An Improvement Upon the Bounds for the Local Leakage Resilience of Shamir's Secret Sharing Scheme

Dustin Kasser

University of Georgia, Athens GA 30602
dustin.kasser@uga.edu

Abstract. Shamir's Secret Sharing Scheme allows for the distribution of information amongst n parties so that any nt of them can combine their information to recover the secret, for some parameter $0 < t \leq 1$. By design, it is secure against the total corruption of $nt - 1$ parties, but open questions remain around its security against side-channel attacks, where an adversary may obtain a small amount of information about each of the n party's shares.

An initial result by Benhamouda, Degwekar, Ishai and Rabin showed that if n is sufficiently large and $t \geq 0.907$, then the scheme was secure under one bit of local leakage. These bounds continued to be improved in following works, and most recently Klein and Komargodski introduced a proof using a new analytical proxy that showed leakage resilience for $t \geq 0.69$.

In this paper we will use the analytic proxy of Klein and Komargodski to show leakage resilience for $t \geq 0.668$. We do this by introducing two new bounds on the proxy. The first uses a result from additive combinatorics to improve their original bound on the proxy. The second is an averaging argument that exploits the rarity of worst-case bounds occurring.

1 Introduction

In his 1979 paper "How to Share a Secret" [18], Shamir explains what is now aptly referred to as Shamir's Secret Sharing Scheme. This scheme allows for a secret to be divided among n parties so that if any tn of them work together the secret may be recovered, but a group of $tn - 1$ parties will gain no information about the secret. An example for $tn = 2$ would be to calculate a line $\ell(x)$ that passes through $(0, s)$, where s is the secret. Then each ordered pair $(i, \ell(i))$ could be distributed to each party.

Since Shamir's scheme is secure when at most $tn - 1$ parties are corrupted, it has been used as an important part of a variety of applications [2, 5, 6, 7, 8, 9, 10, 11, 17]. However, the hypothesis that all parties are entirely uncorrupted and pass no information to an adversary is very strong. In recent works it has been examined whether Shamir's scheme is secure if each party leaks a small amount of information to an adversary. Before presenting the results on the security, it may be helpful to begin by defining the scheme and leakage resistance explicitly.

To begin the scheme, a prime $p > n$ is chosen and a secret $s \in \mathbb{F}_p$ is fixed. Then, a $tn - 1$ degree polynomial $\ell \in \mathbb{F}_p[x]$ with $\ell(0) = s$ is randomly chosen. Next, each ordered pair $(i, \ell(i))$ is distributed among the parties.

It is equivalent to consider the vector $x \in \mathbb{F}_p^{tn}$ as representing the coefficients of ℓ, and then to construct the vectors $\ell_i \in \mathbb{F}_p^{tn}$, where each $\ell_i = (i, i^2, i^3, ..., i^{tn})$ so that $\ell_i \cdot x = \ell(i)$. In this case, each $(i, \ell_i \cdot x)$ is distributed among the parties. It is this perspective that we shall use for the remainder of the paper.

The adversary is allowed to construct some leakage functions $f_i : \mathbb{F}_p^t \to \{-1, 1\}$ and obtains the pairs $(i, f_i(\ell_i \cdot x))$, from which they aim to reconstruct some information about the secret. The scheme is considered secure if the amount of information gained tends to zero as n grows to infinity. In Appendix B **X**, we formally state the definition of security, but throughout this paper we will focus on using the analytic proxy of Klein and Komargodski.

The scheme was originally shown to be secure when $t \geq 0.907$ by Benhamouda, Degwekar, Ishai, and Rabin [3], in which they presented an analytic proxy to bound the leakage. These results were independently improved to $t \geq 0.8675$ by Maji, Paskin-Cherniavski, Suad, and Wang [14] and to $t \geq 0.85$ by Benhamouda et al [4], and then further to $t \geq 0.78$ by Maji, Ngyuen, Paskin-Cherniavski, and Wang [15]. A new analytic proxy was later introduced by Klein and Komargodski in [12], which improved the bound to $t \geq 0.688$ [12]. In a negative result, Nielsen and Simkin showed that Shamir's scheme is known to not be leakage resilient if $tn = O(n/\log(n))$ [16].

Before reading the proxy of Klein and Komargodski, it may be helpful to the reader to refer to Appendix B, where we formally define the Fourier transform. In this paper, we use a normalized Fourier transform so that for $f_i : \mathbb{F}_p \to \{-1, 1\}$, $\left\|\hat{f_i}\right\|_{\mathrm{L}^2} = 1$. Before continuing, we also define the function $f_S : \mathbb{F}_p^{tn}$ as

$$f_S(x) = \prod_{i \in S} f_i(x \cdot \ell_i)\,,$$

The proxy of Klein and Komargodski implies that if

$$2\left(p^3 \sum_{k \in \mathbb{F}_p \setminus 0} \sum_{S \subseteq [n]} \left|\hat{f_S}(k \cdot \ell_0)\right|^2\right)^{1/4} \tag{1}$$

decays to zero, then so too does the information available to an adversary. Because we have a term that is polynomial in p, we will need that $p = O(2^n)$ in order to gain our convergence results. They are able to obtain decay in (1) by proving that

$$\left|\hat{f_S}(k \cdot \ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{2tn - |S|}, \tag{2}$$

and that when $|S| < tn$,

$$\left|\hat{f_S}(k \cdot \ell_0)\right| = 0$$

when $k \neq 0$. Then by a counting argument, it follows that (1) decays when $t \geq 0.688$.

In this paper, we will focus on showing that each

$$\sum_{\substack{S \subseteq [n] \\ |S|=(t+a)n}} \left| \hat{f}_S(\ell_0) \right|^2$$

decays to zero for $a \in \mathbb{N}$. We will use the slightly more general setting where the ℓ_i are any collection of vectors in $\mathbb{F}_p^{tn}$ so that every tn of them are linearly independent. The ℓ_i given by the secret sharing scheme satisfy this, but in this setting we may drop the k from $\hat{f}_S(k \cdot \ell_0)$ at the cost of a factor of at most p. We introduce two new bounds, described below, in order to give leakage resistance for $t \geq 0.668$.

Before illustrating our methods, we quickly examine in more detail how Klein and Komargodski obtained the bound in (2). We begin by assuming that $t > 0$. For each set $|S| = (t+a)n$ for some parameter $0 < a < 1-t$, Klein and Komargodski show that they may bound $\left| \hat{f}_S(\ell_0) \right|$ by

$$\left| \hat{f}_S(\ell_0) \right| \leq \prod_{i \in A_1} \left\| \hat{f}_i \right\|_{\mathrm{L}^2} \prod_{j \in A_2} \left\| \hat{f}_j \right\|_{\mathrm{L}^2} \prod_{k \in B} \left\| \hat{f}_k \right\|_{\mathrm{L}^\infty} \tag{3}$$

where $|A_1| = |A_2| = an$ and $|B| = (t-a)n$. Using Plancherel, each $\left\| \hat{f}_i \right\|_{\mathrm{L}^2} = 1$. When the mean of f_i is small, $\left\| \hat{f}_i \right\|_{\mathrm{L}^\infty} \leq 2/\pi$. Their induction argument covered the cases when the mean of f_i is large replacing each term of $\left\| \hat{f}_i \right\|_{\mathrm{L}^\infty}$ with a $2/\pi$ to obtain the bound

$$\left| \hat{f}_S(\ell_0) \right| \leq \left(\frac{2}{\pi} \right)^{(t-a)n}, \tag{4}$$

which is equivalent to (2). The reader can find a similar proof of a slightly general version of this bound in Appendix A.

In Section 3 we are able to improve the bound to

$$\left| \hat{f}_S(\ell_0) \right| \leq \left(\frac{2}{\pi} \right)^{(t-0.66a)n}, \tag{5}$$

though we need the even more restrictive requirement that $a \leq t/4$. We instead use

$$\left| \hat{f}_S(\ell_0) \right| \leq \prod_{i \in A_1} \left\| \hat{f}_i \right\|_{\mathrm{L}^4} \prod_{i \in A_2} \left\| \hat{f}_i \right\|_{\mathrm{L}^4} \prod_{i \in A_3} \left\| \hat{f}_i \right\|_{\mathrm{L}^4} \prod_{i \in A_4} \left\| \hat{f}_i \right\|_{\mathrm{L}^4} \prod_{k \in C} \left\| \hat{f}_k \right\|_{\mathrm{L}^\infty}$$

and use a result of Lev [13] to obtain a bound on the L^4 norms. We then prove the bound using an induction argument similar to that of [12], as well as a counting argument to handle its failure cases.

Unfortunately, this L^4-style bound does not give much improvement, as the decay fails near $a = 0$ for both our bound and that of [12]. To obtain an improvement we also introduce an averaging argument. The core of the idea is that if two sets, S and T, share most elements, then if $\hat{f_S}(\ell_0)$ is large, $\hat{f_T}(\ell_0)$ should not be. In order to argue this more rigorously, we fix a set S' and choose another set T randomly, so that $S = S' \cup T$. For different choices of T, we would expect $\widehat{f_{S' \cup T}}(\ell_0)$ to not take consistent values. We can then average across all T to obtain the estimate that, if $|T| = (K + a)n$ for a parameter K fulfilling $a \leq K \leq t/2 - a$,

$$\sum_T |f_{S' \cup T}| \leq \left(\frac{2}{\pi}\right)^{2(t-K-3a)n} . \tag{6}$$

When we then sum across choices of S', we are over-counting our entries of $\left|\hat{f_S}(\ell_0)\right|$, and measuring this over-counting gives the bound

$$\sum_{|S|=(t+a)n} \left|\widehat{f}_S(\ell_0)\right|^2 \leq \binom{(t+a)n}{(t-K)n}^{-1} \cdot \binom{n}{(t-K)n} \cdot \left(\frac{2}{\pi}\right)^{2(t-K-3a)} . \tag{7}$$

Finally, we spend Section 5 showing that the bounds from (4) and (5), combined with the original bound in (2), indeed gives that Shamir's secret sharing scheme is secure for $t \geq 0.668$. We state this formally in the following theorem.

Theorem 1. *Let $n, t \in \mathbb{N}$ and $0 < t \leq 1$. Let $p = O(2^n)$. Then let $\{\ell_i\}_{i=0}^n$ be vectors in $\mathbb{F}_p^{tn}$ such that every tn of them are linearly independent. Let $\{f_i\}_{i=0}^n$ be some functions $f_i : \mathbb{F}_p \to \{-1, 1\}$. Let $f_S(x) = \prod f_i(\ell_i \cdot x)$. Then for $t \geq 0.668$,*

$$\sum_{S \subseteq [n]} \left|\hat{f_S}(k \cdot \ell_0)\right|^2 = 2^{-\Omega(n)} \tag{8}$$

As a final note on the structure of the paper, the reader may notice that we break from the notation of Klein and Komargodski, which would take $t \in \mathbb{N}$. We found that by taking $t, a \in [0, 1]$ it was easier to think of them as variables with which to graph various bounds; these graphs will appear throughout the paper, and may be accessed directly via links in Appendix C for the readers convenience.

2 Establishing a Bound on $\left\|\hat{f_i}\right\|_{\mathbf{L}^q}$

We will begin by introducing a Theorem that follows from Corollary 2 in [13] by Lev.

Theorem 2. *Let $f : \mathbb{F}_p \to \{0, 1\}$ be an arbitrary function. Let $g : \mathbb{F}_p \to \{0, 1\}$ be a function such that $\|g\|_{L^1} = \|f\|_{L^1}$ and g is the indicator function for the set $[-a, b]$, where $|b - a| \leq 1$. Then for each $k \in \mathbb{N}$,*

$$\left\|\hat{f}\right\|_{L^{2k}} \leq \|\hat{g}\|_{L^{2k}} .$$

This allows us to move from examining arbitrary functions to indicators of intervals, where we may explicitly compute their L^{2k} norms, which we claim correspond to the following function.

Definition 1. *For $q > 2$, $q \in 2\mathbb{N}$, we define the function $L_q(\mu)$ as*

$$L_q(\mu) = 2\sum_{k=1}^{\sqrt{p}} \left| \frac{2}{\pi} \cdot \frac{\sin\left(\pi k \frac{\mu+1}{2}\right)}{k} \right|^q \tag{9}$$

While we will only use $L_4(\mu)$ in this paper, we state the results of this section in higher generality in case it is useful to others.

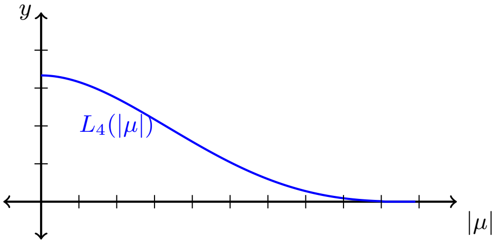


Fig. 1: A graph of $L_4(|\mu|)$ on $[0, 1]$ with increments at 0.1 intervals.

Lemma 1. *If $f : \mathbb{F}_p \to \{-1, 1\}$ with $0 < \mu = \mathbb{E}f$, then for all $q \in 2\mathbb{N}$, $q > 2$,*

$$\sum_{k\neq 0} \left|\hat{f}(k)\right|^q \leq L_q(\mu) + O\left(\frac{1}{\sqrt{p}}\right) ,$$

Proof. We will start by bounding f above by the indicator function of an interval of the form $[-a, a]$. We define the function $g : \mathbb{F}_p \to \{0, 1\}$ as

$$g(x) = \frac{f(x) + 1}{2}$$

so that $g : \mathbb{F}_p \to \{0, 1\}$. Further,

$$\sum_{k\neq 0} \left|\hat{f}(k)\right|^q = 2\sum_{k\neq 0} |\hat{g}(k)|^q .$$

Since g is in the proper form to apply Theorem 2, we will focus on bounding it instead. Let $\nu = \|g\|_{\mathrm{L}^1}/p$ be its density of non-zero entries. Let $a, b \in \mathbb{Z}_{\geq 0}$ such that $|b - a| \leq 1$ and if $s(x)$ is the indicator function for $[-a, b]$, then $\|s\|_{\mathrm{L}^1} = \nu p$. From here, we may apply Theorem 2 to g and s so that

$$\sum_{k\neq 0} |\hat{g}(k)|^q \leq \sum_{k\neq 0} |\hat{s}(k)|^q .$$

Finally, we introduce the function $h : F_p \to \{0,1\}$, defined as

$$h(x) = \begin{cases} 1 & : x \in \left[-\lfloor \frac{p\nu}{2} \rfloor, \lfloor \frac{p\nu}{\rfloor} \right] \\ 0 & : x \notin \left[-\lfloor \frac{p\nu}{2} \rfloor, \lfloor \frac{p\nu}{2} \rfloor\right] \end{cases}$$

The number of non-zero outputs for $h(x)$ and $s(x)$ differs by at most one, and so since our Fourier transform is normalized by $1/p$,

$$\sum_{k \neq 0} |\hat{s}(k)|^q \leq \sum_{k \neq 0} \left(\left| h\hat{(k)} \right| + 1/p \right)^q .$$

Factoring out the right-hand side, we obtain the inequality

$$\sum_{k \neq 0} |\hat{s}(k)|^q \leq \sum_{k \neq 0} \sum_{j=1}^{q} \left| \hat{h}(k)^j \right| \cdot (1/p)^{q-i} \cdot \binom{q}{i} .$$

We next exchange the order of the sums, to obtain

$$\sum_{k \neq 0} |\hat{s}(k)|^q \leq \sum_{i=0}^{q} \sum_{k \neq 0} \left| \hat{h}(k) \right|^i \cdot (1/p)^{q-i} \cdot \binom{q}{i} .$$

Since $\|h\|_{\mathrm{L}^r} \leq 1$ for $r \geq 1$, all terms with $q > i \geq 2$ are $O(1/p)$. When $i < 2$, $q - i > 1$, and so for $i = 1$ or $i = 0$,

$$\sum_{k \neq 0} \left| \hat{h}(k) \right|^i \cdot (1/p)^{q-i} \cdot \binom{q}{i} \leq \sum_{k \neq 0} 1 \cdot 1/p^2 \cdot q^2 \leq (p-1) \cdot q^2/p^2 = O(1/p) . \quad (10)$$

As we wish to examine the term when $i = q$, we reduce to the inequality

$$\sum_{k \neq 0} |\hat{s}(k)|^q \leq \left(\sum_{k \neq 0} \left| \hat{h}(k) \right|^q \right) + O(1/p) .$$

As

$$\sum_{k \neq 0} \left| \hat{f}(x) \right|^q \leq \sum_{k \neq 0} \left| 2\hat{h}(k) \right|^q + O(1/p)$$

we shall proceed by obtaining estimates on each $\hat{h}(k)$. Notice that

$$\hat{h}(k) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} h(x) e^{\frac{2\pi i}{p} kx} = \frac{1}{p} \sum_{\frac{-p\nu}{2} \leq x \leq \frac{p\nu}{2}} \left(\cos\left(\frac{2\pi}{p} xk \right) + i \sin\left(\frac{2\pi}{p} xk \right) \right)$$

As our sum is over x values that are symmetric about 0, our sine terms cancel. Then

$$\hat{h}(k) = \frac{1}{p} \sum_{\frac{-p\nu}{2} \leq x \leq \frac{p\nu}{2}} \cos\left(\frac{2\pi}{p} xk \right) .$$

Note that for each $z \in \mathbb{Z}$,

$$\left| \int_{z}^{z+1} \cos\left(\frac{2\pi}{p}kx\right) dx - \cos\left(\frac{2\pi}{p}kn\right) \right| \leq \frac{4\pi k}{p} .$$

Then when $|k| < \sqrt{p}$, we may write

$$\hat{h}(k) = \frac{1}{p} \int_{\frac{-p\nu}{2}}^{\frac{p\nu}{2}} \left(\cos\left(\frac{2\pi}{p}xk\right) + O\left(\frac{1}{\sqrt{p}}\right) \right) dx$$

Since $\nu \leq 1$, pulling out the $O(1/\sqrt{p})$ leaves our original term unaffected, so that

$$\hat{h}(k) = O\left(\frac{1}{\sqrt{p}}\right) + \frac{1}{p} \int_{\frac{-p\nu}{2}}^{\frac{p\nu}{2}} \cos\left(\frac{2\pi}{p}xk\right) dx$$

Making a u substitution for $u = 2\pi xk/p$, we have that

$$\hat{h}(k) = O\left(\frac{1}{\sqrt{p}}\right) + \frac{1}{p} \int_{\frac{-2\pi k\nu}{2}}^{\frac{2\pi k\nu}{2}} \cos(u) \frac{p}{2\pi k} du = O\left(\frac{1}{\sqrt{p}}\right) + \frac{1}{\pi k} \int_{0}^{\pi k\nu} \cos(u)\, du$$

and so

$$\hat{h}(k) = O\left(\frac{1}{\sqrt{p}}\right) + \frac{\sin(\pi k\nu)}{\pi k}$$

We now only need to show that when $|k| > \sqrt{p}$, $\hat{h}(k) = O(1/\sqrt{p})$.
Let $J \in \mathbb{N}$ and $j = j(J) \in \mathbb{F}_p$ with $J \equiv j \mod p$. We choose J to be minimal such that $jk \in [-\sqrt{p}, \sqrt{p}]$. Note that $J \leq \sqrt{p}$ by the pigeonhole principle.
Suppose that $\nu p \leq J$; then $\nu \leq \frac{1}{\sqrt{p}}$, and so

$$\left| \frac{1}{p} \sum_{\frac{-p\nu}{2} \leq x \leq \frac{p\nu}{2}} e^{\frac{2\pi i}{p}kx} \right| \leq \frac{p\nu}{p} = O\left(\frac{1}{\sqrt{p}}\right) .$$

It also follows that for any $|c|, |d| < 1/\sqrt{p}$, we may say that

$$\left| \frac{1}{p} \sum_{\frac{-p\nu}{2} - c \leq x \leq \frac{p\nu}{2} + d} e^{\frac{2\pi i}{p}kx} \right| = \left| \frac{1}{p} \sum_{\frac{-p\nu}{2} \leq x \leq \frac{p\nu}{2}} e^{\frac{2\pi i}{p}kx} \right| + O\left(\frac{1}{\sqrt{p}}\right) .$$

Rather than examining the sum over all $x \in \mathbb{F}_p$, we will instead examine a partial sum, where the values range between $m+1$ and $m+J$ for a parameter m.

$$\sum_{x=m+1}^{m+J} e^{\frac{2\pi i}{p}kx} . \tag{11}$$

We may rewrite this as

$$\sum_{x=1}^{J} e^{\frac{2\pi i}{p}k(x+m)} .$$

We begin by noting that there must be some element $y = a/J \in \mathbb{Q}$ satisfying $y \in [-\sqrt{p}/J, \sqrt{p}/J]$ and $yJ \equiv kj \mod p$. Then it follows that $yJ \equiv kJ \mod p$.

$$\sum_{x=1}^{J} e^{\frac{2\pi i}{p}k(x+m)} = \sum_{x=1}^{J} e^{\frac{2\pi i}{p}(k(x+m)-yx)} + \left(e^{\frac{2\pi i}{p}k(x+m)} - e^{\frac{2\pi i}{p}(k(x+m)-yx)}\right) .$$

Notice that

$$\sum_{x=1}^{J} e^{\frac{2\pi i}{p}(k(x+m)-yx)} = e^{\frac{2\pi i}{p}km} \sum_{x=1}^{J} e^{\frac{2\pi i}{p}(k-y)x} .$$

Since $kJ - yJ \equiv 0 \mod p$, it follows that $k - y = zp/J$ for some $z \in \mathbb{Z}$. As $k > \sqrt{p} > y$, it follows that $z \neq 0$. Then

$$\sum_{x=1}^{J} e^{\frac{2\pi i}{p}(k(x+m)-yx)} = e^{\frac{2\pi i}{p}km} \sum_{x=1}^{J} e^{\frac{2\pi i}{J}zx} .$$

Since $e^{\frac{2\pi i}{J}zx}$ is a J-th root of unity, it follows that

$$\sum_{x=1}^{J} e^{\frac{2\pi i}{p}(k(x+m)-yx)} = 0.$$

Then we may rewrite (11) again as

$$\sum_{x=m+1}^{m+J} e^{\frac{2\pi i}{p}kx} = \sum_{x=1}^{J} \left(e^{\frac{2\pi i}{p}k(x+m)} - e^{\frac{2\pi i}{p}(k(x+m)-yx)}\right) = e^{\frac{2\pi ikm}{p}} \sum_{x=1}^{J} \left(e^{\frac{2\pi i}{p}kx} - e^{\frac{2\pi i}{p}(kx-yx)}\right) .$$

It is now useful to define the constant

$$\sum_{x=1}^{J} \left(e^{\frac{2\pi i}{p}kx} - e^{\frac{2\pi i}{p}(kx-yx)}\right) = \lambda_k ,$$

so that

$$\sum_{x=1}^{j} e^{\frac{2\pi i}{p}k(x+m)} = \lambda_k \cdot e^{\frac{2\pi i}{p}km} .$$

Note that for $\theta, \phi \in \mathbb{R}$,

$$\left|e^{i\theta} - e^{i\phi}\right| \leq |\theta - \phi| ,$$

and so

$$|\lambda_k| \leq \sum_{x=1}^{J} \left|\left(\frac{2\pi}{p}kx - \frac{2\pi}{p}(kx - yx)\right)\right| \leq \frac{2\pi}{p} \sum_{x=1}^{J} |yx| = \frac{2\pi}{p} |y| \frac{J(J+1)}{2} .$$

Since $|y| \leq \sqrt{p}/J$,

$$|\lambda_k| \leq \frac{2\pi}{p} \frac{\sqrt{p}}{J} \frac{J(J+1)}{2} \leq \frac{4\pi J}{\sqrt{p}} .$$

By our previous remark, we will rewrite $\hat{h}(k)$ as a sum over partial sums of length J, incurring at most $O(1/\sqrt{p})$ error. We state this formally below.

$$\left|\hat{h}(k)\right| = \left|\frac{1}{p} \sum_{\frac{-p\nu}{2} \leq x \leq \frac{p\nu}{2}} e^{\frac{2\pi i}{p}kx}\right| = \frac{1}{p} \sum_{m=-J\left\lfloor \frac{p\nu}{2J}\right\rfloor}^{m=J\left\lfloor \frac{p\nu}{2J}\right\rfloor} \sum_{x=m+1}^{m+J} e^{\frac{2\pi i}{p}kx} + O\left(\frac{1}{\sqrt{p}}\right) . \quad (12)$$

We use our bounds from above to write

$$\left|\hat{h}(k)\right| \leq \frac{1}{p} \left|\lambda_k\right| 3 \left\lfloor \frac{p\nu}{2J} \right\rfloor \leq \frac{1}{p} \frac{4\pi J}{\sqrt{p}} 3 \left\lfloor \frac{p\nu}{2J} \right\rfloor .$$

Simplifying, it follows that

$$\left|\hat{h}(k)\right| \leq \frac{6\pi}{\sqrt{p}} .$$

Then it follows that

$$\sum_{k\neq 0} \left|\hat{f}(k)\right|^q \leq \sum_{k\neq 0} \left|2\hat{h}(k)\right|^q + O(1/p) \leq \sum_{k\neq 0} \left|2 \cdot \frac{1}{\pi} \frac{\sin\left(\pi k \nu\right)}{k}\right|^q + O\left(\frac{1}{\sqrt{p}}\right) .$$

Notice that combining our positive and negative k,

$$\sum_{k\neq 0} \left|\hat{f}(k)\right|^q \leq 2 \sum_{k=1}^{\sqrt{p}} \left|\frac{2}{\pi} \cdot \frac{\sin\left(\pi k \nu\right)}{k}\right|^q + O\left(\frac{1}{\sqrt{p}}\right) .$$

Note that $\nu = (\mu + 1)/2$, and so

$$\sum_{k\neq 0} \left|\hat{f}(k)\right|^q \leq 2 \sum_{k=1}^{\sqrt{p}} \left|\frac{2}{\pi} \cdot \frac{\sin\left(\pi k \frac{\mu+1}{2}\right)}{k}\right|^q + O\left(\frac{1}{\sqrt{p}}\right) ,$$

which is as we claimed.

3 A New Bound on $\left|\hat{f}_S(\ell_0)\right|$

In this section we will be relying on Lemma 1. As we will eventually be forced to round certain terms up, we will suppress the error term of $O(1/\sqrt{p})$. We will simply ask that p be sufficiently large that the error caused by the $O(1/\sqrt{p})$ term fits under the error induced by rounding.

Theorem 3. *Let $S \subset \mathbb{F}_p$ such that $|S| = (t+a)n$ with $a \leq t/4$. Then for n sufficiently large,*

$$\left|\hat{f}_S(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{(t-0.66a)n} .$$

Lemma 2. *Let $S \subset \mathbb{F}_p$ and $T \subset S$ such that $|S| = (t+a)n$ and $|T| = 4an$. Then*

$$\left|\hat{f}_S(\ell_0)\right| \leq \prod_{i \in T} \left\|\hat{f}_i\right\|_{L^4} \cdot \prod_{j \in S\backslash T} \left\|\hat{f}_j\right\|_{L^\infty} .$$

This is a similar result to Corollary 4.4 of [12]. We provide proofs for a similar result in Lemma 8 and Corollary 1 in Appendix A. For this reason, we will omit the proof of this Lemma.

Recall $L_q(|\mu|)$,

$$L_q(\mu) = 2\sum_{k=1}^{\sqrt{p}} \left| \frac{2}{\pi} \cdot \frac{\sin\left(\pi k \frac{\mu+1}{2}\right)}{k} \right|^q \tag{13}$$

as defined in Definition 1. Then we define $K : [0,1] \to [0,1]$ as

$$K(|\mu|) = \left(L_4(|\mu|) + |\mu|^4\right)^{\frac{1}{4}} .$$

Notice that for each i,

$$\left\|\hat{f}_i\right\|_{\mathrm{L}^4} \leq K(|\mu_i|) .$$

It is easy to verify through an approximation of K that for all $x \in [0, 0.75]$, $K(x) \leq K(0)$, and the K is increasing on $[0.75, 1]$. We state the following Lemma, which will have an inductive proof using techniques from [12].

Lemma 3. *Let $S \subset \mathbb{F}_p$ and $T \subset S$ such that $|S| = (t+a)n$, $|T| = 4an$. Let $B \subset T$ such that for each $i \in B$, $|\mu_i| > 0.836$. Let $G \subset T$ such that for each $i \in G$, $|\mu_i| \leq 2/\pi$. Further, let $|G| = 3\,|B|$. Then*

$$\left|\hat{f}_S(\ell_0)\right| \leq (K(0))^{4|B|} \prod_{i \in T\backslash(B\cup G)} \left\|\hat{f}_i\right\|_{L^4} \cdot \prod_{j \in S\backslash T} \left\|\hat{f}_j\right\|_{L^\infty} .$$

Proof. We will induct on $|B|$, beginning by noting that when $|B| = 0$ the lemma holds by Lemma 2. Suppose then that $|B| > 0$. Then choose some $b \in B$ and a set $G' \subset G$ with $|G'| = 3$. To ease our notational burden we will assume without loss of generality that $\mu_b \geq 0$. Then notice that we may rewrite

$$\hat{f}_S(\ell_0) = \mu_b \widehat{f_{S\backslash b}}(\ell_0) + \widehat{(f_b - \mu_b) f_{S\backslash b}}(\ell_0) . \tag{14}$$

We will bound the two terms separately. First, notice that by the induction hypothesis on $|B|$, choosing $\bar{T} = T\backslash(b \cup G')$, $\bar{B} = B\backslash b$, and $\bar{G} = G\backslash G'$,

$$\left|\mu_b \hat{f}_{S\backslash b}(\ell_0)\right| \leq \mu_b \cdot \prod_{i \in G'} \left\|\hat{f}_i\right\|_{\mathrm{L}^\infty} \cdot (K(0))^{4|B|-4} \cdot \prod_{i \in \bar{T}\backslash(\bar{B}\cup\bar{G})} \left\|\hat{f}_i\right\|_{\mathrm{L}^4} \cdot \prod_{j \in S\backslash(\bar{T}\cup b \cup G')} \left\|\hat{f}_j\right\|_{\mathrm{L}^\infty} .$$

Firstly, note that $\bar{T}\backslash(\bar{B}\cup\bar{G}) = T\backslash(B \cup G)$. Further, $S\backslash(\bar{T}\cup b \cup G') = S\backslash T$. Finally, by hypothesis on G, for each $i \in G'$,

$$\left\|\hat{f}_i\right\|_{\mathrm{L}^\infty} \leq \left(\frac{2}{\pi K(0)}\right) K(0) ,$$

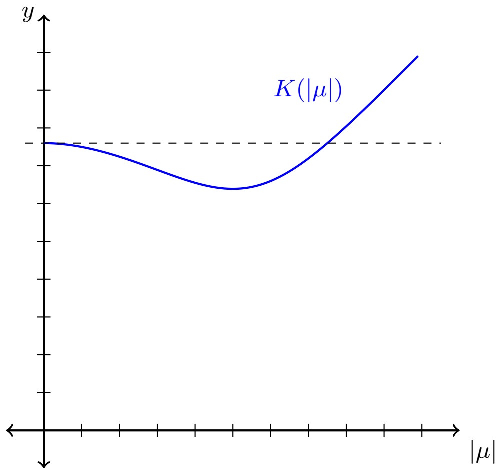


Fig. 2: A graph of $K(|\mu|)$ on $[0, 1]$ with increments at 0.1 intervals.

and so we may conclude that

$$\left|\mu_b \hat{f}_{S\setminus b}(\ell_0)\right| \leq \mu_b \cdot \left(\frac{2}{\pi K(0)}\right)^3 \cdot (K(0))^{4|B|-1} \cdot \prod_{i\in T\setminus(B\cup G)} \left\|\hat{f}_i\right\|_{\mathrm{L}^4} \cdot \prod_{j\in S\setminus T} \left\|\hat{f}_j\right\|_{\mathrm{L}^\infty} .$$

Applying the induction hypothesis to the second term of (14), $\left|\widehat{(f_b - \mu_b) f_{S\setminus b}}\right|$ is bounded by

$$\left\|\widehat{f_b - \mu_b}\right\|_{\mathrm{L}^4} \cdot \prod_{i\in G'} \left\|\hat{f}_i\right\|_{\mathrm{L}^4} \cdot (K(0))^{4|B|-4} \prod_{i\in\bar{T}\setminus(\bar{B}\cup\bar{G})} \left\|\hat{f}_i\right\|_{\mathrm{L}^4} \cdot \prod_{j\in S\setminus(\bar{T}\cup b\cup G')} \left\|\hat{f}_j\right\|_{\mathrm{L}^\infty} .$$

We rewrite (3), using that for each $i \in G'$, $\left\|\hat{f}_i\right\|_{\mathrm{L}^4} \leq K(0)$, and so

$$\left|\widehat{(f_b - \mu_b) f_{S\setminus b}}\right| \leq \left(L_4(\mu_b)\right)^{1/4} \cdot (K(0))^{4|B|-1} \prod_{i\in T\setminus(B\cup G)} \left\|\hat{f}_i\right\|_{\mathrm{L}^4} \cdot \prod_{j\in S\setminus T} \left\|\hat{f}_j\right\|_{\mathrm{L}^\infty} .$$

Then it suffices to show that

$$\mu_b \cdot \left(\frac{2}{\pi K(0)}\right)^3 + \left(L(\mu_b)\right)^{1/4} \leq K(0) .$$

Unfortunately, this only holds for when $\mu_b \geq 0.836$, leading to the use of that bound, rather than the more desirable 0.75.

It is useful to note that

$$\mu_b \cdot \left(\frac{2}{\pi K(0)}\right)^3 + \left(L(\mu_b)\right)^{1/4} = K(\mu_b)$$

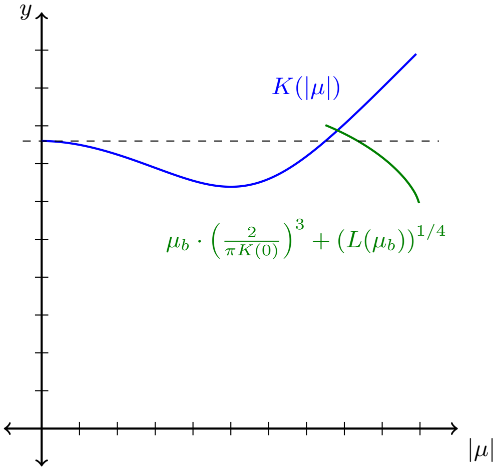


Fig. 3: A graph of displaying the induction bound compared against $K(|\mu|)$.

at approximately $\mu_b = 0.7817$. Since

$$\mu \cdot \left(\frac{2}{\pi K(0)}\right) + (L(\mu))^{1/4}$$

is decreasing in μ, we may run this argument again, but using a bound of $K(0.7818)$, by our remark above, to handle terms with $\mu \in (0.7817, 0.836]$ to gain the following Lemma.

Lemma 4. *Let $S \subset \mathbb{F}_p$ and $T \subset S$ such that $|S| = (t+a)n$, $|T| = 4an$. Let $B_1, B_2 \subset T$ such that for each $i \in B_1$, $|\mu_i| > 0.836$ and for each $j \in B_2$, $|\mu_j| \in (0.7817, 0.836]$. Let $G \subset T$ such that for each $i \in G$, $|\mu_i| \leq 2/\pi$. Further, let $|G| = 3\,|B_1 \cup B_2|$. Then*

$$\left|\hat{f}_S(\ell_0)\right| \leq (K(0))^{4|B_1|+3|B_2|} \cdot (K(0.7818))^{|B_2|} \prod_{i \in T \setminus (B_1 \cup B_2 \cup G)} \left\|\hat{f}_i\right\|_{L^4} \cdot \prod_{j \in S \setminus T} \left\|\hat{f}_j\right\|_{L^\infty}.$$

As an additional note, in the above Lemma our induction gives $K(0)^{|3|B_2||}$, which are the terms coming from our set G used to induct on B_2. The terms directly from B_2 provide the $K(0.7818)^{|B_2|}$.

From here we will restate the bound derived in [12], though we will preserve the extra terms

$$H(|\mu|) = \frac{2}{\pi}\,|\mu| + \cos\left(\frac{\pi}{2}\,|\mu|\right)$$

that come out of the induction argument. The reader may refer to a similar argument using L^2 bounds in the Appendix in Lemma 7, though one would modify it by taking $B = A$ and preserving the terms that come out due to induction. To avoid needless repetition of the argument, we omit the proof of Lemma 5.

Lemma 5. *Let $S \subset \mathbb{F}_p$ with $|S| = (t+a)n$, $a \leq 1-t$. Then let $B \subset T$ with $|B| \leq (t-a)n$ and for each $i \in B$, $|\mu_i| \geq 2/\pi$. Then*

$$\left|\hat{f}_S(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{(t-a)n} \cdot \prod_{i \in B} H(|\mu_i|) \,.$$

To prove Theorem 3, we would like to get an extra saving of $(2/\pi)^{0.34an}$. This could happen if there are enough functions with large μ_i that the savings that we from $H(\mu)$ would give us this without a need for an L^4 argument. We proceed by examining when this occurs for some bounds on $|\mu|$.
We begin with the set

$$A = \{i \in S : |\mu_i| \in [0.836, 1]\} \ ,$$

which act as B_1 for Lemma 4. Then notice that

$$\prod_{i \in A} H(|\mu_i|) \leq (H(0.836))^{|A|} \leq \left(\frac{2}{\pi}\right)^{0.555|A|} \quad .$$

Our second set is

$$B = \{i \in S : |\mu_i| \in [0.7817, 0.836)\} \ ,$$

which will act as B_2 for Lemma 4. Then we see that

$$\prod_{i \in B} H(|\mu_i|) \leq (H(0.7817))^{|B|} \leq \left(\frac{2}{\pi}\right)^{0.4|B|} \quad .$$

Our third set is

$$C = \{i \in S : |\mu_i| \in [0.75, 0.7817)\} \ ,$$

for which we automatically obtain that $\left\|\hat{f}_i\right\|_{\mathrm{L}^4} \leq K(0.7817)$. We observe that

$$\prod_{i \in C} H(|\mu_i|) \leq (H(0.75))^{|C|} \leq \left(\frac{2}{\pi}\right)^{\frac{|C|}{3}} \quad .$$

We now define our fourth set,

$$D = \{i \in S : |\mu_i| \in [2/\pi, 0.75)\} \ ,$$

which are the functions with $\left\|\hat{f}_i\right\|_{\mathrm{L}^4} \leq K(0)$, but $i \notin G$. Finally, we have that

$$\prod_{i \in E} H(|\mu_i|) \leq \left(H\left(\frac{2}{\pi}\right)\right)^{|D|} \leq \left(\frac{2}{\pi}\right)^{0.1238|D|} \quad .$$

In the following proof, we will begin by arguing that if $|A \cup B \cup C \cup D|$ is large, then Lemma 5 gives us our result immediately. Then when $|A \cup B \cup C \cup D|$ is small, we may find a large enough set G to apply Lemma 4 and obtain our bound in this way.

Proof (Proof of Theorem 3). As $a < t/4$, it follows that $t - a > 3a$. Let our sets A, B, C, and D be defined as above. If $|A \cup B \cup C \cup D| > 3an$, we will remove elements from them until they are of size $3an$. Then notice that by Lemma 5,

$$\left|\hat{f}(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{tn-an+0.555|A|+0.4|B|+\frac{|C|}{3}+0.1238|D|} .$$

It follows that if $0.555\,|A|+0.4\,|B|+\frac{|C|}{3}+0.1238\,|D| \geq 0.34an$, then we are done. We will assume then that

$$0.555\,|A| + 0.4\,|B| + \frac{|C|}{3} + 0.1238\,|D| \leq 0.34an\,, \tag{15}$$

Notice that for every $i \notin A \cup B \cup C \cup D$, $|\mu_i| \leq 2/\pi$. We want to construct a set G and a set T with $|T| = 4an$ and $G = 3(|A| + |B|$ so that $G, A, B, C, D \subseteq T$ in order to apply Lemma 4. We get this if we can obtain the bound that

$$3(|A| + |B|) \leq 4an - (|A| + |B| + |C| + |D|)\,. \tag{16}$$

We will begin by noticing that, by (15),

$$0.1238(|C| + |D|) \leq \frac{|C|}{3} + 0.1238\,|D| \leq \\ 0.34an - 0.555\,|A| - 0.4\,|B| \leq 0.34an - 0.4\,(|A| + |B|)\ .$$

It follows that

$$|C| + |D| \leq \frac{0.34}{0.1238}an - \frac{0.4}{0.1238}\,(|A| + |B|)\ .$$

We now examine the right-hand side of (16), and see that

$$\begin{aligned} 4an - |A| - |B| - |C| - |D| &\geq 4an - |A| - |B| - \frac{0.34}{0.1238}an + \frac{0.4}{0.1238}(|A| + |B|) \\ &\geq 1.25an + 2.232(|A| + |B|)\,. \end{aligned}$$

Then (16) holds if

$$3(|A| + |B|) \leq 1.25an + 2.232(|A| + |B|)\,.$$

By moving over the $2.232(|A| + |B|)$ term and rounding aggressively, it suffices to prove that

$$|A| + |B| \leq an\,.$$

We immediately have this, as (15) gives that

$$0.555\,|A| + 0.4\,|B| \leq 0.34an\,,$$

and so we conclude that

$$3(|A| + |B|) \leq 4an - |A| - |B| - |C| - |D|\ .$$

Then let T be any set of size $4an$ with $A, B, C, D \subset T \subset S$. Let $G \subset T$ with $G \cap (A \cup B \cup C \cup D) = \emptyset$ and $|G| = 3(|A| + |B|)$. We let $B_1 = A$ and $B_2 = B$. Then we may apply Lemma 4 to obtain the bound

$$\left|\hat{f}_S(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{(t-3a)n} (K(0))^{4an-|B|-|C|} \cdot (K(0.7818))^{|B|+|C|} .$$

It is clear that this bound is decreasing in $|B| + |C|$, but as we have from (15) that

$$|B| + |C| \leq 1.02an \,,$$

it follows that

$$\left|\hat{f}_S(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{t-3a} (K(0))^{2.98an} \cdot (K(0.7818))^{1.02an} .$$

From here, approximating $K(0)$ and $K(0.7818)$ gives that

$$\left|\hat{f}_S(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{(t-3a)n} \cdot \left(\frac{2}{\pi}\right)^{2.35an} ,$$

which suffices for our bound.

Remark 1. This argument was run for $q = 4$, but it could plausibly be run for higher choices of q. It is worthwhile to note though, that

$$L_q(0) \geq \frac{2}{\pi} \cdot 2^{1/q} \tag{17}$$

for each q. Any application of Hölder along the lines of this argument will give

$$\left|\hat{f}_S(\ell_0)\right| \leq \prod_{i \in A} \left\|\hat{f}_i\right\|_{\mathrm{L}^q} \cdot \prod_{i \in B} \left\|\hat{f}_i\right\|_{\mathrm{L}^\infty} \tag{18}$$

where $|A| = qan$ and $|B| = (t + a - qa)n$. So, even with a successful induction argument, one should not expect these techniques to give bounds better than

$$\left|\hat{f}_S(\ell_0)\right| \leq 2^{an} \cdot \left(\frac{2}{\pi}\right)^{(t+a)n} \leq \left(\frac{2}{\pi}\right)^{(t-0.53a)n} . \tag{19}$$

4 A Bound via Subset Averaging

Theorem 4. *For each $0 \leq a \leq t/4$, and for every choice of K satisfying $a \leq K \leq t/2 - a$, the following bound holds.*

$$\sum_{|S|=(t+a)n} \left|\widehat{f_S}(\ell_0)\right|^2 \leq O\left(\binom{(t+a)n}{(t-K)n}^{-1} \cdot \binom{n}{(t-K)n} \cdot \left(\frac{2}{\pi}\right)^{2n(t-K-3a)} \right) .$$

Proof (Proof of Theorem 4).
Let $0 \leq a \leq 1-t$ such that $an \in \mathbb{N}$. We aim to give a bound on the size of

$$\sum_{|S|=n(t+a)} \left|\hat{f}_S\left(\ell_0\right)\right|^2 .$$

We start by choosing a parameter $K = K(a,t)$ which fulfills

$$a \leq K \leq t/2 - a .$$

We further require that $Kn \in \mathbb{N}$. Fix an $S' \subset [n]$ such that $|S'| = (t-K)n$. Next, select an $\tilde{S} \subseteq S'$ such that $\left|\tilde{S}\right| = (K+2a)n$. Finally, let $T \subset [n]$ be an arbitrary set such that $|T| = (K+a)n$ and $T \cap S' = \emptyset$.

Remark 2. In this argument, we will let $\tilde{S}$ be an arbitrary subset of S' of size $(K+2a)n$; however, we leave the choice of $\tilde{S}$ available in the argument in case others can find a way to exploit it.

Definition 2. *Let $\varphi \in \mathbb{F}_p^{S' \cup T}$. We say that (T, φ) is a* ***valid pair*** *if it satisfies*

$$\ell_0 = \sum_{i \in S'} \varphi_i \cdot \ell_i + \sum_{k \in T} \varphi_k \cdot \ell_k . \tag{20}$$

To clarify our notation, we consider $\mathbb{F}_p^{S' \cup T}$ to the space of $|S' \cup T|$-dimensional vectors with values in $\mathbb{F}_p$ and entries indexed by $S' \cup T$.
We next define $\lambda(T)$ to be a choice of vector such that $(T, \lambda(T))$ is a valid pair and

$$\prod_{i \in \tilde{S}} \left|\widehat{f_i}(\lambda_i(T))\right|$$

is maximized.
Let $\theta \in \mathbb{F}_p^{\tilde{S}}$ and define C_θ as the set of all valid pairs $(T, \lambda(T))$ such that $\forall i \in \tilde{S}$, $\lambda_i(T) = \theta_i$. Choose two valid pairs $(T, \lambda(T)), (T', \lambda(T')) \in C_\theta$. Notice that since each is a valid pair, we can subtract the two equations given by (20), to obtain

$$0 = \left(\sum_{k \in S' \backslash \tilde{S}} (\lambda_k(T) - \lambda_k(T')) \cdot \ell_k\right) + \left(\sum_{i \in T} \lambda_i(T) \cdot \ell_i\right) + \left(\sum_{j \in T'} \lambda_j(T') \cdot \ell_j\right) .$$

Then 0 is expressed as the sum of some vectors. We notice that the number of distinct vectors is at most

$$|T| + |T'| + \left|S' \backslash \tilde{S}\right| = n(K+a) + n(K+a) + n(t-K) - n(K+2a) = nt$$

vectors. But as any tn vectors are linearly independent, it follows that either $(T, \lambda(T)) = (T', \lambda(T'))$ or $\lambda(T')_i = 0$ for all $i \in (S' \backslash \tilde{S}) \cup T$. The second option would imply that

$$\ell_0 = \sum_{i \in \tilde{S}} \theta_i \cdot \ell_i ,$$

which cannot happen as $\tilde{S}$ contains less than tn vectors. Then we conclude that $|C_\theta| \leq 1$.

Lemma 6. *For fixed S', $\tilde{S}$, and T, where $|T| \geq 2an$, we have that*

$$\left|\widehat{f}_{S'\cup T}\right| \leq O\left(\prod_{i\in\tilde{S}}\left|\widehat{f}_i\left(\lambda_i(T)\right)\right| \cdot \left(\frac{2}{\pi}\right)^{n(t-K-3a)}\right). \tag{21}$$

This Lemma uses an argument modified from that of Lemma 4.2 in [12]. The reader may find our proof in Appendix A.
We may reindex our summation so that

$$\sum_T \left|\widehat{f}_{S'\cup T}(\ell_0)\right|^2 = \sum_{\theta\in\mathbb{F}_p^{\tilde{S}}}\left(\sum_{T\in C_\theta}\left|\widehat{f}_{S'\cup T}(\ell_0)\right|^2\right).$$

Applying Lemma 6, it follows that

$$\sum_T \left|\widehat{f}_{S'\cup T}(\ell_0)\right|^2 \leq \sum_{\theta\in\mathbb{F}_p^{\tilde{S}}}\left(\sum_{T\in C_\theta} O\left(\prod_{i\in\tilde{S}}\left|\widehat{f}_i\left(\lambda_i(T)\right)\right|^2 \cdot \left(\frac{2}{\pi}\right)^{2n(t-K-3a)}\right)\right).$$

As each C_θ contains at most one element, we may rewrite this bound as

$$\sum_T \left|\widehat{f}_{S'\cup T}(\ell_0)\right|^2 = O\left(\left(\frac{2}{\pi}\right)^{2n(t-K-3a)} \cdot \sum_{\theta\in\mathbb{F}_p^{\tilde{S}}}\left(\prod_{i\in\tilde{S}}\left|\widehat{f}_i\left(\theta_i\right)\right|^2\right)\right).$$

We may re-order our sum in θ again so that

$$\prod_{i\in\tilde{S}}\left|\widehat{f}_i\left(\theta_i\right)\right|^2 = \prod_{i\in\tilde{S}}\sum_{k\in\mathbb{F}_p}\left|\hat{f}_i(k\right|^2 = \prod_{i\in\tilde{s}}\left\|\hat{f}_i\right\|_{\mathrm{L}^2}.$$

By Plancherel,

$$\sum_T \left|\widehat{f}_{S'\cup T}(\ell_0)\right|^2 = O\left(\left(\frac{2}{\pi}\right)^{2n(t-K-3a)}\right).$$

Notice that we may represent any $|S| = (t+a)n$ as $S' \cup T$ in $\binom{(t+a)n}{(t-k)n}$ different ways. Then

$$\sum_{|S|=(t+a)n}\left|\widehat{f}_S(\ell_0)\right|^2 = \binom{(t+a)n}{(t-k)n}^{-1} \cdot \sum_{|S'|=(t-k)n}\ \sum_{|T|=(k+a)n}\left|\widehat{f}_{S'\cup T}(\ell_0)\right|^2.$$

Using our previous bounds, we see that

$$\sum_{|S|=(t+a)n}\left|\widehat{f}_S(\ell_0)\right|^2 \leq O\left(\binom{(t+a)n}{(t-k)n}^{-1} \cdot \sum_{|S'|=(t-k)n}\left(\frac{2}{\pi}\right)^{2n(t-k-3a)}\right).$$

Counting our choices of S', we finally obtain that

$$\sum_{|S|=(t+a)n}\left|\widehat{f}_S(\ell_0)\right|^2 \leq O\left(\binom{(t+a)n}{(t-k)n}^{-1} \cdot \binom{n}{(t-k)n} \cdot \left(\frac{2}{\pi}\right)^{2n(t-k-3a)}\right).$$

5 Convergence when $t \geq 0.67$

What remains is to show that the results come together to give our promised result. We'll begin by examining the range of a over which our averaging argument, Theorem 4, gives decay. Recall that it says that, taking $K = a$,

$$\sum_{|S|=(t+a)n} \left|\widehat{f}_S(\ell_0)\right|^2 \leq \binom{(t+a)n}{(t-a)n}^{-1} \cdot \binom{n}{(t-a)n} \cdot \left(\frac{2}{\pi}\right)^{2(t-4a)n} .$$

Using Stirling's Approximation, we may rewrite this as, for n large,

$$\sum_{|S|=t+a} \left|\widehat{f}_S(\ell_0)\right|^2 \leq 2 \cdot \frac{\sqrt{4\pi an}(2an)^{2an} \cdot \sqrt{2\pi(t-a)n}((t-a)n)^{(t-a)n}}{\sqrt{2\pi(t+a)n}\,(n(t+a))^{n(t+a)}}$$
$$\cdot \frac{\sqrt{2\pi n}n^n}{\sqrt{2\pi(t-a)n}((t-a)n)^{(t-a)n} \cdot \sqrt{2\pi(n-nt+na)}(n-nt+na)^{n-nt+na}}$$
$$\cdot \left(\frac{2}{\pi}\right)^{2(t-4a)n} .$$

Simplifying, this reduces to

$$\sum_{|S|=t+a} \left|\widehat{f}_S(\ell_0)\right|^2 \leq 2\sqrt{\frac{2a}{(t+a)(1-t+a)}}$$
$$\cdot \left(\frac{(2a)^{2a}}{(t+a)^{t+a} \cdot (1-t+a)^{1-t+a}} \cdot \left(\frac{2}{\pi}\right)^{2(t-4a)}\right)^n .$$

Then it suffices to examine when

$$E_1(t,a) = \frac{(2a)^{2a}}{(t+a)^{t+a} \cdot (1-t+a)^{1-t+a}} \cdot \left(\frac{2}{\pi}\right)^{2(t-4a)} < 1 . \tag{22}$$

Here we may plug in $t = 0.668$ from Theorem 1, and we see that (22) reaches 1 at approximately $a = 0.0054$ and $a = 0.0991$, and so we gain exponential decay for $x \in (0.0054, 0.0991)$. Applying logarithms and differentiating, we find that (22) is decreasing in t if

$$\frac{1-t+a}{t+a} \cdot \frac{4}{\pi^2} < 1 , \tag{23}$$

which holds for $t > 0.668$ as $1 - t + a < t + a$ for such values.
To cover the gap where $a \leq 0.0054$, we repeat this process with $K = t/2 - a$, so that

$$\sum_{|S|=(t+a)n} \left|\widehat{f}_S(\ell_0)\right|^2 \leq \binom{(t+a)n}{(t/2+a)n}^{-1} \cdot \binom{n}{(t/2+a)} \cdot \left(\frac{2}{\pi}\right)^{2(t/2-2a)n} ,$$

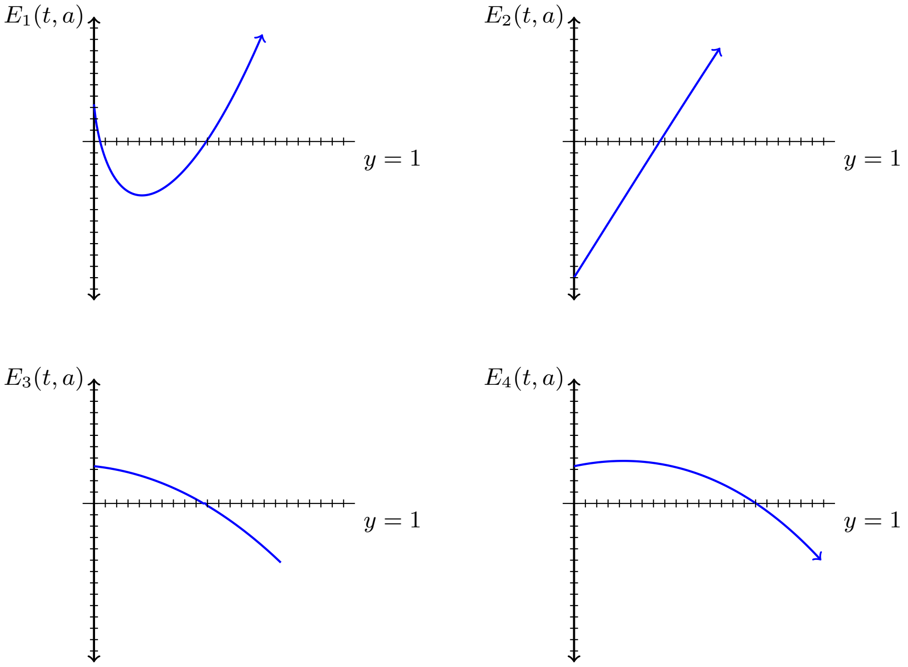


Fig. 4: Truncated graphs of each of the estimation functions E_i with $t = 0.688$. Each tick represents a length of 0.01. Except for E_3, which ends its domain at $a = t/4$, the other functions have extended domains that are truncated here for space. Rather than the a-axis, the line is drawn at $y = 1$, to make it clear when the E_i cross the threshold.

and so by Stirling's Approximation, it suffices to examine when

$$E_2(t,a) = \frac{(t/2)^{(t/2)}}{(t+a)^{t+a} \cdot (1-t/2-a)^{1-t/2-a}} \cdot \left(\frac{2}{\pi}\right)^{2(t/2-2a)} < 1.$$

Once again taking $t = 0.668$, we compute that the value is 0.8801 when $a = 0$, and the next time that it reaches 1 when $a = 0.07557$. Similarly applying logarithms and differentiating one may see that this is decreasing in t at fixed values of a.

We now may examine the efficacy of Theorem 3. This gives us that

$$\sum_{|S|=(t+a)n} \left|\widehat{f_S}(\ell_0)\right|^2 \le \binom{n}{(t+a)n} \cdot \left(\frac{2}{\pi}\right)^{(t-0.66a)2n}$$

Once again, we may apply Stirling's Approximation, and it suffices to examine when

$$E_3(t,a) = \frac{1}{(t+a)^{t+a} \cdot (1-t-a)^{1-t-a}} \left(\frac{2}{\pi}\right)^{2(t-0.66a)} < 1\,,$$

and taking $t = 0.668$, we see that it holds when $a > 0.0936$. However, as our theorem requires that $a < t/4$, this only applies when $a < 0.167$. Once again, one may take logarithms and differentiate to show that this bound decreases in t.

We will finally apply the bound from [12], that

$$\sum_{|S|=(t+a)n} \left|\widehat{f_S}(\ell_0)\right|^2 \le \binom{n}{(t+a)n} \cdot \left(\frac{2}{\pi}\right)^{(t-a)2n}\,.$$

By Stirling's approximation, we may instead examine when

$$E_4(t,a) = \frac{1}{(t+a)^{t+a} \cdot (1-t-a)^{1-t-a}} \left(\frac{2}{\pi}\right)^{2(t-a)} < 1\,.$$

This holds when $a > 0.1604$, Applying logarithms and derivatives, we see that these are decreasing in t for fixed a as well, and so our result holds, as we have covered all values of $0 \le a < 1-t$ for $t \ge 0.668$.

6 Discussion

In a 2019 paper [1], Balister et al proved a result implies the existence of functions $f_i : \mathbb{F}_p \to \{-1,1\}$ so that for each $k \in \mathbb{F}_p$, $\left|\hat{f_i}(k)\right| \ge \delta/\sqrt{p}$, for p sufficiently large and some small fixed $\delta > 0$. This unfortunately means that one should not expect purely functional-analytic methods to work when $t \le 1/2$, as the triangle inequality used one the convolution behaves as we highlight below. Recall that, for $|S| = n$,

$$\left|\hat{f_S}(\ell_0)\right| \le \sum_{\substack{\lambda_1,\ldots\lambda_n \\ \sum_{i=1}^n \lambda_i \ell_i = \ell_0}} \prod_{i=1}^{n} \left|f_i\hat{(}\lambda_i\right| \qquad (24)$$

is an inequality that is taken in obtaining our bounds. But for functions as generated by [1], and using our argument that $n - tn$ of the ℓ_i determine the convolution,

$$\sum_{\substack{\lambda_1,\dots\lambda_n \\ \sum_{i=1}^n \lambda_i\ell_i=\ell_0}} \prod_{i=1}^n \left|f_i\hat{(}\lambda_i\right| \geq \sum_{\substack{\lambda_1,\dots\lambda_n \\ \sum_{i=1}^n \lambda_i\ell_i=\ell_0}} \prod_{i=1}^n \frac{\delta}{\sqrt{p}} = p^{n-tn} \cdot \frac{\delta^n}{p^{n/2}} = p^{n/2-tn}\delta^n \,. \tag{25}$$

Then if $tn < n/2$, clearly the sum after taking the triangle inequality is large. We would like to note that this does not necessarily mean that the analytic proxy fails in these cases, or that functional analytic techniques are useless, only that some additional argument that does not use these techniques will be necessary to handle functions that have this lower bound on their Fourier transforms.

We'll now attempt a more direct commentary on generalizing the techniques presented here. We suspect that one cannot push the bounds in Section 2 and Section 3 much further; as we remarked, the bounds on $\|f_i\|_{\mathrm{L}^q}$ can't do better than $2^{1/q} \cdot 2/\pi$. That said, these results may be useful for others, or in cases where a functional-analytic bound is useful after some additional cancellation argument has been made. We are hopeful that if an improved bound on $\left|\hat{f_S}(\ell_0\right|$ is found, then the argument made in Section 4 may be adapted to that setting. Most of the properties of the bound in [12] are not used directly, so it may be possible to use this argument to boost other bounds in future papers.

Acknowledgements

Thank you to Dr Simkin for introducing me to this problem. An additional thank you to Dr Magyar, Dr. Petridis, and Ms LaRue for helping refine the proof and writing. Thank you for the thoughtful comments of the reviewers to help improve this paper. This material is based upon work supported by the National Science Foundation under Grant No. 2054214.

7 Appendix A

We will re-state Lemma 6 in slightly more general terms here that will be easier to remember throughout this proof. We begin by defining the set V, which we will use throughout this proof.

Definition 3. *Let V be the set of all $\varphi \in \mathbb{F}_p^{(t+a)n}$ such that*

$$\ell_0 = \sum_{i=1}^{(t+a)n} \varphi_i \cdot \ell_i \,. \tag{26}$$

Lemma 7. *For each $S \subset [n]$, $|S| = (t+a)n$ for $0 \le t \le 1$ and $0 \le a \le t$, let $B \subseteq S$ where $|B| = (t-a)n$ and let $A \subseteq B$. Then*

$$\left|\widehat{f_{S'\cup T}}(\ell_0)\right| \le O\left(\left(\sup_{\varphi\in V}\prod_{i\in B\setminus A}\left|\hat{f}_i(\varphi_i\right|\right)\left(\frac{2}{\pi}\right)^{|A|}\right)$$

We define $\pi_1(\varphi) : \mathbb{F}_p^{tn+an} \to \mathbb{F}_p^{tn}$ as

$$\pi_1(\varphi) = \sum_{i=1}^{an} \varphi_i \ell_i \,.$$

Similarly, we define

$$\pi_2(\varphi) = \sum_{i=tn+1}^{tn+an} \varphi_i \ell_i$$

and

$$\pi_3(\varphi) = \sum_{i=an+1}^{tn} \varphi_i \ell_i \,.$$

We can now state and prove a variant of Lemma 4.3 from [12], page 17.

Lemma 8. *Let $0 < t \le 1$, $nt \in \mathbb{N}$, $0 \le a \le 1-t$, and $\{\ell_i\}_{i=0}^{(t+a)n}$ be vectors in $\mathbb{F}_p^{tn}$ such that every tn of them are linearly independent. Let $A, B : \mathbb{F}_p^{an} \to \{-1, 1\}$ and $C : \mathbb{F}_p^{(t-a)n} \to \{-1, 1\}$ be any functions. We write*

$$F(x) = A(\ell_1 \cdot x, ..., \ell_{an} \cdot x) \cdot C(\ell_{an+1} \cdot x, ..., \ell_{tn} \cdot x) \cdot B(\ell_{tn+1} \cdot x, ..., \ell_{(t+a)n} \cdot x) \,. \tag{27}$$

Then

$$\left|\widehat{F}(\ell_0)\right| \le \|A\|_{L^2} \cdot \|B\|_{L^2} \cdot \sup_{\varphi\in V}\left|\widehat{C}(\pi_3(\varphi))\right| \tag{28}$$

Proof. We write $A'(x)$, $B'(x)$, and $C'(x)$ to suppress the use of the ℓ_i such that $F(x) = A'(x) \cdot B'(x) \cdot C'(x)$. As the Fourier transformation of a product is a convolution of Fourier transformations, we may write

$$\widehat{F}(\ell_0) = \left(\widehat{A' \cdot B' \cdot C'}\right)(\ell_0) = \sum_{\beta+\gamma+\delta=\ell_0} \widehat{A'}(\beta)\widehat{B'}(\gamma)\widehat{C'}(\delta) \tag{29}$$

We claim that we may rewrite this again to have that

$$\hat{F}(\ell_0) = \sum_{\varphi \in V} \widehat{A'}(\pi_1(\varphi))\widehat{B'}(\pi_2(\varphi))\widehat{C'}(\pi_3(\varphi)) \,. \tag{30}$$

To prove this, consider $\hat{A}'(\beta)$ for some β linearly independent of $\{\ell_i\}_{i=1}^{an}$. Then choose some vector ℓ^* that is orthogonal to the ℓ_i so that for some k_i, k^*,

$$\beta = k^*\ell^* + \sum_{i=1}^{an} k_i \ell_i \,.$$

Let $\perp \ell^*$ be the set of vectors in $\mathbb{F}_p^{tn}$ perpendicular to ℓ^*. Recall that

$$\hat{A}'(\beta) = \frac{1}{p^t} \sum_{x \in \perp \ell^*} \sum_{k \in \mathbb{F}_p} A'(x + k\ell^*) e^{\frac{2\pi i}{p}(x+k\ell^*)\cdot\beta}$$

Since each $\ell_i \cdot \ell^* = 0$, it follows that

$$\hat{A}'(\beta) = \frac{1}{p^t} \sum_{x \in \perp \ell^*} A'(x) \sum_{k \in \mathbb{F}_p} e^{\frac{2\pi i}{p}(x+k\ell^*)\cdot\beta} = 0 \,.$$

Therefore, we will only sum over precisely those β such that $\beta = \pi_1(\varphi)$, $\varphi \in \mathbb{F}_p^{tn+an}$. We may do an identical argument for B' and C'. Then for such a φ, it is necessary that $\pi_1(\varphi) + \pi_2(\varphi) + \pi_3(\varphi) = \ell_0$, and so $\varphi \in V$, which proves our claim.
Then we may write that

$$\left|\widehat{F}(\ell_0)\right| \leq \sup_{\varphi \in V} \left|\widehat{C'}(\pi_3(\varphi))\right| \cdot \sum_{\varphi \in V} \left|\widehat{A'}(\pi_1(\varphi))\widehat{B'}(\pi_2(\varphi))\right| \,.$$

If we fix $\pi_1(\varphi)$, notice that

$$\ell_0 - \sum_{i=1}^{an} \varphi_i \ell_i = \sum_{i=an+1}^{an+tn} \varphi_i \ell_i \,.$$

There are exactly tn vectors on the right-hand side of the equation, and thus we conclude that $\pi_2(\varphi)$ and $\pi_3(\varphi)$ are determined by $\pi_1(\varphi)$ when $\varphi \in V$. Then if W is the span of $\{\ell_i\}_{i=1}^{an}$, we may define $\pi_1^{-1} : W \to V$ in the natural way. Thus,

$$\left|\widehat{F}(\ell_0)\right| \leq \sup_{\varphi \in V} \left|\widehat{C'}(\pi_3(\varphi))\right| \cdot \sum_{\phi \in W} \left|\widehat{A'}(\phi)\widehat{B'}(\pi_2\left(\pi_1^{-1}(\phi)\right))\right| \,.$$

It follows that our previous logic that $\pi_2\left(\pi_1^{-1}(\phi)\right)$ is a bijection onto the span of ℓ_i for $i \in [tn+1, tn+an]$, and so we may apply Cauchy-Schwartz and Plancherel to obtain our result.

We now begin by stating an analogue of Corollary 4.4 from page 17 of [12].

Corollary 1. *Let $B \subset S$ with $|B| = (t-a)n$. Then*

$$|f_S(\ell_0)| \leq \sup_{\varphi \in V} \left(\prod_{i \in B} \left\| \widehat{f_i} \right\|_{L^\infty} \right) . \tag{31}$$

Proof. Choose two sets, T_1, T_2 with $|T_1| = |T_2| = an$ and $T_1 \sqcup T_2 \sqcup B = S$. Then we define

$$A' = \prod_{i \in T_1} f_i(\ell_i \cdot x) \tag{32}$$

$$B' = \prod_{i \in T_2} f_i(\ell_i \cdot x) \tag{33}$$

$$C' = \prod_{i \in B} f_i(\ell_i \cdot x) \, . \tag{34}$$

We can apply Lemma 8 in the natural way to, we have that

$$\left| \widehat{f_S}(\ell_0) \right| \leq \left(\prod_{i \in T_1} \left\| \widehat{f_j} \right\|_{\mathrm{L}^2} \right) \cdot \left(\prod_{j \in T_2} \left\| \widehat{f_j} \right\|_{\mathrm{L}^2} \right) \cdot \left(\sup_{\varphi \in V} \prod_{B} \left| \widehat{f_i}(\varphi_i) \right| \right) \tag{35}$$

As each f_i maps to either 1 or -1, it follows that for all i, $\left\| \hat{f}_i \right\|_{\mathrm{L}^2} = 1$

Before proceeding with our proof of Lemma 6, we recall Claim 4.5 from [12], which we will use directly.

Lemma 9. *Let $f : \mathbb{F}_p \to [-1, 1]$ be a function with $\mathbb{E}[f] = \mu$. Then for all $k \neq 0$ we have*

$$\left| \widehat{f}(k) \right| \leq \frac{2}{\pi} \cos\left(\frac{\pi}{2} \mu \right) + O(1/p^2) \, . \tag{36}$$

Proof (Proof of Lemma 7). Notice that if $B = S' \cup T'$ and $A = (S' \cup T') \backslash \tilde{S}$, our statement implies Lemma 6.
We will follow with the convention in [12] by suppressing the extra $O(1/p^2)$ term that comes from Lemma 9.
Let $|S| = tn + an$. Note that the bound trivially holds when $an < 0$, as $\hat{f}_S(\ell_0) = 0$. Then we will begin by inducting on an for $an \geq 0$. By Corollary 1, the bound holds whenever $|A| = 0$, so we will also induct on $|A|$, assuming that the bound holds for all $|A'| < |A|$.
We will begin by selecting an arbitrary index $I \in A$. Notice that if $\left\| \widehat{f_I} \right\|_{\mathrm{L}^\infty} \leq \frac{2}{\pi} + O(1/p^2)$, then we apply the induction hypothesis on $A \backslash \{I\}$ so that

$$\left| \widehat{f_S}(\ell_0) \right| \leq \left(\frac{2}{\pi} \right)^{|A|-1} \cdot \sup_{\varphi \in V} \left(\prod_{i \in B \backslash (A \backslash \{I\})} \left| \widehat{f_i}(\varphi_i) \right| \right) . \tag{37}$$

We may extract a term of $\left\|\hat{f}_I\right\|_{\mathrm{L}^\infty}$ from the second term in the product, and this gives us the extra factor of $2/\pi$ that we need to conclude the proof.

Then consider the case when $\left\|\widehat{f_I}\right\|_{\mathrm{L}^\infty} \geq 2/\pi$; if this is the case, then $|\mathbb{E}[f_i]| = |\mu_i| \geq 2/\pi$, as Lemma 9 tells us that the largest value of $\widehat{f_I}$ away from 0 cannot be larger that $2/\pi$. We will now define the balance function $g = f_I - \mu$. Applying Lemma 9 to f_I, along with the fact that $\widehat{\mu}(k) = 0$ for $k \neq 0$, it follows that $\|g\|_{\mathrm{L}^\infty} \leq 2/\pi \cos(\pi\mu/2)$.

Notice that we may write

$$\widehat{f_S}(\ell_0) = \mu \cdot \widehat{f}_{S\setminus\{I\}}(\ell_0) + \widehat{\left(g \cdot f_{S\setminus\{I\}}\right)}(\ell_0) \tag{38}$$

We will bound the two terms in Equation (38) separately using the induction hypothesis, and this will give us our result.

To bound $\mu \cdot \widehat{f}_{S\setminus\{I\}}(\ell_0)$, we begin by noticing that if $an - 1 < 0$, we are done, as $\widehat{f}_{S\setminus\{I\}}(\ell_0) = 0$ in that case. We assume then that $an > 0$.

Choose two indices $J, K \in S\setminus B$. We define the sets $A' = (A\setminus\{I\}) \cup \{J, K\}$, $B' = (B\setminus\{I\}) \cup \{J, K\}$, and $S' = S\setminus\{I\}$. We may apply the induction hypothesis for $|S'| = tn + an - 1$ to see that

$$\left|\mu \cdot \widehat{f}_{S\setminus\{I\}}(\ell_0)\right| \leq |\mu| \cdot \left(\frac{2}{\pi}\right)^{|A'|} \cdot \sup_{\varphi\in V}\left(\prod_{i\in B'\setminus A'}\left|\widehat{f_i}(\varphi_i)\right|\right). \tag{39}$$

First notice that $B'\setminus A' = B\setminus A$. Further, we may compute that $|A'| = |A| + 1$, and so

$$\left|\mu \cdot \widehat{f}_{S\setminus\{I\}}(\ell_0)\right| \leq |\mu| \cdot \left(\frac{2}{\pi}\right)^{|A|+1} \cdot \sup_{\varphi\in V}\left(\prod_{i\in B\setminus A}\left|\widehat{f_i}(\varphi_i)\right|\right). \tag{40}$$

Bounding the second term of (38) is simpler, as we will simply choose $A' = A\setminus\{I\}$ and apply the induction hypothesis for $|A| - 1$ to see that

$$\left|\widehat{\left(g \cdot f_{S\setminus\{I\}}\right)}(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{|A'|} \cdot \sup_{\varphi\in V}\left(|\hat{g}(\varphi_I)| \cdot \prod_{i\in B\setminus A}\left|\widehat{f_i}(\varphi_i)\right|\right). \tag{41}$$

We now apply that $\|\hat{g}\|_{\mathrm{L}^\infty} \leq 2/\pi \cos(\pi/2\mu)$ to say that

$$\left|\widehat{\left(g \cdot f_{S\setminus\{I\}}\right)}(\ell_0)\right| \leq \left(\frac{2}{\pi}\right)^{|A|-1} \cdot \left|\frac{2}{\pi}\cos\left(\frac{\pi}{2}\mu\right)\right| \cdot \sup_{\varphi\in V}\left(\prod_{i\in B\setminus A}\left|\widehat{f_i}(\varphi_i)\right|\right). \tag{42}$$

Then it suffices to show that

$$|\mu| \cdot \left(\frac{2}{\pi}\right)^{|A|+1} \cdot \sup_{\varphi \in V} \left(\prod_{i \in B \setminus A} \left| \widehat{f_i}(\varphi_i) \right| \right) + \left(\frac{2}{\pi}\right)^{|A|-1} \cdot \left| \frac{2}{\pi} \cos\left(\frac{\pi}{2}\mu\right) \right| \cdot \sup_{\varphi \in V} \left(\prod_{i \in B \setminus A} \left| \widehat{f_i}(\varphi_i) \right| \right) \leq \left(\frac{2}{\pi}\right)^{|A|} \cdot \sup_{\varphi \in V} \left(\prod_{i \in B \setminus A} \left| \widehat{f_i}(\varphi_i) \right| \right) . \tag{43}$$

We may divide through by the common terms, and so it is sufficient to show that

$$\frac{2}{\pi} |\mu| + cos\left(\frac{\pi}{2}\mu\right) \leq 1 . \tag{44}$$

As we are working under the restriction that $2/\pi \leq |\mu| \leq 1$, this holds for all $|\mu|$ in the range, concluding our proof.

8 Appendix B

In this Appendix we will briefly state our definitions of the Fourier transform, as well as some standard results on them.
We define the characters of the group $\mathbb{F}_p$ as $\chi_k : \mathbb{F}_p \to \mathbb{C}$ as

$$\chi_k(x) = e^{-\frac{2\pi i}{p} kx}$$

and the characters of $\mathbb{F}_p^{tn}$, $\chi_\varphi : \mathbb{F}_p^t \to \mathbb{C}$, as

$$\chi_\varphi(x) = e^{\frac{2\pi i}{p} \phi \cdot x} \tag{45}$$

Then for $f : \mathbb{F}_p \to \mathbb{C}$, $k \in \mathbb{F}_p$, we define

$$\hat{f}(k) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} f(x) \chi_k(x) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} f(x) e^{\frac{2\pi i}{p} k \cdot x}$$

and for $g \in \mathbb{F}_p^{tn}$, $\varphi \in \mathbb{F}_p^{tn}$,

$$\hat{g}(\varphi) = \frac{1}{p^{tn}} \sum_{x \in \mathbb{F}_p} g(x) \chi_\varphi(x) = \frac{1}{p^{tn}} \sum_{x \in \mathbb{F}_p} g(x) e^{\frac{2\pi i}{p} \varphi \cdot x} .$$

One of the Fourier-analytic theorems that we use in this paper are Plancherel's theorem, which states that, for $f_i : \mathbb{F}_p \to \mathbb{C}$,

$$\|f_i\|_{\mathrm{L}^2} = p \left\| \hat{f}_i \right\|_{\mathrm{L}^2} ,$$

and similarly for $g_i : \mathbb{F}_p^{tn} \to \mathbb{C}$, we have that $\|g_i\|_{\mathrm{L}^2} = p^{tn}\,\|\hat{g}_i\|_{\mathrm{L}^2}$. We also use the fact that for two functions $f, g : \mathbb{F}_p \to \mathbb{C}$,

$$\widehat{fg}(\varphi) = \sum_{\alpha+\beta=\varphi} \hat{f}(\alpha) \cdot \hat{g}(\beta) = (\hat{f} * \hat{g})(\varphi)\,.$$

We also will take the time here to formally define leakage resilience. We begin by defining the function $leak : \mathbb{F}_p^{tn} \to \mathbb{F}_p^n$ as $leak(x) = (f_1(\ell_1 \cdot x), ..., f_n(\ell_n \cdot x))$, representing the leaked bits that the adversary sees. Then the adversary can expect that one secret s is more likely than another s', given a fixed $leak(x) = A$, if

$$|P\left(leak(x) = A|\ell_0 \cdot x = s\right) - P\left(leak(x) = A|\ell_0 \cdot x = s'\right)|$$

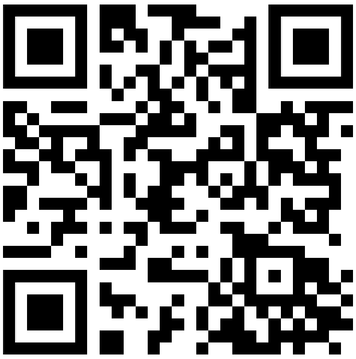
is large. Here we use probability and conditional probability in the standard ways. We say that the scheme is leakage resilient if the expected amount of information gained,

$$\sum_{A \in \mathbb{F}_p^n} |P\left(leak(x) = A|\ell_0 \cdot x = s\right) - P\left(leak(x) = A|\ell_0 \cdot x = s'\right)|\ ,$$

tends to zero for each s, s' as n tends to infinity.

9 Appendix C

Desmos Link for Figure 1



Desmos Link for Figure 2

Desmos Link for Figure 3

Desmos Link for Figure 4

References

[1] Paul Balister et al. “Flat Littlewood polynomials exist”. In: *Annals of Mathematics* 192.3 (2020), pp. 977–1004. DOI: `10.4007/annals.2020.192.3.6`. URL: `https://doi.org/10.4007/annals.2020.192.3.6`.

[2] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. "Completeness theorems for non-cryptographic fault-tolerant distributed computation". In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. STOC '88. Chicago, Illinois, USA: Association for Computing Machinery, 1988, pp. 1–10. ISBN: 0897912640. DOI: 10.1145/62212.62213. URL: https://doi.org/10.1145/62212.62213.

[3] Fabrice Benhamouda et al. "On the Local Leakage Resilience of Linear Secret Sharing Schemes". In: *Journal of Cryptology* 34 (2018). URL: https://api.semanticscholar.org/CorpusID:206716311.

[4] Fabrice Benhamouda et al. "On the Local Leakage Resilience of Linear Secret Sharing Schemes". In: *Journal of Cryptology* 34.2 (Apr. 2021). Publisher Copyright: © 2021, The Author(s), under exclusive licence to International Association for Cryptologic Research. ISSN: 0933-2790. DOI: https://doi.org/10.1007/s00145-021-09375-2.

[5] David Chaum, Claude Crépeau, and Ivan Damgard. "Multiparty unconditionally secure protocols". In: *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*. STOC '88. Chicago, Illinois, USA: Association for Computing Machinery, 1988, pp. 11–19. ISBN: 0897912640. DOI: 10.1145/62212.62214. URL: https://doi.org/10.1145/62212.62214.

[6] Alfredo De Santis et al. "How to share a function securely". In: *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing*. STOC '94. Montreal, Quebec, Canada: Association for Computing Machinery, 1994, pp. 522–533. ISBN: 0897916638. DOI: 10.1145/195058.195405. URL: https://doi.org/10.1145/195058.195405.

[7] Yvo Desmedt and Yair Frankel. "Threshold cryptosystems". In: *Advances in Cryptology — CRYPTO' 89 Proceedings*. Ed. by Gilles Brassard. New York, NY: Springer New York, 1990, pp. 307–315. ISBN: 978-0-387-34805-6.

[8] Sebastian Faust et al. "Protecting Circuits from Leakage: the Computationally-Bounded and Noisy Cases". In: *Advances in Cryptology – EUROCRYPT 2010*. Ed. by Henri Gilbert. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 135–156. ISBN: 978-3-642-13190-5.

[9] Yair Frankel. "A Practical Protocol for Large Group Oriented Networks". In: *Advances in Cryptology — EUROCRYPT '89*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Berlin, Heidelberg: Springer Berlin Heidelberg, 1990, pp. 56–61. ISBN: 978-3-540-46885-1.

[10] O. Goldreich, S. Micali, and A. Wigderson. "How to play ANY mental game". In: *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*. STOC '87. New York, New York, USA: Association for Computing Machinery, 1987, pp. 218–229. ISBN: 0897912217. DOI: 10.1145/28395.28420. URL: https://doi.org/10.1145/28395.28420.

[11] Yuval Ishai, Amit Sahai, and David Wagner. "Private Circuits: Securing Hardware against Probing Attacks". In: *Advances in Cryptology - CRYPTO 2003*. Ed. by Dan Boneh. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 463–481. ISBN: 978-3-540-45146-4.

[12] Ohad Klein and Ilan Komargodski. *New Bounds on the Local Leakage Resilience of Shamir's Secret Sharing Scheme.* Cryptology ePrint Archive, Paper 2023/805. `https://eprint.iacr.org/2023/805`. 2023. URL: `https://eprint.iacr.org/2023/805`.

[13] Vsevolod F. Lev. "Linear equations over $\mathbb{F}_p$ and moments of exponential sums". In: *Duke Mathematical Journal* 107.2 (2001), pp. 239–263. DOI: `10.1215/S0012-7094-01-10722-9`. URL: `https://doi.org/10.1215/S0012-7094-01-10722-9`.

[14] Hemanta K. Maji et al. "Constructing Locally Leakage-Resilient Linear Secret-Sharing Schemes". In: *Advances in Cryptology – CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Proceedings.* Ed. by Tal Malkin and Chris Peikert. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Publisher Copyright: © 2021, International Association for Cryptologic Research.; 41st Annual International Cryptology Conference, CRYPTO 2021 ; Conference date: 16-08-2021 Through 20-08-2021. Springer Science and Business Media Deutschland GmbH, 2021, pp. 779–808. ISBN: 9783030842512. DOI: `10.1007/978-3-030-84252-9_26`.

[15] Hemanta K. Maji et al. "Improved Bound on the Local Leakage-resilience of Shamir's Secret Sharing". In: *2022 IEEE International Symposium on Information Theory (ISIT).* Espoo, Finland: IEEE Press, 2022, pp. 2678–2683. DOI: `10.1109/ISIT50566.2022.9834695`. URL: `https://doi.org/10.1109/ISIT50566.2022.9834695`.

[16] Jesper Buus Nielsen and Mark Simkin. *Lower Bounds for Leakage-Resilient Secret Sharing.* Advances in Cryptology - EUROCRYPT. `https://eprint.iacr.org/2019/181`. 2020. URL: `https://eprint.iacr.org/2019/181`.

[17] Guy N. Rothblum. "How to Compute under AC0 Leakage without Secure Hardware". In: *Advances in Cryptology – CRYPTO 2012.* Ed. by Reihaneh Safavi-Naini and Ran Canetti. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 552–569. ISBN: 978-3-642-32009-5.

[18] Adi Shamir. "How to share a secret". In: *Commun. ACM* 22.11 (Nov. 1979), pp. 612–613. ISSN: 0001-0782. DOI: `10.1145/359168.359176`. URL: `https://doi.org/10.1145/359168.359176`.