flags, and in particular there exists an $i \leq L - \epsilon^2 L$ that is a Green ℓ -flag. If $\ell \geq \epsilon^5 L$, then by Lemma 3.5, the interval $I = [i, i + \ell - 1]$ of size at least $\epsilon^5 L$ gives that w_I is imbalanced, so w has type Imbalanced. If $\ell \leq \epsilon^5 L$, then w has type ℓ -Green.

If w satisfies Case 3 of Lemma 4.1 with parameter m , then there are at least $\epsilon^2 L$ indices with $b_w(i) \geq \epsilon^2 L$, and the number of Red ℓ -flags in w is at most $600\epsilon L$ for any integer $\ell \geq 2^m$. If there are at least γL indices $i \in [L]$ with $b_w(i) \geq \gamma L$, then some $i \leq L - \gamma L + 1$ satisfies $b_w(i) \geq \gamma L$, so by Lemma 3.5, there exists an interval I of size at least $\gamma L > \epsilon^5 L$ such that w_I is imbalanced, so w is type Imbalanced. Otherwise, for at least $(\epsilon^2 - \gamma)L$ indices $i \in [L]$, we have $2^m \leq b_w(i) \leq \gamma L$, so w is type m -Blue-Yellow. \square

5 The entropy regularity argument

In this section, we prove the regularity-type result Lemma 5.6, which roughly states that in most dyadic substrings of a given string s , the positions of the Blue flags are distributed relatively uniformly. In the Blue-Yellow strategy, we may be matching bits in s and t that lie in nearby but different dyadic intervals (because of our random shifting argument and because the Blue-Yellow strategy consumes ones from s and t at different rates). Because of this, it is helpful to say that there many neighboring pairs of dyadic intervals with similar Blue flag distributions in s and t .

5.1 Flag balance

Define the L^1 distance between two discrete probability distributions p, q to be $\|p - q\|_1 \stackrel{\text{def}}{=} \sum |p(x) - q(x)|$. Recall that $b_w(i)$ is the largest power of two $\ell \in [L]$ such that i is a Blue ℓ -flag in w , and 0 if no such ℓ exists. For a string w with L ones and an interval $I \subset [L]$, let $p_{w,I}$ denote the distribution of the value of $b_w(i)$ over a uniform random $i \in I$. Put another way, the probability mass $p_{w,I}(\ell)$ is the fraction of indices $i \in I$ with $b_w(i) = \ell$.

Definition 5.1 (Blue-flag-balance). For $\beta > 0$, we say that a dyadic interval $I_{m,i}$ is β -Blue-flag-balanced in w if $\|p_{w,I_{m-1,2i-1}} - p_{w,I_{m-1,2i}}\|_1 \leq \beta$. We say that a string w with $L = 2^n$ ones is β -Blue-flag-balanced if the interval $I_{n,1}$ is β -Blue-flag-balanced in w .

Showing Blue-flag balance is useful because we can show that if a Blue-flag-balanced string w has many Blue flags of a certain length, then both halves of w also have many Blue flags of the same length. The next lemma formalizes this idea.

Lemma 5.2. *If string w is β -Blue-flag-balanced with $L = 2^n$ ones, then for any set S of integers, we have*

$$|\Pr_{i \in [L]}[b_w(i) \in S] - \Pr_{i \in [L/2]}[b_w(i) \in S]| \leq \frac{\beta}{2}.$$

Proof. Since w is β -Blue-flag-balanced, interval $I_{n,1}$ is β -Blue-flag-balanced in w . We have

$$\begin{aligned} |\Pr_{i \in [L]}[b_w(i) \in S] - \Pr_{i \in [L/2]}[b_w(i) \in S]| &= \sum_{\ell' \in S} |p_{w,I_{n,1}}(\ell') - p_{w,I_{n-1,1}}(\ell')| \\ &\leq \sum_{\ell'} |p_{w,I_{n,1}}(\ell') - p_{w,I_{n-1,1}}(\ell')| \\ &= \|p_{w,I_{n,1}} - p_{w,I_{n-1,1}}\|_1 \\ &= \left\| \frac{p_{w,I_{n-1,1}} + p_{w,I_{n-1,2}}}{2} \right\|_1 \leq \frac{\beta}{2}. \end{aligned}$$

The third equality uses that $\frac{p_{w,I_{n-1,1}} + p_{w,I_{n-1,2}}}{2} = p_{w,I_{n,1}}$, and the last inequality uses the definition of interval $I_{n,1}$ being β -Blue-flag-balanced in w . \square

5.2 Flag balance of intervals

Our goal is to find a scale at which most intervals are Blue-flag-balanced. We start by proving a simple lemma about probability distributions. Recall that the binary entropy of a discrete probability distribution p is defined as $H(p) \stackrel{\text{def}}{=} -\sum_x p(x) \log p(x)$ over all values x in the support of p , and the logarithms are base 2.

Lemma 5.3. *If p^-, p , and p^+ are three discrete probability distributions supported on a finite domain Ω satisfying $p^-(x) + p^+(x) = 2p(x)$ for all $x \in \Omega$, then*

$$H(p^-) + H(p^+) \leq 2H(p) - \frac{1}{4} \|p^+ - p^-\|_1^2.$$

Proof. We use Pinsker's inequality, which states in the case of discrete probability distributions that the Kullback-Leibler divergence between two distributions P and Q satisfies

$$D_{\text{KL}}(P \| Q) = \sum_i P(i) \log \left(\frac{P(i)}{Q(i)} \right) \geq \frac{1}{2} \|P - Q\|_1^2.$$

In particular, applying this to the pairs $(P, Q) = (p^-, p)$ and $(P, Q) = (p^+, p)$, we obtain

$$\begin{aligned}
2H(p) - H(p^-) - H(p^+) &= \sum_i (p^-(i) \log p^-(i) + p^+(i) \log p^+(i) - 2p(i) \log(p(i))) \\
&= D_{\text{KL}}(p^- \| p) + D_{\text{KL}}(p^+ \| p) \\
&\geq \frac{1}{2} \|p^- - p\|_1^2 + \frac{1}{2} \|p^+ - p\|_1^2 \\
&= \frac{1}{4} \|p^+ - p^-\|_1^2. \quad \square
\end{aligned}$$

We now obtain with a regularity argument the following lemma, which is the most substantial result in this section.

Lemma 5.4 (Interval Blue-flag-balance). *For $\beta > 0$, $n \geq 2$, and any $w \in \{0, 1\}^N$ with $L = 2^n$ ones, except for at most $32\beta^{-3} \log n$ values of $m \in [0, n]$, the following holds: the number of dyadic intervals $I_{m,i}$ that are not β -Blue-flag-balanced in w is less than $\beta \cdot 2^{n-m}$.*

Proof. Consider the expression

$$E_m \stackrel{\text{def}}{=} 2^m \cdot \sum_{i=1}^{2^{n-m}} H(p_{w, I_{m,i}}).$$

By the definition of an β -Blue-flag-balanced interval, we obtain that whenever interval $I_{m,i}$ is not β -Blue-flag-balanced in w ,

$$\|p_{w, I_{m-1, 2i-1}} - p_{w, I_{m-1, 2i}}\|_1 \geq \beta,$$

and so if there are t_m dyadic intervals $I_{m,i}$ that are not β -Blue-flag-balanced in w , we obtain

$$E_{m-1} \leq E_m - 2^{m-1} \cdot t_m \cdot \frac{1}{4} \beta^2 \leq E_m - 2^{m-3} t_m \beta^2,$$

by Lemma 5.3. Since $b_w(i) \leq L$ is either 0 or a power of two for all indices $i \in [L]$, we have that $b_w(i)$ takes on one of $n+2$ values. Thus, we have $E_n = 2^n \cdot H(p_{w, I_{n,1}}) \leq \log(n+2) \cdot 2^n$. Since we also have $E_0 \geq 0$, at most $8\beta^{-3} \log(n+2) < 32\beta^{-3} \log n$ values of t_m are at least $\beta \cdot 2^{n-m}$, completing the proof. \square

5.3 Flag balance of substrings

In Lemma 5.4 we showed that there exists many scales m where many (dyadic) *intervals* were β -Blue-flag-balanced in the sense of Definition 5.1. For technical reasons, it is helpful to establish that there are many *substrings* that are β -Blue-flag-balanced, and we do so in this section. The distinction here is that certain one-bits in the interval I may be Blue ℓ -flags in w , but not Blue ℓ -flags in w_I once the zeros to the right of I are taken out of consideration.

For a string w with L ones, let $p_w \stackrel{\text{def}}{=} p_{w, [L]}$. Note that the distribution $p_{w, I}$ may be different from the distribution p_{w_I} , because indices $i \in I$ that are Blue ℓ -flags in string w may not correspond to Blue ℓ -flags in substring w_I . However, the converse is true: for $I = [x, y]$, if $i - x + 1$ is a Blue ℓ -flag of substring w_I , then i is a Blue ℓ -flag of string w . Because of this, we can show that $p_{w, I}$ and p_{w_I} are similar in distribution under certain conditions.

Lemma 5.5. *Let $\beta > 0$, w be a string with L ones, $I \subset [L]$ be an interval, and ℓ_0 be an integer, such that at most $\beta|I|$ indices $i \in I$ satisfy $b_w(i) \geq \ell_0$. Then*

$$\|p_{w, I} - p_{w_I}\|_1 \leq 2 \left(\beta + \frac{\ell_0}{|I|} \right).$$

Proof. Recall that $b_w(i)$ is the largest power of two such that the i -th one of w is an $b_w(i)$ -flag of w (or 0 if no such power of two exists). For an interval $I = [x, y]$, if index $i - x + 1$ is a Blue ℓ -flag of w_I , then index i is a Blue ℓ -flag of w , and furthermore if index i is a Blue ℓ -flag of w and $x \leq i \leq y - \ell$, then index $i - x + 1$ is a Blue ℓ -flag of w_I as well. Hence, for all $x \leq i \leq y - \ell_0$ with $b_w(i) \leq \ell_0$, we have that $b_w(i) = b_{w_I}(i - x + 1)$. Thus, by the union bound,

$$\Pr_{i \in I}[b_w(i) \neq b_{w_I}(i - x + 1)] \leq \Pr_{i \in I}[i \geq y - \ell_0] + \Pr_{i \in I}[b_w(i) \geq \ell_0] \leq \frac{\ell_0}{|I|} + \beta, \quad (7)$$

We also have

$$\|p_{w, I} - p_{w_I}\|_1 = \sum_{\ell'} |p_{w, I}(\ell') - p_{w_I}(\ell')| = \sum_{\ell'} \frac{1}{|I|} \left| \sum_{i \in I} \mathbb{1}(b_w(i) = \ell') - \sum_{i \in I} \mathbb{1}(b_{w_I}(i - x + 1) = \ell') \right|$$

Thus, the expression $\|p_{w, I} - p_{w_I}\|_1$ is a $\frac{1}{|I|}$ -Lipschitz function in the indicator functions $\mathbb{1}(b_w(i) = \ell')$ for $i \in I$ and ℓ' a power of two or 0. Changing the value of any single $b_w(i)$ changes the value of at most two such indicator functions, and furthermore we know that changing the value of $|I| \cdot \Pr_{i \in I}[b_w(i) \neq b_{w_I}(i - x + 1)]$ values of $b_w(i)$ makes the expression $\|p_{w, I} - p_{w_I}\|_1$ equal to 0, so we have that

$$\|p_{w, I} - p_{w_I}\|_1 \leq \frac{1}{|I|} \cdot 2 \cdot |I| \cdot \Pr_{i \in I}[b_w(i) \neq b_{w_I}(i - x + 1)] \leq 2 \cdot \Pr_{i \in I}[b_w(i) \neq b_{w_I}(i - x + 1)] \quad (8)$$

Combining (7) and (8) gives the desired result. \square

Lemma 5.4 argues about the Blue-flag-balance of intervals. Combining Lemma 5.4 with Lemma 5.5, we obtain the following result about the Blue-flag-balance of substrings.

Lemma 5.6 (Substring Blue-flag-balance). *Let $\beta > 0$, and n be sufficiently large in terms of β . Let $w \in \{0, 1\}^N$ be a string with $L = 2^n$ ones, and suppose that at most $\beta^2 L$ indices $i \in [L]$ satisfy $b_w(i) \geq 2^{n-200\beta^{-3}\log n}$. Then, except for at most $32\beta^{-3}\log n$ values of $m \in [n - 150\beta^{-3}\log n, n]$ the following holds: the number of $i \in [2^{n-m}]$ for which $w_{m,i}$ is not 6β -Blue-flag-balanced is less than $3\beta \cdot 2^{n-m}$.*

Proof. Let $m \in [n - 150\beta^{-3}\log n, n]$ be any value such that there are at most $\beta \cdot 2^{n-m}$ dyadic intervals $I_{m,i}$ that are not β -Blue-flag-balanced in w . By Lemma 5.4, all but $32\beta^{-3}\log n$ values of m have this property. We show that each such m satisfy the requirements of the lemma.

Call an index $i \in [2^{n-m}]$ *good* if (1) the dyadic interval $I_{m,i}$ is β -Blue-flag-balanced in w , and (2) for both intervals $I \in \{I_{m-1,2i-1}, I_{m-1,2i}\}$, there are at most $\beta|I|$ indices $i \in I$ with $b_w(i) \geq 2^{n-200\beta^{-3}\log n}$. By the choice of m , there are less than $\beta \cdot 2^{n-m}$ choices of $i \in [2^{n-m}]$ that violate requirement (1). Next, we use the assumption that in total at most $\beta^2 L$ indices $i \in [L]$ satisfy $b_w(i) \geq 2^{n-200\beta^{-3}\log n}$. Thus, at most $\beta \cdot 2^{n-m+1}$ of the dyadic intervals I of size 2^{m-1} contain at least $\beta|I|$ indices $i \in I$ satisfying $b_w(i) \geq 2^{n-200\beta^{-3}\log n}$. Hence, at most $2\beta \cdot 2^{n-m}$ choices of $i \in [2^{n-m}]$ violate requirement (2). We see that all but less than $3\beta \cdot 2^{n-m}$ choices of $i \in [2^{n-m}]$ are good.

We now show that for each good index $i \in [2^{n-m}]$, the substring $w_{m,i}$ is 6β -Blue-flag-balanced. By Lemma 5.5, for each good i and either interval $I \in \{I_{m-1,2i-1}, I_{m-1,2i}\}$, we have

$$\|p_{w, I} - p_{w_I}\|_1 \leq 2 \left(\beta + \frac{2^{n-200\beta^{-3}\log n}}{2^m} \right) \leq 2 \left(\beta + 2^{-50\beta^{-3}\log n} \right).$$

Since interval $I_{m,i}$ is β -Blue-flag-balanced with respect to w , we have by the triangle inequality

$$\begin{aligned} \|p_{w_{m-1,2i-1}} - p_{w_{m-1,2i}}\|_1 &\leq \|p_{w_{m-1,2i-1}} - p_{w_{I_{m-1,2i-1}}}\|_1 + \|p_{w_{m-1,2i}} - p_{w_{I_{m-1,2i}}}\|_1 + \|p_{w_{I_{m-1,2i-1}}} - p_{w_{I_{m-1,2i}}}\|_1 \\ &\leq 4(\beta + 2^{-50\beta^{-3}\log n}) + \beta < 6\beta, \end{aligned}$$

assuming n is sufficiently large. Hence, for each good i , the substring $w_{m,i}$ is 6β -Blue-flag-balanced, as desired. \square

6 Green case

Call a pair of strings (s,t) a *Green pair* if

1. s and t have the same number L of ones, and
2. there exists an $1 \leq \ell \leq \varepsilon^5 L$ such that s and t are both type ℓ -Green.

In this section, we implement the Green strategy in the Overview (Section 2). Specifically, we show (Lemma 6.2) that when we have strings s and t and some scale m^* with many Green pairs $(s_{m^*,i}, t_{m^*,i})$, then we can find a common subsequence of s and t of length $(0.5 + \delta)|s|$. At the highest level, we do this by finding common subsequences within the Green pairs, and matching ones elsewhere, using the Prefix/Suffix LCS Lemma (Lemma 3.7).

Within the Green pairs, we match ones everywhere, except that we switch to matching zeros at Green flags in s and t .

Lemma 6.1 (Green matching lemma). *Let L be a power of two. Let (s,t) be a Green pair where strings s and t have L ones each. Then for Δ uniformly random in $[-L, L]$, we have*

$$\mathbf{E}_\Delta [\text{LCS}(\text{Trim}_\Delta(s), \text{Trim}_{-\Delta}(t)) + |\Delta|] \geq L + \frac{\varepsilon^5}{8}L.$$

Proof. For a fixed Δ in $[-L, L]$, let G'_Δ be the set of indices $i \in [L]$ such that i is Green ℓ -flag of s and $i + \Delta \in [L]$ and $i + \Delta$ is a Green ℓ -flag of t . Let $G_\Delta \subseteq G'_\Delta$ be a subset of size at least $|G'_\Delta|/\ell - 1$ such that any two distinct $i, i' \in G_\Delta$ satisfy $|i - i'| \geq \ell$, and furthermore every $i \in G_\Delta$ satisfies $i + \Delta + \ell \leq L$. Such a G_Δ can be greedily selected from G'_Δ : we can get $|G_\Delta|/\ell$ indices such that any two differ by at least ℓ , and, as any $i \in G'_\Delta$ satisfies $i + \Delta \leq L$, we can guarantee $i + \Delta + \ell \leq L$ for all $i \in G_\Delta$ by removing the largest index.

Since s and t are type ℓ -Green, both s and t have at least $\varepsilon^2 L$ Green ℓ -flags. Thus, for each Green ℓ -flag $i \in [L]$ of s , there are at least $\varepsilon^2 L$ values of Δ such that $i \in G'_\Delta$. Hence, $\Pr_{\Delta \in [-L, L]}[i \in G'_\Delta] \geq \frac{\varepsilon^2 L}{2L+1} > \frac{\varepsilon^2}{3}$. By linearity of expectation, we have $\mathbf{E}_{\Delta \sim [-L, L]}[|G'_\Delta|] \geq \frac{\varepsilon^2}{3} \cdot \varepsilon^2 L = \frac{\varepsilon^4}{3}L$. Hence, as $|G_\Delta| \geq |G'_\Delta|/\ell - 1$, we have

$$\mathbf{E}_{\Delta \sim [-L, L]}[|G_\Delta|] \geq \frac{\varepsilon^4 L}{3\ell} - 1 > \frac{\varepsilon^4 L}{4\ell}. \quad (9)$$

Here we used that $\ell \leq \varepsilon^5 L$.

It suffices to construct a large matching between the bits of s and the bits of t such that only equal bits are matched and such that the matching is “non-crossing”, meaning that earlier bits of s are matched with earlier bits of t . Indeed, the number of pairs in a non-crossing matching corresponds to the length of a common subsequence of s and t .

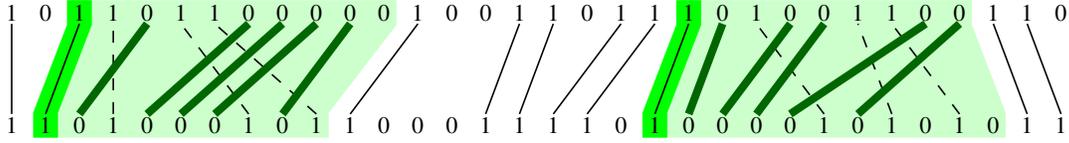


Figure 5: The matching strategy for Lemma 6.1. In this example $\ell = 4$ and $\Delta = 0$. The darker Green one-bits are Green ℓ -flags, and the light Green substrings following them are relatively zero-rich. The solid and dashed black lines indicate the initial matching of ones, and the thick dark-green lines indicate matchings of zeros that replace the matchings of ones. The matchings of ones that are replaced are dashed.

Consider the matching where we match the i -th one in s with the $(i + \Delta)$ -th one in t . This matches $L - |\Delta|$ ones. In particular, for each $i \in G_\Delta$, the ones in substring $s_{[i+1, i+\ell-1]}$ are exactly matched with the ones in substring $t_{[i+\Delta+1, i+\Delta+\ell-1]}$. In this matching, for each $i \in G_\Delta$, replace the matching between the ones of $s_{[i+1, i+\ell-1]}$ and the ones of $t_{[i+\Delta+1, i+\Delta+\ell-1]}$ with a matching between the zeros of $s_{[i, i+\ell-1]}$ and the zeros of $t_{[i+\Delta, i+\Delta+\ell-1]}$. All of the zeros of $s_{[i, i+\ell-1]}$ come after the i -th one of s , and all the zeros of $t_{[i+\Delta, i+\Delta+\ell-1]}$ come after the $(i + \Delta)$ -th one of t , which stays matched to the i -th one of s , so the matching stays non-crossing after this replacement. Furthermore, since any two $i \in G_\Delta$ differ by at least ℓ , the substrings $s_{[i, i+\ell-1]}$ and $t_{[i+\Delta, i+\Delta+\ell-1]}$ across $i \in G_\Delta$ are pairwise disjoint, so these $|G_\Delta|$ replacements can be done simultaneously while keeping the matching non-crossing and thus valid.

Substrings $s_{[i, i+\ell-1]}$ and $t_{[i+\Delta, i+\Delta+\ell-1]}$ each have at least $\max(1, (1 + \varepsilon)(\ell - 1))$ zeros because i is a Green ℓ -flag of s and $i + \Delta$ is a Green ℓ -flag of t . Thus, each replacement deletes $(\ell - 1)$ pairs of ones and adds at least $\max(1, (1 + \varepsilon)(\ell - 1))$ pairs of zeros. If $\ell \geq 2$, each replacement increases the number of pairs matched by $\varepsilon(\ell - 1) > \frac{\varepsilon}{2}\ell$, so the total number of bits in the new matching is at least $L - |\Delta| + \frac{\varepsilon}{2}\ell|G_\Delta|$. If $\ell = 1$, each replacement increases the number of pairs matched by at least 1, so the total number of pairs in the new matching is $L - |\Delta| + |G_\Delta|$ which is also at least $L - |\Delta| + \frac{\varepsilon}{2}\ell|G_\Delta|$. Thus, for all Δ , we have shown

$$\text{LCS}(\text{Trim}_\Delta(s), \text{Trim}_{-\Delta}(t)) \geq L - |\Delta| + \frac{\varepsilon}{2}\ell|G_\Delta|.$$

Hence, we have by linearity of expectation and (9),

$$\mathbf{E}_{\Delta \sim [-L, L]} [\text{LCS}(\text{Trim}_\Delta(s), \text{Trim}_{-\Delta}(t)) + |\Delta|] \geq L + \frac{\varepsilon}{2}\ell \cdot \mathbf{E}_{\Delta \sim [-L, L]} [|G_\Delta|] \geq L + \frac{\varepsilon^5}{8}L,$$

as desired. \square

To find strings s and t that have LCS beating the $1/2$ barrier, it is not enough to assume that s and t form a Green pair and use Lemma 6.1, because we lose by the size of the random shift $|\Delta|$. To remedy this, we break s and t into shorter substrings so that the loss from the random shift is at most the length of a single substring. If a substantial fraction of these substrings form Green pairs, then we can combine the gains using the Shifted LCS Lemma (Lemma 3.7) to get a large overall LCS, and the loss from the random shift is negligible. The following lemma implements this idea, showing that many Green pairs gives large overall LCS.

Lemma 6.2 (Many Green pairs implies large LCS). *Let s and t be strings with the same length and the same number $L = 2^n$ of ones, and let $m^* \leq n - 10 - \log \varepsilon^{-5}$. Suppose there exists a set $Z \subset [2^{n-m^*}]$ such that $|Z| > 2^{n-m^*}/10$ and for all $i \in Z$, the pair of substrings $(s_{m^*, i}, t_{m^*, i})$ is a Green pair. Then*

$$\text{LCS}(s, t) \geq \left(0.5 + \frac{\varepsilon^5}{5000}\right) |s|.$$

Proof. Let $L^* = 2^{m^*}$. We may assume $L \geq (0.5 - \frac{\epsilon^5}{1000})|s|$ or else we are done by having an LCS of $(0.5 + \frac{\epsilon^5}{1000})|s|$ zeros. By Lemma 6.1, we have, for all $i \in Z$,

$$\mathbf{E}_{\Delta \sim [-L^*, L^*]} [\text{LCS}(\text{Trim}_\Delta(s_{m^*,i}), \text{Trim}_{-\Delta}(t_{m^*,i})) + |\Delta|] \geq L^* + \frac{\epsilon^5}{8}L^*.$$

We have, by linearity of expectation,

$$\begin{aligned} \mathbf{E}_{\Delta \sim [-L^*, L^*]} \left[\sum_{i \in Z} (\text{LCS}(\text{Trim}_\Delta(s_{m^*,i}), \text{Trim}_{-\Delta}(t_{m^*,i})) + |\Delta|) \right] \\ = \sum_{i \in Z} \mathbf{E}_{\Delta \sim [-L^*, L^*]} [\text{LCS}(\text{Trim}_\Delta(s_{m^*,i}), \text{Trim}_{-\Delta}(t_{m^*,i})) + |\Delta|] \\ \geq |Z| \cdot \left(L^* + \frac{\epsilon^5}{8}L^* \right). \end{aligned}$$

Hence, we may fix a single Δ for which $|\Delta| \leq L^*$ and

$$\sum_{i \in Z} \text{LCS}(\text{Trim}_\Delta(s_{m^*,i}), \text{Trim}_{-\Delta}(t_{m^*,i})) \geq |Z| \cdot \left(L^* - |\Delta| + \frac{\epsilon^5}{8}L^* \right).$$

Thus, the set Z satisfies the setup of Lemma 3.7 with $n' = n$ and $m' = m^*$ and $L' = L$ and $\delta' = \frac{\epsilon^5}{8}$. Therefore we get

$$\text{LCS}(s, t) \geq \left(1 + \frac{\epsilon^5}{160}\right)L > \left(1 + \frac{\epsilon^5}{160}\right) \left(0.5 - \frac{\epsilon^5}{1000}\right)|s| > \left(0.5 + \frac{\epsilon^5}{5000}\right)|s|. \quad \square$$

7 Blue-Yellow case

In this section, we implement the Blue-Yellow strategy described in the Overview (Section 2), which is the most intricate part of our argument. Call a pair of strings (s, t) a *Blue-Yellow pair* if:

1. The strings s and t have the same length and the same number of ones.
2. There exists an m such that s and t are both of type m -Blue-Yellow.
3. Both s and t are 6γ -Blue-flag-balanced.

Note that (s, t) is a Blue-Yellow pair if and only if (t, s) is a Blue-Yellow pair.

We show that when we have strings s and t and some scale m^* with many Blue-Yellow pairs $(s_{m^*,i}, t_{m^*,i})$ among their substrings at scale m^* , then we can find a common subsequence of s and t of length $(1/2 + \delta)|s|$. At the highest level (Lemma 7.3), we do this by finding common subsequences within the Blue-Yellow pairs, and matching ones elsewhere. To find large common subsequences within Blue-Yellow pairs, we use Lemma 7.1 and Lemma 7.2.

Lemma 7.1 shows that, for a Blue-Yellow pair (s_i, t_i) , we can find substrings s'_i and t'_i of s_i and t_i which “gain in span,” meaning that $\text{LCS}(s'_i, t'_i) > (1/4 + \delta)(|s'_i| + |t'_i|)$. To do this, we match ones of s_i with ones of t_i , and switch to matching zeros when we simultaneously encounter a Blue flag in s_i and Yellow flag in t_i of the appropriate lengths. However, despite gaining in span, the lengths of s_i and t_i may be quite different (this offset comes from the zeros of the Blue flags in s_i spanning fewer ones than the zeros of the Yellow

flags in t_i), so repeatedly applying Lemma 7.1 is insufficient. Indeed, this would cause us to systematically match shorter substrings in s with longer substrings in t , leading the common subsequence obtained to reach the end of t well before reaching the end of s .

The subsequent lemma, Lemma 7.2, shows that if two Blue-Yellow pairs (s_i, t_i) and (s_{i+1}, t_{i+1}) occur consecutively in a string, then we can find a common subsequence that gains in span, like Lemma 7.1, but also uses the same number of ones in both strings, creating a balanced matching. Roughly, the proof follows by applying Lemma 7.1 twice, once on the pair (s_i, t_i) , matching more bits in t_i , and once on the pair (t_{i+1}, s_{i+1}) , matching more bits in s_{i+1} , so that together the number of bits used from s and t is equal. As a result, in total our common subsequence spans the same number of bits in s and t but still gains in span. We refer the reader to Figure 6 below for a visual illustration of this argument.

Thanks to Lemma 7.2, it follows that if we have many Blue-Yellow pairs, then we have many pairs of subsequences $(s_i s_{i+1}, t_i t_{i+1})$ of s and t where there is a common subsequence that gains in span. Thus, using Lemma 3.7, we can piece these subsequences together, matching ones in between, giving a large LCS overall; this is the content of Lemma 7.3.

Lemma 7.1 (Blue-Yellow matching lemma). *Let (s, t) be a Blue-Yellow pair where each string has $L = 2^n$ ones. Then, for Δ uniformly random in $[L/4]$,*

$$\Pr_{\Delta} [\text{LCS}(s_{[1, (0.5+0.01\epsilon)L]}, t_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta])} \geq (0.5 + 0.24\epsilon)L] \geq 0.9.$$

Proof. This proof is long, so we organize it into four parts. First, we use the assumptions to find many disjoint Blue flags in s . Next, we match the Blue flags in s with candidate Yellow flags in t . We then show that, on average, most of these candidate flags are in fact Yellow flags in t . Finally, with these ingredients in place, we show the desired lower bound on the expected LCS over the random offset Δ .

Finding many disjoint Blue flags in s . Since (s, t) is a Blue-Yellow pair, the strings s and t are both type m -Blue-Yellow for some integer m . Because s is type m -Blue-Yellow, the fraction of indices $i \in [L]$ with $b_s(i) \in [2^m, \gamma L]$ is at least $\epsilon^2 - \gamma$. As s is 6γ -Blue-flag-balanced, by Lemma 5.2, the fraction of indices $i \in [L/2]$ with $b_s(i) \in [2^m, \gamma L]$ is at least $\epsilon^2 - 4\gamma$. Let $1 \leq i_1 < i_2 < \dots$ be such that $i_k \in [L/2]$ is the smallest index satisfying $b_s(i_k) \in [2^m, \gamma L]$ and, if $k > 1$, $i_k \geq i_{k-1} + b_s(i_{k-1})$. Intuitively, $(i_k)_{k \geq 1}$ is a maximal sequence of non-overlapping Blue flags in $[L/2]$.

We claim that there is a smallest index d such that $\sum_{k=1}^d b_s(i_k) \geq 0.5(\epsilon^2 - 4\gamma)L$. By the minimality of each i_k , the intervals $[i_k, i_k + b_s(i_k) - 1]$ for $k = 1, \dots, k'$ together contain all indices $i < i_{k'+1}$ with $b_s(i) \in [2^m, \gamma L]$. Since there are at least $0.5(\epsilon^2 - 4\gamma)L$ such indices $i \in [L/2]$, as long as $\sum_{k=1}^{k'} b_s(i_k) < 0.5(\epsilon^2 - 4\gamma)L$, the index $i_{k'+1}$ is well defined, so in particular d is well defined. Furthermore, by minimality of d , we have $\sum_{k=1}^d b_s(i_k) \leq 0.5(\epsilon^2 - 4\gamma)L + \gamma L < 0.5\epsilon^2 L$. We thus have found indices i_1, \dots, i_d where

$$i_d \leq L/2, \quad i_{k+1} \geq i_k + b_s(i_k) \text{ for each } k < d, \text{ and } \sum b_s(i_k) \in [0.5(\epsilon^2 - 4\gamma)L, 0.5\epsilon^2 L].$$

Matching Blue flags in s with candidate Yellow flags in t . Define $i_0 = 1$, $\ell_{s,0} = 0$, and $i_{d+1} = \lfloor (0.5 + 0.01\epsilon)L \rfloor$. For $k \in [d]$, let $\ell_{s,k} \stackrel{\text{def}}{=} b_s(i_k) > 1$ for the lengths of these Blue flags in s , and let $\ell_{t,k} \stackrel{\text{def}}{=} \lceil 0.56\epsilon^{-1} \ell_{s,k} \rceil$ for $k \in [0, d]$, corresponding to Yellow flag length we want to match in t . Here the constant $0.56\epsilon^{-1}$ above is chosen so that $0.9(\ell_{t,k} - 1) \geq 0.5\epsilon^{-1} \ell_{s,k}$, so that a Yellow $\ell_{t,k}$ -flag guarantees roughly the same number of zeros in t as a Blue $\ell_{s,k}$ -flag does in s .

For a subset $K \subset [0, d]$, define $\ell_{s,K} \stackrel{\text{def}}{=} \sum_{k \in K} \ell_{s,k}$, and define $\ell_{t,K}$ similarly. Recall the shift Δ is to be chosen uniformly from $[L/4]$. For $k \in [0, d+1]$, let $j_k \stackrel{\text{def}}{=} i_k + \Delta + \ell_{t,[k-1]} - \ell_{s,[k-1]}$. This j_k is the index in t

that we would like to be a Yellow $\ell_{t,k}$ -flag to be matched with the Blue $\ell_{s,k}$ -flag at i_k . The indices i_k and j_k partition s and t into substrings as follows. Let

$$\begin{aligned} s'_k &\stackrel{\text{def}}{=} s_{[i_k, i_k + \ell_{s,k} - 1]} && \text{for } k \in [1, d] \\ s''_k &\stackrel{\text{def}}{=} s_{[i_k + \ell_{s,k}, i_{k+1} - 1]} && \text{for } k \in [0, d] \\ t'_k &\stackrel{\text{def}}{=} t_{[j_k, j_k + \ell_{t,k} - 1]} && \text{for } k \in [1, d] \\ t''_k &\stackrel{\text{def}}{=} t_{[j_k + \ell_{t,k}, j_{k+1} - 1]} && \text{for } k \in [0, d]. \end{aligned}$$

By construction of i_0, \dots, i_d , we have $i_k + \ell_{s,k} \leq i_{k+1}$ for $k \in [0, d-1]$, and also $i_d + \ell_{s,d} \leq L/2 + \gamma L < i_{d+1}$. Thus, the substrings defined above give a partition $s_{[1, (0.5+0.01\epsilon)L]} = s''_0 s'_1 s''_1 s'_2 s''_2 \dots s'_d s''_d$, where the substrings alternate between the regions s'_k corresponding to Blue flags and the regions s''_k in between. Similarly, for $k \in [0, d-1]$ we have

$$j_k + \ell_{t,k} = i_k + \Delta + \ell_{t,k} - \ell_{s,[k-1]} = j_{k+1} - (i_{k+1} - i_k - \ell_{s,k}) \leq j_{k+1},$$

and

$$\begin{aligned} j_{d+1} &= i_{d+1} + \ell_{t,[d]} - \ell_{s,[d]} + \Delta \\ &\leq 1 + L/2 + \gamma L + 0.57\epsilon^{-1} \cdot \ell_{s,[d]} + \Delta \\ &\leq 1 + L/2 + 0.01\epsilon L + 0.57\epsilon^{-1} \cdot 0.5\epsilon^2 L + \Delta \\ &\leq 1 + (0.5 + 0.3\epsilon)L + \Delta. \end{aligned}$$

Thus, we have that $t''_0 t'_1 t''_1 t'_2 t''_2 \dots t'_d t''_d$ is a prefix of $t_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta]}$, alternating between the regions t'_k that we would like to be Yellow flags and the regions t''_k in between.

Showing many j_k 's are Yellow flags of t . We next show that typically, most of the j_k 's as defined above are Yellow flags. Let K be the set of $k \in [d]$ for which the j_k is a Yellow $\ell_{t,k}$ -flag of string t . Call a shift $\Delta \in [L/4]$ *good* if $\ell_{t,K} \geq (1 - 24000\epsilon)\ell_{t,[d]}$, i.e. that when weighted by flag length, the set K comprises most of $[d]$. Since string t has type m -Blue-Yellow and $\ell_{t,k} > \ell_{s,k} \geq 2^m$ for every $k \in [d]$, we know that for every $k \in [d]$, at most $600\epsilon L$ of the indices in $[L]$ are not Yellow $\ell_{t,k}$ -flags in string t . Hence, if Δ is chosen uniformly at random in $[L/4]$, for each $k \in [d]$, the probability that $k \notin K$ is at most $600\epsilon L / (L/4) = 2400\epsilon$. By linearity of expectation,

$$\mathbf{E}_{\Delta \sim [L/4]}[\ell_{t,[d]} - \ell_{t,K}] \leq 2400\epsilon \ell_{t,[d]},$$

As $\ell_{t,K} \leq \ell_{t,[d]}$ always, we have by Markov's inequality on $\ell_{t,[d]} - \ell_{t,K}$ that

$$\Pr[\Delta \text{ is good}] = 1 - \Pr[\ell_{t,[d]} - \ell_{t,K} \geq (24000\epsilon)\ell_{t,[d]}] \geq 1 - \frac{2400\epsilon \ell_{t,[d]}}{24000\epsilon \ell_{t,[d]}} = 0.9.$$

Lower bounding expected LCS. Since $s''_0 s'_1 s''_1 s'_2 s''_2 \dots s'_d s''_d = s_{[1, (0.5+0.01\epsilon)L]}$ and $t''_0 t'_1 t''_1 t'_2 t''_2 \dots t'_d t''_d$ is a prefix of $t_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta+1]}$, it suffices to show that, when Δ is good,

$$\text{LCS}(s''_0 s'_1 s''_1 s'_2 s''_2 \dots s'_d s''_d, t''_0 t'_1 t''_1 t'_2 t''_2 \dots t'_d t''_d) \geq (0.5 + 0.24\epsilon)L.$$

As the index i_k is a Blue $\ell_{s,k}$ -flag in s , substring s'_k has at least $\epsilon^{-1}(\ell_{s,k} - 1) \geq 0.5\epsilon^{-1}\ell_{s,k}$ zeros. If $k \in K$, then j_k is a Yellow $\ell_{t,k}$ -flag in t , so substring t'_k has at least $0.9(\ell_{t,k} - 1) > 0.5\epsilon^{-1}\ell_{s,k}$ zeros as well. Hence, for $k \in K$, we have

$$\text{LCS}(s'_k, t'_k) \geq 0.5\epsilon^{-1}\ell_{s,k}.$$

Furthermore, for $k \in [0, d]$, we have that s_k'' has $i_{k+1} - i_k - \ell_{s,k}$ ones, and the number of ones in t_k'' is also

$$j_{k+1} - j_k - \ell_{t,k} = (i_{k+1} + \Delta + \ell_{t,k} - \ell_{s,[k]}) - (i_k + \Delta + \ell_{t,[k-1]} - \ell_{s,[k-1]}) - \ell_{t,k} = i_{k+1} - i_k - \ell_{s,k},$$

so for all $k \in [0, d]$,

$$\text{LCS}(s_k'', t_k'') \geq i_{k+1} - i_k - \ell_{s,k}.$$

Indeed, we now have that for any good Δ ,

$$\begin{aligned} \text{LCS}(s_{[1, (0.5+0.01\epsilon)L]}, t_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta]}) &\geq \sum_{k=1}^d \text{LCS}(s_k', t_k') + \sum_{k=0}^d \text{LCS}(s_k'', t_k'') \\ &\geq \sum_{k \in K} \text{LCS}(s_k', t_k') + \sum_{k=0}^d (i_{k+1} - i_k - \ell_{s,k}) \\ &\geq 0.5\epsilon^{-1} \ell_{s,K} + (i_{d+1} - i_0 - \ell_{s,[d]}) \tag{10} \\ &\geq 0.5\epsilon^{-1} (1 - 24000\epsilon) \ell_{s,[d]} + (0.5 + 0.01\epsilon)L - 2 - \ell_{s,[d]} \tag{11} \\ &= 0.5\epsilon^{-1} (1 - 24002\epsilon) \ell_{s,[d]} + (0.5 + 0.01\epsilon)L - 2 \\ &\geq 0.5\epsilon^{-1} (1 - 24002\epsilon) (0.5(\epsilon^2 - 4\gamma)L) + (0.5 + 0.01\epsilon)L \tag{12} \\ &\geq (0.5 + 0.24\epsilon)L. \tag{13} \end{aligned}$$

In (10), we used that $\ell_{s,0} = 0$. In (11), we used that $i_{d+1} - i_0 = \lfloor (0.5 + 0.01\epsilon)L \rfloor - 1 > (0.05 + 0.01\epsilon)L - 2$. In (12), we used that $\ell_{s,[d]} = \sum_{k=1}^d b_s(i_k) \geq 0.5(\epsilon^2 - 4\gamma)L$ by construction of i_1, \dots, i_d . In (13), we used that $\epsilon \leq 10^{-6}$ and $\gamma \leq 0.001\epsilon^2$. This completes the proof as the probability that $\Delta \in [L/4]$ is good is at least 0.9. \square

The next lemma shows that when two Blue-Yellow pairs occur consecutively (for technical reasons, we require that the second Blue-Yellow pair occurs on the reversed strings), we get a large common subsequence that also spans the same number of ones in both s and t . This allows us to piece together many such matchings and apply the Prefix/Suffix LCS Lemma (Lemma 3.7), giving an overall gain in LCS over the 1/2 barrier.

Lemma 7.2 (Blue-Yellow balanced matching lemma). *Let $s = s_1 s_2$ and $t = t_1 t_2$ such that substrings s_1, s_2, t_1, t_2 each have L ones and start with a one, and the pairs (s_1, t_1) and $(\text{rev}(t_2), \text{rev}(s_2))$ are Blue-Yellow pairs. Then for Δ uniformly random in $[L/4]$, we have*

$$\mathbf{E}_{\Delta \sim [L/4]} [\text{LCS}(\text{Trim}_\Delta(s), \text{Trim}_{-\Delta}(t)) + \Delta] \geq 2L + 0.12\epsilon L.$$

Proof. We have $\text{Trim}_\Delta(s)$ and $\text{Trim}_{-\Delta}(t)$ each have $2L - \Delta$ ones, so we always have

$$\text{LCS}(\text{Trim}_\Delta(s), \text{Trim}_{-\Delta}(t)) + \Delta \geq 2L.$$

Thus, because $0.8 \cdot 0.16\epsilon L > 0.12\epsilon L$, it suffices to show that

$$\Pr_{\Delta \sim [L/4]} [\text{LCS}(\text{Trim}_\Delta(s), \text{Trim}_{-\Delta}(t)) + \Delta \geq 2L + 0.16\epsilon L] \geq 0.8.$$

Call Δ *good* if both of the following inequalities are true:

$$\text{LCS}((s_1)_{[1, (0.5+0.01\epsilon)L]}, (t_1)_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta]}) \geq (0.5 + 0.24\epsilon)L \tag{14}$$

$$\text{LCS}(\text{rev}(t_2)_{[1, (0.5+0.01\epsilon)L]}, \text{rev}(s_2)_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta]}) \geq (0.5 + 0.24\epsilon)L. \tag{15}$$

By Lemma 7.1, first applied to the Blue-Yellow pair (s_1, t_1) , then applied to the Blue-Yellow pair $(\text{rev}(t_2), \text{rev}(s_2))$, each of (14) and (15) holds with probability at least 0.9 for Δ sampled uniformly from $[L/4]$, so a random Δ in $[L/4]$ is good with probability at least 0.8.

Fix a good Δ . We show that

$$\text{LCS}(\text{Trim}_\Delta(s), \text{Trim}_{-\Delta}(t)) \geq 2L - \Delta + 0.16\epsilon L. \quad (16)$$

By the second part of Lemma 3.1,

$$\begin{aligned} \text{rev}(t_2)_{[1, (0.5+0.01\epsilon)L]} &= \text{rev}((t_2)_{[1+(0.5-0.01\epsilon)L, L]}) \\ \text{rev}(s_2)_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta]} &= \text{rev}((s_2)_{[1+(0.5-0.3\epsilon)L-\Delta, L-\Delta]}). \end{aligned}$$

Hence since $\text{rev}(\cdot)$ preserves LCS (Lemma 3.3), we have

$$\begin{aligned} &\text{LCS}((t_2)_{[1+(0.5-0.01\epsilon)L, L]}, (s_2)_{[1+(0.5-0.3\epsilon)L-\Delta, L-\Delta]}) \\ &= \text{LCS}(\text{rev}(t_2)_{[1, (0.5+0.01\epsilon)L]}, \text{rev}(s_2)_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta]}) \\ &\geq (0.5 + 0.24\epsilon)L. \end{aligned}$$

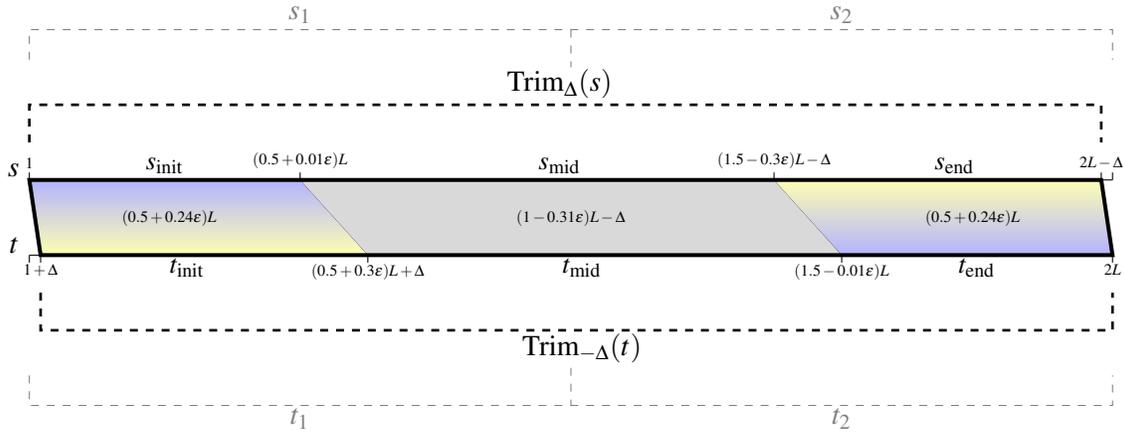


Figure 6: Lemma 7.2. We obtain two “trapezoids” with good LCS obtained from applying Lemma 7.1 to two Blue-Yellow pairs, (s_1, t_1) and $(\text{rev}(s_2), \text{rev}(t_2))$, and match ones in between (in the grey region), giving an improved LCS for $\text{Trim}_\Delta(s)$ and $\text{Trim}_{-\Delta}(t)$.

Writing $\text{Trim}_\Delta(s) = s_{\text{init}}s_{\text{mid}}s_{\text{end}}$ and $\text{Trim}_{-\Delta}(t) = t_{\text{init}}t_{\text{mid}}t_{\text{end}}$ where (see Figure 6)⁵

$$\begin{aligned} s_{\text{init}} &\stackrel{\text{def}}{=} s_{[1, (0.5+0.01\epsilon)L]} &&= (s_1)_{[1, (0.5+0.01\epsilon)L]} \\ s_{\text{mid}} &\stackrel{\text{def}}{=} s_{[(0.5+0.01\epsilon)L, (1.5-0.3\epsilon)L-\Delta+1]} \\ s_{\text{end}} &\stackrel{\text{def}}{=} s_{[(1.5-0.3\epsilon)L-\Delta+1, 2L-\Delta]} &&= (s_2)_{[(0.5-0.3\epsilon)L-\Delta+1, L-\Delta]} \\ t_{\text{init}} &\stackrel{\text{def}}{=} t_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta]} &&= (t_1)_{[1+\Delta, (0.5+0.3\epsilon)L+\Delta]} \\ t_{\text{mid}} &\stackrel{\text{def}}{=} t_{[(0.5+0.3\epsilon)L+\Delta, (1.5-0.01\epsilon)L+1]} \\ t_{\text{end}} &\stackrel{\text{def}}{=} t_{[(1.5-0.01\epsilon)L+1, L]} &&= (t_2)_{[(0.5-0.01\epsilon)L+1, L]}. \end{aligned}$$

⁵A negligible detail: we do not need to shift the endpoints of substrings s_{mid} and t_{mid} by 1 because L is a power of two so ϵL is never an integer

We have s_{mid} and t_{mid} both have at least $(1 - 0.31\varepsilon)L - \Delta$ ones. Hence, we have

$$\begin{aligned} \text{LCS}(\text{Trim}_\Delta(s), \text{Trim}_{-\Delta}(t)) &\geq \text{LCS}(s_{\text{init}}, t_{\text{init}}) + \text{LCS}(s_{\text{mid}}, t_{\text{mid}}) + \text{LCS}(s_{\text{end}}, t_{\text{end}}) \\ &\geq (0.5 + 0.24\varepsilon)L + (1 - 0.31\varepsilon)L - \Delta + (0.5 + 0.24\varepsilon)L \\ &> 2L - \Delta + 0.16\varepsilon L, \end{aligned}$$

establishing (16) as desired. \square

Combining Lemma 7.2 with the Prefix/Suffix LCS Lemma (Lemma 3.7) shows that when two strings have many Blue-Yellow pairs among their substrings at some scale, we get a large LCS.

Lemma 7.3 (Many Blue-Yellow pairs implies good LCS). *Let s and t be strings with the same length and the same number $L = 2^n$ of ones, and let $m^* \leq n - 10 - \log \varepsilon^{-1}$. Suppose there exists a set $Z \subset [2^{n-m^*-1}]$ such that $|Z| > 2^{n-m^*-1}/10$ and for all $i \in Z$, the substring pairs $(s_{m^*, 2i-1}, t_{m^*, 2i-1})$ and $(\text{rev}(s_{m^*, 2i}), \text{rev}(t_{m^*, 2i}))$ are Blue-Yellow pairs. Then,*

$$\text{LCS}(s, t) > (1 + 0.0001\varepsilon)|s|. \quad (17)$$

Proof. Let $L^* = 2^{m^*}$. We may assume $L \geq (0.5 - 0.001\varepsilon)|s|$ or else we are done by having an LCS of $(0.5 + 0.001\varepsilon)|s|$ zeros. For all $i \in Z$, substrings $s_{m^*+1, i} = s_{m^*, 2i-1}s_{m^*, 2i}$ and $t_{m^*+1, i} = t_{m^*, 2i-1}t_{m^*, 2i}$ satisfy the setup of Lemma 7.2 with $L = L^*$, so we have, for all $i \in Z$,

$$\mathbf{E}_{\Delta \sim [L^*/4]} [\text{LCS}(\text{Trim}_\Delta(s_{m^*+1, i}), \text{Trim}_{-\Delta}(t_{m^*+1, i})) + \Delta] \geq 2L^* + 0.12\varepsilon L^*.$$

By linearity of expectation, we have

$$\mathbf{E}_{\Delta \sim [L^*/4]} \left[\sum_{i \in Z} [\text{LCS}(\text{Trim}_\Delta(s_{m^*+1, i}), \text{Trim}_{-\Delta}(t_{m^*+1, i})) + \Delta] \right] \geq |Z| \cdot (2L^* + 0.12\varepsilon L^*).$$

Hence, we may fix a $\Delta \in [L^*/4]$ for which

$$\sum_{i \in Z} \text{LCS}(\text{Trim}_\Delta(s_{m^*+1, i}), \text{Trim}_{-\Delta}(t_{m^*+1, i})) \geq |Z| \cdot (2L^* - \Delta + 0.12\varepsilon L^*).$$

Thus, set Z satisfies the setup of Lemma 3.7 with $n' = n$ and $m' = m^* + 1$ and $L' = 2L^*$ and $\delta' = 0.06\varepsilon$. Hence, by Lemma 3.7,

$$\text{LCS}(s, t) \geq \left(1 + \frac{0.06\varepsilon}{20}\right)L \geq (1 + 0.003\varepsilon)(0.5 - 0.001\varepsilon)|s| > (0.5 + 0.0001\varepsilon)|s|. \quad \square$$

8 Putting it all together

8.1 Statistics

We now prove our main theorem. The first step is to define the *statistics* of a string w .

Definition 8.1 (Statistics). Let w be a string with $L = 2^n$ ones, and let $n_0 \stackrel{\text{def}}{=} \max(0, n - 200\gamma^{-3} \log n)$. Let the *statistics* of string w be a table of the following data:

1. For all $m \geq n_0$ and $i \geq 1$, the number of zeros and the number of ones in $w_{m,i}$ (the number of ones is always 2^m).
2. For all $m \geq n_0$ and $i \geq 1$, the type (see Definition 4.3) of string $w_{m,i}$.
3. The set $\mathcal{I}^{n_0}(w)$ of pairwise disjoint intervals $I \subset [L]$ that each have size $|I| \geq 2^{n_0}$ such that w_I is imbalanced for each $I \in \mathcal{I}^{n_0}(w)$, and the sum $\sum_{I \in \mathcal{I}^{n_0}(w)} |I|$ is maximized (if multiple such $\mathcal{I}^{n_0}(w)$ exist, break the tie arbitrarily).
4. For each $I \in \mathcal{I}^{n_0}(w)$, the indices x and y such that substring w_I starts at the x -th bit and ends at the y -th bit of s .

We say two strings s and t agree on statistics if their tables of statistics are identical.

This next lemma shows that it is possible to pigeonhole strings by their statistics, by showing that there are not too many possible statistics for a string.

Lemma 8.2. *There are at most $2^{\text{poly log } N}$ possible tables of statistics for a string of length N .*

Proof. A string w of length N has at most

$$\sum_{m=n_0}^n 2^{n-m} = \text{poly log } N$$

substrings $w_{m,i}$ that are considered in its table of statistics. Furthermore, for each substring $w_{m,i}$, there are at most N choices for the number of zeros and the number of ones, and at most $O(N)$ choices for the type of $w_{m,i}$ (there is one Imbalanced type, $O(N)$ Green types, and $O(\log N)$ Blue-Yellow types), so there are at most $2^{\text{poly log } N}$ choices for all the types and zero/one-counts in the table. Lastly, $\mathcal{I}^{n_0}(w)$ has at most $2^{n-n_0} = \log^{O_\varepsilon(1)} N$ intervals (because intervals have length at least 2^{n_0} and are disjoint), so there are at most $2^{\text{poly log } N}$ choices for $\mathcal{I}^{n_0}(w)$ and the locations of the endpoints of the intervals in $\mathcal{I}^{n_0}(w)$. \square

8.2 The Imbalanced case

This next lemma covers an easy case, when s has many large imbalanced intervals. In this case, our pigeonholing by statistics guarantees that s and t are imbalanced in common locations, allowing us to apply the imbalanced strategy to find a large LCS.

Lemma 8.3. *Let s and t be strings that each start with a one, agree on statistics, and have $L = 2^n$ ones where n is sufficiently large. Suppose there exists a set \mathcal{I} of pairwise disjoint intervals I that each satisfy $|I| \geq 2^{n-200\gamma^{-3} \log n}$ such that s_I is imbalanced for each $I \in \mathcal{I}$ and $\sum_{I \in \mathcal{I}} |I| \geq \frac{\varepsilon^5}{10} L$. Then*

$$\text{LCS}(s, t) \geq \left(0.5 + \frac{\varepsilon^6}{150}\right) |s|.$$

Proof. Let $n_0 = n - 200\gamma^{-3} \log n$. We may assume that $L \geq \frac{|s|}{3}$, or else s and t each have $\frac{2|s|}{3}$ zeros and $\text{LCS}(s, t) \geq \frac{2}{3}|s| > \left(0.5 + \frac{\varepsilon^6}{150}\right)|s|$. Since s and t agree on statistics, we have $\mathcal{I}^{n_0}(s) = \mathcal{I}^{n_0}(t)$. Furthermore, as $\mathcal{I}^{n_0}(s)$ maximizes the sum $\sum_{I \in \mathcal{I}^{n_0}(s)} |I|$, we have $\sum_{I \in \mathcal{I}^{n_0}(s)} |I| \geq \sum_{I \in \mathcal{I}} |I| \geq \frac{\varepsilon^5}{10} L$. Let $\mathcal{I}^{n_0}(s) = \mathcal{I}^{n_0}(t) =$

$\{I_1, \dots, I_k\}$, with $I_1 < I_2 < \dots < I_k$ (these intervals are pairwise disjoint so the order is the obvious one). We thus may write

$$s = s''_0 s'_1 s''_1 s'_2 s''_2 \cdots s'_k s''_k, \quad t = t''_0 t'_1 t''_1 t'_2 t''_2 \cdots t'_k t''_k$$

where $s'_j = s_{I_j}$ for $j \in [1, k]$, and substring s''_j consists of the bits between the end of substring s'_j (or the beginning of string s if $j = 0$) and the beginning of substring s'_{j+1} (or the end of string s if $j = k$), and the partition of t is defined analogously. By the definitions of s_{I_j} and t_{I_j} , for $j \in [1, k]$, s'_j and t'_j have the same number $|I_j|$ of ones, and for $j \in [0, k]$, s''_j and t''_j have the same number of ones as well. Further, since s and t agree on statistics, for all $j \in [1, k]$, substrings s_{I_j} and t_{I_j} start and end in the same positions in their respective strings s and t . In particular, s'_j and t'_j have the same length for all $j \in [1, k]$, and s''_j and t''_j have the same length for all $j \in [0, k]$.

For each $j \in [0, k]$, the substrings s''_j and t''_j have the same length and the same number of ones, so $\text{LCS}(s''_j, t''_j) \geq |s''_j|/2$. Additionally, for $j \in [1, k]$ the number of zeros in substrings s'_j and t'_j are equal and not in $(1 \pm \varepsilon)|s'_j|$. Hence, by Lemma 3.6, we have $\text{LCS}(s'_j, t'_j) \geq (1/2 + \varepsilon/5)|s'_j|$. Therefore we have

$$\begin{aligned} \text{LCS}(s, t) &\geq \sum_{j=1}^k \text{LCS}(s'_j, t'_j) + \sum_{j=0}^k \text{LCS}(s''_j, t''_j) \geq \sum_{j=1}^k \left(\frac{1}{2} + \frac{\varepsilon}{5} \right) |s'_j| + \sum_{j=0}^k \frac{|s''_j|}{2} \\ &= \frac{|s|}{2} + \frac{\varepsilon}{5} \sum_{j=1}^k |s'_j| \geq \frac{|s|}{2} + \frac{\varepsilon^6 L}{50} \geq \left(\frac{1}{2} + \frac{\varepsilon^6}{150} \right) |s|, \end{aligned}$$

where the last two inequalities used that $|s'_j| \geq |I_j|$, $\sum_{j=1}^k |I_j| \geq \frac{\varepsilon^5 L}{10}$, and $L \geq \frac{|s|}{3}$. \square

8.3 Combining the arguments for the Imbalanced, Green, and Blue-Yellow cases

We now prove the main technical lemma, which shows that two strings that agree on statistics have LCS beating the $1/2$ barrier. This establishes Theorem 1.1 up to a pigeonhole argument and an assumption about the number of ones being a power of two. The proof consists of piecing together (1) the Imbalanced case, when s and t have many substrings of Imbalanced type, Lemma 8.3, (2) the Green case, when s and t have many substrings of Green type, and (3) the Blue-Yellow case, when s and t have many substrings of Blue-Yellow type. These three cases correspond to the three matching strategies stated in the Overview (Section 2).

Lemma 8.4. *There exists an absolute constant $\delta = \frac{\varepsilon^6}{150}$ such that the following holds for n sufficiently large. Let s and t be strings that each start with a one, have $L = 2^n$ ones each, such that s and t agree on statistics, and $\text{rev}(s)$ and $\text{rev}(t)$ agree on statistics. Then $\text{LCS}(s, t) \geq (0.5 + \delta)|s|$.*

Proof. First, suppose that at least $\gamma^2 L$ values of $i \in [L]$ satisfy $b_s(i) \geq 2^{n-200\gamma^{-3} \log n}$. Define $1 \leq i_1 < \dots < i_d$ such that i_k is the smallest index such that $b_s(i_k) \geq 2^{n-200\gamma^{-3} \log n}$ and $i_k \geq i_{k-1} + b_s(i_{k-1})$ if $k > 1$, and d is the largest index such that i_d is well-defined. By the definition of $b_s(i_k)$, index i_k is a Blue $b_s(i_k)$ -flag in s , so for the interval $I_k \stackrel{\text{def}}{=} [i_k, \min(i_k + b_s(i_k) - 1, L)]$, substring s_{I_k} is imbalanced by Lemma 3.5. Furthermore, since $i_k + b_s(i_k) \leq i_{k+1}$ for $k = 1, \dots, d-1$, we have I_1, \dots, I_d are pairwise disjoint. Lastly, by minimality of each i_k , each index $i \in [L]$ with $b_s(i) \geq 2^{n-200\gamma^{-3} \log n}$ is in some interval I_k . Thus, $\sum |I_k| \geq \gamma^2 L > \frac{\varepsilon^5}{10}$. Thus, we may apply Lemma 8.3 to strings s and t , giving $\text{LCS}(s, t) \geq (0.5 + \delta)|s|$. Hence, we may assume for the rest of the argument that

- At most $\gamma^2 L$ values of $i \in [L]$ satisfy $b_s(i) \geq 2^{n-200\gamma^{-3} \log n}$.

Similarly, we may assume

- At most $\gamma^2 L$ values of $i \in [L]$ satisfy $b_{\text{rev}(s)}(i) \geq 2^{n-200\gamma^{-3}\log n}$ (applying Lemma 8.3 to $\text{rev}(s)$ and $\text{rev}(t)$),
- At most $\gamma^2 L$ values of $i \in [L]$ satisfy $b_t(i) \geq 2^{n-200\gamma^{-3}\log n}$ (applying Lemma 8.3 to t and s), and
- At most $\gamma^2 L$ values of $i \in [L]$ satisfy $b_{\text{rev}(t)}(i) \geq 2^{n-200\gamma^{-3}\log n}$ (applying Lemma 8.3 to $\text{rev}(t)$ and $\text{rev}(s)$).

Hence, we may apply the Substring Blue-flag-balance Lemma, Lemma 5.6, to each of the strings s , $\text{rev}(s)$, t , and $\text{rev}(t)$ with $\beta = \gamma$. This shows the existence of some scale m^* with $n - 10 - \log \delta^{-1} \geq m^* \geq n - 150\gamma^{-3}\log n$ such that the following hold:

- For at least $(1 - 3\gamma) \cdot 2^{n-m^*}$ values of $i \in [2^{n-m^*}]$, the substring $s_{m^*,i}$ is 6γ -Blue-flag-balanced,
- For at least $(1 - 3\gamma) \cdot 2^{n-m^*}$ values of $i \in [2^{n-m^*}]$, the substring $\text{rev}(s_{m^*,i})$ is 6γ -Blue-flag-balanced,
- For at least $(1 - 3\gamma) \cdot 2^{n-m^*}$ values of $i \in [2^{n-m^*}]$, the substring $t_{m^*,i}$ is 6γ -Blue-flag-balanced, and
- For at least $(1 - 3\gamma) \cdot 2^{n-m^*}$ values of $i \in [2^{n-m^*}]$, the substring $\text{rev}(t_{m^*,i})$ is 6γ -Blue-flag-balanced.

Indeed, for each bullet, Lemma 5.6 implies there are at most $32\gamma^{-3}\log n$ values of m^* for which the condition does not hold, so among $150\gamma^{-3}\log n - 10 - \log \delta^{-1} > 128\gamma^{-3}\log n$ values of m^* , some m^* allows all four conditions to hold. Fix this m^* and let

$$L^* \stackrel{\text{def}}{=} 2^{m^*}.$$

Since the number of ones in s and t are a power of two, s and t agree on statistics, and $m^* > n_0$, where n_0 is from Definition 8.1, we have $s = s_{m^*,1} \cdots s_{m^*,2^{n-m^*}}$ and $t = t_{m^*,1}, \dots, t_{m^*,2^{n-m^*}}$, where, for all $i = 1, \dots, 2^{n-m^*}$, substrings $s_{m^*,i}$ and $t_{m^*,i}$ have the same number L^* of ones and the also the same number of zeros, and thus have the same length. Similarly, we may write $\text{rev}(s) = \text{rev}(s_{m^*,2^{n-m^*}}) \cdots \text{rev}(s_{m^*,1})$ and $\text{rev}(t) = \text{rev}(t_{m^*,2^{n-m^*}}) \cdots \text{rev}(t_{m^*,1})$.

Since n is sufficiently large, for all $i \in [2^{n-m^*}]$, substrings $s_{m^*,i}$ and $\text{rev}(s_{m^*,i})$ have types by Lemma 4.4. Let Z_1 (resp. \bar{Z}_1) be the set of $i \in [2^{n-m^*}]$ such that substring $s_{m^*,i}$ (resp. $\text{rev}(s_{m^*,i})$) is Imbalanced. Let Z_2 (resp. \bar{Z}_2) be the set of $i \in [2^{n-m^*}]$ such that substring $s_{m^*,i}$ (resp. $\text{rev}(s_{m^*,i})$) is ℓ -Green for some ℓ . Let Z_3 (resp. \bar{Z}_3) be the set of $i \in [2^{n-m^*}]$ such that substring $s_{m^*,i}$ (resp. $\text{rev}(s_{m^*,i})$) is m -Blue-Yellow for some m . Since $|Z_1| + |Z_2| + |Z_3| = |\bar{Z}_1| + |\bar{Z}_2| + |\bar{Z}_3| = 2^{n-m^*}$, we have the following cases covering all possibilities.

Case 1a. $|Z_1| \geq 2^{n-m^*}/10$. In this case, for each $i \in Z_1$, because $s_{m^*,i}$ is type Imbalanced, there exists some interval $J_i \subset I_{m^*,i}$ with $|J_i| \geq \varepsilon^5 L^* > 2^{n-200\gamma^{-3}\log n}$ such that s_{J_i} is imbalanced. Since the intervals $I_{m^*,i}$ are pairwise disjoint, the intervals J_i are pairwise disjoint. Then setting $\mathcal{J}' = \{J_i : i \in Z_1\}$, we have that $\sum_{J \in \mathcal{J}'} |J| \geq \varepsilon^5 L^* \cdot |Z_1| = \frac{\varepsilon^5}{10} \cdot L$. Hence, by Lemma 8.3, we have $\text{LCS}(s, t) \geq (0.5 + \frac{\varepsilon^6}{150})|s| = (0.5 + \delta)|s|$.

Case 1b. $|\bar{Z}_1| \geq 2^{n-m^*}/10$. By an identical argument to Case 1a, we can show $\text{LCS}(\text{rev}(s), \text{rev}(t)) \geq (0.5 + \delta)|s|$, which implies that $\text{LCS}(s, t) \geq (0.5 + \delta)|s|$.

Case 2a. $|Z_2| \geq 2^{n-m^*}/10$. Since $m^* \leq n - 10 - \log \varepsilon^{-5}$ by definition of m^* , we may apply Lemma 6.2 to strings s and t with subset $Z \subset [2^{n-m^*}]$. By Lemma 6.2, we have $\text{LCS}(s, t) \geq (0.5 + \frac{\varepsilon^5}{5000})|s| > (0.5 + \delta)|s|$.

Case 2b. $|\bar{Z}_2| \geq 2^{n-m^*}/10$. By an identical argument to Case 2a, we can show $\text{LCS}(\text{rev}(s), \text{rev}(t)) \geq (0.5 + \delta)|s|$, which implies that $\text{LCS}(s, t) \geq (0.5 + \delta)|s|$.

Case 3. $|Z_3| \geq \frac{4}{5} \cdot 2^{n-m^*}$ and $|\bar{Z}_3| \geq \frac{4}{5} \cdot 2^{n-m^*}$. Let Z'_3 be the set of $i \in [2^{n-m^*-1}]$ such that the following hold:

- Substring $s_{m^*,2i-1}$ is 6γ -Blue-flag-balanced.
- Substring $t_{m^*,2i-1}$ is 6γ -Blue-flag-balanced.
- Substring $\text{rev}(s_{m^*,2i})$ is 6γ -Blue-flag-balanced.
- Substring $\text{rev}(t_{m^*,2i})$ is 6γ -Blue-flag-balanced.
- We have $2i-1 \in Z_3$.
- We have $2i \in \bar{Z}_3$.

By choice of m^* , the first four conditions above each fail for at most $3\gamma \cdot 2^{n-m^*}$ values of $i \in [2^{n-m^*-1}]$. Since $|Z_3| \geq \frac{4}{5} \cdot 2^{n-m^*}$, the fifth condition fails for at most $\frac{1}{5} \cdot 2^{n-m^*}$ values of i , and similarly the last condition fails for at most $\frac{1}{5} \cdot 2^{n-m^*}$ values of i . Since there are $\frac{1}{2} \cdot 2^{n-m^*}$ values of $i \in [2^{n-m^*-1}]$, we have that Z'_3 has size at least $(\frac{1}{2} - 12\gamma - \frac{2}{5}) \cdot 2^{n-m^*} > \frac{1}{10} \cdot 2^{n-m^*-1}$ (recall $\gamma = 10^{-15}$ is very small).

Fix $i \in Z'_3$. We claim that strings s and t with parameter m^* and set Z satisfy the setup of Lemma 7.3. The bound on $m^* \leq n - 10 - \log \varepsilon^{-1}$ follows from the definition of m^* . We thus need to show that, for all $i \in Z'_3$, the pairs $(s_{m^*,2i-1}, t_{m^*,2i-1})$ and $(\text{rev}(s_{m^*,2i}), \text{rev}(t_{m^*,2i}))$ are a Blue-Yellow pairs. Since $2i-1 \in Z_3$, there exists some integer m such that substring $s_{m^*,2i-1}$ is type m -Blue-Yellow, and since s and t agree on statistics, substring $t_{m^*,2i-1}$ is also type m -Blue-Yellow. Since $i \in Z'_3$, we have that strings $s_{m^*,2i-1}$ and $t_{m^*,2i-1}$ are both 6γ -Blue-flag-balanced, so $(s_{m^*,2i-1}, t_{m^*,2i-1})$ form a Blue-Yellow pair. Similarly, since $2i \in \bar{Z}_3$ and $\text{rev}(s)$ and $\text{rev}(t)$ agree on statistics, there exists some integer m' such that substrings $\text{rev}(s_{m^*,2i}) = \text{rev}(s)_{m^*,2^{n-m^*}-(2i-1)}$ and $\text{rev}(t_{m^*,2i})$ have type m' -Blue-Yellow. Since $i \in Z'_3$, we have that strings $\text{rev}(s_{m^*,2i})$ and $\text{rev}(t_{m^*,2i})$ are both 6γ -Blue-flag-balanced, so $(\text{rev}(s_{m^*,2i}), \text{rev}(t_{m^*,2i}))$ form a Blue-Yellow pair, as desired. Thus, by Lemma 7.3, we have

$$\text{LCS}(s, t) \geq (0.5 + 0.0001\varepsilon) |s| > (0.5 + \delta) |s|.$$

In all cases we have shown that $\text{LCS}(s, t) \geq (0.5 + \delta) |s|$, proving the lemma. \square

8.4 Finishing the proof

To prove the main theorem, we need to find two strings that agree on statistics, and remove the assumption that the number of ones is a power of two.

Theorem 8.5. *There exists absolute constants $A > 0$ and $\delta = \frac{\varepsilon^6}{900}$ such that the following holds for N sufficiently large. Let $C \subset \{0, 1\}^N$ be a code with at least $2^{\log^A N}$ strings. Then C contains two strings s and t such that $\text{LCS}(s, t) \geq (0.5 + \delta)N$.*

Proof. By Lemma 8.2, there exists a constant A' such that the number of possible tables of statistics for a string of length N is at most $2^{O(\log^{A'} N)}$. We pick $A = A' + 1$. By removing at most half of the elements of C , we may assume that every string in C starts with the same bit, and without loss of generality we may assume that every string starts with a one. Let 2^n be the largest power of two less than $N/3$, so that $2^n \geq N/6$. If there exist two strings s and t in C with less than 2^n ones, then we have $\text{LCS}(s, t) \geq 2N/3$, so we may assume that all but at most one string in C has at least 2^n ones.

By the pigeonhole principle, there exist two strings $s, t \in C$ such that

- s and t have the same number $L \geq 2^n$ of ones,
- $s_{n,1}$ and $t_{n,1}$ agree on statistics, and
- $\text{rev}(s_{n,1})$ and $\text{rev}(t_{n,1})$ agree on statistics.

Indeed, the total number of tables of statistics for each of substrings $s_{n,1}$ and $\text{rev}(s_{n,1})$ is at most $2^{O(\log^A N)}$, so the total number of pigeonholes here is at most $2^{O(\log^A N)} < 2^{\log^A N} = |C|$ if N is sufficiently large.

Let $s = s_{n,1}s'$ and $t = t_{n,1}t'$. Since strings s and t have the same length and same number of ones, and substrings $s_{n,1}$ and $t_{n,1}$ agree on statistics, we have that the suffixes s' and t' have the same length and the same number of ones as well. Thus, $\text{LCS}(s', t') \geq |s'|/2$. By applying Lemma 8.4 to strings $s_{n,1}$ and $t_{n,1}$, we have

$$\text{LCS}(s_{n,1}, t_{n,1}) \geq \left(0.5 + \frac{\varepsilon^6}{150}\right) |s_{n,1}|.$$

Hence, we have

$$\text{LCS}(s, t) \geq \text{LCS}(s_{n,1}, t_{n,1}) + \text{LCS}(s', t') \geq \left(0.5 + \frac{\varepsilon^6}{150}\right) |s_{n,1}| + 0.5|s'| = 0.5N + \frac{\varepsilon^6}{150}|s_{n,1}| \geq (0.5 + \delta)N,$$

as desired. In the last inequality, we used that $|s_{n,1}| \geq 2^n \geq N/6$. \square

9 Conclusion and open questions

We gave the first non-trivial upper bound the zero-rate threshold for bit-deletions, showing that it is strictly less than $1/2$. We achieved this via a structural lemma that classifies the oscillation patterns of 0's and 1's in a balanced string, and then exploiting it to carefully orchestrate a noticeable advantage over just matching 1's by switching to matching 0's at judicious points.

Now that we finally have a resolution to the first order question of whether $p_{\text{del}}^{\text{thr}} = 1/2$, it opens up the opportunity to address several related questions. We list some salient directions for future work below.

1. An obvious and major challenge is to determine the exact value of the zero-rate threshold for bit-deletions which remains unknown. Our current state of knowledge is $\sqrt{2} - 1 \leq p_{\text{del}}^{\text{thr}} \leq 1/2 - \delta_0$, for $\delta_0 > 0$ given by Theorem 1.1. The true value of $1/2 - p_{\text{del}}^{\text{thr}}$ is presumably much bigger than the minuscule δ_0 our proof yields. We made no attempt to optimize δ_0 , but it is likely to be very small regardless. We hazard a guess that the true value might be closer to the lower bound. More audaciously, one might even postulate that $p_{\text{del}}^{\text{thr}} = \sqrt{2} - 1$ since this threshold appears to be the limit of the techniques in the spirit of [BGH17].
2. As an interesting and necessary step toward improving the upper bound on $p_{\text{del}}^{\text{thr}}$, can one obtain better upper bounds on the *span* of a large enough code (which are implied by, but possibly easier to establish than, a lower bound on LCS)? Here, we define the *span* of two strings s and t as the minimum ratio $(|s'| + |t'|)/\text{LCS}(s', t')$ over all pairs of (contiguous) substrings $s' \subseteq s$ and $t' \subseteq t$ which are of lengths $|s'| \geq \Omega(|s|)$, $|t'| \geq \Omega(|t|)$, and the span of a code is the minimum span between any two distinct strings in the code. Note that if C has span α , then the LCS of any two distinct strings in C is at most $2N/\alpha$. The codes of [BGH17] are based on the construction of codes (a variant of the Bukh-Ma code) of growing size with span at least $2 + \sqrt{2}$. Prior to our work, no non-trivial upper bound (bounded away from the trivial limit of 4) was known on the span of positive-rate codes.

We point out that using our techniques, proving that there exist two codewords with span at most $4 - \delta_0$ is easier than proving there exist two codewords with LCS at least $(1/2 + \delta)N$. To show span at most $4 - \delta_0$, matched flags do not have to be at similar locations in the two strings, so we have more flexibility with our random shifting argument. In particular, we can apply the structure lemma to entire codewords rather than dyadic substrings as we do in Lemma 8.4, so we do not need to combine LCS in prefixes/suffixes with Lemma 3.7. Furthermore, in the Blue-Yellow case, it is okay to use an imbalanced matching where say, we match Blue flags only in s , consuming more ones in t , and hence we do not need the string regularity and string reversal $\text{rev}(\cdot)$ arguments which were used to ensure a balanced matching.

3. Our quasi-polynomial in N upper bound on the size of codes $C \subset \{0, 1\}^N$ with $\text{LCS}(C) \leq (1/2 + \delta_0)N$ can likely be improved with some more care in the argument, though we settled for it for sake of simplicity. We conjecture that in fact $|C| \leq O(\log N)$. This would be tight, as the Bukh-Ma code has size $\Omega(\log N)$ and $\text{LCS}(C) \leq (1/2 + \delta_0)N$. As evidence towards this conjecture, our techniques can be used to show that $|C| \leq O(\log N)$ when any two codewords have span at most $4 - \delta_0$, by following the sketch in the previous item.
4. For the q -ary alphabet, the q -ary codes in [BGH17] correct a fraction of deletions approaching $1 - \frac{2}{q + \sqrt{q}}$, and thus we have

$$1 - \frac{2}{q + \sqrt{q}} \leq p_{\text{del}}^{\text{thr}}(q) \leq 1 - \frac{1 + 2\delta_0}{q}. \quad (18)$$

An interesting question is to determine the infimum of constants c such that $p_{\text{del}}^{\text{thr}}(q) \geq 1 - c/q$ for large enough q . The bounds in (18) imply that $c \in [1 + 2\delta_0, 2]$.

5. In the list-decoding model, there are codes of rate $\text{poly}(\varepsilon)$ which can be list-decoded from a fraction $1/2 - \varepsilon$ of deletions with list-size $\text{poly}(1/\varepsilon)$. Can one prove a lower bound $L(\varepsilon)$ on the list-size for list decoding from $(1/2 - \varepsilon)$ fraction of deletions such that $L(\varepsilon) \rightarrow \infty$ as $\varepsilon \rightarrow 0$? What is the optimal growth rate of the list-size as a function of ε ? (For correcting bit-flips, the optimal list-size is known to be $\Theta(1/\varepsilon^2)$ [Bli86, GV10].)
6. A *pair of twins* in a string s is a pair of two disjoint subsequences (recall that in our language *subsequences* of strings are not necessarily contiguous, unlike substrings) of s which are identical. A natural question to consider is: what is the length $t(N)$ of the longest pair of twins guaranteed to exist in any $s \in \{0, 1\}^N$? This question is relevant for two reasons. First, the question of finding twins within a single string is closely related to the problem of finding longest common subsequences between distinct strings. Second, the twins problem was solved asymptotically by [APP13] using the regularity technique, which is also one of the ingredients in our work. It is now known that

$$\frac{N}{2} - O\left(\frac{N(\log \log N)^{1/4}}{(\log N)^{1/4}}\right) \leq t(N) \leq \frac{N}{2} - \Omega(\log N),$$

and it would be interesting to determine the exact growth rate of the lower-order term.

Acknowledgments. The authors are grateful to Jacob Fox for helpful conversations and for bringing [APP13] to our attention.

References

- [ACK⁺19] Sergey Avgustinovich, Julien Cassaigne, Juhani Karhumäki, Svetlana Puzynina, and Aleks Saarela. On abelian saturated infinite words. *Theoretical Computer Science*, 792:154–160, 2019.
- [APP13] Maria Axenovich, Yury Person, and Svetlana Puzynina. A regularity lemma and twins in words. *Journal of Combinatorial Theory, Series A*, 120(4):733–743, 2013.
- [BGH17] Boris Bukh, Venkatesan Guruswami, and Johan Håstad. An improved bound on the fraction of correctable deletions. *IEEE Trans. Inf. Theory*, 63(1):93–103, 2017.
- [BGZ18] Joshua Brakensiek, Venkatesan Guruswami, and Samuel Zbarsky. Efficient low-redundancy codes for correcting multiple deletions. *IEEE Trans. Inf. Theory*, 64(5):3403–3410, 2018.
- [Bli86] Vladimir M. Blinovsky. Bounds for codes in the case of list decoding of finite volume. *Problems of Information Transmission*, 22(1):7–19, 1986.
- [BM14] Boris Bukh and Jie Ma. Longest common subsequences in sets of words. *SIAM J. Discrete Math.*, 28(4):2042–2049, 2014.
- [BZ16] Boris Bukh and Lidong Zhou. Twins in words and long common subsequences in permutations. *Israel Journal of Mathematics*, 213(1):183–209, 2016.
- [CJLW18] Kuan Cheng, Zhengzhong Jin, Xin Li, and Ke Wu. Deterministic document exchange protocols, and almost optimal binary codes for edit errors. In *Proceedings of the 59th IEEE Annual Symposium on Foundations of Computer Science*, pages 200–211, 2018.
- [CR21] Mahdi Cheraghchi and João L. Ribeiro. An overview of capacity results for synchronization channels. *IEEE Trans. Inf. Theory*, 67(6):3207–3232, 2021.
- [CS75] Václav Chvatal and David Sankoff. Longest common subsequences of two random sequences. *Journal of Applied Probability*, pages 306–315, 1975.
- [GHS20] Venkatesan Guruswami, Bernhard Haeupler, and Amirbehshad Shahrabi. Optimally resilient codes for list-decoding from insertions and deletions. In *Proceedings of the 52nd Annual ACM Symposium on Theory of Computing*, pages 524–537, 2020.
- [GL16] Venkatesan Guruswami and Ray Li. Efficiently decodable insertion/deletion codes for high-noise and high-rate regimes. In *IEEE International Symposium on Information Theory, ISIT 2016, Barcelona, Spain, July 10-15, 2016*, pages 620–624. IEEE, 2016.
- [GL20] Venkatesan Guruswami and Ray Li. Coding against deletions in oblivious and online models. *IEEE Trans. Inf. Theory*, 66(4):2352–2374, 2020.
- [GMR⁺21] Venkatesan Guruswami, Jonathan Mosheiff, Nicolas Resch, Shashwat Silas, and Mary Wootters. Sharp threshold rates for random codes. In *12th Innovations in Theoretical Computer Science Conference*, volume 185 of *LIPICs*, pages 5:1–5:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

- [GV10] Venkatesan Guruswami and Salil P. Vadhan. A lower bound on list size for list decoding. *IEEE Trans. Inf. Theory*, 56(11):5681–5688, 2010.
- [GW17] Venkatesan Guruswami and Carol Wang. Deletion codes in the high-noise and high-rate regimes. *IEEE Trans. Information Theory*, 63(4):1961–1970, 2017.
- [Hae19] Bernhard Haeupler. Optimal document exchange and new codes for insertions and deletions. In *Proceedings of the 60th IEEE Annual Symposium on Foundations of Computer Science*, pages 334–347, 2019.
- [HKPS21] Hiep Hàn, Marcos Kiwi, and Matías Pavez-Signé. Quasi-random words and limits of word sequences. In *Latin American Symposium on Theoretical Informatics*, pages 491–503. Springer, 2021.
- [HS18] Bernhard Haeupler and Amirbehshad Shahrasbi. Synchronization strings: explicit constructions, local decoding, and applications. In *STOC’18—Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 841–854. ACM, New York, 2018.
- [HS21] Bernhard Haeupler and Amirbehshad Shahrasbi. Synchronization strings and codes for insertions and deletions - A survey. *IEEE Trans. Inf. Theory*, 67(6):3190–3206, 2021.
- [KLM04] Marcos Kiwi, Martin Loeb, and Jiří Matoušek. Expected length of the longest common subsequence for large alphabets. *Advances in Mathematics*, 197:480–498, November 2004.
- [KMTU11] Ian A Kash, Michael Mitzenmacher, Justin Thaler, and Jonathan Ullman. On the zero-error capacity threshold for deletion channels. In *2011 Information Theory and Applications Workshop*, pages 1–5. IEEE, 2011.
- [Lev66] Vladimir I. Levenshtein. Binary codes capable of correcting deletions, insertions and reversals. *Soviet Physics Dokl. (English Translation)*, 10(8):707–710, 1966.
- [Lue09] George S Lueker. Improved bounds on the average length of longest common subsequences. *Journal of the ACM (JACM)*, 56(3):1–38, 2009.
- [Mit09] Michael Mitzenmacher. A survey of results for deletion channels and related synchronization channels. *Probability Surveys*, 6:1–33, 2009.
- [SB21] Jin Sima and Jehoshua Bruck. On optimal k -deletion correcting codes. *IEEE Trans. Inf. Theory*, 67(6):3360–3375, 2021.
- [SGB20] Jin Sima, Ryan Gabrys, and Jehoshua Bruck. Syndrome compression for optimal redundancy codes. In *IEEE International Symposium on Information Theory*, pages 751–756, 2020.
- [SZ99] Leonard J. Schulman and David Zuckerman. Asymptotically good codes correcting insertions, deletions, and transpositions. *IEEE Transactions on Information Theory*, 45(7):2552–2557, 1999.
- [Ull67] Jeffrey D. Ullman. On the capabilities of codes to correct synchronization errors. *IEEE Transactions on Information Theory*, 13(1):95–105, 1967.
- [Wan15] Carol Wang. *Beyond unique decoding: topics in error-correcting codes*. PhD thesis, Carnegie Mellon University, 2015.

- [ZBJ20] Yihan Zhang, Amitalok J Budkuley, and Sidharth Jaggi. Generalized list decoding. In *2020 Information Theory and Applications Workshop (ITA)*, pages 51–1. IEEE, 2020.