SEPARATING WORDS AND TRACE RECONSTRUCTION

ZACHARY CHASE

Abstract. We prove that for any distinct $x, y \in \{0,1\}^n$, there is a deterministic finite automaton with $\widetilde{O}(n^{1/3})$ states that accepts x but not y. This improves Robson's 1989 bound of $\widetilde{O}(n^{2/5})$. Using a similar complex analytic technique, we improve the upper bound on worst case trace reconstruction, showing that any unknown string $x \in \{0,1\}^n$ can be reconstructed with high probability from $\exp(\widetilde{O}(n^{1/5}))$ independently generated traces.

1. Introduction

Telling two strings apart using a small collection of tools or a limited amount of data is a basic problem of the sciences. In this paper, we study two such problems and initiate the exploitation of the fruitful connection between them and a third closely related problem.

The separating words problem asks for the smallest deterministic finite automaton needed to separate two given 0-1 strings of length n, in the worst case as a function of n. Specifically, for distinct $x, y \in \{0,1\}^n$, let $f_n(x,y)$ denote the smallest positive integer m such that there exists a deterministic finite automaton with m states that accepts x but not y (one easily has $f_n(x,y) = f_n(y,x)$). Defining $f(n) := \max_{x \neq y \in \{0,1\}^n} f_n(x,y)$, the "separating words problem" is to determine the asymptotic behavior of $f(n)$. An easy example [14] shows $f(n) = \Omega(\log n)$, which is the best lower bound known to date. Goralcik and Koubek [14] in 1986 proved an upper bound of $f(n) = o(n)$, and Robson [25] in 1989 proved an upper bound of $f(n) = O(n^{2/5} \log^{3/5} n)$. Our first contribution is breaking the longstanding $\widetilde{O}(n^{2/5})$ barrier and improving the upper bound to $\widetilde{O}(n^{1/3})$.

Theorem 1. *For any distinct $x, y \in \{0,1\}^n$, there is a deterministic finite automaton with $O(n^{1/3} \log^7 n)$ states that accepts x but not y.*

Motivated by the study of reconstructing DNA, the trace reconstruction problem asks to determine an unknown string $x \in \{0,1\}^n$ from many traces of x. Specifically, a *trace* of x is obtained by deleting each bit of x with probability q, independently, and concatenating the remaining string. For example, a trace of 11001 could be 101, obtained by deleting the second and third bits. The trace reconstruction question asks for the minimum $T = T(n)$ such that any $x \in \{0,1\}^n$ can be reconstructed with probability at least 0.99 from T independently generated traces of x. For a more precise statement of the problem, see Section 3.

Holenstein, Mitzenmacher, Panigrahy, and Wieder [17] established an upper bound, that $\exp(\widetilde{O}(n^{1/2}))$ traces suffice. Nazarov and Peres [23] and De, O'Donnell, and Servedio [11] simultaneously obtained the (previous) best upper bound known, that $\exp(O(n^{1/3}))$ traces

Date: April 12, 2020.

The author is partially supported by Ben Green's Simons Investigator Grant 376201 and gratefully acknowledges the support of the Simons Foundation.

suffice. Batu et. al. [3] proved a lower bound of n, which was improved to $\widetilde{\Omega}(n^{5/4})$ by Holden and Lyons [15], which was then improved to $\widetilde{\Omega}(n^{3/2})$ by the author [7]. There has been a surge of interest in the trace reconstruction problem in the last four years – see, e.g. [24], [16], [1], [2], [10], [9], [4], [21], [19], [22].

Our second contribution is an improvement to the upper bound, to $\exp(\widetilde{O}(n^{1/5}))$.

Theorem 2. *For any deletion probability $q \in (0,1)$ and any $\delta > 0$, there exists $C > 0$ so that any unkown string $x \in \{0,1\}^n$ can be reconstructed with probability at least $1-\delta$ from $\exp(Cn^{1/5}\log^5 n)$ independent traces of x.*

Here is an outline of the paper. In Section 2, we explain the connections between the separating words problem, trace reconstruction, and a third closely related problem. In Section 3, we rigorously define the separating words problem and the trace reconstruction problem. In Section 4, we set our notation for the paper. In Section 5, we sketch the proofs Theorems 1 and 2. In Section 6, we prove Theorems 1 and 2 assuming two complex analytic theorems, that we then prove in Section 7, modulo a technical lemma that we prove in the Appendix.

2. Connections

The catalyst behind the development of the technical methods used to establish Theorems 1 and 2 was the exploration of the deep connections between the separating words problem, trace reconstruction, and a third problem, which we now mention.

What is the minimum k such that for any distinct $x, y \in \{0,1\}^n$, there is some $w \in \{0,1\}^k$ appearing a different number of times in x and y as a subsequence (i.e., a not-necessarily-contiguous substring)? The best upper bound known to date is $k = O(\sqrt{n})$, due to Krasikov and Roditty [18], and the best lower bound is $e^{\Omega(\sqrt{\log n})}$, due to Dudik and Schulman [13]. This problem is referred to as the "reconstruction from subsequences" problem, or as the "k-deck" problem.

The connections between the k-deck problem, trace reconstruction, and the separating words problem are abundant, but have not seemed to have been mentioned, or exploited, before in the literature[1]. Even at a basic level, there are intriguing similarities between the three problems. For example, for seemingly completely different reasons, pairs $x, y \in \{0,1\}^n$ without "padding" (i.e., pairs for which there is some small i with $x_i \neq y_i$) can be separated by a DFA with few states, and can be distinguished with high probability from few traces. More importantly, the proof of the $\exp(O(n^{1/3}))$ upper bound for trace reconstruction is an analytic version of the proof of the upper bound of $O(\sqrt{n})$ for the k-deck problem (both proofs use a form of "single bit statistics"); and a number theoretic version of the proof yields an $\widetilde{O}(n^{1/2})$ bound for the separating words problem (explained in Section 5). Additionally, currently, very self-similar strings, such as the Thue-Morse sequence (and its complement, each with some padding), are strings we do not know how to handle in any of the three problems.

[1]The connections between the k-deck problem and trace reconstruction have been mentioned in the literature.

In this paper, we exploit the connection between the three problems by using another proof of the $\widetilde{O}(\sqrt{n})$ upper bound for the k-deck problem, by Scott [26]. Specifically, we reverse an implication of his, noting the basic fact that if two sets $A, B \subseteq [n]$ have a different small moment (i.e., there is some small $m \in \mathbb{Z}^{\geq 0}$ with $\sum_{a \in A} a^m \neq \sum_{b \in B} b^m$), then there is some small prime p and some residue $i \in [p]$ with $|\{a \in A : a \equiv i \bmod p\}| \neq |\{b \in B : b \equiv i \bmod p\}|$. We then develop new complex analytic methods, building upon the complex analytic methods previously used in the k-deck problem and the trace reconstruction problem, to improve the upper bound on the separating words problem by showing that any distinct well-separated sets $A, B \subseteq [n]$ have a different small moment (see Theorem 2). Complex analytic methods have not previously been used to attack the separating words problem.

Our complex analytic arguments are then further built upon to improve the upper bound on the trace reconstruction problem, using also the observation (discovered independently in [8] and in [22]) that (weighted) substring counts can be reconstructed from few traces.

We hope this paper will initiate further research into the connections between the three mentioned problems, leading to further progress on each.

3. Formal Problem Statements

3.1. **The Separating Words Problem.**

A deterministic finite automaton (DFA) M is a 4-tuple (Q, δ, q_1, F) consisting of a finite set Q, a function $\delta : Q \times \{0,1\} \to Q$, an element $q_1 \in Q$, and a subset $F \subseteq Q$. We call elements $q \in Q$ "states". We call q_1 the "initial state" and the elements of F the "accept states". We say M accepts $x = x_1, \ldots, x_n \in \{0,1\}^n$ if and only if the sequence defined by $r_1 = q_1, r_{i+1} = \delta(r_i, x_i)$ for $1 \leq i \leq n$, has $r_{n+1} \in F$.

For distinct $x, y \in \{0,1\}^n$, let $f_n(x,y)$ denote the smallest positive integer m such that there exists a deterministic finite automaton with m states that accepts x but not y. Define $f(n) := \max_{x \neq y \in \{0,1\}^n} f_n(x,y)$. The "separating words problem" is to determine the asymptotic behavior of $f(n)$.

3.2. **Trace Reconstruction.**

Fix $\delta \in (0,1)$ and $q \in (0,1)$. For strings w, x, let $f(w;x)$ denote the number of times w appears as a subsequence in x; that is, $f(w;x)$ equals the number of strictly increasing tuples $(i_0, \ldots, i_{|w|-1})$ such that $x_{i_j} = w_j$ for $0 \leq j \leq |w| - 1$. For each $x \in \{0,1\}^n$, let μ_x denote the probability distribution on $\{0,1\}^{\leq n}$ given by $\mu_x(w) = (1-q)^{|w|} q^{n-|w|} f(w;x)$. Let μ_x^T denote the product measure on $(\{0,1\}^{\leq n})^T$ induced by μ_x.

Take $n \geq 1$. We say we can reconstruct any string $x \in \{0,1\}^n$ from T traces if there exists a function $F : (\{0,1\}^{\leq n})^T \to \{0,1\}^n$ satisfying

$$\mathbb{P}_{\widetilde{U}^1, \ldots, \widetilde{U}^T \sim \mu_x^T}[F(\widetilde{U}^1, \ldots, \widetilde{U}^T) = x] \geq 1 - \delta$$

for each $x \in \{0,1\}^n$ (where the $\widetilde{U}^j$ denote the T independently generated traces).

The trace reconstruction problem is to determine the smallest value $T = T(n, q, \delta)$ for which we can reconstruct any string $x \in \{0,1\}^n$ from T traces. The most common (and natural) regime is having a fixed q and δ, and asking for the asymptotics of T as a function of n (going to infinity).

4. Notation

For a positive integer n, we write $[n]$ for $\{1, \dots, n\}$. We write $\sim$ as shorthand for $= (1 + o(1))$. In our inequalities, C and c refer to (large and small, respectively) absolute constants that sometimes change from line to line. For functions f and g, we say $f = \widetilde{O}(g)$ if $|f| \leq C|g| \log^C |g|$ for some constant C. We say a set $A \subseteq [n]$ is d-separated if $a, a' \in A, a \neq a'$ implies $|a - a'| \geq d$. For a set $A \subseteq [n]$, a prime p, and a residue $i \in [p]$, let $A_{i,p} = \{a \in A : a \equiv i \pmod p\}$. For a string $x = x_1, \dots, x_n \in \{0,1\}^n$ and a (sub)string $w = w_1, \dots, w_l \in \{0,1\}^l$, let $\mathrm{pos}_w(x) := \{j \in \{1, \dots, n - l + 1\} : x_{j+k-1} = w_k \text{ for all } 1 \leq k \leq l\}$ denote the set of all (starting) positions at which w occurs as a substring in x.

For strings w, x, we sometimes write $1_{x_{k+i}=w_i}$ as shorthand for $\prod_{i=0}^{|w|-1} 1_{x_{k+i}=w_i}$. Let $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$. The symbol $\mathbb{E}_x$ denotes the expectation under the probability distribution over traces generated by the string x. For a trace $\widetilde{U}$, we define $\widetilde{U}_j = 2$ for $j > |\widetilde{U}|$; this is simply to make "$\widetilde{U}_j = 0$" and "$\widetilde{U}_j = 1$" each false. We use $0^0 := 1$. For a function f and a set E, denote $||f||_E := \max_{z \in E} |f(z)|$.

5. Sketches of Proofs

5.1. **Separating Words.** In this subsection, we sketch an argument of an $\widetilde{O}(n^{1/2})$ upper bound for the separating words problem, and then how to generalize that argument to obtain $\widetilde{O}(n^{1/3})$.

For any two distinct strings $x, y \in \{0,1\}^n$, the sets $\mathrm{pos}_1(x)$ and $\mathrm{pos}_1(y)$ are of course different. A natural way, therefore, to try to separate different strings x, y is to find a small prime p and a residue $i \in [p]$ so that $|\mathrm{pos}_1(x)_{i,p}| \neq |\mathrm{pos}_1(y)_{i,p}|$; if we can find such a p and i, then since there will be a prime q of size $q = O(\log n)$ with $|\mathrm{pos}_1(x)_{i,p}| \not\equiv |\mathrm{pos}_1(y)_{i,p}| \pmod q$, there will be a deterministic finite automaton with $2pq = O(p \log n)$ states that accepts one string but not the other (see Lemma 2). We are thus led to the following problem.

Problem 5.1. For given n, determine the minimum k such that for any distinct $A, B \subseteq [n]$, there is some prime $p < k$ and some $i \in [p]$ for which $|A_{i,p}| \neq |B_{i,p}|$.

Problem 5.1 has been considered in [26] and in [27][2] (and possibly other places) and was essentially solved in each. We present a simple solution, also discovered in [27].

Claim 5.1. *For any distinct $A, B \subseteq [n]$, there is some prime $p = O(\sqrt{n \log n})$ and some $i \in [p]$ for which $|A_{i,p}| \neq |B_{i,p}|$.*

Proof. (Sketch) Fix distinct $A, B \subseteq [n]$. Suppose k is such that $|A_{i,p}| = |B_{i,p}|$ for all primes $p \leq k$ and all $i \in [p]$. For a prime p, let $\Phi_p(x)$ denote the p^{th} cyclotomic polynomial, of degree $p - 1$. Then since $\sum_{j=1}^n 1_A(j) e^{2\pi i \frac{aj}{p}} = \sum_{j=1}^n 1_B(j) e^{2\pi i \frac{aj}{p}}$ for all $p \leq k$ and all

[2] In the latter reference, they look for an *integer* $m < k$ and some $i \in [m]$ for which $|A_{i,m}| \neq |B_{i,m}|$, which is of course more economical. We decided to restrict to primes for aesthetic reasons.

$a \in [p]$, the polynomials $\Phi_p(x)$, for $p \leq k$, divide $\sum_{j=1}^{n}(1_A(j) - 1_B(j))x^j =: f(x)$. Therefore, $\prod_{p\leq k} \Phi_p(x)$ divides $f(x)$. Since $A \neq B$, f is not identically 0 and thus must have degree at least $\sum_{p\leq k}(p-1) \sim \frac{1}{2}\frac{k^2}{\log k}$. Since the degree of f is obviously at most n, we must have $\frac{k^2}{\log k} \leq 3n$. The result follows. □

A natural idea to improve this $\widetilde{O}(\sqrt{n})$ bound for the separating words problem is to consider the sets $\mathrm{pos}_w(x)$ and $\mathrm{pos}_w(y)$ for longer w. The length of w is actually not important in terms of its "cost" to the number of states needed, just as long as it is at most p, where we will be considering $|\mathrm{pos}_w(x)_{i,p}|$ and $|\mathrm{pos}_w(y)_{i,p}|$ (see Lemma 2). One immediate benefit of considering longer w is that the sets $\mathrm{pos}_w(x)$ and $\mathrm{pos}_w(y)$ are *smaller* than $\mathrm{pos}_1(x)$ and $\mathrm{pos}_1(y)$; indeed, for example, it can be shown without much difficulty that for any distinct $x, y \in \{0,1\}^n$, there is some w of length $n^{1/3}$ such that $\mathrm{pos}_w(x)$ and $\mathrm{pos}_w(y)$ are distinct sets of size at most $n^{2/3}$. Thus, to get a bound of $\widetilde{O}(n^{1/3})$, it suffices to show the following.

Problem 5.2. For any distinct $A, B \subseteq [n]$ of sizes $|A|, |B| \leq n^{2/3}$, there is some prime $p = \widetilde{O}(n^{1/3})$ and some $i \in [p]$ such that $|A_{i,p}| \neq |B_{i,p}|$.

As in the proof sketch above, this problem is equivalent to a statement about a product of cyclotomic polynomials dividing a sparse polynomial of small degree (see the last page of [27]). We were not able to solve Problem 5.2. However, we make the additional observation that we can take w so that $\mathrm{pos}_w(x)$ and $\mathrm{pos}_w(y)$ are *well-separated* sets. Indeed, if w has length $2n^{1/3}$ and has no period of length at most $n^{1/3}$, then $\mathrm{pos}_w(x)$ and $\mathrm{pos}_w(y)$ are $n^{1/3}$-separated sets. Lemmas 1 and 2 of [25] show that such w are common enough to ensure there is a choice with $\mathrm{pos}_w(x) \neq \mathrm{pos}_w(y)$. Our main theorem is the following[3].

Theorem 3. *Let A, B be distinct subsets of $[n]$ that are each $n^{1/3}$-separated. Then there is some prime $p = \widetilde{O}(n^{1/3})$ and some $i \in [p]$ so that $|A_{i,p}| \neq |B_{i,p}|$.*

Although Theorem 2 is also equivalent to a question about a product of cyclotomic polynomials dividing a certain type of polynomial, we were not able to make progress through number theoretic arguments. Rather, we reverse the argument of Scott [26], by noting that if there is some small m so that the m^{th}-moments of A and B differ, i.e. $\sum_{a\in A} a^m \neq \sum_{b\in B} b^m$, then there is some small p and some $i \in [p]$ so that $|A_{i,p}| \neq |B_{i,p}|$. The benefit of considering the moments problem is that it is more susceptible to complex analytic techniques. Borwein, Erdélyi, and Kós [6] use complex analytic techniques to show that for any distinct $A, B \subseteq [n]$, there is some $m \leq C\sqrt{n}$ with $\sum_{a\in A} a^m \neq \sum_{b\in B} b^m$. They gave two proofs. One was to find a polynomial p of degree at most $C\sqrt{n}$ such that $|p(0)| > |p(1)| + \cdots + |p(n)|$; another was to show that any polynomial p of degree n with $|p(0)| = 1$ and coefficients bounded by 1 in absolute value must be at least $\exp(-C\sqrt{n})$ at some point close to 1. We were able to greatly expand upon this second proof to handle sparser polynomials, which we encounter due to the fact that our sets A, B are $n^{1/3}$-separated.

5.2. **Trace Reconstruction.**

We suppose the deletion probability, q, is equal to $\frac{1}{2}$ for this section.

[3]See page 7 for a more specific formulation.

To obtain the upper bound of $\exp(O(n^{1/3}))$, one first notes that it suffices to distinguish between any two distinct strings $x, y \in \{0,1\}^n$ (see [23] for details). Then, the main idea is to count the number of traces with a 1 at a certain index j (depending on x and y); there is some choice j such that the count for x will differ substantially enough from the count for y, in expectation. To establish the existence of such a j, it suffices to show that the polynomial $\sum_{k=0}^{n-1}[x_k - y_k]z^k$ is not too small for some z close to 1 on the unit circle. The sufficiency stems from the identity

$$\mathbb{E}_x\left[\sum_{j=0}^{n-1} 1_{\widetilde{U}_j=1}(2z-1)^j\right] = \frac{1}{2}\sum_{k=0}^{n-1} x_k z^k, \tag{1}$$

valid for any complex number $z \in \mathbb{C}$, where $\widetilde{U}$ denotes a random trace of x.

Two recent papers on trace reconstruction, [8] and [22], made the observation that, from not too many traces of a given $x \in \{0,1\}^n$, one can determine the number of times a given string w appears as a contiguous substring of x. The identity allowing one to do this is significantly more nontrivial than (1). For example, setting $z = 1$ in (1) merely recovers the easy fact that the expected number of 1s in a trace of x is equal to half of the number of 1s in x; however, the following identity, counting the number of contiguous 01's appearing in x, is far from obvious at first sight:

$$\mathbb{E}_x\left[\sum_{0\le j_0<j_1\le n-1} 1_{\widetilde{U}_{j_0}=0}1_{\widetilde{U}_{j_1}=1}(-1)^{j_1-j_0-1}\right] = \frac{1}{4}\#\{0 \le k \le n-2 : x_k = 0, x_{k+1} = 1\}.$$

In this paper, we weight the various j_0's differently, in analogy to (1):

$$\mathbb{E}_x\left[\sum_{0\le j_0<\cdots<j_{l-1}\le n-1}\left(\prod_{i=0}^{l-1} 1_{\widetilde{U}_{j_i}=w_i}\right)(2z-1)^{j_0}\left(\prod_{i=1}^{l-1}(-1)^{j_i-j_{i-1}-1}\right)\right] = 2^{-l}\sum_{k=0}^{n-1}\left(\prod_{i=0}^{l-1} 1_{x_{k+i}=w_i}\right)z^k,$$

valid for any $l \ge 1$, any $w = w_0, \ldots, w_{l-1} \in \{0,1\}^l$, and any $z \in \mathbb{C}$. See Proposition 6.2 for a generalization and a proof.

What we capitalize on is that, for suitable choices of w, the polynomial $\sum_{k=0}^{n-1}\left(\prod_{i=0}^{l-1} 1_{x_{k+i}=w_i}\right)z^k$ is far sparser than $\sum_{k=0}^{n-1} 1_{x_k=1}z^k$. See Theorem 5.

6. Proofs of Main Theorems

Let $\mathcal{P}_n^\mu$ be the collection of all polynomials[4] $p(z) = 1 - \epsilon z^d + \sum_{j=n^\mu}^{n} c_j z^j$ with $1 \le d < n^\mu, \epsilon \in \{0,1\}$, and $|c_j| \le 1$ for each j. We prove the following two complex analytic theorems in the appendix. We assume them to be true for the rest of the present section.

Theorem 4. *For any $\mu \in (0,1)$, there is some $C_1 > 0$ so that for all $n \ge 2$ and all $p \in \mathcal{P}_n^\mu$, it holds that*

$$\max_{x\in[1-n^{-2\mu},1]} |p(x)| \ge \exp(-C_1 n^\mu \log^5 n).$$

We will be applying Theorem 4 with $\mu = \frac{1}{3}$.

[4]Throughout the paper, we omit floor functions when they don't meaningfully affect anything.

Theorem 5. *For any $\mu \in (0,1)$, there is some $C_2 > 0$ so that for any $n \geq 2$ and any $p \in \mathcal{P}_n^\mu$, it holds that*

$$\max_{|\theta| \leq n^{-2\mu}} |p(e^{i\theta})| \geq \exp(-C_2 n^\mu \log^5 n).$$

We will be applying Theorem 5 with $\mu = \frac{1}{5}$.

6.1. **Proof of Theorem 1.** The idea of the proof (assuming Theorem 4) is as follows. As sketched in Section 5 (and as we will rigorously prove soon), it suffices to show that any distinct $n^{1/3}$-separated sets $A, B \subseteq [n]$ have some different small moment. The sets A, B having a different small moment is equivalent to the polynomial $p(x) := \sum_{n \in A} x^n - \sum_{n \in B} x^n$ not being divisible by a large power of $x - 1$, which is roughly equivalent to $p(x)$ not being uniformly too small in some interval $[1 - \epsilon, 1]$. And we know by Theorem 4 that this is true.

We will use part of Lemma 5.4 of [6], stated below.

Lemma 1. *Suppose $f(x) = \sum_{j=0}^n a_j x^j$ has $a_j \in \mathbb{C}, |a_j| \leq 1$ for each j. If $(x-1)^k$ divides $f(x)$, then $\max_{1 - \frac{k}{9n} \leq x \leq 1} |f(x)| \leq (n+1)(\frac{e}{9})^k$.*

Proposition 6.1. *There exists an absolute constant $C > 0$ so that for all $n \geq 1$ and all $p(x) \in \mathcal{P}_n^{1/3}$, the polynomial $(x-1)^{\lfloor Cn^{1/3} \log^5 n \rfloor}$ does not divide $p(x)$.*

Proof. Take $C > 0$ large. Take $p(x) \in \mathcal{P}_n^{1/3}$. Suppose for the sake of contradiction that $(x-1)^{Cn^{1/3} \log^5 n}$ divided $p(x)$. Then, by Lemma 1 and Theorem 4,

$$\begin{aligned}
(n+1)(\frac{e}{9})^{Cn^{1/3} \log^5 n} &\geq \max_{x \in [1 - \frac{C}{9} n^{-2/3} \log^5 n, 1]} |p(x)| \\
&\geq \max_{x \in [1 - n^{-2/3} \log^5 n, 1]} |p(x)| \\
&\geq e^{-C_1 n^{1/3} \log^5 n},
\end{aligned}$$

which is a contradiction if C is large enough. □

Theorem 6. *Let A, B be distinct subsets of $[n]$ that are each $n^{1/3}$-separated. Then there is some non-negative integer $m = O(n^{1/3} \log^5 n)$ such that $\sum_{a \in A} a^m \neq \sum_{b \in B} b^m$.*

Proof. Let $f(x) = \sum_{j=0}^n \epsilon_j x^j$, where $\epsilon_j := 1_A(j) - 1_B(j)$. Let $\tilde{f}(x) = \frac{f(x)}{x^r}$, where r is maximal with respect to $\epsilon_0, \ldots, \epsilon_{r-1} = 0$. We may assume without loss of generality that $\tilde{f}(0) = 1$. Then the fact that A, B are $n^{1/3}$-separated implies $\tilde{f}(x) \in \mathcal{P}_n^{1/3}$. By Proposition 6.1, $(x-1)^{Cn^{1/3} \log^5 n}$ does not divide $\tilde{f}(x)$ and thus does not divide $f(x)$. This means that there is some $k \leq Cn^{1/3} \log^5 n - 1$, $k \geq 0$, so that $f^{(k)}(1) \neq 0$. Take a minimal such k. If $k = 0$, we're of course done. Otherwise, since $f^{(m)}(1) = \sum_{j=0}^n j(j-1)\ldots(j-m+1)\epsilon_j$ for $m \geq 1$, it's easy to inductively see that $\sum_{j \in A} j^m = \sum_{j \in B} j^m$ for all $0 \leq m \leq k-1$ and then $\sum_{j \in A} j^k \neq \sum_{j \in B} j^k$. □

Theorem 2. *Let A, B be distinct subsets of $[n]$ that are each $n^{1/3}$-separated. Then there is some prime $p \in [\frac{1}{2} C' n^{1/3} \log^6 n, C' n^{1/3} \log^6 n]$ and some $i \in [p]$ so that $|A_{i,p}| \neq |B_{i,p}|$. Here, $C' > 0$ is an absolute constant.*

Proof. By Theorem 6, take $m = O(n^{1/3}\log^5 n)$ such that $\sum_{a\in A} a^m \neq \sum_{b\in B} b^m$. Since $\left|\sum_{a\in A} a^m - \sum_{b\in B} b^m\right| \leq n\, n^m \leq \exp(O(n^{1/3}\log^6 n))$, by basic estimates on the prime counting function there is some prime $p \in [\frac{1}{2}C'n^{1/3}\log^6 n, C'n^{1/3}\log^6 n]$ such that $\sum_{a\in A} a^m \not\equiv \sum_{b\in B} b^m \pmod p$. Noting that $\sum_{a\in A} a^m \equiv \sum_{i=0}^{p-1} |A_{i,p}| i^m \pmod p$ and $\sum_{b\in B} b^m \equiv \sum_{i=0}^{p-1} |B_{i,p}| i^m \pmod p$, we see that there is some $i \in [p]$ for which $|A_{i,p}| \not\equiv |B_{i,p}| \pmod p$. □

With our main technical theorem proven, we now establish the improved upper bound for the separating words problem.

Recall that, for a string $x = x_1, \ldots, x_n \in \{0,1\}^n$ and a (sub)string $w = w_1, \ldots, w_l \in \{0,1\}^l$, we defined $\mathrm{pos}_w(x) = \{j \in \{1, \ldots, n-l+1\} : x_{j+k-1} = w_k \text{ for all } 1 \leq k \leq l\}$.

Lemma 2. *Let m, n be positive integers, $i \in [m]$ a residue mod m, q a prime number, $a \in [q]$ a residue mod q, and $w \in \{0,1\}^l$ a string of length $l \leq m$. Then there is a determinsitic finite automaton with $2mq$ states that accepts a string $x \in \{0,1\}^n$ if and only if $|\{j \in \mathrm{pos}_w(x) : j \equiv i \pmod m\}| \equiv a \pmod q$.*

Proof. Write $w = w_1, \ldots, w_l$. We assume $l > 1$; a minor modification to the following yields the result for $l = 1$. We interpret indices of w mod m, which we may, since $l \leq m$. Let the states of the DFA be $\mathbb{Z}_m \times \{0,1\} \times \mathbb{Z}_q$. The initial state is $(1,0,0)$. If $j \not\equiv i \pmod m$ and $\epsilon \in \{0,1\}$, set $\delta((j,0,s),\epsilon) = (j+1,0,s)$. If $j \equiv i \pmod m$, set $\delta((j,0,s),w_1) = (j+1,1,s)$ and $\delta((j,0,s),1-w_1) = (j+1,0,s)$. If $j \not\equiv i+l-1 \pmod m$, set $\delta((j,1,s),w_{j-i+1}) = (j+1,1,s)$ and $\delta((j,1,s),1-w_{j-i+1}) = (j+1,0,s)$. Finally, if $j \equiv i+l-1 \pmod m$, set $\delta((j,1,s),w_l) = (j+1,0,s+1)$ and $\delta((j,1,s),1-w_l) = (j+1,0,s)$. The accept states are $\mathbb{Z}_m \times \{0,1\} \times \{a\}$. □

We are now ready to prove Theorem 1, restated below.

Theorem 1. *For any distinct $x, y \in \{0,1\}^n$, there is a deterministic finite automaton with $O(n^{1/3}\log^7 n)$ states that accepts x but not y.*

Proof. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be two distinct strings in $\{0,1\}^n$. If $x_i \neq y_i$ for some $i < 2n^{1/3}$, then we are of course done, so we may suppose otherwise. Let $i \geq 2n^{1/3}$ be the first index with $x_i \neq y_i$. Let $w' = x_{i-2n^{1/3}+1}, \ldots, x_{i-1}$ be a (sub)string of length $2n^{1/3}-1$. By Lemma 1 and Lemma 2 of [25], there is some choice $w \in \{w'0, w'1\}$ for which $A := \mathrm{pos}_w(x)$ is $n^{1/3}$-separated and $B := \mathrm{pos}_w(y)$ is $n^{1/3}$-separated. Clearly $A \neq B$, so Corollary 2 implies there is some prime $p \in [\frac{1}{2}C'n^{1/3}\log^6 n, C'n^{1/3}\log^6 n]$ and some $i \in [p]$ for which $|A_{i,p}| \neq |B_{i,p}|$. Since $|A_{i,p}|$ and $|B_{i,p}|$ are at most n, there is some prime $q = O(\log n)$ for which $|A_{i,p}| \not\equiv |B_{i,p}| \pmod q$. Since $|w| = 2n^{1/3} \leq p$, by Lemma 2 there is a deterministic finite automaton with $2pq = O(n^{1/3}\log^7 n)$ states that accepts x but not y. □

6.2. **Proof of Theorem 2.** Fix $q \in (0,1)$, and let $p = 1-q$. Our starting point is the following identity (see Section 5 for an introduction to it).

Proposition 6.2. *For any $x \in \{0,1\}^n, l \geq 1, w \in \{0,1\}^l$, and $z_0, \ldots, z_{l-1} \in \mathbb{C}$, we have*

$$\mathbb{E}_x \left[p^{-l} \sum_{\substack{0 \leq j \leq n-1 \\ \Delta_1, \ldots, \Delta_{l-1} \geq 1}} 1_{\widetilde{U}_j = w_0} \left(\prod_{i=1}^{l-1} 1_{\widetilde{U}_{j+\Delta_1+\cdots+\Delta_i} = w_i} \right) (\frac{z_0 - q}{p})^j \left(\prod_{i=1}^{l-1} (\frac{z_i - q}{p})^{\Delta_i - 1} \right) \right]$$
$$= \sum_{k_0 < \cdots < k_{l-1}} \left(\prod_{i=0}^{l-1} 1_{x_{k_i} = w_i} \right) z_0^{k_0} \left(\prod_{i=1}^{l-1} z_i^{k_i - k_{i-1} - 1} \right).$$

Proof. By basic combinatorics, the left hand side is

$$p^{-l} \sum_{j, \Delta_1, \ldots, \Delta_{l-1}} \sum_{k_0 < \cdots < k_{l-1}} 1_{\substack{x_{k_i} = w_i \\ \forall 0 \leq i \leq l-1}} \binom{k_0}{j} \binom{k_1 - k_0 - 1}{\Delta_1 - 1} \binom{k_2 - k_1 - 1}{\Delta_2 - 1} \cdots \binom{k_{l-1} - k_{l-2} - 1}{\Delta_{l-1} - 1}$$
$$\times p^{j + \Delta_1 + \cdots + \Delta_{l-1} + 1} q^{k_{l-1} + 1 - (j + \Delta_1 + \cdots + \Delta_{l-1} + 1)}$$
$$\times (\frac{z_0 - q}{p})^j (\frac{z_1 - q}{p})^{\Delta_1 - 1} \cdots (\frac{z_{l-1} - q}{p})^{\Delta_{l-1} - 1}$$
$$= \sum_{k_0 < \cdots < k_{l-1}} 1_{\substack{x_{k_i} = w_i \\ \forall 0 \leq i \leq l-1}} \left(\sum_j \binom{k_0}{j} (z_0 - q)^j q^{k_0 - j} \right) \left(\sum_{\Delta_1} \binom{k_1 - k_0 - 1}{\Delta_1 - 1} (z_1 - q)^{\Delta_1 - 1} q^{k_1 - k_0 - 1 - (\Delta_1 - 1)} \right)$$
$$\times \cdots \times \left(\sum_{\Delta_{l-1}} \binom{k_{l-1} - k_{l-2} - 1}{\Delta_{l-1} - 1} (z_{l-1} - q)^{\Delta_{l-1} - 1} q^{k_{l-1} - k_{l-2} - 1 - (\Delta_{l-1} - 1)} \right)$$
$$= \sum_{k_0 < \cdots < k_{l-1}} 1_{\substack{x_{k_i} = w_i \\ \forall 0 \leq i \leq l-1}} z_0^{k_0} z_1^{k_1 - k_0 - 1} \cdots z_{l-1}^{k_{l-1} - k_{l-2} - 1}.$$

□

Proposition 6.3. *For any distinct $x, y \in \{0,1\}^n$, if $x_i = y_i$ for all $0 \leq i < 2n^{1/5} - 1$, then there are $w \in \{0,1\}^{2n^{1/5}}$ and $z_0 \in \{e^{i\theta} : |\theta| \leq n^{-2/5}\}$ such that*

$$\left| \sum_k [1_{x_{k+i} = w_i} - 1_{y_{k+i} = w_i}] z_0^k \right| \geq \exp(-Cn^{1/5} \log^5 n).$$

Proof. Let $i \geq 2n^{1/5} - 1$ be the first index with $x_i \neq y_i$. Let $w' = x_{i - 2n^{1/5} + 1}, \ldots, x_{i-1}$. Lemmas 1 and 2 of [25] imply that there is some choice $w \in \{w'0, w'1\}$ such that the indices k for which $x_{k+i} = w_i$ for all $0 \leq i \leq 2n^{1/5} - 1$ are $n^{1/5}$-separated, and such that the indices k for which $y_{k+i} = w_i$ for all $0 \leq i \leq 2n^{1/5} - 1$ are $n^{1/5}$-separated. Therefore, if $p(z) := \sum_k [1_{x_{k+i} = w_i} - 1_{y_{k+i} = w_i}] z^k$, then $\epsilon \frac{p(z)}{z^m} \in \mathcal{P}_n^{1/5}$ for some $\epsilon \in \{-1, 1\}$ and $0 \leq m \leq n$. Thus, by Theorem 5, there is some $\theta \in [-n^{-2/5}, n^{-2/5}]$ such that $\exp(-C_2 n^{1/5} \log^5 n) \leq |\epsilon \frac{p(e^{i\theta})}{e^{im\theta}}| = |p(e^{i\theta})|$. Take $z_0 = e^{i\theta}$. □

In a previous version of this paper, we used Proposition 6.2 with $z_1, \ldots, z_{l-1} = 0$ and z_0 chosen according to Proposition 6.3 to prove Theorem 2, which only worked for $q \leq 1/2$, for if $q > 1/2$, then $(-q/p)^{\Delta_i - 1}$ would be too large in magnitude (for $\Delta_i \approx n$), leading to too large a variance to well-enough approximate $\sum_k [1_{x_{k+i} = w_i} - 1_{y_{k+i} = w_i}] z_0^k$ with few traces.

The idea of Shyam Narayanan was to choose $z_1, \dots, z_{l-1}$ close to 1 so that $(\frac{z_i - q}{p})^{\Delta_i - 1}$ would no longer be too large in magnitude, while also keeping the right hand side of Proposition 6.2 not too small. The following corollary, due to him, establishes the existence of such $z_1, \dots, z_{l-1}$.

Corollary 6.1. *For any distinct $x, y \in \{0,1\}^n$, if $x_i = y_i$ for all $0 \le i < 2n^{1/5} - 1$, then there are $w \in \{0,1\}^{2n^{1/5}}, z_0 \in \{e^{i\theta} : |\theta| \le n^{-2/5}\}, z_1, \dots, z_{2n^{1/5}-1} \in [1-2p, 1]$ such that, for $l := 2n^{1/5}$,*

$$\left| \sum_{k_0 < \cdots < k_{l-1}} [1_{x_{k_i} = w_i} - 1_{y_{k_i} = w_i}] z_0^{k_0} z_1^{k_1 - k_0 - 1} \dots z_{l-1}^{k_{l-1} - k_{l-2} - 1} \right| \ge \exp(-C' n^{1/5} \log^5 n).$$

Proof. Let w and z_0 be those guaranteed by Proposition 6.3. Let

$$f(z_1) = \binom{n}{2n^{1/5}}^{-1} \sum_{k_0 < \cdots < k_{l-1}} [1_{x_{k_i} = w_i} - 1_{y_{k_i} = w_i}] z_0^{k_0} z_1^{k_{l-1} - k_0 - (l-1)}.$$

Note that f is a polynomial in z_1 with each coefficient trivially upper bounded by 1 in absolute value. Therefore, by Theorem 5.1 of [6],

$$\begin{aligned}
\binom{n}{2n^{1/5}} \max_{z_1 \in [1-2p,1]} |f(z_1)| &\ge \binom{n}{2n^{1/5}} |f(0)|^{c_1/(2p)} \exp(-\frac{c_2}{2p}) \\
&\ge \binom{n}{2n^{1/5}} \left(\binom{n}{2n^{1/5}}^{-1} \exp(-C n^{1/5} \log^5 n) \right)^{c_1/(2p)} \exp(-\frac{c_2}{2p}) \\
&\ge \exp(-C' n^{1/5} \log^5 n).
\end{aligned}$$

The corollary follows by taking a z_1 realizing this maximum and then setting $z_2, \dots, z_{l-1} = z_1$. □

Proof of Theorem 2. Take distinct $x, y \in \{0,1\}^n$. If $x_i \ne y_i$ for some $i < 2n^{1/5} - 1$, then, by Lemma 4.1 of [24], x and y can be distinguished with high probability with $\exp(O(n^{1/15})) \le \exp(C'' n^{1/5} \log^5 n)$ traces. So suppose otherwise. Let $w, z_0, z_1, \dots, z_{2n^{1/5}-1}$ be those guaranteed by Corollary 6.1. Since $z_1, \dots, z_{2n^{1/5}-1} \in [1-2p, 1]$, each of $\frac{z_i - q}{p}$, $1 \le i \le 2n^{1/5} - 1$, is between -1 and 1, and so the expression in brackets in Proposition 6.2 has magnitude upper bounded by $n|2z_0 - 1|^n 2^{2n^{1/5}}$, which by [23], is upper bounded by $n \exp(\frac{n}{n^{4/5}}) 2^{2n^{1/5}}$. Therefore, since the expression in brackets in Proposition 6.2 is a function of just the observed traces, by Corollary 6.1 and a standard Höeffding inequality argument (see [23] for details; note the pigeonhole is not necessary), we see $\exp(C''' n^{1/5} \log^5 n)$ traces suffice to distinguish between x and y. As explained in [23], this suffices to establish Theorem 2. □

7. Proofs of Theorems 4 and 5

We may of course assume n is large.

Let $a = n^{-2\mu}$ and $r = a^{-1/2}$. Let $r_* \in [r]$ be such that

$$\sum_{j=1}^{r_*} \frac{1}{\log^2(j+3)} - \sum_{j=r_*+1}^{r} \frac{1}{\log^2(j+3)} \in [20, 21];$$

such an r_* clearly exists. Let

$$\begin{cases} \epsilon_j = +1 & \text{if } 1 \le j \le r_* \\ \epsilon_j = -1 & \text{if } r_* + 1 \le j \le r \end{cases}.$$

Let $\lambda_a \in (1,2)$ be such that

$$\sum_{j=1}^{r} \frac{\lambda_a}{j^2 \log^2(j+3)} = 1.$$

Let

$$d_j = \frac{\lambda_a}{j^2 \log^2(j+3)}.$$

Define

$$\widetilde{h}(z) = \widetilde{\lambda}_a \sum_{j=1}^{r} \epsilon_j d_j z^j,$$

where $\widetilde{\lambda}_a \in (1,2)$ is such that $\widetilde{h}(1) = 1$. Define

$$h(z) = (1 - a^{10})\widetilde{h}(z).$$

Define $\widetilde{E}_a$ to be the ellipse with foci at $1-a$ and $1-a+\frac{1}{4}a$ and with major axis $[1-a-\frac{a}{32}, 1-a+\frac{9a}{32}]$. Let

$$\alpha = e^{ia}, \beta = e^{-ia},$$

and denote

$$I_t = \{z \in \mathbb{C} : \arg(\frac{\alpha - z}{z - \beta}) = t\}$$

for $t \ge 0$. Note that I_0 is the line segment connecting α and β and $I_a = \{e^{i\theta} : |\theta| \le a\}$ is the set on which we wish to lower bound p at some point. Let

$$G_a = \{z \in \mathbb{C} : \arg(\frac{\alpha - z}{z - \beta}) \in (\frac{a}{2}, a)\}$$

be the open region bounded by $I_{a/2}$ and I_a.

We needed our choice of h to satisfy (i) $|h(e^{2\pi i t})| \le 1 - c|t|$ for $|t| > a^{1/2}$ (up to logs), (ii) $|h(e^{2\pi i t})| \ge 1 - Ca^2$ for $|t| \approx a$, and (iii) $h(\partial\mathbb{D}) \subseteq \overline{\mathbb{D}}$. Some thought shows that a polynomial with positive coefficients will not work. A summation by parts argument shows (i) holds, regardless of the values of ϵ_j. We had roughly half of the ϵ_j's be -1 so that (ii) holds. However, due to our required normalization that $h(1)$ is basically 1, the negative coefficients make it so that h might not map into the unit disk. Luckily, though, $\widetilde{h}$, and thus h, *does* map into the unit disk. We prove that in the appendix.

Lemma 3. *For any $t \in [-\pi, \pi]$, $\widetilde{h}(e^{it}) \in \overline{\mathbb{D}}$.*

Lemma 4. *There are absolute constants $c_4, c_5, C_6 > 0$ such that the following hold for $a > 0$ small enough. First, $h(e^{2\pi it}) \in G_a$ for $|t| \le c_4 a$. Second, $|h(e^{2\pi it})| \le 1 - c_5 \frac{|t|}{\log^2(a^{-1})}$ for $t \in [\frac{-1}{2}, \frac{1}{2}] \setminus [-C_6 a^{1/2}, C_6 a^{1/2}]$.*

Proof. Take $|t| \le a$. Then,

$$\widetilde{h}(e^{2\pi it}) = \widetilde{\lambda}_a \sum_{j=1}^{r_*} \frac{\lambda_a}{j^2 \log^2(j+3)}(1 + 2\pi itj - 2\pi^2 t^2 j^2 + O(t^3 j^3))$$
$$- \widetilde{\lambda}_a \sum_{j=r_*+1}^{r} \frac{\lambda_a}{j^2 \log^2(j+3)}(1 + 2\pi itj - 2\pi^2 t^2 j^2 + O(t^3 j^3)).$$

By our choice of r_*, $h(e^{2\pi it}) = 1 - \delta + \epsilon i$ for $\delta := c_1 t^2 + a^{10} + O(\frac{t^3 r^2}{\log^2 r})$ and $\epsilon := c_2 t + O(\frac{t^3 r^2}{\log^2 r})$, where c_1, c_2 are bounded positive constants that are bounded away from 0. By multiplying the denominator by its conjugate, we have

$$\arg\left(\frac{e^{ia} - (1-\delta+\epsilon i)}{(1-\delta+\epsilon i) - e^{-ia}}\right) = \arg\Big(\big[e^{ia} - (1-\delta+\epsilon i)\big] \cdot \big[(1-\delta-\epsilon i) - e^{ia}\big]\Big).$$

The ratio of the imaginary part to the real part of the term inside $\arg(\cdot)$ is

$$\frac{2(1-\delta-\cos(a))\sin(a)}{-\cos^2(a) + 2(1-\delta)\cos(a) - (1-\delta)^2 + \sin^2(a) - \epsilon^2}.$$

Writing $\cos(a) = 1 - \frac{1}{2}a^2 + O(a^4)$ and $\sin(a) = a + O(a^3)$, and using $\delta = O(a^2)$, the above simplifies to

$$\frac{a^3 - 2a\delta + O(a^4)}{a^2 - \epsilon^2 + O(a^3)}.$$

If $|t| \le c_4 a$, then, as $\delta = c_1 t^2 + a^{10} + O(\frac{t^3 r^2}{\log^2 r}), \epsilon = c_2 t + O(\frac{t^3 r^2}{\log^2 r})$, the inverse tangent of the above is at least $\frac{a}{2}$; the arctangent is at most a, since, by Lemma 3, $h(e^{2\pi it})$ lies in the unit disk (alternatively, one may note $2a\delta > \epsilon^2$).

We now establish the second part of the lemma. Take some $m \le r$ (for now). By summation by parts, for any $z \in \mathbb{C}$, we have

$$\sum_{j=1}^{m} \frac{\lambda_a z^j}{j^2 \log^2(j+3)} = \frac{\lambda_a \sum_{j=1}^{m} z^j}{m^2 \log^2(m+3)} + 2\lambda_a \int_1^m \frac{\left(\sum_{j \le x} z^j\right)\left(\log(x+3) + \frac{x}{x+3}\right)}{x^3 \log^3(x+3)} dx. \tag{2}$$

Quickly note that, for $z = 1$, (2) gives

$$1 = \frac{\lambda_a}{m \log^2(m+3)} + 2\lambda_a \int_1^m \frac{\lfloor x \rfloor \left(\log(x+3) + \frac{x}{x+3}\right)}{x^3 \log^3(x+3)} dx. \tag{3}$$

Trivially, for any $z \in \partial\mathbb{D}$, we have

$$\left|\frac{\lambda_a \sum_{j=1}^{m} z^j}{m^2 \log^2(m+3)}\right| \le \frac{\lambda_a}{m \log^2(m+3)}. \tag{4}$$

Note that, for any $x \ge 1$,

$$\left|\sum_{j \le x} z^j\right| = \left|z \frac{1 - z^{\lfloor x \rfloor}}{1 - z}\right| \le \frac{2}{|1-z|} \le t^{-1} \tag{5}$$

for all $z = e^{2\pi it}$ with $t \in (0, \frac{1}{2}]$. For $z = e^{2\pi it}$ with $t \in (0, 3m^{-1})$, (5) and (3) imply

$$\left| 2\lambda_a \int_1^m \frac{\left(\sum_{j \le x} z^j\right)\left(\log(x+3) + \frac{x}{x+3}\right)}{x^3 \log^3(x+3)} dx \right| \le$$

$$2\lambda_a \int_1^{3t^{-1}} \frac{\lfloor x \rfloor \left(\log(x+3) + \frac{x}{x+3}\right)}{x^3 \log^3(x+3)} dx + 2\lambda_a \int_{3t^{-1}}^m \frac{t^{-1}\left(\log(x+3) + \frac{x}{x+3}\right)}{x^3 \log^3(x+3)} dx$$

$$= 1 - 2\lambda_a \int_{3t^{-1}}^m \frac{(\lfloor x \rfloor - t^{-1}) \cdot \left(\log(x+3) + \frac{x}{x+3}\right)}{x^3 \log^3(x+3)} dx - \frac{\lambda_a}{m \log^2(m+3)}. \tag{6}$$

Observe $\lfloor x \rfloor - t^{-1} \ge \frac{1}{2} x$ for $x \ge 3t^{-1}$. Therefore,

$$2\lambda_a \int_{3t^{-1}}^m \frac{(\lfloor x \rfloor - t^{-1}) \cdot \left(\log(x+3) + \frac{x}{x+3}\right)}{x^3 \log^3(x+3)} dx \ge \lambda_a \int_{3t^{-1}}^m \frac{1}{x^2 \log^2(x+3)} dx$$

$$\ge \frac{\lambda_a}{\log^2(m+3)} \int_{3t^{-1}}^m \frac{1}{x^2} dx$$

$$= \frac{\lambda_a t}{3 \log^2(m+3)} - \frac{\lambda_a}{m \log^2(m+3)}. \tag{7}$$

Combining (2), (4), (6), and (7), we conclude that, for any $t > 3m^{-1}$,

$$\left| \tilde{h}(e^{2\pi it}) \right| = \left| \sum_{j=1}^m \frac{\lambda_a e^{2\pi ijt}}{j^2 \log^2(j+3)} \right| \le 1 - \frac{\lambda_a t}{3 \log^2(m+3)} + \frac{\lambda_a}{m \log^2(m+3)}. \tag{8}$$

By symmetry, we see

$$\left| \tilde{h}(e^{2\pi it}) \right| = \left| \sum_{j=1}^m \frac{\lambda_a e^{2\pi ijt}}{j^2 \log^2(j+3)} \right| \le 1 - \frac{\lambda_a |t|}{3 \log^2(m+3)} + \frac{\lambda_a}{m \log^2(m+3)}$$

for any $t \in [-1/2, 1/2] \setminus [-3m^{-1}, 3m^{-1}]$. For $m = r_*$, if $|t| > C_6 a^{1/2}$, for say $C_6 = 100$, then certainly $|t| > 3m^{-1}$, and so we have

$$\left| \sum_{j=1}^{r_*} \frac{\lambda_a e^{2\pi itj}}{j^2 \log^2(j+3)} \right| \le 1 - c \frac{|t|}{\log^2(a^{-1})}. \tag{9}$$

for some absolute $c > 0$. We can crudely bound

$$\left| \sum_{j=r_*+1}^{r} \frac{\lambda_a e^{2\pi itj}}{j^2 \log^2(j+3)} \right| \le \frac{4}{\log^2(a^{-1})} \frac{1}{r_*}. \tag{10}$$

Combining (9) and (10), we obtain

$$\left| \sum_{j=1}^{r} \frac{\lambda_a \epsilon_j e^{2\pi itj}}{j^2 \log^2(j+3)} \right| \le 1 - c_5' \frac{|t|}{\log^2(a^{-1})}$$

for $|t| \geq C_6 r^{-1}$, with $c_5' > 0$ small and C_6 large enough. Now, since

$$\begin{aligned}\widetilde{\lambda}_a^{-1} &= \sum_{j=1}^{r_*} \frac{\lambda_a}{j^2 \log^2(j+3)} - \sum_{j=r_*+1}^{r} \frac{\lambda_a}{j^2 \log^2(j+3)} \\ &= 1 - 2 \sum_{j=r_*+1}^{r} \frac{\lambda_a}{j^2 \log^2(j+3)} \\ &\geq 1 - 2\frac{2}{\log^2(a^{-1})}\frac{2}{r_*} \\ &\geq 1 - \frac{20}{r \log^2(a^{-1})},\end{aligned}$$

we see

$$\left| \widetilde{\lambda}_a \sum_{j=1}^{r} \frac{\lambda_a \epsilon_j e^{2\pi i t j}}{j^2 \log^2(j+3)} \right| \leq 1 - c_5 \frac{|t|}{\log^2(a^{-1})}$$

for $|t| \geq C_6 r^{-1}$, provided C_6 is large enough. Since $1 - a^{10} \leq 1$, we are done. □

Let $m = c_4^{-1} n^{2\mu}$, $J_1 = c_5^{-1} n^{-\mu} m \log^4 n$, and $J_2 = m - J_1$.

Lemma 5. *Let $u(z) = \zeta - z^d$ for some $\zeta \in \partial\mathbb{D}$ and some $d \leq n^\mu$. Then, for any $\delta \in [0,1)$, we have $\prod_{j=J_1}^{J_2-1} |\widetilde{p}(h(e^{2\pi i \frac{j+\delta}{m}}))| \leq \exp(Cn^\mu \log^5 n)$.*

Proof. First note that

$$|u(h(e^{2\pi i\theta}))| \geq 1 - |h(e^{2\pi i\theta})|^d \geq 1 - (1-a^{10})^d \geq a^{10}. \tag{11}$$

Define $g(t) = 2\log|u(h(e^{2\pi i(t+\frac{\delta}{m})}))|$. For notational ease, we assume $\delta = 0$; the argument about to come works for all $\delta \in [0,1)$. Since (11) implies g is C^1, by the mean value theorem we have

$$\begin{aligned}\left| \frac{1}{m} \sum_{j=J_1}^{J_2-1} g\left(\frac{j}{m}\right) - \int_{J_1/m}^{J_2/m} g(t)dt \right| &= \left| \sum_{j=J_1}^{J_2-1} \int_{j/m}^{(j+1)/m} \left(g(t) - g\left(\frac{j}{m}\right) \right) dt \right| \\ &\leq \sum_{j=J_1}^{J_2-1} \int_{j/m}^{(j+1)/m} \left(\max_{\frac{j}{m} \leq y \leq \frac{j+1}{m}} |g'(y)| \right) \frac{1}{m} dt \\ &\leq \frac{1}{m^2} \sum_{j=J_1}^{J_2-1} \max_{\frac{j}{m} \leq y \leq \frac{j+1}{m}} |g'(y)|. \qquad (12)\end{aligned}$$

Since $w \mapsto \log|u(h(w))|$ is harmonic and $\log|u(h(0))| = \log|u(0)| = 0$, we have

$$\int_0^1 g(t)dt = 2\int_0^1 \log|u(h(e^{2\pi i t}))|dt = 0,$$

and therefore

$$\left| \int_{J_1/m}^{J_2/m} g(t)dt \right| \leq \left| \int_0^{J_1/m} g(t)dt \right| + \left| \int_{J_2/m}^1 g(t)dt \right|. \tag{13}$$

Since

$$a^{10} \leq \left| u(h(e^{2\pi i t})) \right| \leq 2$$

for each t, we have

$$\left|\int_0^{J_1/m} g(t)dt\right| + \left|\int_{J_2/m}^1 g(t)dt\right| \leq 20\left(\frac{J_1}{m} + (1-\frac{J_2}{m})\right)\log n \leq C\frac{\log^5 n}{n^\mu}. \tag{14}$$

By (12), (13), and (14), we have

$$\left|\frac{1}{m}\sum_{j=J_1}^{J_2-1} g(\frac{j}{m})\right| \leq C\frac{\log^5 n}{n^\mu} + \frac{1}{m^2}\sum_{j=J_1}^{J_2-1}\max_{\frac{j}{m}\leq t\leq\frac{j+1}{m}}|g'(t)|.$$

Multiplying through by m, changing C slightly, and exponentiating, we obtain

$$\prod_{j=J_1}^{J_2-1}\left|u(h(e^{2\pi i\frac{j}{m}}))\right|^2 \leq \exp\left(Cn^\mu\log^5 n + \frac{1}{m}\sum_{j=J_1}^{J_2-1}\max_{\frac{j}{m}\leq t\leq\frac{j+1}{m}}|g'(t)|\right). \tag{15}$$

Note

$$g'(t_0) = \frac{\frac{\partial}{\partial t}\left[|u(h(e^{2\pi it}))|^2\right]\Big|_{t=t_0}}{|u(h(e^{2\pi it_0}))|^2}.$$

We first show

$$\frac{\partial}{\partial t}\left[|u(h(e^{2\pi it}))|^2\right]\Big|_{t=t_0} \leq 500d \tag{16}$$

for each $t_0 \in [0,1]$. Let $\widetilde{d}_j = \widetilde{\lambda}_a\epsilon_j d_j$ so that $h(e^{2\pi it}) = (1-a^{10})\sum_{j=1}^r \widetilde{d}_j e^{2\pi itj}$. Then,

$$\left|u\left(h(e^{2\pi it})\right)\right|^2 = \left|(1-a^{10})^d\left(\sum_{j=1}^r \widetilde{d}_j e^{2\pi ijt}\right)^d - \zeta\right|^2$$

$$= (1-a^{10})^{2d}\left[\left|\sum_{j=1}^r \widetilde{d}_j e^{2\pi ijt}\right|^2\right]^d - 2\,\mathrm{Re}\left[(1-a^{10})^d\overline{\zeta}\left(\sum_{j=1}^r \widetilde{d}_j e^{2\pi ijt}\right)^d\right] + 1. \tag{17}$$

The derivative of the first term of (17) is

$$(1-a^{10})^{2d}d\left[\left|\sum_{j=1}^r \widetilde{d}_j e^{2\pi ijt}\right|^2\right]^{d-1}\sum_{j_1,j_2=1}^r \widetilde{d}_{j_1}\widetilde{d}_{j_2}2\pi(j_1-j_2)e^{2\pi i(j_1-j_2)t}. \tag{18}$$

Since

$$\sum_{j=1}^r |\widetilde{d}_j| = \widetilde{\lambda}_a \leq 1 + 4a^{1/2}$$

and

$$\sum_{j=1}^r j|\widetilde{d}_j| \leq 4,$$

we can upper bound (18) by

$$d(1+4a^{1/2})^{2(d-1)}(1+4a^{1/2})4,$$

which is upper bounded by $250d$ (say), since $d \le a^{-1/2}$. As the second term of (17) is

$$2(1-a^{10})^d\overline{\zeta} \sum_{1\le j_1,\dots,j_d\le r} \widetilde{d}_{j_1}\dots\widetilde{d}_{j_d}\cos\left(2\pi(j_1+\dots+j_d)t\right),$$

the derivative of the second term of (17) is

$$-2(1-a^{10})^d\overline{\zeta} \sum_{1\le j_1,\dots,j_d\le r} 2\pi(j_1+\dots+j_d)\widetilde{d}_{j_1}\dots\widetilde{d}_{j_d}\sin\left(2\pi(j_1+\dots+j_d)t\right),$$

which is also upper bounded by (crudely) $250d$. We've thus shown (16).

Recall $|u(h(e^{2\pi i\theta}))| \ge 1-|h(e^{2\pi i\theta})|^d$. For $j \in [J_1, J_2] \subseteq [C_6a^{1/2}m, (1-C_6a^{1/2})m]$, we use (by Lemma 4)

$$|h(e^{2\pi i\frac{j}{m}})| \le 1 - c_5\frac{\min(\frac{j}{m}, 1-\frac{j}{m})}{\log^2 n}$$

to obtain

$$\frac{1}{m}\sum_{j=J_1}^{J_2-1} \frac{500d}{\left(1-(1-c_5\frac{\min(\frac{j}{m},1-\frac{j}{m})}{\log^2 n})^d\right)^2}.$$

Up to a factor of 2, we may deal only with $j \in [J_1, \frac{m}{2}]$. Let $J_* = c_5^{-1}d^{-1}m\log^2 n$. Note that $j \le J_*$ implies $c_5\frac{j}{m\log^2 n} \le d^{-1}$ and $j \ge J_*$ implies $c_5\frac{j}{m\log^2 n} \ge d^{-1}$. Thus, using $(1-x)^d \le 1-\frac{1}{2}xd$ for $x \le \frac{1}{d}$, we have

$$\begin{aligned}
\frac{1}{m}\sum_{j=J_1}^{\min(J_*,\frac{m}{2})} \frac{500d}{\left(1-(1-c_5\frac{j}{m\log^2 n})^d\right)^2} &\le \frac{500d}{m}\sum_{j=J_1}^{\min(J_*,\frac{m}{2})} \frac{1}{\left(\frac{1}{2}c_5\frac{j}{m\log^2 n}d\right)^2} \\
&= \frac{2000m\log^4 n}{c_5^2 d}\sum_{j=J_1}^{\min(J_*,\frac{m}{2})}\frac{1}{j^2} \\
&\le \frac{2000m\log^4 n}{c_5^2 d}\frac{2}{J_1} \\
&\le Cn^\mu. \qquad (19)
\end{aligned}$$

Finally, since there is some $c>0$ such that $(1-x)^l \le 1-c$ for all $l \in \mathbb{N}$ and $x \in [l^{-1}, 1]$, using the notation $\sum_{i=a}^b x_i = 0$ if $a > b$, we see

$$\begin{aligned}
\frac{1}{m}\sum_{j=\min(J_*,\frac{m}{2})+1}^{m/2} \frac{500d}{\left(1-(1-c_5\frac{j}{m\log^2 n})^d\right)^2} &\le \frac{500d}{m}\sum_{j=\min(J_*,\frac{m}{2})+1}^{m/2} c^{-2} \\
&\le Cd \\
&\le Cn^\mu. \qquad (20)
\end{aligned}$$

Combining (19) and (20), we obtain

$$\frac{1}{m}\sum_{j=J_1}^{J_2-1}\max_{\frac{j}{m}\le\frac{j+1}{m}}|g'(t)| \le Cn^\mu.$$

Plugging this upper bound into (15) yields the desired result. □

Let $\mathcal{Q}_n^\mu$ denote all polynomials of the form $(z-\alpha)(z-\beta)p(z)$ for $p \in \mathcal{P}_n^\mu$.

Corollary 7.1. *For any $q \in \mathcal{Q}_n^\mu$ and $\delta \in [0,1)$, $\prod_{j\notin\{0,m-1\}} |q(h(e^{2\pi i\frac{j+\delta}{m}}z))| \le \exp(Cn^\mu \log^5 n)$.*

Proof. Take $q \in \mathcal{Q}_n$; say $q(z) = (z-\alpha)(z-\beta)p(z)$ for $p \in \mathcal{P}_n^\mu$. For $j \in \{1,\dots,J_1-1\}$ and for $j \in \{J_2,\dots,m-2\}$, by Lemma 3 we can bound $|q(h(e^{2\pi i\frac{j}{m}}z))| \le 4n$, to obtain

$$\prod_{j\notin\{J_1,\dots,J_2-1\}} |q(h(e^{2\pi i\frac{j+\delta}{m}}))| \le (4n)^{J_1-1+m-J_2-1} \le e^{Cn^\mu \log^5 n}. \tag{21}$$

By applying Lemma 5 to $u(z) := \alpha - z$ and to $u(z) := \beta - z$ and multiplying the results, we see

$$\prod_{j=J_1}^{J_2-1} |\overline{u}(h(e^{2\pi i\frac{j+\delta}{m}}))| \le e^{Cn^\mu \log^5 n}, \tag{22}$$

where $\overline{u}(z) := (z-\alpha)(z-\beta)$. Let $\widetilde{p}(z) \in \{1, 1-z^d\}$ be the truncation of p to terms of degree less than n^μ. Then, since Lemma 4 gives

$$|h(e^{2\pi i\frac{j+\delta}{m}})| \le 1 - c_5\frac{\min\left(\frac{j}{m}+\delta, 1-(\frac{j}{m}+\delta)\right)}{\log^2 n} \le 1 - c'n^{-\mu}\log^2 n$$

for $j \in \{J_1,\dots,J_2-1\}$, we see

$$\left|p\Big(h(e^{2\pi i\frac{j+\delta}{m}})\Big) - \widetilde{p}\Big(h(e^{2\pi i\frac{j+\delta}{m}})\Big)\right| \le ne^{-c'\log^2 n} \le e^{-c\log^2 n}. \tag{23}$$

Lemma 5 implies

$$\prod_{j=J_1}^{J_2-1} |\widetilde{p}(h(e^{2\pi i\frac{j+\delta}{m}}))| \le e^{Cn^\mu \log^5 n}. \tag{24}$$

The estimates (23) and (24) combine to give

$$\prod_{j=J_1}^{J_2-1} |p(h(e^{2\pi i\frac{j+\delta}{m}}))| \le e^{C'n^\mu \log^5 n}. \tag{25}$$

Combining (21), (22), and (25), the proof is complete. □

Proposition 7.1. *For any $q \in \mathcal{Q}_n$, it holds that*

$$\max_{w\in\widetilde{E}_a} |q(w)| \ge \exp(-Cn^\mu \log^5 n)$$

and

$$\max_{w\in G_a} |q(w)| \ge \exp(-Cn^\mu \log^5 n).$$

Proof. Let $g(z) = \prod_{j=0}^{m-1} q(h(e^{2\pi i\frac{j}{m}}z))$. For $z = e^{2\pi i\theta}$, with, without loss of generality, $\theta \in [0, \frac{1}{m})$, we have by Lemma 4 and Corollary 7.1

$$|g(z)| \le \left(\max_{w\in G_a}|q(w)|\right)^2 \prod_{j\notin\{0,m-1\}} |q(h(e^{2\pi i(\frac{j}{m}+\theta)}))| \le \left(\max_{w\in G_a}|q(w)|\right)^2 \exp(Cn^\mu \log^5 n).$$

Thus, $(\max_{w\in G_a}|q(w)|)^2\exp(Cn^\mu\log^5 n)\geq\max_{z\in\partial\mathbb{D}}|g(z)|\geq|g(0)|=1$, where the last inequality used the maximum modulus principle (clearly g is analytic). The same proof applies to $\widetilde{E}_a$ in place of G_a. □

7.1. **Proof of Theorem 4.**

The following lemma was proven[5] in [6] (see Corollary 5.3):

Lemma 6. *For every $n\geq 1$, $p\in\mathcal{P}_n^\mu$, and $a>0$, we have $\left(\max_{z\in\widetilde{E}_a}|p(z)|\right)^2\leq\frac{64}{39a}\max_{x\in[1-a,1]}|p(x)|$.*

Proof of Theorem 4. Using Proposition 7.1 and Lemma 6, we obtain

$$\begin{aligned}\max_{x\in[1-n^{-2\mu},1]}|p(x)| &= \max_{x\in[1-a,1]}|p(x)|\\ &\geq \frac{39a}{64}\exp(-Cn^\mu\log^5 n)\\ &\geq \exp(-C'n^\mu\log^5 n).\end{aligned}$$

This completes the proof of Theorem 4. □

7.2. **Proof of Theorem 5.**

The following lemma was proven in [5] (see Lemma 4.3).

Lemma 7. *Suppose g is an analytic function in the open region bounded by I_0 and I_a, and suppose g is continuous on the closed region between I_0 and I_a. Then,*

$$\max_{z\in I_{a/2}}|g(z)|\leq\left(\max_{z\in I_0}|g(z)|\right)^{1/2}\left(\max_{z\in I_a}|g(z)|\right)^{1/2}.$$

Proof of Theorem 5. Take $f\in\mathcal{P}_n^\mu$, and let $g(z)=(z-\alpha)(z-\beta)f(z)$. A straightforward geometric argument yields

$$|g(z)|\leq\frac{|(z-\alpha)(z-\beta)|}{1-|z|}\leq\frac{2}{\sin(a)}\leq 3n^{2\mu}$$

for $z\in I_0$. Letting $L=||g||_{I_a}$, Lemma 7 then gives

$$\max_{z\in I_{a/2}}|g(z)|\leq(3Ln^{2\mu})^{1/2}.$$

Since we then have

$$\max_{z\in I_{a/2}\cup I_a}|g(z)|\leq\max(L,(3Ln^{2\mu})^{1/2}),$$

the maximum modulus principle implies

$$\max_{z\in G_a}|g(z)|\leq\max(L,(3Ln^{2\mu})^{1/2}).$$

By Proposition 7.1, we conclude

$$\exp(-Cn^\mu\log^5 n)\leq\max\left(L,(3Ln^{2\mu})^{1/2}\right).$$

[5]They state Lemma 6 for $p\in\mathcal{S}$; they define $\mathcal{S}$ to be the set of all analytic functions f on the (open) unit disk such that $|f(z)|\leq\frac{1}{1-|z|}$ for each $z\in\mathbb{D}$. It is clear $\mathcal{P}_n^\mu\subseteq\mathcal{S}$ for each n.

Thus,

$$||f||_{I_a} \geq \frac{1}{4}||g||_{I_a} = \frac{L}{4} \geq \exp(-C' n^{\mu} \log^5 n),$$

as desired. □

8. Appendix: Proof of Lemma 3

We thank Fedor Nazarov for a simpler proof of Lemma 3, which we include below.

Claim 8.1. *Let $\mathcal{F}$ be a compact family of (uniformly) bounded Lipschitz functions on $[0,1]$ such that $\int_0^{1/2} f < \int_{1/2}^1 f$ for every $f \in \mathcal{F}$. Then there exists $R, \epsilon > 0$ so that if $m > M$ and $m_* \in ((\frac{1}{2}-\epsilon)m, (\frac{1}{2}+\epsilon)m)$, it holds for all $f \in \mathcal{F}$ that*

$$\sum_{j=1}^{m_*} \frac{1}{\log^2(j+3)} f\left(\frac{j}{m}\right) < \sum_{j=m_*+1}^{m} \frac{1}{\log^2(j+3)} f\left(\frac{j}{m}\right). \tag{26}$$

Proof. By compactness, there exists $\epsilon > 0$ so that for all $\gamma \in (\frac{1}{2}-\epsilon, \frac{1}{2}+\epsilon)$ and all $f \in \mathcal{F}$, we have

$$\int_0^{\gamma} f < \int_{\gamma}^1 f - \epsilon. \tag{27}$$

Quickly note that

$$\begin{aligned}
\frac{1}{m}\sum_{j=1}^{m} \left[\frac{1}{\log^2(j+3)} - \frac{1}{\log^2(m+3)}\right] \left| f\left(\frac{j}{m}\right)\right| &\leq C\frac{1}{m}\left[\sum_{j=1}^{\frac{m}{\log^3(m+3)}} 1 + \sum_{j=\frac{m}{\log^3(m+3)}}^{m} \frac{\log\log(m+3)}{\log^3(m+3)}\right] \\
&\leq C\frac{\log\log(m+3)}{\log^3(m+3)} \\
&= o(\frac{1}{\log^2(m+3)})
\end{aligned}$$

as $m \to \infty$. As (26) is equivalent to

$$\frac{\log^2(m+3)}{m}\sum_{j=1}^{m_*} \frac{1}{\log^2(j+3)} f\left(\frac{j}{m}\right) < \frac{\log^2(m+3)}{m}\sum_{j=m_*+1}^{m} \frac{1}{\log^2(j+3)} f\left(\frac{j}{m}\right),$$

by the above quick note it suffices to prove

$$\frac{1}{m}\sum_{j=1}^{m_*} f(\frac{j}{m}) < \frac{1}{m}\sum_{j=m_*+1}^{m} f(\frac{j}{m}) - \frac{\epsilon}{2},$$

say (for m large enough and $m_* \in ((\frac{1}{2}-\epsilon)m, (\frac{1}{2}+\epsilon), m)$). But the LHS becomes arbitrarily close to $\int_0^{m_*/m} f(\frac{j}{m})$, and the RHS becomes arbitrarily close to $\int_{m_*/m}^1 f(\frac{j}{m}) - \frac{\epsilon}{2}$, so we're done by (27). □

Let $f(x) = \frac{1}{2} - \frac{1}{2}\left(\frac{\sin(x/2)}{x/2}\right)^2$ for $x \in (0,1]$ and $f(0) = 0$. Let$f_c(x) = c^{-4} f(cx)$ for $c > 0$ and $f_0(x) = \frac{x^4}{24}$. We will apply Claim 8.1 to the family $\mathcal{F} := \{f_c(x) : c \in [0, C]\}$, for a suitable absolute $C > 0$. An easy computation shows that $\mathcal{F}$ is a compact family of bounded

Lipschitz functions. The condition that $\int_0^{1/2} f_c < \int_{1/2}^1 f_c$ for every $c \in [0, C]$ is equivalent to $\int_0^a f(x)dx < \int_a^{2a} f(x)$ for all $a > 0$, which is equivalent to

$$\int_0^b \left(\frac{\sin x}{x}\right)^2 dx > \int_b^{2b} \left(\frac{\sin x}{x}\right)^2 dx$$

for all $b > 0$, which is easily verified.

Proof of Lemma 3. The proof of Lemma 4 shows that $\tilde{h}(e^{it}) \in \overline{D}$ if $t \in [-\pi, \pi] \setminus [-\frac{1}{100}, \frac{1}{100}]$, say, so assume $|t| \leq \frac{1}{100}$. First note that

$$\begin{aligned}\left|\mathrm{Im}[\widetilde{h}(e^{it})]\right| &= \widetilde{\lambda}_a \sum_{j=1}^r \epsilon_j d_j \sin(jt) \\ &\leq \widetilde{\lambda}_a \sum_{j=1}^r d_j j|t| \\ &\leq 2|t|.\end{aligned}$$

Also,

$$\begin{aligned}\mathrm{Re}[\widetilde{h}(e^{it})] &= \widetilde{\lambda}_a \sum_{j=1}^r \epsilon_j d_j \cos(jt) \\ &\geq \widetilde{\lambda}_a \sum_{j=1}^r \epsilon_j d_j \left(1 - \frac{j^2t^2}{2}\right) \\ &= 1 - \frac{1}{2}t^2\widetilde{\lambda}_a \sum_{j=1}^r \epsilon_j j^2 d_j \\ &\geq 1 - \frac{1}{2}t^2\widetilde{\lambda}_a(21) \\ &> 0.\end{aligned}$$

Finally,

$$\begin{aligned}\mathrm{Re}[\widetilde{h}(e^{it})] = \widetilde{\lambda}_a &\left[\sum_{j=1}^{r_*} \frac{1}{\log^2(j+3)} \left(\frac{1}{j^2} - \frac{t^2}{2}\right) - \sum_{j=r_*+1}^{r} \frac{1}{\log^2(j+3)} \left(\frac{1}{j^2} - \frac{t^2}{2}\right)\right] \\ &+\widetilde{\lambda}_a r^4 t^6 \left[\sum_{j=1}^{r_*} \frac{1}{\log^2(j+3)} f_{tr}(\frac{j}{r}) - \sum_{j=r_*+1}^{r} \frac{1}{\log^2(j+3)} f_{tr}(\frac{j}{r})\right],\end{aligned}$$

where we used

$$\frac{\cos x - 1 + \frac{x^2}{2}}{x^2} = \frac{1}{2} - \frac{1}{2}\left(\frac{\sin(x/2)}{x/2}\right)^2,$$

is by Claim 8.1 at most

$$\widetilde{\lambda}_a \left[\sum_{j=1}^{r_*} \frac{1}{\log^2(j+3)} \left(\frac{1}{j^2} - \frac{t^2}{2}\right) - \sum_{j=r_*+1}^{r} \frac{1}{\log^2(j+3)} \left(\frac{1}{j^2} - \frac{t^2}{2}\right)\right],$$

which is at most $1 - 10t^2$ by our choice of r_*. Combining everything, we see

$$\begin{aligned}\left|\widetilde{h}(e^{it})\right|^2 &= \left(\mathrm{Re}[\widetilde{h}(e^{it})]\right)^2 + \left(\mathrm{Im}[\widetilde{h}(e^{it})]\right)^2 \\ &\leq (1-10t^2)^2 + 4t^2 \\ &\leq 1 - 6t^2 \\ &\leq 1,\end{aligned}$$

as desired. □

9. Acknowledgments

I would like to thank Omer Tamuz for introducing me to the wonderful trace reconstruction problem. I also thank Shyam Narayanan for providing an extension of Theorem 2 to all $q \in (0,1)$, and Fedor Nazarov for a shorter proof of Lemma 3.

References

[1] F. Ban, X. Chen, A. Freilich, R. Servedio, and S. Sinha. Beyond trace reconstruction: population recovery from the deletion channel. ArXiv e-prints, April 2019, 1904.05532.

[2] Frank Ban, Xi Chen, Rocco A. Servedio, and Sandip Sinha. Efficient average-case population recovery in the presence of insertions and deletions. In APPROX/RANDOM 2019, volume 145 of LIPIcs, pages 44:1–44:18. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2019.

[3] T. Batu, S. Kannan, S. Khanna, and A. McGregor. Reconstructing strings from random traces. *In Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 910–918. ACM, New York*, 2004.

[4] Joshua Brakensiek, Ray Li, and Bruce Spang. Coded trace reconstruction in a constant number of traces.CoRR, abs/1908.03996, 2019.

[5] P. Borwein and T. Erdélyi. Littlewood-type problems on subarcs of the unit circle. Indiana Univ. Math. J., 46(4):1323–1346, 1997.

[6] P. Borwein, T. Erdélyi, and G. Kós. Littlewood-type problems on $[0,1]$. *Proc. London Math. Soc. (3)*, 79(1):22–46, 1999.

[7] Z. Chase. New Lower Bounds for Trace Reconstruction. To appear in *Annales Institute Henri Poincare: Probability and Statistics*, May 2019, 1905.03031.

[8] X. Chen, A. De, C. Lee, R. Servedio, S. Sinha. Polynomial-time trace reconstruction in the smoothed complexity model. ArXiv e-prints, August 2020, 2008.12386.

[9] M. Cheraghchi, R. Gabrys, O. Milenkovic, J. Ribeiro. Coded Trace Reconstruction. In *IEEE Transactions on Information Theory*, doi: 10.1109/TIT.2020.2996377.

[10] S. Davies, M. Racz, and C. Rashtchian. Reconstructing trees from traces. ArXiv e-prints, February 2019, 1902.05101.

[11] A. De, R. O'Donnell, and R. A. Servedio. Optimal mean-based algorithms for trace reconstruction. In *STOC'17—Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1047–1056. ACM, New York, 2017.

[12] E.D. Demaine, S. Eisenstat, J. Shallit, D.A. Wilson, Remarks on Separating Words, *Holzer, M. (ed.) DCFS 2011. LNCS, vol. 6808*, 147-157, 2011.

[13] M. Dudik and L. Schulman, Reconstruction from subsequences, *Journal of Combinatorial Theory, Series A, vol. 103, no. 2*, pp. 337–348, 2003.

[14] P. Goralcik and V. Koubek, On discerning words by automata, *13th Internat. Colloquium on Automate Languages and Programming, Lecture Notes Comput. Sci. 226* (Springer, Berlin, 1986) 116-122, 1986.

[15] N. Holden and R. Lyons. Lower bounds for trace reconstruction. To appear in *Annals of Applied Probability*, 2019.

[16] N. Holden, R. Pemantle, Y. Peres, A. Zhai. Subpolynomial trace reconstruction for random strings and arbitrary deletion probability. In *Proceedings of the 31st Conference On Learning Theory*, PMLR 75:1799-1840, 2018.

[17] T. Holenstein, M. Mitzenmacher, R. Panigrahy, and U. Wieder. Trace reconstruction with constant deletion probability and related results. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 389–398. ACM, New York*, 2008.

[18] I. Krasikov and Y. Roditty, On a reconstruction problem for sequences, *J. Combin. Theory Ser. A 77*, 344–348 1997.

[19] A. Krishnamurthy, A. Mazumdar, A. McGregor, S. Pal. Trace reconstruction: generalized and parameterized. ArXiv e-prints, April 2019, 1904.09618.

[20] A. McGregor, E. Price, and S. Vorotnikova. Trace reconstruction revisited. In *Proceedings of the 22nd Annual European Symposium on Algorithms*, pages 689–700, 2014.

[21] S. Narayanan. Population recovery from the deletion channel: Nearly matching trace reconstruction bounds. CoRR, abs/2004.06828, 2020.

[22] S. Narayanan, M. Ren. Circular Trace Reconstruction. ArXiv e-prints, September 2020, 2009.01346.

[23] F. Nazarov and Y. Peres. Trace reconstruction with $\exp(O(n^{1/3}))$ samples. In *STOC'17— Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1042–1046. ACM, New York, 2017.

[24] Y. Peres and A. Zhai. Average-case reconstruction for the deletion channel: subpolynomially many traces suffice. In 58th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2017, pages 228–239. IEEE Computer Soc., Los Alamitos, CA, 2017. MR3734232

[25] J. M. Robson, Separating strings with small automata, *Information Processing Letters, 30* (4): 209–214, 1989.

[26] A. Scott, Reconstructing sequences, *Discrete Mathematics, 175* (1):231–238, 1997.

[27] M. N. Vyalyı and R. A. Gimadeev, On separating words by the occurrences of subwords, *Diskretn. Anal. Issled. Oper.*, 21(1):3–14, 2014.

Mathematical Institute, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, UK

E-mail address: zachary.chase@maths.ox.ac.uk