Fractional Pseudorandom Generators and Bounded Fourier Tails: A Literature Review

1 Introduction

In the evolving field of circuit complexity theory, the development of pseudorandom generators (PRGs) tailored for restricted models of computation, such as $AC^0[\oplus]$, presents both a challenging and crucial endeavor. This survey paper aims to synthesize and analyze significant recent advancements in PRG constructions that utilize polarizing random walks, as introduced in three pioneering studies. These contributions mark a departure from traditional frameworks, such as those that utilize expander-graphs or hardness vs randomness, proposing a novel approach that specifically addresses the construction of PRGs within restricted computational settings.

We begin by discussing the 2018 work of Chattopadhyay et al.[CHHL19], which introduces an innovative framework for designing PRGs based on Fourier tail bounds for Boolean functions. This framework posits that with exponential bounds uniformly applied across all levels of Boolean functions, one can effectively construct PRGs suitable for specific complexity classes. The most significant contribution of this paper is the establishment of a generic PRG construction framework from *polarizing random walks* for classes of boolean functions with bounded Fourier tails[HH23, CHHL19]. The emphasis on the semantic properties of boolean functions, that are independent of their implementations as boolean circuits, simplify the complexity involved in PRG constructions.

Subsequent research further refines this approach by developing an alternative pseudorandom generator that necessitates bounds only on the second level of the Fourier tails, rather than the entire spectrum. This method significantly simplifies the construction requirements and posits a critical conjecture regarding bounds on low-degree polynomials over the finite field $\mathbb{F}_2$. If resolved, this conjecture could efficiently address a well-known open problem in complexity theory concerning the efficiency of PRGs for the $AC^0[\oplus]$ circuit class[CHRT18]. This development underscores the targeted and refined nature of recent theoretical advancements, which aim to reduce the computational overhead of constructing effective PRGs.

Moreover, the latest results discussed in this survey exploit L_1 Fourier tail bounds to create PRGs that adjust the seed length based on specific Fourier levels. This novel approach does not require bounds on the entire tail but focuses on bounding a single Fourier coefficent[CGL^+21]. This method not only interpolates and builds upon previous works but also proposes a model that

adapts more flexibly to the requirements of different functions, showcasing a significant reduction in the complexity of PRG design.

We aim to provide a comprehensive analysis of these developments, exploring both the theoretical underpinnings and the practical implications of this new framework. By examining the collective contributions of these papers, we highlight a shift towards more practical solutions in pseudorandom generation within restricted computational models. Our discussion will not only contextualize these advancements within the broader landscape of complexity theory but also illustrate the potential pathways for future research and applications in the field. Through this survey, we hope to foster a deeper understanding and appreciation of how modern complexity theory continues to evolve, driven by innovative approaches to longstanding computational challenges. We do wish to note, however, that our survey is not an exhaustive reconstruction of the aforementioned papers. We instead selectively choose aspects of all three papers to underscore the deep and illuminating relationship between the construction of unconditional pseudorandom generators, and the inherent, salient properties of boolean functions that they attempt to fool.

2 Preliminaries

We now review some background information that is utilized throughout the survey.

2.1 Fourier Analysis

To begin with our background, we think of boolean functions of the form $f : \{-1,1\}^n \to \{-1,1\}$. Throughout this document, we will interpret -1 as TRUE and 1 as false. When analyzing the semantic properties of a boolean function, it is useful to use the Fourier expansion of a boolean function.

Definition 1 (Fourier Expansion, [O'D21])**.** *The Fourier expansion is the unique multi-linear polynomial that agrees with f on $\{-1,1\}^n$ (the uniqueness would require a proof).*

The Fourier expansion reveals many of the spectral properties of a boolean function by revealing the weight associated with each subset of distinct interactions over its boolean domain. To that end, each basis vector that arises from the expansion corresponds to a unique subset of boolean variables, that is indexed by a set $S \in [n]$. A basis vector is called a *character* and is denoted χ_S and defined as

$$\chi_S = \prod_{i \in S} x_i$$

Due to the fact that there are 2^n characters associated with any n-variate boolean function, there are 2^n orthonormal basis vectors. The original function,

f, when expanded, is of form $f : \mathbb{R}^n \to \mathbb{R}$ and is of form

$$f(x) = \sum_{S \in [n]} \hat{f}(S) \cdot \chi_S = \sum_{S \in [n]} \hat{f}(S) \cdot \prod_{i \in S} x_i$$

The Fourier expansion of f allows us to view it as vector in $\mathbb{R}^{2^n}$. Conversely, we can define $\mathbb{R}^{2^n}$ as not just a vector space, but an inner-product space. Specifically, we can define inner products in a manner that relate to correlations between boolean functions.

Definition 2 (Inner-product/Correlation over boolean functions, [O'D21])**.** *Let $f, g \in \mathbb{R}^{2^n}$ and $\langle f, g \rangle$ be defined as*

$$\langle f, g \rangle = \mathbb{E}_{x \leftarrow_U \{-1,1\}^n}[f(x) \cdot g(x)]$$

, then $\langle \cdot, \cdot \rangle$ defines an inner product over $\mathbb{R}^{2^n}$ and equivalently defines the correlation between two boolean functions.

Note that we can now make interesting, semantic claims about arbitrary boolean functions. The first interesting claim is *Plancheral's Inequality.*

Theorem 1 (Plancheral's Inequality, [O'D21])**.** *Let f, g be two boolean functions, then it is true that*

$$\langle f, g \rangle = \sum_{S \in [n]} \hat{f}(S) \cdot \hat{g}(S)$$

The proof of this statement is derived from the fact that each character function is orthonormal. Therefore only coefficients that share the same basis can be multiplied together. From these result, we get another crucial identity.

Theorem 2 (Parseval's Identity)**.** *Let $f \in \mathbb{R}^{2^n}$ be a boolean function, then*

$$\langle f, f \rangle = \sum_{S \in [n]} \hat{f}(S)^2$$

Furthermore, because $\mathbb{E}_{x \leftarrow_U \{-1,1\}^n}[(f(x))^2] = 1$, it is true that

$$\langle f, f \rangle = \sum_{S \in [n]} \hat{f}(S)^2 = 1$$

With the ability to view a boolean function in this new manner, we will now consider some non-trivial operations we can perform on them. The goal of using these operations on boolean function will be to reveal their salient, semantic properties.

2.2 Restrictions

The first interesting operation on an arbitrary boolean function $f \in \{-1,1\}^n$ we will consider has the goal of "limiting" or *restricting* the effect on an input on f. To achieve this goal, we need a new type of object called a *restriction* introduced Subbotovskaya [**?**].

Definition 3 ([HH23])**.** *A restriction is a string of form* $R \in \{-1,1,*\}^n$

Oftentimes, it will be useful to consider restrictions as being functions themselves. That is, we will consider a restriction $R : \{-1,1\}^n \to \{-1,1\}^n$ to be defined element-wise on each x_i in the following manner

$$R(x_i) = \begin{cases} R_i & \text{if } R_i \in \{-1,1\}, \\ x_i & \text{if } R_i = *. \end{cases}$$

Using this object, we can declare a restriction of a boolean function $f : \{-1,1\}^n \to \{-1,1\}$ as follows

$$f_{|_R}(x) = f(R(x))$$

By utilizing the restriction and limiting x's effect on f, we gain the ability to analyze f's behavior on sub-cubes in $\{-1,1\}^n$. This is possible because a restriction has the effect of simplifying f through its effects on arbitrary inputs x. To control the degree to which a restriction has an effect on $x \in \{-1,1\}$, we introduce the notion of a p-random restriction.

Definition 4 (p-random restriction, [HH23])**.** *A p-random restriction is a restriction* $R \in \{-1,1,*\}^n$ *such that the following is true for any* i^{th} *element* R_i

$$R_i = \begin{cases} * & w.p\ p \\ -1 & w.p\ \frac{1-p}{2} \\ 1 & w.p\ \frac{1-p}{2} \end{cases}$$

Thus, we can think of $\mathcal{R}_p$ *as a discrete product distribution over* $\{-1,1,*\}^n$ *that is parameterized by a survival parameter p. When referred to any particular p-random restriction, we will claim that it is drawn* $R \leftarrow \mathcal{R}_p$ *uniformly at random.*

2.3 Closure under restrictions

We now introduce the concept of closure under restrictions. Informally, a class of boolean functions is said to be closed under restrictions if replacing a subset of variables with constant values induces functions that remains in the same class. For our analysis, it will suffice if this closure property is achieved with high-probability, as opposed to complete certainty.

Formally, we can describe closure under restrictions, with high-probability, as follows.

Definition 5 (Closure under restriction, [HH23]). *Let $\mathcal{F}$ be a class of boolean functions of form $f : \{-1,1\}^n \to \{-1,1\}$. Suppose we say that we have identified values, $p, \delta > 0$ such that the following is true:*

$$Pr[f|_R \in \mathcal{F}] \geq 1 - \delta$$

Where $R \leftarrow R_p$ is drawn uniformly at random.

This concept will be crucial when we define both standard and fractional pseudorandom generators, which will be next.

2.4 Pseudorandom Generators

Before we proceed with the definition of a pseudorandom generator, we introduce the concept of ϵ-fooling a class of boolean functions.

Definition 6 (ϵ-fooling, [HH23]). *Let $\mathcal{F}$ be a class of boolean functions of form $f : \{-1,1\}^n \to \mathbb{R}$, $X \in \{-1,1\}^n$ be a random variable, and $\epsilon > 0$. We say that X ϵ-fools $\mathcal{F}$ if, for every $f \in \mathcal{F}$, the following is true:*

$$|\mathbb{E}[f(X)] - \mathbb{E}[f(U_n)]| \leq \epsilon$$

Where $U_n \in \{-1,1\}^n$ denotes the uniform distribution of the defined support.

Throughout this text, we will denote $\mathbb{E}[f] = \mathbb{E}[f(U_n)]$. With this definition, we are now ready to define pseudorandom generators that ϵ-fool classes of boolean functions.

Definition 7 (Psuedorandom Generators). *Let $\mathcal{F}$ be a class of boolean functions of form $f : \{-1,1\}^n \to \mathbb{R}$, $\epsilon > 0$, and $G : \{-1,1\}^s \to \{-1,1\}^n$, where $s < n$. We say that G is an ϵ-PRG for $\mathcal{F}$ if, for every $f \in \mathcal{F}$, the following is true:*

$$|\mathbb{E}[f(G(U_s))] - \mathbb{E}[f]| \leq \epsilon$$

Where $U_s \in \{-1,1\}$ is the uniform distribution over its mentioned support.

We are now ready to begin discussing *fractional pseudorandom generators.*

2.5 Fractional Pseudorandom Generators

To meaningfully engage in discussions around fractional-pseudorandom number generators, some more notations must be introduced. Note that over this course of this section, we primarily review results from [CHHL19] that have been refined in [HH23].

Definition 8 (Product Distribution Notation). *Fix a value $x \in [-1,1]^n$. Denote $\Pi_x \in \{-1,1\}^n$ be the unique random variable such that*

$$\mathbb{E}[\Pi_x] = x$$

Note that for any product distribution over $\{-1,1\}^n$ and any fourier expanded boolean function (with domain and range restricted) $f : [-1,1]^n \to \mathbb{R}$, multlinearilty of expectation causes Jensen's inequality to evaluate to strict equality. Formally, we can say the following

Lemma 1 (Jensen's Inequality)**.** *Let $f : [-1,1]^n \to \mathbb{R}$ be a Fourier expanded boolean function over the domain $[-1,1]^n$. For any product distribution of form $\Pi_x \in \{-1,1\}$, it holds that*

$$\mathbb{E}(f(\Pi_x)) = f(\mathbb{E}[\Pi_x]) = f(x)$$

Where $\mathbb{E}[\Pi_x] = x$.

Note that as an immediate consequence, it holds that

$$\mathbb{E}(f(U_n)) = f(0^n)$$

With the aforementioned notations, we are ready to define fractional pseudorandom generators as follows.

Definition 9 (Fractional Pseudorandom Generators, [CHHL19, HH23])**.** *Let $\mathcal{F}$ be a class of boolean functions of form $f : \{-1,1\}^n \to \mathbb{R}$ and $\epsilon > 0$. A fractional pseudorandom generator for $\mathcal{F}$ is a function $G : \{-1,1\}^s \to [-1,1]^n$ such that for any Fourier expanded $f \in \mathcal{F}$, the following is true:*

$$|\mathbb{E}[f(G(U_s))] - f(0^n)| \leq \epsilon$$

Note that with this definition, we can trivially fool all classes of boolean functions by having $G(U_s) = 0$. However, as our goal is to construct standard pseudorandom generators from fractional ones, we will need the value of $G(U_s)$ to be bounded away from 0^n, while having its mean be 0^n. For this reason, we now define *q-noticeability*. Furthermore, for brevity, we will let $X = G(U_s)$ and will refer to G through X.

Definition 10 (q-noticeability, [CHHL19], [HH23])**.** *Let $X \in [-1,1]^n$ be a random variable. We say that it is q-noticeable, for some value $q \in [0,1]$, if, for all X_i, it holds that*

$$\mathbb{E}[X_i^2] \geq q$$

Note that as an immediate consequence, we can bound the distance that any X_i has from the endpoints $\{-1,1\}$. This can be seen through the following

$$\mathbb{E}[|X_i|] \leq \mathbb{E}[X_i^2]^{1/2}$$

Therefore,

$$1 - \mathbb{E}[|X_i|] \geq 1 - \mathbb{E}[X_i^2]^{1/2}$$

As a technical aside, we will ned to define the notion of a *symmetric random variable* over the continuous domain $[-1,1]^n$.

Definition 11 ([HH23]). *Let X be a random variable distributed over $[-1,1]^n$. We say that X is symmetric if, for every $x \in [-1,1]^n$, we have that $Pr[X = x] = Pr[X = -x]$.*

Note that creating a symmetric, q-noticeable ϵ-PRG G for a class of boolean functions $\mathcal{F}$ is straightforward if we already have an asymmetric q-noticeable ϵ-PRG for $\mathcal{F}$, G'. We can do so in the following manner. Assume that G' has seed-length s, we can construct G, with seed length $s+1$ by utilizing the extra, truly random bit, to flip the value of G'. Formally, we can let G be defined as follows:

$$G(x,b) = (-1)^b \cdot G^{'}(x)$$

Given a symmetric $q-$noticeable random variable, we can bound its expected value through the Markov Inequality. To do so, we will not bound $\mathbf{E}[\mathbf{X}]$ directly(as its support includes negative values), we will bound $\mathbb{E}[\sqrt{1-\mathbf{X}}]$. To that end, we have the following lemma.

Lemma 2 ([HH23]). *Let $\mathbf{X}$ be a symmetric, q-noticeable random variable with support defined over $[-1,1]$. Then the following holds true:*

$$\mathbb{E}[X] \leq 1 - \frac{q}{8}$$

Proof. We can prove this claim by decomposing X over two random variables, $Y \in [0,1]$ and $Z \in \{-1,1\}$. Specifically, we let $Y = |X|$ and Z be drawn uniformly at random over the set $\{-1,1\}$. We can now consider the expectation of X in the following manner. First, fix a value $y \in [0,1]$

$$(\mathbb{E}[\sqrt{1-yZ}])^2 = (\frac{\sqrt{1-y}+\sqrt{1+y}}{2})^2 = \frac{1+\sqrt{1-y^2}}{2} \leq 1 - \frac{y^2}{4}$$

As a result, we can say that

$$\mathbb{E}[\sqrt{1-\mathbf{X}}] = \mathbb{E}_Y(\mathbb{E}_Z[\sqrt{1-YZ}]) \leq \mathbb{E}_Y[\sqrt{1-\frac{Y^2}{4}}] \leq \mathbb{E}[1-\frac{Y^2}{8}] \leq 1 - \frac{q}{8}$$

■

Next, we define the notion of *almost d-wise independence.*

Definition 12 (Almost $d-$wise independence, [CHHL19]). *A random variable $\mathbb{Z} \in \{-1,1\}^n$ is ϵ-almost, d-wise independent if, for any restriction of $\mathbb{Z}$ to d coordinates, the marginal distribution of has statistical distance at most ϵ from the uniform distribution on $\{-1,1\}^d$*

The following notion of a λ-approximation Gaussian will be utilized to design an explicit fractional PRG in future sections.

Definition 13 (λ-Approximate Gaussian, [Kan14]). *A random variable* $\mathbf{W} \in \mathbb{R}$ *is* λ*-approximate Gaussian if there is a correlated standard Gaussian* $\mathbf{W}' \sim \mathcal{N}(0,1)$ *s.t.*

$$\Pr[|W - W'| > \lambda] < \lambda.$$

Theorem 7 shows how to approximate a Gaussian using only a few randomness (considering randomness as expensive resources like time and space).

The next set of preliminary information involves the Fourier tails of classes of boolean functions.

2.6 Fourier Tails

In this section, we formally define the notion of *Fourier tails* and *Fourier Mass* at arbitrary levels.

Definition 14 (Level-k Fourier tails, [CHRT18, O'D21]). *Let* $\mathcal{F}$ *be a class of* n*-variate Boolean function, and* $f \in \mathcal{F}$*, we say its level-*k *Fourier tails for* $k = 1, \ldots, n$ *are*

$$\mathcal{L}_{1,k}(f) = \sum_{S \subseteq [n] : |S| = k} |\hat{f}(S)|,$$

which is really the L_1 *equivalent of Fourier weight at* k*-th level. Then, we can quite naturally define this for the entire class of Boolean functions,*

$$\mathcal{L}_{1,k}(\mathcal{F}) = \max_{f \in \mathcal{F}} \{\mathcal{L}_{1,k}(f)\}.$$

We will sometimes explicitly reference the L_1 tail bounds of boolean functions through the following definition

Definition 15 (L_1 Tail Bounds, [CHRT18, O'D21]). *For* $a, b \geq 1$*, we denote* $\mathcal{L}_1^n(a,b)$ *the family of* n*-variate boolean functions* $f : \{-1,\}^n \to \{-1, 1\}$ *which satisfy*

$$\sum_{S \subseteq [n], |S| = k} |\hat{f}(S)| \leq a \cdot b^k$$

For all $k \in [n]$

Definition 16. *The level-*k *absolute Fourier sum of* f *is defined as*

$$M_k(f) := \max_{x \in \{\pm 1\}^n} \left| \sum_{S \subseteq [n], |S| = k} \hat{f}(S) \cdot \chi_S(x) \right|$$

Naturally, for function classes $\mathcal{F}$ we define $L_{1,k}(\mathcal{F})$ and $M_k(\mathcal{F})$ respectively as $\max_{f \in \mathcal{F}} L_{1,k}(f)$ and $\max_{f \in \mathcal{F}} M_k(f)$.

With preliminaries out of the way, we are ready to summarize the first set of results that are primarily concerned with the construction of pseudorandom generators from polarizing random walks.

3 Pseudorandom Generators from Polarizing Random Walks

The central concept involves constructing a fractional PRG for functions over the interval $[-1,1]^n$ that efficiently converges. To facilitate this, we introduce a mechanism known as the random walk gadget, which not only implements the random walk but also promotes rapid polarization, leading to quick convergence.

3.1 Random Walk Gadget

We now describe the random walk gadget: a concrete implementation of the polarizing random walk involving samples from a q-noticeable fractional-PRG.

Definition 17 (Random Walk Gadget, [CHHL19])**.** *For any $t \geq 1$, the random walk gadget $g_t : [-1,1]^t \to [-1,1]$ is defined recursively as follows: Let $a_1, \ldots, a_t \in [-1,1]$. Define $g_1(a_1) := a_1$, and for $t > 1$,*

$$g_t(a_1, \ldots, a_t) := g_{t-1}(a_1, \ldots, a_{t-1}) + (1 - |g_{t-1}(a_1, \ldots, a_{t-1})|)a_t.$$

This gadget can be extended to operate on bit-vectors as follows:

$$g_t^n(x_1, \ldots, x_t) = (g_t(x_{1,1}, \ldots, x_{t,1}), \ldots, g_t(x_{1,n}, \ldots, x_{t,n})),$$

where $x_1, \ldots, x_t \in [-1,1]^n$ and the operation is applied column-wise to construct a $t \times n$ matrix, transforming it into a vector in $[-1,1]^n$.

Alternatively, we will view the random walk gadget through the following algorithm as described in [HH23].

Algorithm 1 RandomWalkGadget($\{X_i\}_{i\in[t]}$)

Require: $t = 16\log(n/\epsilon)/p$ ▷ We will show why this value of t suffices
  $Y^0 \leftarrow 0$
  for $j \in [t]$ **do**
    $Y^j \leftarrow Y^{j-1} + \delta_{Y^{j-1}} \odot X^j$
  end for
  Return sign(Y^t)

Where δ_{Y^j} is defined in the following manner for all $j \in [t]$

Definition 18 ([HH23, CHHL19])**.** *Fix a value $y \in [-1,1]$, and denote δ_y to be the following, for each $i \in [n]$:*

$$(\delta_y)_i = 1 - |y_i|$$

Furthermore, for any x, z, denote $x \odot z$ as follows for each $i \in [n]$:

$$(x \odot z)_i = x_i z_i$$

3.1.1 Amplification Theorem

The amplification theorem demonstrates how to leverage the random walk gadget to boost the efficacy of fractional PRGs by employing a polarization strategy.

Theorem 3. *Let $\mathcal{F}$ be a family of n-variate Boolean functions closed under restrictions. Assume $X \in [-1,1]^n$ is a symmetric p-noticeable fractional PRG for $\mathcal{F}$ with error ϵ. Define $t = O(\log(n/\epsilon)/p)$ and let $X_1, \ldots, X_t$ be i.i.d. copies of X. Then, the random variable G,*

$$G := G(X_1, \ldots, X_t) = sign(g_t^n(X_1, \ldots, X_t)),$$

is a PRG for $\mathcal{F}$ with error $(t+3)\epsilon$.

This theorem underscores the potential to enhance fractional PRGs through the random walk gadget, resulting in a more robust PRG by amplifying the initial error across multiple iterations, thereby attaining a desired level of pseudorandomness for the target function class.

To prove this theorem, we will work with the explicit random walk gadget algorithm1 to show that the PRG has three properties. To see why this construction works, we show that the random walk has three properties:

- Each step introduces little error. That is for every $f \in \mathcal{F}$ and $j \in [t]$

$$|\mathbb{E}[f(Y^j)] - \mathbb{E}[f(Y^{j-1})] \leq \epsilon.$$

- The walk polarizes with high probability

$$Pr[||\delta_{Y^t}||_\infty \leq \epsilon/n] \geq 1 - \epsilon.$$

- The final rounding operation introduces little error: for every $f \in \mathcal{F}$

$$|f(Y^t) - f(sign(Y^t))| \leq \epsilon$$

3.1.2 Each step introduces small error

We first prove the following lemma.

Lemma 3 (Each step introduces small error, [HH23])**.** *Let $\mathcal{F}$ be a family of functions $f : \{-1,1\} \to \mathbb{R}$ that is closed under restrictions, and suppose that $X \in [-1,1]^n$ ϵ-fools $\mathcal{F}$. Then, for every $f \in \mathcal{F}$ and $y \in [-1,1]^n$, it holds that*

$$|f(y) - \mathbb{E}[f(y + \delta_y \odot X)]| \leq \epsilon$$

And that for every $j \in [t]$, for suitable t,

$$|\mathbb{E}[f(Y^j)] - \mathbb{E}[f(Y^{j-1})]| \leq \epsilon$$

Proof. Let $y \in [-1,1]^n$ be fixed. Furthermore, let $R \in \{-1,1,*\}^n$ be sampled according to

$$R_i = \begin{cases} sign(y_i) & \text{w.p } |y_i| \\ * & \text{w.p } 1-|y_i| \end{cases}$$

Then for each $i \in [n]$, and a fixed $x \in [-1,1]^n$, we can note the following observation

$$\mathbb{E}_R[(R \circ x)_i] = |y_i| \cdot sign(y_i) + (1-|y_i|) \cdot x_i$$

Which implies that

$$\mathbb{E}_R[R \circ x] = y + \delta_y \odot x$$

From here, we can note that the relationship between the expected values of the composition, and how these quantities relate to the Fourier expansion of f. Namely, we can see that

$$\mathbb{E}_R[f|_R(x)] = \mathbb{E}_R[f(R \circ x)] = f(\mathbb{E}_R[R \circ x]) = f(y + \delta_y \odot x)$$

As a result, we can see that

$$|f(y) - \mathbb{E}_X[f(y + \delta_y \odot X)]| \leq \mathbb{E}[|f|_R(0^n) - \mathbb{E}_X[f|_R(X)]|] \leq \epsilon$$

■

3.1.3 Polarization Occurs with High Probability

With this proof in hand, the next set of steps is to prove that the random walk, that yields our ultimate pseudorandom value, polarizes with high probability. For the following proof, we will assume that $\mathbf{X}$ is a symmetric random variable. Furthermore, to simplify our analysis we will consider random variables of form $\{\mathbf{Y^j} \in [-1,1]\}_{j \in [t]}$ and $\{\mathbf{X^j} \in [-1,1]\}_{j \in [t]}$ for a value j that is to be determined.

Lemma 4 (Polarization occurs with high probability, [HH23])**.** *Let* $\{\mathbf{X^j} \in [-1,1]\}_{j \in [t]}$ *be independent, symmetric random variables. Furthermore, define* $\mathbf{Y}^0 = 0$ *and for all* $j \in [t]$*, let*

$$\mathbf{Y}^j = \mathbf{Y}^{j-1} + (1 - |\mathbf{Y}^{j-1}|) \cdot \mathbf{X^j}$$

Then, $Pr[1 - |\mathbf{Y}^j| \geq e^{-\frac{tq}{8}}] \leq e^{-\frac{tq}{16}}$

Proof. Note that for any $\mathbf{Y}^j$, we can bound $1 - |\mathbf{Y}^j|$ in the following manner

$$1 - |\mathbf{Y}^j| \leq (1 - |\mathbf{Y}^{j-1}|) \cdot (1 - \mathbf{X}^j \cdot sign(\mathbf{Y}^{j-1}))$$

Now, due to the assumption that each of our random variables $\{X^j\}_{j \in [t]}$ are symmetric, each step in the walk is also symmetric. Furthermore, due to independence between $(1 - |\mathbf{Y}^{j-1}|)$ and $sign(\mathbf{Y}^{j-1}))$, we can compute expected values

$$\mathbb{E}[1 - |\mathbf{Y}^j|] \leq \mathbb{E}[(1 - |\mathbf{Y}^{j-1}|)] \cdot \mathbb{E}(1 - \mathbf{X}^j \cdot sign(\mathbf{Y}^{j-1}))$$

We can now invoke the bounds established earlier to say that

$$\mathbb{E}[\sqrt{1-|\mathbf{Y}^j|}] \leq \mathbb{E}[\sqrt{1-|\mathbf{Y}^{j-1}|}] \cdot (1-\frac{q}{8})$$

Thus, by induction, we can say that

$$\mathbb{E}[\sqrt{1-|\mathbf{Y}^j|}] \leq (1-\frac{q}{8})^t \leq e^{-\frac{qt}{8}}$$

Thus, we can invoke Markov's Inequality to prove the bound. ■

3.1.4 Overall error bounds

The final aspect of the proof is to show that rounding at the last step in the random walk does not incur excessive error.

Lemma 5 ([HH23]). *Let $f : \{-1,1\}^n \to \{-1,1\}$ be a function and utilize the Fourier-expansion to the domain $[-1,1]^n$, then for every $y \in [-1,1]^n$*

$$|f(y) - f(sign(y))| \leq \sum_{i=1}^{n}(1-|y_i|) \leq n \cdot ||\delta||_\infty$$

Proof. We can say that

$$\begin{aligned}|f(y) - f(sign(y))| &= |\mathbb{E}[f(\Pi_y)] - f(sign(y))| \\ &\leq 2 \cdot Pr[\Pi_y \neq sign(y)] \\ &\leq 2 \cdot \sum_{i=1}^{n} \frac{1-|y_i|}{2}\end{aligned}$$

Now, if we let $t = 16\log(n/\epsilon)/q$, we can have proof that, even with the error incurred by the final rounding step, the random walk yields a fractional PRG for $\mathcal{F}$ with error $O(\epsilon \log(n/\epsilon)/q)$. Furthermore, we can say that the seed-length for the standard PRG has length $ts = O(s\log(n/\epsilon)/q)$. Furthermore, we let E denote the event that $||\delta_{\mathbf{Y}^t}||_\infty \leq \epsilon^{-tq/8} \leq \epsilon/n$.

We show this in the following manner.

$$\begin{aligned}|\mathbb{E}[f(sign(\mathbf{Y}^t))] - \mathbb{E}[f]| &\leq |\mathbb{E}[f(sign(\mathbf{Y}^t))] - \mathbb{E}[f(\mathbf{Y}^t)]| + \sum_{j=1}^{t} |\mathbb{E}[f(\mathbf{Y}^j)] - \mathbb{E}[f(\mathbf{Y}^{j-1})]| \\ &\leq |\mathbb{E}[f(sign(\mathbf{Y}^t))] - \mathbb{E}[f(\mathbf{Y}^t)]| + \epsilon \cdot t \\ &\leq |\mathbb{E}[f(sign(\mathbf{Y}^t)) - f(\mathbf{Y}^{\mathbf{t}})|E]| + 2Pr[\overline{E}] + \epsilon t \\ &\leq n \cdot \mathbb{E}\left[\|\delta_{\mathbf{Y}_t}\|_\infty | E\right] + 2n \cdot e^{-tq/16} + \epsilon t \\ &\leq n \cdot \frac{\epsilon}{n} + (t+2)\epsilon \\ &\leq (t+3)\epsilon \\ &\leq O(\epsilon \log(n/\epsilon)/q)\end{aligned}$$

■

Thus, we have proved the correctness of the amplification theorem3, and that a fractional, q-noticeable ϵ-PRG for $\mathcal{C}$ can be converted into a standard PRG for $\mathcal{F}$ with error $O(\epsilon \cdot \log(n/\epsilon)/q)$.

With correctness established, we are now ready to proceed with applying the aforementioned PRGs for functions with bounded Fourier tails.

3.2 Fooling functions with bounded Fourier Tails

Due to the fact that L_2 bounds imply L_1 bounds, it suffices to focus on the class of functions with bounded L_1 Fourier tails. Thus, we will focus our attention on designing PRGs for classes of boolean functions with bounded L_1 Fourier tails.

In the following lemma, we summarize the construction of a fractional PRG for this class of functions based on a scaling of almost d-wise independent random variables.

Lemma 6 ([CHHL19])**.** *Fix $n, a, b \geq 1$ and $\epsilon > 0$. There exists a fractional PRG $\mathbf{X} \in [-1,1]^n$ that fools $\mathcal{L}_1^n(a,b)$ with error ϵ, such that*

1. *$\mathbf{X}$ is p-noticeable for $p = \frac{1}{4b^2}$*
2. *The seed length of $\mathbf{X}$ is $O(\log\log n + \log(a/\epsilon))$*

Proof. Fix an $f \in \mathcal{L}_1^n(a,b)$. Let

- $d = \lceil \frac{\log 2a}{\epsilon} \rceil$
- $\delta = \frac{\epsilon}{2a}$
- $\beta = \frac{1}{2b}$

Next, let $\mathbf{Z} \in \{-1,1\}^n$ be a δ-almost d-wise independent random variable and $\mathbf{X} = \beta\mathbf{Z}$. Notice that $\mathbf{X} \in \{-\beta, \beta\}^n$. Note that $\mathbf{X}$ is $\frac{1}{4b^2}$-noticeable. We can also prove that $\mathbf{X}$ ϵ-fools $\mathcal{F}$, where $\mathcal{F}$ is closed under restrictions.

Consider a function f from a family $\mathcal{F}$, and examine its Fourier expansion:

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) x^S.$$

The objective is to demonstrate that the expected value of $f(X)$ is proximate to $f(0)$. This involves averaging $f(X)$ over the random variable X, leading to:

$$|\mathbb{E}[f(X)] - f(0)| = \left| \sum_{|S|>0} \hat{f}(S) \cdot \mathbb{E}[X^S] \right|.$$

Next, we introduce a bound for $\mathbb{E}[Z^S]$. For any set S with $|S| \leq d$, it's evident that $\mathbb{E}[Z^S] \leq \delta$. For larger sets where $|S| > d$, the bound is based on

$W_k = \sum_{|S|=k} |\hat{f}(S)|$ which, by assumption, satisfies $W_k \leq a \cdot b^k$. Hence, we can establish that:

$$|\mathbb{E}[f(X)] - f(0)| \leq \sum_{k=1}^{d} W_k \beta^k + a \sum_{k>d} (\beta b)^k.$$

Utilizing $\beta = \frac{1}{2b}$, the summation simplifies and enables us to define error bounds effectively:

$$|\mathbb{E}[f(X)] - f(0)| \leq \delta a \sum_{k=1}^{d} (\beta b)^k + a \sum_{k>d} (\beta b)^k \leq \delta a + 2^{-d} a.$$

This calculation culminates with a chosen error margin, setting $\delta = e/2a$ and ensuring that $2^{-d} \leq e/2a$, which solidifies the proof under specified conditions. ■

With this proof in hand, we can conclude this section with the following theorem.

Theorem 4. *[CHHL19] Let $\mathcal{F}$ be a family of n-variate Boolean functions closed under restrictions. Assume that $\mathcal{F} \subset \mathcal{L}_1^n(a, b)$. For any, $\epsilon \leq \frac{1}{poly(b \log n)}$ there exists an explicit PRG $\mathbf{X} \in \{-1, 1\}^n$ which fools $\mathcal{F}$ with error $\epsilon > 0$, whose seed-length is $O(\log(n/\epsilon)(\log\log n + \log(\frac{a}{\epsilon}))b^2)$*

With these results established, we now progress towards summarizing the design of an alternative pseudorandom generator that only requires bounds on the second level of Fourier Tails based on the work of Raz and Tal[**?**]. An application of this result yields a conjecture for the bounds on the second level of Fourier tails for low-degree $\mathbb{F}_2$ polynomials. If this conjecture is proven to be true, then it would imply an efficient PRG for $\mathbf{AC}^0[\oplus]$.

4 Pseudorandom Generators from the Second Fourier Level

In this next line of work, the authors were primarily concerned with relaxing the assumptions associated with Fourier tails[CHRT18]. That is, rather requiring bounds on all values $k \in [n]$, the investigated if bound were required for only a few values of k. They proved that the latter was indeed the case, and that it suffices to obtain bounds for the second Fourier level of a class of boolean functions to design explicit PRGs the aforementioned class. That is, they proved that

Theorem 5 (Level-2 Fourier Bounds imply Explicit PRGs, [CHRT18])**.** *Let $\mathcal{F}$ be a family of n-variate Boolean functions that is closed under restrictions. Assume for some $t \geq 1$ it holds that*

$$\mathcal{L}_{1,2}(\mathcal{F}) \leq t.$$

Then, for any $\epsilon > 0$, $\exists$ an explicit PRG *for $\mathcal{F}$ with error ϵ and seed length* $\mathsf{poly}(t, \log(n), 1/\epsilon) = O\left((t/\epsilon)^{2+o(1)} \cdot \mathsf{polylog}(n)\right)$.

The proof of this statement is similar to what has been presented earlier. The key steps of which are: constructing a fractional-PRG for $\mathcal{F}$ that is p-noticeable and utilizing a polarizing random walk to convert the fractional PRG into a standard PRG.

Thus, to prove the aforementioned theorem5, it suffices to construct an appropriate fractional PRG. Namely, we will wish to prove the following:

Lemma 7 ([CHRT18])**.** *Let $\mathcal{F}$ be a family of n-variate Boolean functions closed under restrictions. Assume that for some $t \geq 1$, it holds that*

$$\mathcal{L}_{1,2}(\mathcal{F}) \leq t.$$

Then, for any $\epsilon > 0$, there exists an explicit p-noticeable fractional PRG *for $\mathcal{F}$ with error ϵ and seed length s where:*

- $1/p = O(\log(n/\epsilon))$.
- $s = O\left((t/\epsilon)^{2+o(1)} \cdot \log(n) \cdot \log(n/\epsilon)\right)$.

The construction of such a fractional PRG will be the focal point of our attention for the next few sections.

4.1 Explicit Fractional Pseudorandom Generator

The crux of this proof lies results of Raz and Tal. Which is rephrased as the following lemma. Here, Multivariate Gaussian is abbreviated as MVG.

Theorem 6 ([RT22], Recall)**.** *Let $n, t \geq 1, \delta \in (0, 1)$. Let $Z \in \mathbb{R}^n$ be a zero-mean* MVG *random variable with the following properties:*

- *For $i \in [n]$:* $\mathsf{Variance}[Z_i] \leq \frac{1}{8\ln(n/\delta)}$.
- *For $i, j \in [n], i \neq j$:* $|\mathsf{Covariance}[Z_i, Z_j]| \leq \delta$.

Let $\mathcal{F}$ be a class of n-variate Boolean functions closed under restrictions. Then, $\forall f \in \mathcal{F}$, it holds that

$$|\mathbb{E}[f(\mathsf{trunc}(Z))] - f(\vec{0})| \leq O(\delta \cdot t).$$

Using this theorem, the authors construct a p-noticeable PRG, where $1/p = O(\log(n/\epsilon))$ for $\mathcal{F}$ with error ϵ and seed length $s = poly(t, \log n, 1/\epsilon)$.

This construction is shown in two steps. The first step hinges on showing that a MVG distribution with the parameters defined in the aforementioned theorem 6 can be of rank $l = poly(\log n, t, 1\epsilon)$. In other words, l independent standard normal random variables are sampled and an explicit linear transformation $T : \mathbf{R}^l \to \mathbf{R}^n$ is applied to get a random variable that satisfies the two conditioned laid out in theorem 6. The second step hinges on discretizing the process.

4.2 Dimension Reduction

To get our intended result l, we first look at how it is used. We let $\delta = \epsilon/t$, and let $\mathcal{C}$ be a code on $\{0,1\}^l$ with at least n codewords and that $\mathcal{C}$ is alas δ-balanced (as in, $\forall c \in \mathcal{C}$, the Hamming distance of c from $\vec{0}$ is between $[(\frac{1}{2}-\delta)l, (\frac{1}{2}+\delta)l]$), constructible by [TS17] with $l = (\log(n))/\delta^{2+o(1)}$.

Select $c^1, \ldots, c^n \in \mathcal{C}$ as distinct codewords with l bits, i.e. $c^i = (c^i_1, \ldots, c^i_l)$ (by definition these distinct elements do exist). Then, we define the linear transformation as

$$A, \text{ where } A_{i,j} = \sqrt{\frac{1}{8\ln(n/\delta)} \cdot \frac{\delta^{2+o(1)}}{\log(n)}} \cdot (-1)^{c^i_j}.$$

We can then check, given $Y \in \mathbb{R}^l$ where Y_i's are independently sampled $\mathcal{N}(0,1)$ random variables, $Z = AY$ is our intended $\mathbb{R}^n$ random variable that satisfies the properties in theorem 6.

4.3 Discretizing the Process

The next step involves discretizing the randomness. The authors achieve this by proving the following lemma.

Lemma 8 ([CHRT18])**.** *For $l, \eta > 0$, there exists $s = O(l \cdot \log(l/n))$ and an explicit generator $G : \{0,1\}^s \to \mathbb{R}^l$ such that the following holds: Let $f : [-1,1]^n \to [-1,1]$ be a multi-linear function, $A \in [-1,1]^{n \times l}$ and Y be a random variable over $\mathbb{R}^l$ where each Y_i is an independent $\mathcal{N}(0,1)$ Gaussian random variable. Then,*

$$|\mathbb{E}[f(\mathsf{trunc}(A\mathbf{Y}))] - \mathbb{E}[f(\mathsf{trunc}(AG\mathcal{U}_s))]| \leq \eta(n+2).$$

Once proved, this lemma allows one to approximately sample a standard MVC $\mathbf{Y} \in \mathbb{R}^l$ using a few random bits. In the following lemma, the authors utilize a lemma by Kane, which is the following:

Theorem 7 ([Kan14])**.** *There is an explicit construction of a λ-approximate Gaussian random variable using $O(\log(1/\lambda))$ bits of randomness.*

Next, we set $\mathbf{Y}' := G(\mathcal{U}_s)$ and $\mathbf{Y} :=$ coupled standard MVG in $\mathbb{R}^l$. Also, let $\mathcal{E}$ be the event where

$$\|\mathbf{Y} - \mathbf{Y}'\|_\infty \leq \lambda.$$

By a simple union bound, we have

$$\Pr(\mathcal{E}) \geq 1 - \eta \implies \|\mathsf{trunc}(A\mathbf{Y}) - \mathsf{trunc}(A\mathbf{Y}')\|_\infty \leq \eta.$$

Now, it suffices to show lemma 9 to show the multi-linearity and boundedness of f:

Lemma 9 ([CHRT18])**.** *Let $f : [-1,1]^n \to [-1,1]$ be a multi-linear function. Then, for every $x, y \in [-1,1]^n$, we have $|f(x) - f(y)| \leq n \cdot \|x - y\|_\infty$.*

Proof (Lemma 9). $\forall i \in [n] \cup \{0\}$, let $z^{(i)} = (x_1, \ldots, x_i, y_{i+1}, \ldots, y_n)$. Clearly, $z^{(0)} = y$ and $z^{(n)} = x$. Thus, we have:

$$\begin{aligned}
|f(x) - f(y)| &= \left| \sum_{i=1}^{n} f(z^{(i)}) - f(z^{(i-1)}) \right| \\
&\overset{\triangle}{\leq} \sum_{i=1}^{n} \left| f(z^{(i)}) - f(z^{(i-1)}) \right| \\
&= \sum_{i=1}^{n} \left| h_i(x_i) - h_i(y_i) \right|, \ [h_i(z) = f(x_1, \ldots, x_{i-1}, z, y_{i+1}, \ldots, y_n), \text{ multi-linear}] \\
&\leq \sum_{i=1}^{n} |x_i - y_i|, \ [\text{because } h_i \text{ is an affine function}] \\
&\leq n \cdot \|x - y\|_\infty .
\end{aligned}$$

■

Thus, by using lemma 9 on event $\mathcal{E}$, we have

$$\begin{aligned}
&|f(\mathsf{trunc}(A\mathbf{Y})) - f(\mathsf{trunc}(A\mathbf{Y}'))| \leq \eta n \\
\implies &|\mathbb{E}[f(\mathsf{trunc}(A\mathbf{Y}))] - \mathbb{E}[f(\mathsf{trunc}(A\mathbf{Y}'))]| \leq \eta n + 2\Pr[\neg\mathcal{E}] \leq \eta(n+2).
\end{aligned}$$

4.4 Level one Fourier Bounds for $\mathbf{F}_2$ polynomials

In this section, we summarize the results that address bounding the level one Fourier tail of low-degree polynomials over $\mathbb{F}_2$. These results establish necessary conditions for the explict construction of fractional PRGs for such boolean functions.

Theorem 8. *[CHRT18] Let $p : \mathbb{F}_2^n \to \mathbb{F}_2$ be a polynomial of degree d, and let $f(x) = (-1)^{p(x)}$. Then the level one Fourier tail of f, defined as $L_{1,1}(f)$, satisfies:*

$$L_{1,1}(f) = \sum_{i=1}^{n} |\hat{f}(i)| \leq Sd.$$

Proof. For simplicity, we assume n is even; the proof for an odd n follows similarly. We start by expressing:

$$\sum_{i=1}^{n} |\hat{f}(i)| = \sum_{i=1}^{n} |E[f(z)(-1)^{z_i}]|,$$

where s_i denotes the sign of $\hat{f}(i)$. We can generalize without loss by assuming $s_i = 1$ for all i, and switching z_i with $1 - z_i$ when $s_i = -1$. This allows us to

focus on bounding the expression:

$$E = \left| E\left[f(z) \sum_{i=1}^{n} (-1)^{z_i} \right] \right|.$$

Defining the functions $T_t : \{0,1\}^n \to \{-1,0,1\}$ for $t = 1, \ldots, n/2$ as:

$$T_t(z) = \begin{cases} -1 & \text{if } \sum_{i=1}^{n} z_i \geq n/2 + t \\ 1 & \text{if } \sum_{i=1}^{n} z_i \leq n/2 - t \\ 0 & \text{otherwise} \end{cases},$$

we find that:

$$E = 2 \sum_{t=1}^{n/2} \left| E\left[f(z) T_t(z) \right] \right|.$$

Further definitions involve $U_t = \{z \in \{0,1\}^n : |\sum_{i=1}^{n} z_i - n/2| \geq t\}$ and the mappings M_0, M_1 defined on U_t, resulting in a consideration of the dimensionality of function spaces. Employing a dimension argument and considering the space of functions $g : A \to \mathbb{F}_2$, we decompose any function g into g_1, g_2 over polynomial spaces and conclude:

$$|A| \leq \sum_{i=0}^{n/2+d} \binom{n}{i}.$$

We apply these insights to derive an upper bound for e_t and subsequently for E, confirming the theorem by showing:

$$E \leq 4 \sum_{t=1}^{n/2} e_t \leq 4 \sum_{t=1}^{n/2} \sum_{i=1}^{d} \binom{n}{n/2 + t + i} \leq 4d.$$

■

4.5 Bounding the second Fourier Level from the first

We introduce a straightforward argument to demonstrate that for any family F of n-variate Boolean functions that adhere to restrictions, a bound of $L_{1,1}(F) \leq t$ leads directly to a bound of $L_{1,2}(F) \leq O(t\sqrt{n \log n})$. We deduce that polynomials of degree polylog(n) obtain $L_{1,2}(F)$ at most $\sqrt{n} \cdot \text{polylog}(n)$. This improvement, though modest, suggests a significant enhancement for the construction of pseudorandom generators (PRGs) for polynomial-degree $\mathbb{F}_2$-polynomials and $\text{AC}^0[\oplus]$ circuits.

Theorem 9. *[CHRT18] Let F be a class of n-variate Boolean functions that is closed under restrictions. If $L_{1,1}(F) \leq t$, then $L_{1,2}(F) \leq t \cdot O(\sqrt{n \log n})$*

Proof. Consider any Boolean function f in F, defined from $\{-1,1\}^n$ to $\{-1,1\}$. We approach this by bounding $L_{1,2}(f)$ using the assumption $L_{1,1}(f) = t$. This involves partitioning the set of indices into two disjoint parts and considering only the cross-terms, leading to:

$$L_{1,1}(X,Y) = \sum_{i\in X, j\in Y} |\hat{f}(i,j)|.$$

Assuming a random partition, the expected value satisfies:

$$\mathbb{E}_{X,Y}[L_{1,1}(X,Y)] = \frac{L_{1,2}(f)}{2}.$$

We continue by fixing a partition and simplifying the expression for $L_{1,1}(X,Y)$:

$$L_{1,1}(X,Y) = \sum_{i\in X, j\in Y} s_i s_j |\hat{f}(i,j)|,$$

where s_i is the sign of $\hat{f}(i)$. Assuming $s_i = 1$ simplifies our calculations.

The resulting bound on $L_{1,1}(X,Y)$ becomes:

$$L_{1,1}(X,Y) \leq \mathbb{E}\left[\sum_{i\in X, j\in Y} s_i x_i f_{x_j}(y)\right],$$

where f_{x_j} denotes a restricted version of f, leading to the following inequality:

$$\mathbb{E}\left[\sum_{i\in X, j\in Y} s_i x_i \cdot \mathbb{E}[f_{x_j}(y)]\right] \leq \mathbb{E}\left[\sum_{i\in X, j\in Y} s_i x_i \cdot \sum_{\ell\in Y} |\hat{f}(j,\ell)|\right].$$

By considering the maximum values of these expressions, the conclusion is that $L_{1,2}(f)$ is at most twice the bound on $L_{1,1}(X,Y)$, satisfying the theorem. ■

4.6 Towards an explict pseudorandom generator for $\mathbf{AC}^0[\oplus]$

It is well-established that the ability to devise explicit pseudorandom generators (PRGs) is deeply intertwined with proving correlation bounds across various Boolean functions. Although it is known that the $AC^0[\oplus]$, which includes constant-depth polynomial-size Boolean circuits with AND, OR, NOT, and PARITY gates, lacks such generators, this is not the case for the class of F_2-polynomials. Pioneering works have demonstrated that $AC^0[\oplus]$ cannot efficiently approximate functions like MAJORITY, yet constructing explicit PRGs for this class remains a challenging open problem in computational complexity theory.

Conjecture 1. *Let $P : \mathbb{F}_2^n \to \mathbb{F}_2$ be a polynomial of degree d, and define $f(x) = (-1)^{P(x)}$. Then:*

$$\sum_{i,j\in[n], i<j} |\hat{f}(i,j)| = O(d^2).$$

If true, combining this conjecture with existing theoretical frameworks could lead to significant advancements in pseudorandom generator construction for $AC^0[\oplus]$ circuits and low-degree F_2-polynomials.

Claim 4. Assuming 1 holds, for any error $\epsilon > 0$, there exists an explicit PRG for $AC^0[\oplus]$ circuits of size n and depth e on n inputs, with error ϵ and seed length $\text{poly}(\log(s/\epsilon), \log n, 1/\epsilon)$.

Thus, with the work presented earlier in this section, it appears feasible that an explicit pseudorandom generator for $\mathbf{AC}^0[\oplus]$.

In the previous sections, we have emphasized the need for bounded Fourier Tails to allow for explicit constructions of fractional pseudorandom generators. In the previous section, we summarized an investigation into a weaker assumption, and showed bounding the L_1 Fourier tails at the second level sufficed to construct an explicit pseudorandom generator. The next section focuses on investigating an even weaker assumption.

5 Fractional Pseudorandom generators from Any Fourier Level

The question asked by the authors of [**?**] was the following: is it necessary to assume that a class of n-variate boolean functions $\mathcal{F}$ has bounded Fourier mass at every level $k \in [n]$. It turns out the answer is an emphatic no. In fact, it turns out that it suffices to bound only a single Fourier coefficient.

The main theorem to this effect (due to [CGL$^+$21]) is stated below:

Theorem 10 ([CGL$^+$21])**.** *Let $\mathcal{F}$ be a class of n-variate boolean functions such that*

1. *$\mathcal{F}$ is closed under restrictions.*
2. *$M_k(\mathcal{F}) \leq b^k$ for some $b \geq 1$ and $k \geq 1$.*

Then, for every $\epsilon > 0$, there exists a $\Omega(\epsilon^{2/k}/b^2)$-noticeable fractional PRG for $\mathcal{F}$ with error ϵ and seed length $O(k \log n)$.

The idea here is to show that we can approximate a high-degree multilinear polynomial (i.e., a polynomial where a variable has degree at most one within each term) with a low-degree multilinear polynomial. This is equivalent to bounding, for a multilinear polynomial f, the contribution of its terms of order at least k which we write as $f_{\geq k}$. We will state the crucial lemma below, and later explain how it enables the creation of fractional PRGs (so therefore regular PRGs as discussed above):

Theorem 11 ([CGL$^+$21])**.** *If $\mathcal{F}$ is closed under random restrictions, then for any $f \in \mathcal{F}$ and $c \in (0, 1)$ we have*

$$\max_{\mathbf{x} \in [-c,c]^n} \left| f_{\geq k}(\mathbf{x}) \leq \left(\frac{c}{1-c}\right)^k M_k(\mathcal{F}) \right|$$

For $c = 1$ (the entire hypercube), a low-order approximation would be asking too much: it is known that any approximation for PARITY requires degree at least $\Omega(n)$. However, for $c < 1$ we can actually do better, and ecause a fractional PRG cares about the value of the function *within* the boolean hypercube, this is sufficient for our purposes.

It is easy to fool degree-k polynomials (with k-wise independent distributions using $O(k \log n)$ seed length). Therefore, our plan is to fool the low-order component of a function f and bound the contribution of the high-order component to be at most ϵ using the above lemma.

5.1 Fractional PRGs from Low-Degree Approximations

We will defer the proof of Theorem 11 to the next section, and first show formally how low-degree approximations can be used to construct fractional PRGs. It is helpful to reframe Theorem 11 with some new definitions: let $\epsilon_{c,k}(f)$ be the ℓ_∞ distance over the hypercube $[-c, c]^n$ of f to the nearest degree-$(k-1)$ multilinear polynomial. In other words

$$\epsilon_{c,k}(f) := \inf_{g:\deg(g)<k} \max_{\mathbf{x}\in[-c,c]^n} |f(\mathbf{x}) - g(\mathbf{x})|$$

Extend this function to classes $\mathcal{F}$ via

$$\epsilon_{c,k}(\mathcal{F}) := \max_{f\in\mathcal{F}} \epsilon_{c,k}(f)$$

and define $c_k(\epsilon, \mathcal{F})$ to be the width c of the zero-centered hypercube where $\mathcal{F}$ is well-approximated by low-degree polynomials, formally

$$c_k(\epsilon, \mathcal{F}) := \max\{c \geq 0, \epsilon_{c,k}(\mathcal{F}) \leq \epsilon\}$$

Then we have the following restatement of Theorem 11

Corollary 1 ([CGL$^+$21])**.** *For any class $\mathcal{F}$ closed under restrictions ant $\epsilon > 0$, $k \leq n$:*

$$c_k(\epsilon, \mathcal{F}) = \Omega\left(\left(\frac{\epsilon}{M_k(\mathcal{F})}\right)^{1/4}\right)$$

Proof. Set

$$c = \Omega\left(\left(\frac{\epsilon}{M_k(\mathcal{F})}\right)^{1/4}\right)$$

in Theorem 11 so the RHS is bounded by ϵ, and apply the definition of c_k. ■

From the above, we see that to show Theorem 10 it is sufficient to prove the following lemma:

Lemma 10. *[CGL$^+$21] Let $\mathcal{F}$ be closed under restrictions. Then there exists a fractional PRG for $\mathcal{F}$ with error ϵ and seed length $O(k \log n)$ which is $(c_k(\epsilon/2, \mathcal{F}))^2$-noticeable.*

Proof. Let $c = \min\left(c_k(\epsilon/2, \mathcal{F}), \frac{1}{2}\right)$. Define our PRG $\mathbf{X}$ as a $(k-1)$-wise independent distribution over $\{-c, c\}^n$–clearly this can be sampled with seed length $O(k \log n)$ as discussed in lecture. For any $f \in \mathcal{F}$, the definition of c_k guarantees a degree-k multilinear polynomial p which approximates f well on $[-c, c]^n$; in other words

$$\max_{y \in [-c,c]^n} |f(y) - p(y)| \leq \frac{\epsilon}{2}$$

Therefore,

$$|\mathbb{E}[f(\mathbf{X})] - f(0)| \leq \frac{\epsilon}{2} + |\mathbb{E}[f(\mathbf{X})] - p(0)| = \frac{\epsilon}{2} + |\mathbb{E}[f(\mathbf{X}) - p(\mathbf{X})]|$$

(the equality follows from p being of degree $(k-1)$ and $\mathbf{X}$ being $(k-1)$-wise independent)

$$\leq \frac{\epsilon}{2} + \mathbb{E}\left[|f(\mathbf{X}) - p(\mathbf{X})|\right] \leq \epsilon$$

and our distribution $\mathbf{X}$ is actually a PRG as desired. Its $(c_k(\epsilon/2, \mathcal{F}))^2$-noticeability is also clear from its definition. ■

5.2 Approximation by Low-Degree Polynomials

Recall our goal is to approximate f well by a low-degree polynomial over the range $\mathbf{x} \in [-c, c]^n$ (as formalized in Theorem 11). We begin by bounding the magnitude of a degree-k component in terms of the level-k absolute Fourier sum as follows:

Lemma 11 ([CGL$^+$21])**.** *Let $\mathcal{F}$ be closed under restrictions and denote conv($\mathcal{F}$) the convex closure of $\mathcal{F}$. Let f_k denote the degree-k component of f. Then for all $f \in$ conf($\mathcal{F}$), $c \in (0, 1)$, $\mathbf{x} \in [-c, c]^n$, we have*

$$|f_k(\mathbf{x})| \leq c^k M_k(\mathcal{F})$$

Proof. Reparameterize $x = cy$, so $y \in [-1, 1]^n$. Because f_k is homogenous,

$$|f_k(x)| = c^k |f_k(y)| \leq c^k M_k(\mathrm{conv}(\mathcal{F})) = c^k M_k(\mathcal{F})$$

■

We will also need the following basic analysis fact:

Lemma 12 ([CGL$^+$21])**.** *For multilinear $f : \mathbb{R}^n \to \mathbb{R}$ and $\mathbf{x} \in \mathbb{R}^n$, define $g(t) = f(t\mathbf{x})$. Then*

$$g^{(k)}(0) = k! \cdot f_k(\mathbf{x})$$

Proof. We first use multilinearity to write g in terms of the Fourier basis, i.e.

$$g(t) = \sum_{S \subseteq [n]} t^{|S|} \hat{f}(S) x^S$$

and then differentiate to find

$$g^{(k)}(t) = \sum_{S:|S|\geq k} \left(\prod_{i=0}^{k-1} (|S| - i) \right) t^{|S|-k} \hat{f}(S) \mathbf{x}^S$$

The theorem then follows from substituting $t = 0$ into the above expression. ■

We finally are ready to prove Theorem 11:

Proof of Theorem 11. Let $f \in \mathcal{F}$, $\mathbf{x} \in [-c, c]^n$, and let $g(t) = f(t\mathbf{x})$. We write $g(1)$ in terms of the Taylor expansion

$$g(1) = \sum_{i<k} \frac{g^{(i)}(0)}{i!} + R_k$$

where R_k is the error term written in Lagrange form

$$R_k = \frac{g^{(k)}(s)}{k!}$$

for some $s \in (0, 1)$. We see that by Theorem 12, the first term is just $f_{<k}$; hence, the last term $R_k = f_{\geq k}$, Therefore, it will suffice to show that

$$|R_k| \leq \max_{s\in(0,1)} \left| \frac{g^{(k)}(s)}{k!} \right| \leq \left(\frac{c}{1-c} \right)^k M_k(\mathcal{F})$$

Fix any $s \in (0, 1)$, and define $\tilde{f}(\mathbf{y}) = f(s\mathbf{x} + (1 - c)\mathbf{y})$ (remember that $\mathbf{x}$ was arbitrarily fixed and its definition determines g). Define $\tilde{g}(t) = \tilde{f}(t\mathbf{x}) = g(s + t(1 - c))$. Differentiating via the chain rule shows

$$(1 - c)^k g^{(k)}(s) = \tilde{g}^{(s)}(0)$$

and Lemma 12 gives

$$\tilde{g}^{(k)}(0) = k! \cdot \tilde{g}^{(k)}(\mathbf{x})$$

Hence, we get

$$|g^{(k)}(s)| = \left| \frac{\tilde{g}^{(k)}(0)}{(1-c)^k} \right| = \frac{k!}{(1-c)^k} \left| \tilde{f}_k(\mathbf{x}) \right| \tag{1}$$

As was crucially shown in the original polarizing random walks frameworks, closure under restrictions implies that $\tilde{f} \in \text{conv}(\mathcal{F})$. Therefore, we can conclude using Lemma 11 that

$$|\tilde{f}_k(\mathbf{x})| \leq c^k M_k(\mathcal{F})$$

Substituting this fact and dividing both sides by $k!$ in Equation 1 gives the desired inequality. ■

Thus, with this proof in hand, we may show that fractional pseudorandom generators, and by extensions standard pseudorandom generators, may be explicitly designed with classes of boolean functions with a single bounded Fourier coefficient.

6 Conclusion and Open Problems

Over the course of this survey, we have reviewed and summarized major works regarding the construction of standard pseudoradnom generators from fractional pseudorandom generators for class of boolean functions with bounded Fourier tails. We then reviewed works that further relaxed assumptions regarding bounds on Fourier tails.

We now conclude this literature survey by raising a set of open problems that remain unresolved. These problems are not exhaustive, but form a subset of problems that we believe are tractable enough for further research.

- **Can polarizing random walks be terminated early?** The authors of [CHHL19] require a random walk with $t = O(\log(n/\epsilon)/q)$ steps to design a standard PRG from a q-noticeable ϵ-fractional PRG. A natural question they raise is if there exist classes of boolean functions that can be fooled with $o(\log(n/\epsilon)/q)$ steps. As a preliminary step towards this resolution, the authors consider classes of boolean functions with certain "smoothness" properties(by invoking L-Lipschitz continuity). However, considering noise-stability of classes of boolean functions may yield insight into this direction.

- **Less independence?** The proof of that the random walk converges with high probability hinges on the fact that samples of a fractional PRG are drawn in a mutually-independent. A natural question is to ask if less independence suffices. One path to resolving this question can be by considering each coordinate-wise step of the random walk as an assignment of random variables for a threshold function. If mutually independent samples are used, this threshold function may correspond to an assignment of variables over a linear-threshold function. On the other hand, if samples are repeated in the walk, this threshold function may correspond to an assignment of variables over a *polynomial threshold function*.

- **Resolving weaker conjecture.** The authors of [CGL$^+$21] claim that to get non-trival pseudorandom generators for polynomials of superlogarithmic degree with nontrivial seed length, proving the following conjecture would suffice for $k \leq O(\log n)$:

  $$M_k(\mathcal{F}) \leq (poly(k, \log n) \cdot 2^{o(d)})^k$$

  Where $\mathcal{F}$ is the class of degree-d polynomials over $\mathbb{F}_2$ polynomials. Furthermore, they claim that to break the barrier, it suffices to prove this claim at level $k = 3$.

7 Acknowledgements

We thank Rocco Servedio and Yuhao Li for their generous support and extended guidance.

References

[CGL+21] Eshan Chattopadhyay, Jason Gaitonde, Chin Ho Lee, Shachar Lovett, and Abhishek Shetty. Fractional pseudorandom generators from any fourier level. In *Proceedings of the 36th Computational Complexity Conference*, CCC '21, Dagstuhl, DEU, 2021. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[CHHL19] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, and Shachar Lovett. Pseudorandom generators from polarizing random walks. *Theory of Computing*, 15(1):1–26, 2019.

[CHRT18] Eshan Chattopadhyay, Pooya Hatami, Omer Reingold, and Avishay Tal. Improved pseudorandomness for unordered branching programs through local monotonicity. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 363–375, 2018.

[HH23] Pooya Hatami and William Hoza. Theory of unconditional pseudorandom generators, Mar 2023.

[Kan14] Daniel M Kane. A polylogarithmic prg for degree 2 threshold functions in the gaussian setting. *arXiv preprint arXiv:1404.1103*, 2014.

[O'D21] Ryan O'Donnell. Analysis of boolean functions, 2021.

[RT22] Ran Raz and Avishay Tal. Oracle separation of bqp and ph. *ACM Journal of the ACM (JACM)*, 69(4):1–21, 2022.

[TS17] Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 238–251, 2017.