Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 121 (2020)

Fractional Pseudorandom Generators from Any Fourier Level

Eshan Chattopadhyay*
Cornell University
eshanc@cornell.edu

Jason Gaitonde†
Cornell University
jsg355@cornell.edu

Chin Ho Lee‡
Columbia University
c.h.lee@columbia.edu

Shachar Lovett§
University of California, San Diego
slovett@cs.ucsd.edu

Abhishek Shetty¶
Cornell University
shetty@cs.cornell.edu

August 16, 2020

Abstract

We prove new results on the polarizing random walk framework introduced in recent works of Chattopadhyay et al. [CHHL19, CHLT19] that exploit L_1 Fourier tail bounds for classes of Boolean functions to construct pseudorandom generators (PRGs). We show that given a bound on the k-th level of the Fourier spectrum, one can construct a PRG with a seed length whose quality scales with k. This interpolates previous works, which either require Fourier bounds on all levels [CHHL19], or has polynomial dependence on the error parameter in the seed length [CHLT19], and thus answers an open question in [CHLT19]. As an example, we show that for polynomial error, Fourier bounds on the first $O(\log n)$ levels is sufficient to recover the seed length in [CHHL19], which requires bounds on the entire tail.

We obtain our results by an alternate analysis of fractional PRGs using Taylor's theorem and bounding the degree-k Lagrange remainder term using multilinearity and random restrictions. Interestingly, our analysis relies only on the *level-k unsigned Fourier sum*, which is potentially a much smaller quantity than the L_1 notion in previous works. By generalizing a connection established in [CHH+20], we give a new reduction from constructing PRGs to proving correlation bounds.

Finally, using these improvements we show how to obtain a PRG for $\mathbb{F}_2$ polynomials with seed length close to the state-of-the-art construction due to Viola [Vio09], which was not known to be possible using this framework.

1 Introduction

A central pursuit in complexity theory is to understand the need of randomness in efficient computation. Indeed there are important conjectures (such as $\mathbf{P} = \mathbf{BPP}$) in complexity theory which state that one can completely remove the use of randomness without losing much in efficiency. While we are quite far from proving $\mathbf{P} = \mathbf{BPP}$, a rich line of work has focused on *derandomizing* simpler models of computation (see Vadhan [Vad12] for a survey of prior work on derandomization). A key tool for proving such derandomization results is through the notion of a *pseudorandom generator* defined as follows.

*Supported by NSF grant CCF-1849899.
†Supported by NSF grant CCF-1408673 and AFOSR grant F5684A1.
‡Supported by a fellowship from the Croucher Foundation and by the Simons Collaboration on Algorithms and Geometry.
§Supprted by NSF grants CCF-02006443 and DMS-1953928.
¶Supported by a Cornell University Fellowship and a JP Morgan Chase Faculty Fellowship.

ISSN 1433-8092

Definition 1.1. Let $\mathcal{F}$ be a class of n-variate Boolean functions. Then a *pseudorandom generator* (PRG) for $\mathcal{F}$ with error $\epsilon > 0$ is a random variable $\mathbf{X} \in \{-1,1\}^n$ such that for all $f \in \mathcal{F}$,

$$|\mathbb{E}_{\mathbf{X}}[f(\mathbf{X})] - \mathbb{E}_{\mathbf{U}_n}[f(\mathbf{U}_n)]| \leq \epsilon,$$

where $\mathbf{U}_n$ is the uniform distribution on $\{-1,1\}^n$. If $\mathbf{X} = G(\mathbf{U}_s)$ for some explicit function $G : \{-1,1\}^s \to \{-1,1\}^n$, then $\mathbf{X}$ has *seed length* s.

There is a long line of research on explicit constructions of PRGs (for various classes of Boolean functions) in the literature and it is well beyond our scope to survey prior work here. Instead, we focus on a recent line of work initiated by Chattopadhyay et al. [CHHL19, CHLT19] that provides a framework for constructing pseudorandom generators for any Boolean function class that exhibit Fourier tail bounds (we discuss this in more details in the next subsection; see Section 2.1 for a brief introduction to Fourier analysis of Boolean functions). This provides a unified PRG for several well-studied function classes such as small-depth circuits, low-sensitivity functions, and read-once branching programs that exhibit such Fourier tails. We discuss this new framework in Section 1.1, and present our results in Section 1.2.

1.1 The Polarizing Random Walk Framework

We now briefly explain the *polarizing random walk* framework introduced by [CHHL19]. The authors show that for classes of n-variate Boolean functions that are closed under restrictions, one can quite flexibly construct pseudorandom generators via a local-to-global principle that works as follows: it is sufficient to construct *fractional pseudorandom generators*, a notion that generalizes a PRG to allow the random variable $\mathbf{X}$ (in Definition 1.1) to be supported on the solid cube $[-1,1]^n$ so that it fools the multilinear expansion of each Boolean function in the class. Ideally, the variance of each coordinate of the random variable should be as large as possible while still provably fooling the class. Towards this, define a fractional PRG $\mathbf{X}$ to be p-noticeable if the variance in each of its coordinates is least p. (See Definition 2.5 for a formal definition of a fractional PRG.)

To construct the full pseudorandom generator, the authors give a random walk gadget that composes together independent copies of such a fractional generator as steps in a random walk that polarizes quickly to the Boolean hypercube. The analysis for how the error accumulates in this process relies on interpreting the intermediate points of this pseudorandom walk as an average of *random restrictions* of the original function; because the fractional generator locally fools the class, this interpretation shows that it does not incur much error at each intermediate step, and the rapid polarization shows that it does not take too many steps. Taken together, these two facts imply the resulting random variable successfully fools the class.

The above framework shows that if one can construct non-Boolean random variables, with sufficiently large variance in each coordinate, that can locally fool any function in the class, then one immediately obtains a pseudorandom generator using their random walk gadget. As these generators need not be Boolean, the construction of fractional pseudorandom generators is only easier than constructing pseudorandom generators. To that end, [CHHL19] further show how to construct such fractional pseudorandom generators for any class of functions satisfying *Fourier tail bounds*. Namely, they show that if every function in the class is such that the L_1 Fourier mass at each level $1 \leq k \leq n$ is at most b^k for some fixed $b \geq 1$, then one can construct a fractional pseudorandom generator for error ϵ with seed length $O(\log\log n + \log(1/\epsilon))$ and variance $\Theta(b^{-2})$ in each coordinate. Combining this fractional pseudorandom generator with their random walk gadget yields a pseudorandom generator with seed length $b^2 \cdot \mathrm{polylog}(n/\epsilon)$. As a result, if one can show that a function class admits nontrivial Fourier tail bounds, then the [CHHL19] construction immediately implies a pseudorandom generator. Some examples of classes of Boolean functions that exhibit such tail bounds include $\mathbf{AC}^0$ circuits with

the parameter $b = \text{poly}(\log n)$ [LMN89, Tal17], constant width read-once branching programs with $b = \text{poly}(\log n)$ [CHRT18], and low-sensitivity functions with $b = O(s)$ [GSW16, Tal17]. Using such Fourier bounds, [CHHL19] immediately gave a polylogarithmic seed length PRG for these function classes. It was also conjectured in [CHHL19] that the class of n-variate degree-d polynomials over $\mathbb{F}_2$ satisfy such tail bounds. We discuss this in more detail in Section 1.2.

In the work by [CHLT19], the authors show how to construct fractional pseudorandom generators using far fewer assumptions on the Fourier tails. Building on the analysis of the celebrated work of [RT19], which gave an oracle separation of **BQP** and **PH** (which itself relies on the [CHHL19] random walk framework), they show that one can use this same framework to obtain a pseudorandom generator with seed length depending only on bounds for the *second Fourier level* of the class. However, with these weaker assumptions, they require a different fractional PRG. To do this, they essentially derandomize the result of [RT19], which shows that classes of multilinear functions with low level-two Fourier mass cannot nontrivially distinguish between a suitable variant of the Forrelation distribution and the uniform distribution. It turns out that this can be interpreted via Itô's Lemma, which shows that the local behavior of a smooth function of Brownian motion is essentially determined by the first two derivatives [Wu20]. [CHLT19] show that one can derandomize this analysis by efficiently constructing fractional PRGs that simulate Gaussian random variables with small covariance using the best-known constructions of error-correcting codes. However, this construction incurs exponentially worse dependence on the error parameter in each fractional step to nearly sample sufficiently good Gaussian random variables. The final seed length that this framework obtains has the form $O((b^2/\epsilon)^{2+o(1)}\text{polylog}(n))$, where b^2 is the level-two Fourier mass of the class. Compared to [CHHL19], this yields exponentially worse dependence on the error, as well as quadratically worse dependence on the level-two mass (though [CHLT19] assume nothing about the rest of the Fourier levels).

1.2 Our Contribution

Given these two works, a very natural question (explicitly asked in [CHLT19]) is whether it is possible to interpolate between these constructions by assuming Fourier bounds on an intermediate level. Concretely, can this framework still succeed if one has Fourier control at just level-k? If the class further has such Fourier bounds up to and including level-k, can one interpolate between the seed lengths of [CHHL19] and [CHLT19]? Given Fourier bounds from level-1 up to k, what range of error $\epsilon > 0$ can the resulting PRG tolerate while maintaining polylogarithmic dependence on $1/\epsilon$ in the seed length (or put contrapositively, given a desired error $\epsilon > 0$, how many levels of Fourier bounds are sufficient to ensure that the seed length remains polylogarithmic in $1/\epsilon$)?

Moreover, the recent work by Chattopadhyay et al.[CHH+20] shows that the problem of bounding the level-two *unsigned Fourier sum*, defined by the absolute value of the sum of the Fourier coefficients instead of the sum of their absolute values (as in the definition of L_1 Fourier mass) that is required in [CHHL19, CHLT19], corresponds to the problem of bounding the covariance of the function class and the k-XOR of shifted majority functions. In particular, using this connection to this better-studied object, they explicitly ask whether it suffices to give bounds on the weaker Fourier quantity $M_2(\mathcal{F})$ (or more generally, $M_k(\mathcal{F})$, see Section 2 for the precise definition) to obtain pseudorandom generators. The reason for doing so is that for many classes of functions, we currently do not have strong enough L_1 Fourier tail bounds, like the class of low-degree polynomials over $\mathbb{F}_2$ (though see Section 4). However, if one can show this, one now reduces the construction of pseudorandom generators to proving weaker Fourier bounds, which are hopefully more amenable to known techniques and thereby making the problem easier.

In this work, we make progress on all of these questions, by providing a new analysis of the fractional pseudorandom generator of [CHHL19]. Informally, we show that by only assuming a bound on some

level-k Fourier quantity of the class, the [CHHL19] fractional pseudorandom generator will still be valid. Moreover, our analysis actually shows that the error term that is induced by the high-order component can be improved from $L_{1,k}(\mathcal{F})$ (the level-k Fourier mass) to $M_k(\mathcal{F})$ (the *level-k unsigned Fourier sum*, see Section 2), which is *a priori* significantly smaller. Here,

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

and

$$M_k(f) \triangleq \max_{\mathbf{x}\in[-1,1]^n} \left| \sum_{S:|S|=k} \hat{f}(S)\mathbf{x}^S \right| = \max_{\mathbf{x}\in\{-1,1\}^n} \left| \sum_{S:|S|=k} \hat{f}(S)\mathbf{x}^S \right|.$$

and $L_{1,k}(\mathcal{F})$ and $M_k(\mathcal{F})$ refer to the maximum of $L_{1,k}$ and M_k taken over functions in the class $\mathcal{F}$. Our main result is the following analysis of a fractional pseudorandom generator:

Theorem 1.1. *Let $\mathcal{F}$ be any class of n-variate Boolean functions that is closed under restrictions and negations. Suppose that $M_k(\mathcal{F}) \le b^k$ for some $b \ge 1$ and $k \ge 1$. Then for any $\epsilon > 0$, there exists an explicit $\Omega(\epsilon^{2/k}/b^2)$-noticeable fractional PRG for $\mathcal{F}$ with error ϵ and seed length $O(k \cdot \log(n))$.*[1]

Further, if it holds that $L_{1,i}(\mathcal{F}) \le b^i$ for all $1 \le i < k$, then the seed length can be improved to $O(\log\log(n) + \log k + \log(1/\epsilon))$.

Note that for some Boolean classes of great interest such as the class of low-degree $\mathbb{F}_2$ polynomials, Fourier tail bounds as required by [CHHL19] are not yet known and thus Theorem 1.1 allows us to leverage potentially much weaker bounds proved in [CHHL19] to construct a PRG with polylogarithmic dependence on n/ϵ in the seed length (see Theorem 1.3), almost matching the best known PRG due to Viola [Vio09]. As we discuss below, the results in [CHHL19, CHLT19] are not quite good enough to use known Fourier tail bounds to obtain such a PRG for the class of $\mathbb{F}_2$ polynomials.

Using the fractional pseudorandom generator from Theorem 1.1, we obtain the following consequences almost immediately from the random walk gadget of [CHHL19] (see Theorem 2.2):

1. **Pseudorandom Generators from Fourier Bounds at Level-k**: From our fractional pseudorandom generator, we show that the random walk framework yields nontrivial pseudorandom generators assuming Fourier bounds *just at* level-k of the associated class, with improvements if we assume bounds from level-1 *up to* level-k. The informal statement is the following:

   Theorem 1.2. *Let $\mathcal{F}$ be any class of n-variate Boolean that is closed under restrictions and negations. Suppose that $\mathcal{F}$ satisfies $M_k(\mathcal{F}) \le b^k$ for some $b \ge 1$ and $k > 2$. Then there exists an explicit pseudorandom generator for $\mathcal{F}$ for error ϵ with seed length $k \cdot b^{2+4/(k-2)}\mathrm{polylog}(n/\epsilon)/\epsilon^{2/(k-2)}$. The seed length can be improved if $L_{1,i}(\mathcal{F}) \le b^i$ for all levels $i \le k$.*

   See Theorem 3.7 for the precise statement. One immediate consequence is that if one has comparable Fourier bounds at level $k = 3$, one recovers the seed length in [CHLT19]. Further, from such a Fourier bound for just the level $k = 4$, one obtains quadratically better dependence on the error in the seed length (as well as polylogarithmic factors in n/ϵ) compared to [CHLT19]. In particular, given an appropriate Fourier bound of b^k on just some level $k \le \mathrm{polylog}(n)$, one obtains a pseudorandom generator with error ϵ with seed length $O(b^{2+4/(k-2)}\mathrm{polylog}(n/\epsilon)/\epsilon^{2/(k-2)})$.

[1] We remark that at this level of generality, this linear dependence on k is essentially necessary. Indeed, any Boolean function on n-variables has L_1 level-n mass at most 1, but one cannot hope to generically fool all Boolean functions simultaneously without using n bits.

We note that the fractional PRG from Theorem 1.1 cannot be converted into a PRG for $k = 1, 2$. Informally, this is because of the following reason: The number of steps one needs to take in the random walk gadget of [CHHL19] (with each step using an independent copy of the fractional PRG) scales roughly inversely with linearly with the size (variance in each coordinate) of the fractional PRG, and the error adds up from each step. As is clear from Theorem 1.1, for the size of the fractional PRG to scale sublinearly with the error, one requires $k > 2$. This leads to a non-trivial PRG when $k > 2$. See Remark 3.8 for more discussion.

2. **Pseudorandom Generators with Polylogarithmic Error Dependence from up to Level-k Bounds**: A simple corollary of our fractional pseudorandom generator is that one can recover the polylogarithmic dependence on $1/\epsilon$ from [CHHL19] if $\varepsilon \geq b \cdot \log n \cdot 2^{-O(k)}$ and we have Fourier bounds *up to* level-k.

   Corollary 1.1. *Let $\mathcal{F}$ be any class of n-variate Boolean functions that is closed under restrictions and negations. Suppose that for some level $k > 2$ and $b \geq 1$, we have $M_k(\mathcal{F}) \leq b^k$ and $L_{1,i}(\mathcal{F}) \leq b^i$ for $i < k$. Then, for any $\epsilon \geq b \cdot \log n \cdot 2^{-O(k)}$, there exists an explicit pseudorandom generator for $\mathcal{F}$ for error ϵ with seed length $O(b^2 \mathrm{polylog}(n/\epsilon))$.*

   This actually covers the analysis of [CHHL19] without requiring anything on the full Fourier tail, and addresses an open question of [CHLT19] asking how many levels of Fourier bounds one needs control of to regain polylogarithmic dependence on ε. In particular, if one requires error $\epsilon = 1/\mathrm{poly}(n)$, then it suffices to have Fourier bounds up to level $\Theta(\log(n))$ to get the same dependence.

We view this work as a proof-of-concept that it is indeed possible to interpolate between the two extremes of [CHHL19, CHLT19] in the polarizing random walk framework and obtain better results using weakened Fourier assumptions. We prove Theorem 1.1 in Section 3, from which Theorem 1.2 and Corollary 1.1 follow without much difficulty using the existing random walk technique of [CHHL19].

As a concrete possible application of this approach which would provably improve on these works, both [CHHL19] and [CHLT19] conjecture Fourier bounds on the L_1 mass of the class of $\mathbb{F}_2$ polynomials of degree at most d. The former conjectures that this class satisfies a tail bound of the form c_d^k for some constant c_d at all levels $1 \leq k \leq n$ (so as to apply their approach), while the latter conjectures just that the level-two L_1 mass is $O(d^2)$. While neither conjecture seems close yet to being resolved, one can imagine that should the latter be proved, it may be feasible to extend the analysis to achieve a bound of $(\mathrm{poly}(d))^k$ for $k = \Omega(1)$, or even more optimistically, $k = \Omega(\log n)$. The pseudorandom generator implied by the analysis here would thus apply and yield significantly improved seed length compared to [CHLT19], though we note that our generator does not actually apply if such a bound only holds at level $k = 2$. Such a result would imply a pseudorandom generator with improved seed length compared to [CHLT19] for $\mathbf{AC^0}[\oplus]$ (see the discussion in [CHLT19], using results of Razborov [Raz87] and Smolensky [Smo87, Smo93]). Finally note that we just need to bound the quantity M_k as opposed to $L_{1,k}$ required in prior works.

Nonetheless, our analysis here, coupled with weaker Fourier tail bounds obtained in [CHHL19], immediately implies the following:

Theorem 1.3. *Let $\mathcal{F}$ be the class of degree-d polynomials over $\mathbb{F}_2$ on n variables. Then there exists an explicit pseudorandom generator for $\mathcal{F}$ with error ϵ and seed length $2^{O(d)}\mathrm{polylog}(n/\epsilon)$.*

See Section 4 for the precise dependences in the seed length. While this result does not quite match the current state-of-the-art PRG for this class due to Viola [Vio09] (and similarly, fails to give anything nontrivial for $d = \Omega(\log n)$), we view this as a conceptual contribution that the random walk framework can yield an explicit pseudorandom generator with error dependence that is polylogarithmic

in n/ϵ, which was not previously known from [CHHL19] or [CHLT19]. The Fourier tail bounds that are sufficient for our analysis are too weak to be employed in [CHHL19], and leads to a quadratic error dependence in the level-two fractional pseudorandom generator by [CHLT19]. We present the proof of Theorem 1.3 in Section 4.

Moreover, as stated before, recent work [CHH+20] has shown that it is possible to deduce bounds on $M_2(\mathcal{F})$ using covariance bounds with the XOR of certain resilient functions. As we are able to show that bounds on such quantities imply pseudorandom generators, we give an analogous argument for an appropriate generalization of this result to $M_k(\mathcal{F})$ in Section 5, thus reducing the problem of constructing PRGs in this framework to proving correlation bounds.

1.3 Overview of Our Approach

To prove our results, we rely on an alternate, simple analysis of the fractional pseudorandom generator considered by [CHHL19], where they assume control on the entire Fourier tail, and then use their gadget construction to obtain the full pseudorandom generator. As this latter part can be done in an entirely black-box fashion, we need only focus on the former. For this first part, their approach is the following: consider a random variable $\mathbf{X}$. By writing out f in the multilinear (Fourier) expansion, one has

$$|\mathbb{E}_{\mathbf{X}}[f(\mathbf{X})] - \mathbb{E}_{\mathbf{U}_n}[f(\mathbf{U}_n)]| = \Big|\mathbb{E}_{\mathbf{X}}\Big[\sum_{\emptyset \neq S \subseteq [n]} \hat{f}(S)\mathbf{X}^S\Big]\Big| \tag{1}$$

$$\leq \underbrace{\sum_{i=1}^{k-1} \sum_{S\subseteq[n]:|S|=i} |\hat{f}(S)||\mathbb{E}_{\mathbf{X}}[\mathbf{X}^S]|}_{\text{low-order terms}} + \underbrace{\sum_{i=k}^{n} \sum_{S\subseteq[n]:|S|=i} |\hat{f}(S)||\mathbb{E}_{\mathbf{X}}[\mathbf{X}^S]|}_{\text{high-order terms}}, \tag{2}$$

where we used the triangle inequality in (2). [CHHL19] use two different methods to control each component in (2); the first part is handled by sufficiently strong independence in the coordinates, while the latter is handled by physical smallness of the random variable. To control the low-degree terms, they require $\mathbf{X}$ to be $O(\epsilon)$-almost k-wise independent. By definition, this forces the biases of all the Fourier characters to be small in the low-order component. To deal with the higher-order component, they use the fact that $\mathbf{X}$ *need not be Boolean*; that is, they can scale any such distribution down. Because they assume that the Fourier mass on each level-k is bounded by b^k, it suffices to scale down a $\{\pm 1\}^n$ valued random variable by $\Theta(1/b)$, forcing the higher-order error terms to form a geometric series. One can show that to balance these terms, one may take the threshold at $k = \Theta(\log(1/\epsilon))$ to ensure that this yields ϵ error and seed length $O(\log\log n + \log(1/\epsilon))$ using known explicit constructions of almost k-wise independent distributions.

Our analysis of this fractional PRG is instead driven by exploiting Taylor's theorem, multilinearity, and the technique of random restrictions that is used critically in [CHHL19]. The general approach of using Taylor's theorem in the construction of PRGs has been quite fruitful. The typical way in which it is used is to write some smooth function to be fooled as a low-degree polynomial, which is relatively easy to fool, plus an error term bounded by the next derivatives of the function which ideally is negligible; this approach is often tied to *invariance principles*. We do the same decomposition, which initially agrees with [CHHL19]:

$$|\mathbb{E}_{\mathbf{X}}[f(\mathbf{X})] - \mathbb{E}_{\mathbf{U}}[f(\mathbf{U})]| \leq \underbrace{\sum_{i=1}^{k-1} \sum_{S\subseteq[n]:|S|=i} |\hat{f}(S)||\mathbb{E}_{\mathbf{X}}[\mathbf{X}^S]|}_{\text{low-order terms}} + \underbrace{|\mathbb{E}_{\mathbf{X}}[R_k(\mathbf{X})]|}_{\text{high-order term}}, \tag{3}$$

where our higher order term arises from Taylor's theorem. Naïvely, if one wanted to analyze the quality of a fractional PRG for the multilinear expansion of f using Taylor's theorem, this might do precisely nothing; indeed, the multilinear expansion of f is by definition a polynomial, so is equal to its Taylor series. Therefore, "using Taylor's theorem" would give exactly nothing but the original [CHHL19] approach! To get anything different than [CHHL19], we must truncate the Taylor series up to some level $k-1$ (which exactly agrees up to level $k-1$ with the multilinear expansion) and then study the error term, which is given by some k-th order derivatives of the Fourier expansion. The hope in doing this is that implicitly, Taylor's Theorem collapses the higher-order terms into level-k derivatives. One might then hope that there are significant sign cancellations that thus avoid the use of the complete Fourier tail assumption and triangle inequality as in (2). In particular, we only pay the triangle inequality at level-k by doing so, though we now must study these new error terms.

If these derivatives in the error term were evaluated at the origin $\mathbf{0} \in \mathbb{R}^n$, then we would immediately be able to bound the entire error term by any level-k bounds on our class $\mathcal{F}$. This is because these derivatives at $\mathbf{0}$ are precisely the level-k Fourier coefficients. However, the remainder term is evaluated at some intermediate point on the line between $\mathbf{0}$ and the realization of the supposed fractional PRG $\mathbf{X}$. It turns out, though, that using the closure of the class under restrictions and negations, one can obtain an upper bound on this quantity using just the weaker Fourier quantity $M_k(\mathcal{F})$.

To obtain pseudorandom generators, we then need only apply the random walk gadget of [CHHL19]. We refer the reader to Section 3 for formal proofs of the ideas sketched in this section.

Remark 1.2. *A previous version of this paper took an alternate approach that works as follows: by multilinearity, one can evaluate the error term in the Taylor expansion at the corner of some cube. By leveraging known connections between these derivatives and* $\mathbf{p}$*-biased Fourier coefficients (see, for instance, Chapter 8 of [O'D14]), one can then apply a result of Keller [Kel12] that reduces bounds on the resulting* L_1 *mass of these biased coefficients at level-*k *to the unbiased* L_1 *Fourier mass of some new function defined on* $2n$ *variables that roughly simulates biased bits. For many classes, this reduction comes at little loss in known Fourier bounds, but requires awkward bounds on* an associated class of functions*. While this result still manages to partially interpolate between the previous approaches in [CHHL19, CHLT19], as well as give a new PRG for the class of low-degree* $\mathbb{F}_2$ *polynomials, our new approach removes this artificial caveat, as well as allows for the weaker Fourier requirements via* $M_k(\mathcal{F})$ *as opposed to* $L_{1,k}(\mathcal{F})$*.*

2 Preliminaries

As in [CHHL19] and [CHLT19], we study PRGs for classes $\mathcal{F}$ of n-variate Boolean functions that are closed under restriction and negation (that is, fixing any subset and flipping any subset of the bits of the variables yields a function that remains in the class).

2.1 Fourier Analysis

We briefly recall basic Fourier analysis: any Boolean function $f : \{-1,1\}^n \to \{-1,1\}$ admits a unique multilinear expansion, also known as the *Fourier expansion*, given by

$$f(\mathbf{x}) = \sum_{S \subseteq [n]} \hat{f}(S)\mathbf{x}^S, \tag{4}$$

where we write $\mathbf{x}^S \triangleq \prod_{i \in S} x_i$. The Fourier coefficient $\hat{f}(S)$ is given by

$$\hat{f}(S) = \mathbb{E}_{\mathbf{X} \sim \{-1,1\}^n}[f(\mathbf{X})\mathbf{X}^S].$$

For more on Fourier analysis of Boolean functions, see the excellent book by O'Donnell [O'D14]. One may thus extend the domain of f to $[-1,1]^n$, where $f(\mathbf{x})$ for arbitrary $\mathbf{x}$ is evaluated according to the expression in (4). Note that in this case, $f(\mathbf{0}) = \hat{f}(\emptyset) = \mathbb{E}_{\mathbf{U}_n}[f(\mathbf{U}_n)]$. One of the main parameters of interest from the Fourier expansion for this framework is the following:

Definition 2.1. The *level-k mass of a Boolean function* f is

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

and the *level-k mass of a class* $\mathcal{F}$ is $L_{1,k}(\mathcal{F}) \triangleq \max_{f\in\mathcal{F}} L_{1,k}(f)$.

In this work, we will show how to construct PRGs whose seed length depends on the following, smaller quantity:

Definition 2.2. For any multilinear polynomial $f : \mathbb{R}^n \to \mathbb{R}$ given by $f(\mathbf{x}) = \sum_{S\subseteq[n]} \hat{f}(S)\mathbf{x}^S$, define the level-$k$ part by

$$f_k(\mathbf{x}) \triangleq \sum_{S\subseteq[n]:|S|=k} \hat{f}(S)\mathbf{x}^S, \tag{5}$$

and further define $f_{<k}(\mathbf{x}) \triangleq \sum_{i=0}^{k-1} f_i(\mathbf{x})$ and $f_{\geq k}(\mathbf{x}) \triangleq \sum_{i=k}^{n} f_i(\mathbf{x})$. Then we define the *level-k absolute Fourier sum of* f by

$$M_k(f) \triangleq \max_{\mathbf{x}\in[-1,1]^n} \left| \sum_{S:|S|=k} \hat{f}(S)\mathbf{x}^S \right| = \max_{\mathbf{x}\in\{-1,1\}^n} \left| \sum_{S:|S|=k} \hat{f}(S)\mathbf{x}^S \right| \tag{6}$$

and analogously define $M_k(\mathcal{F}) \triangleq \max_{f\in\mathcal{F}} M_k(f)$ for a class $\mathcal{F}$.

Note that the equality arises by multilinearity, and clearly we have $M_k(f) \leq L_{1,k}(f)$ by the triangle inequality. Without loss of generality, we may further assume that our class is closed under flipping the image, i.e. we may suppose that $f \in \mathcal{F}$ if and only if $-f \in \mathcal{F}$; indeed, this transformation does not change either $L_{1,k}(f)$ or $M_k(f)$, and therefore the same bound on the class still holds when completing it to include all such functions. If this is the case, we get the more striking identity:

Lemma 2.1.

$$M_k(\mathcal{F}) = \max_{f\in\mathcal{F}} \sum_{S:|S|=k} \hat{f}(S) = \max_{f\in\mathcal{F}} f_k(\mathbf{1}). \tag{7}$$

To see this, simply note that, if $(f, \mathbf{z}) \in \mathcal{F} \times \{-1,1\}^n$ are maximizers in the definition of $M_k(\mathcal{F})$ (where we may now assume that sign is positive), then by replacing the function $f(\mathbf{x})$ with $g(\mathbf{x}) = f(\mathbf{x} \circ \mathbf{z})$, where $\circ$ denotes componentwise multiplication, we have

$$M_k(\mathcal{F}) = \left| \sum_{S:|S|=k} \hat{f}(S)\mathbf{z}^S \right| = \sum_{S:|S|=k} \hat{g}(S) = \max_{h\in\mathcal{F}} \sum_{S:|S|=k} \hat{h}(S). \tag{8}$$

In particular, it suffices to bound the *unsigned level-k Fourier sum* of such a class.

Lastly, we require the following notion:

Definition 2.3. Let $\mathcal{F}$ be a class of n-variate multilinear polynomials that is closed under restrictions and negations. Then define $\mathrm{conv}(\mathcal{F})$ as the convex closure of $\mathcal{F}$ i.e.

$$\mathrm{conv}(\mathcal{F}) \triangleq \left\{ \sum_{f\in\mathcal{F}} \lambda_f f \,\middle|\, \sum_{f\in\mathcal{F}} \lambda_f = 1, \lambda_f \geq 0 \ \forall f \in \mathcal{F} \right\}. \tag{9}$$

We briefly note the following two elementary facts: first, by the assumption that $\mathcal{F}$ is closed under restrictions and negations, the same is true of $\mathrm{conv}(\mathcal{F})$. Moreover, we have $M_k(\mathcal{F}) = M_k(\mathrm{conv}(\mathcal{F}))$ by the triangle inequality.

2.2 (Fractional) Pseudorandom Generators

We now recall the (well-known) definition of a pseudorandom generator, as well as the generalization of a fractional pseudorandom generator as introduced by [CHHL19]:

Definition 2.4. Let $\mathcal{F}$ be a class of n-variate Boolean functions. Then a *pseudorandom generator* (PRG) for $\mathcal{F}$ with error $\epsilon > 0$ is a random variable $\mathbf{X} \in \{-1,1\}^n$ such that for all $f \in \mathcal{F}$,

$$|\mathbb{E}_{\mathbf{X}}[f(\mathbf{X})] - \mathbb{E}_{\mathbf{U}_n}[f(\mathbf{U}_n)]| \leq \epsilon,$$

where $\mathbf{U}_n$ is the uniform distribution on $\{-1,1\}^n$. If $\mathbf{X} = G(\mathbf{U}_s)$ for some explicit function $G : \{-1,1\}^s \to \{-1,1\}^n$, then $\mathbf{X}$ has *seed length* s.

Definition 2.5. A *fractional pseudorandom generator* (fractional PRG) for $\mathcal{F}$ with error $\epsilon > 0$ is a random variable $\mathbf{X} \in [-1,1]^n$ such that for all $f \in \mathcal{F}$ (identifying f with its multilinear expansion)

$$|\mathbb{E}_{\mathbf{X}}[f(\mathbf{X})] - f(\mathbf{0})| \leq \epsilon,$$

where the definition of seed length is the same. A fractional PRG is *p-noticeable* if for each $i \in [n]$, $\mathbb{E}[\mathbf{X}_i^2] \geq p$.

We now state the main results of [CHHL19] and [CHLT19] that show how to construct PRGs from suitably combining noticeable fractional PRGs. This is done by the following *amplification theorem*, which roughly composes fractional random variables into a random walk inside the Boolean hypercube:

Theorem 2.2. *Suppose $\mathcal{F}$ is class of n-variate Boolean functions that is closed under restrictions, and that $\mathbf{X}$ is a p-noticeable fractional PRG with error ϵ and seed length s. Then there exists an explicit PRG for $\mathcal{F}$ with seed length $O(s \log(n/\epsilon)/p)$ and error $O(\epsilon \log(n/\epsilon)/p)$.*

Using this result, [CHHL19] proved the following theorem that exploits strong L_1 control of each Fourier level:

Theorem 2.3. *Let $\mathcal{F}$ be any class of n-variate Boolean functions that is closed under restrictions. Suppose that $L_{1,k}(\mathcal{F}) \leq b^k$ for some $b \geq 1$ and all $1 \leq k \leq n$. Then for any $\epsilon > 0$, there exists an explicit PRG for $\mathcal{F}$ with error ϵ and seed length $b^2 \cdot \mathrm{polylog}(n/\epsilon)$.*

This is achieved by constructing a fractional PRG that is a scaled version of a nearly $\log(1/\epsilon)$-wise independent distribution. As we will be analyzing a similar fractional PRG, we defer the details to next section.

To lessen the requisite assumptions on the Fourier spectrum, [CHLT19] derandomize a construction of [RT19] to prove the following result that requires only level-two control, albeit at a cost of exponentially worse dependence on the error ε, and quadratically worse dependence on the level-two mass:

Theorem 2.4. *Let $\mathcal{F}$ be any class of n-variate Boolean functions that is closed under restrictions. Suppose that $L_{1,2}(\mathcal{F}) \leq b^2$ for some $b \geq 1$. Then for any $\epsilon > 0$, there exists an explicit PRG for $\mathcal{F}$ with error ϵ and seed length $O((b^2/\varepsilon)^{2+o(1)}\mathrm{polylog}(n))$.*

3 Fractional PRGs from the k-th Fourier Level

We now turn to the proof of our main result yielding a fractional pseudorandom generator from level-k bounds, Theorem 1.1. Throughout the remainder of this section, we assume that $\mathcal{F}$ is closed under restrictions and negations of variables. We restate the result here:

Theorem 3.1 (Theorem 1.1, restated)**.** *Let $\mathcal{F}$ be any class of n-variate Boolean functions that is closed under restrictions and negations. Suppose that $M_k(\mathcal{F}) \leq b^k$ for some $b \geq 1$ and $k > 2$. Then for any $\epsilon > 0$, there exists a $\Omega(\epsilon^{2/k}/b^2)$-noticeable explicit fractional PRG for $\mathcal{F}$ with error ϵ and seed length $O(k \cdot \log(n))$.*

If it further holds that $L_{1,i}(\mathcal{F}) \leq b^i$ for all $1 \leq i < k$, then the seed length can be improved to $O(\log\log(n) + \log k + \log(1/\epsilon))$.

To set up the proof of this theorem, we require some auxilliary results. The main technical claim we need is the following, which bounds the error term we will encounter using the quantity $M_k(\mathcal{F})$ we defined before (Definition 2.2).

Lemma 3.2. *Let $f \in \mathcal{F}$. Then for all $c \in (0,1)$, we have*

$$\max_{\mathbf{x} \in [-c,c]^n} |f_{\geq k}(\mathbf{x})| \leq \left(\frac{c}{1-c}\right)^k M_k(\mathcal{F}). \tag{10}$$

To prove this lemma, we require the following simple results. The first simply shows that we may always bound the contribution of the level-k part of any function in $\mathcal{F}$ by simply rescaling the argument:

Lemma 3.3. *Let $f \in \mathrm{conv}(\mathcal{F})$. Then, for all $c \in (0,1)$ and $\mathbf{x} \in [-c,c]^n$, we have*

$$|f_k(\mathbf{x})| \leq c^k M_k(\mathcal{F}). \tag{11}$$

Proof. Simply observe that $c^{-1}\mathbf{x} \in [-1,1]^n$ by assumption, and by homogeneity of f_k as a polynomial, we have

$$|f_k(\mathbf{x})| = c^k |f_k(c^{-1}\mathbf{x})| \leq c^k M_k(\mathrm{conv}(\mathcal{F})) = c^k M_k(\mathcal{F}). \tag{12}$$

□

The next simple, but powerful, claim simply shows that one can "recenter" functions in $\mathcal{F}$ and remain in $\mathrm{conv}(\mathcal{F})$ (and therefore, enjoy the same Fourier bounds). This random restriction technique is a key tool in [CHHL19]:

Lemma 3.4. *Let $f \in \mathrm{conv}(\mathcal{F})$ and $\mathbf{a}, \mathbf{b} \in [-1,1]^n$ such that $|a_i| + |b_i| \leq 1$ for all $i \in [n]$. Define $\tilde{f}$ by $\tilde{f}(\mathbf{x}) = f(\mathbf{a} + \mathbf{b} \circ \mathbf{x})$, where $\circ$ denotes componentwise multiplication. Then, $\tilde{f} \in \mathrm{conv}(\mathcal{F})$.*

Proof. Given $\mathbf{a}, \mathbf{b}$, define a distribution D_i on $Z_i = \{-1, 1, x_i, -x_i\}$ where x_i is treated as formal variable, such that $\mathbb{E}_{y_i \sim D_i}[y_i] = a_i + b_i x_i$; note that this is possibly by the assumption that $|a_i| + |b_i| \leq 1$. Let $D = \prod_i D_i$ be the product distribution of the D_i. For any $\mathbf{z} \in \prod_i Z_i$, define $f_{\mathbf{z}}(\mathbf{x})$ as the function obtained by setting $x_i = z_i$ for each i; in particular, each variable gets set to ± 1 or remains a formal variable (or becomes the negation). By our assumption on the closure of $\mathcal{F}$, we clearly have $f_{\mathbf{z}} \in \mathcal{F}$ for any $\mathbf{z}$. By multilinearity and independence of the product distribution, we have $f(\mathbf{a} + \mathbf{b} \circ \mathbf{x}) = \mathbb{E}_{\mathbf{z} \sim D}[f_{\mathbf{z}}(\mathbf{x})]$. Thus $\tilde{f} \in \mathrm{conv}(\mathcal{F})$. □

As mentioned before, our fundamental approach will be to bound the higher-order terms of the Fourier expansion at the fractional points of the fractional generator via the error term that arises in Taylor's theorem. Denote by $h^{(k)}$ the k-th derivative of any C^k function $h : \mathbb{R} \to \mathbb{R}$. We then have the following claim:

Lemma 3.5. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be multilinear and let $\mathbf{x} \in \mathbb{R}^n$. Define $g : \mathbb{R} \to \mathbb{R}$ by $g(t) = f(t\mathbf{x})$. Then,*

$$g^{(k)}(0) = k! \cdot f_k(\mathbf{x}). \tag{13}$$

Proof. From the definition, it follows that

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

Differentiating with respect to t, we get

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

Setting $t = 0$ eliminates all of the monomials with $|S| > k$, giving us the required bound. □

Finally, we connect the function defined in the previous part with our assumed Fourier bounds:

Lemma 3.6. *Let $f \in \mathrm{conv}(\mathcal{F})$, $c \in (0,1)$ and $\mathbf{x} \in [-c,c]^n$. Define g as in Lemma 3.5. Then,*

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

Proof. Fix $s \in [0,1]$ and let $\lambda = 1 - c$. Define the auxiliary function $\tilde{f}(\mathbf{y}) = f(s\mathbf{x} + \lambda \mathbf{y})$. Writing $\mathbf{a} = s\mathbf{x}$ and $\mathbf{b} = (\lambda, \ldots, \lambda)$, we clearly have $s|x_i| + |\lambda| \leq 1$, so we may apply Lemma 3.4 to see that $\tilde{f} \in \mathrm{conv}(\mathcal{F})$. Now writing $\tilde{g}(t) = \tilde{f}(t\mathbf{x}) = f(s\mathbf{x} + \lambda t \mathbf{x})$, we also have $\tilde{g}(t) = g(s + t\lambda)$. By the chain rule, differentiating both sides k times and then setting $t = 0$,

$$\lambda^k g^{(k)}(s) = \tilde{g}^{(k)}(0). \tag{14}$$

On the other hand, by Lemma 3.5, we have $\tilde{g}^{(k)}(0) = k! \cdot \tilde{f}_k(\mathbf{x})$, and as $\tilde{f} \in \mathrm{conv}(\mathcal{F})$ by Lemma 3.4, we conclude using Lemma 3.3 that

$$g^{(k)}(s) = \frac{\tilde{g}^{(k)}(0)}{\lambda^k} \leq \left(\frac{c}{1-c} \right)^k \cdot k! \cdot M_k(\mathcal{F}), \tag{15}$$

as desired. □

With these in order, we can finally return to the proof of Lemma 3.2:

Proof of Lemma 3.2. Let $f \in \mathcal{F}, \mathbf{x} \in [-c,c]^n$ and define $g(t) = f(t\mathbf{x})$. Then, by Taylor expanding about $t = 0$ and evaluating at $t = 1$, we have

$$g(1) = \sum_{i<k} \frac{g^{(i)}(0)}{i!} + R_k, \tag{16}$$

where R_k is the error term and is given in Lagrange form by

$$R_k = \frac{g^{(k)}(s)}{k!} \tag{17}$$

for some $s \in [0,1]$. By Lemma 3.5, we easily see that the first term is precisely $f_{<k}(\mathbf{x})$, and as $g(1) = f(\mathbf{x})$, we clearly then must have $R_k = f_{\geq k}(\mathbf{x})$. But by Lemma 3.6, we obtain

$$|f_{\geq k}(\mathbf{x})| = \left| \frac{g^{(k)}(s)}{k!} \right| \leq \left(\frac{c}{1-c} \right)^k M_k(\mathcal{F}), \tag{18}$$

as desired. □

With these technical results in place, we now have everything we need to easily prove Theorem 1.1.

Proof of Theorem 1.1. Fix $f \in \mathcal{F}$, and let $\mathbf{X}$ be an arbitrary random variable such that $|\mathbf{X}_i| = x \leq 1/2$ for all i for some $x > 0$ we specify momentarily. Then we have, via the Fourier expansion,

$$|\mathbb{E}_{\mathbf{X}}[f(\mathbf{X})] - f(\mathbf{0})| = \left|\mathbb{E}_{\mathbf{X}}\left[\sum_{S\subseteq[n]:1\leq|S|\leq k-1} \hat{f}(S)\mathbf{X}^S\right]\right| + |\mathbb{E}_{\mathbf{X}}[f_{\geq k}(\mathbf{X})]|.$$

To deal with the second term, by Lemma 3.2, we have

$$|\mathbb{E}_{\mathbf{X}}[f_{\geq k}(\mathbf{X})]| \leq \left(\frac{x}{1-x}\right)^k M_k(\mathcal{F}). \tag{19}$$

By assumption, $M_k(\mathcal{F}) \leq b^k$ for some $b \geq 1$; therefore, by taking $x = \Theta(\epsilon^{1/k}/b)$, this term is at most $\epsilon/2$.

To deal with the lower order terms, we take the same approach as [CHHL19]. If no assumptions are made on the level-j mass for $j < k$, then one may take $\mathbf{X} = x \cdot \mathbf{Y}$, where $\mathbf{Y} \in \{-1, 1\}^n$ is $(k-1)$-wise independent to incur zero error on the lower order terms. This has seed length $O(k \log(n))$ [Vad12] and gives no additional error. Note that then $\mathbf{X}$ is $\Theta(\epsilon^{2/k}/b^2)$-noticeable.

If one further assumes that $L_{1,i}(\mathcal{F}) \leq b^i$ for all $i < k$, then one may apply their same analysis and instead let $\mathbf{X} = x \cdot \mathbf{Y}'$, where $\mathbf{Y}'$ is an $(\epsilon/2)$-almost $(k-1)$-wise independent distribution. Then, exactly as in [CHHL19]:

$$\left|\mathbb{E}_{\mathbf{X}}\left[\sum_{S\subseteq[n]:1\leq|S|\leq k-1} \hat{f}(S)\mathbf{X}^S\right]\right| \leq \sum_{i=1}^{k-1} x^i \sum_{S:|S|=i} |\hat{f}(S)||\mathbb{E}[\mathbf{Y}'^S]| \leq (\epsilon/2)\sum_{i=1}^{k-1}(bx)^i \leq \epsilon/2, \tag{20}$$

as we choose x such that $(bx) \leq 1/2$. By standard constructions, such a random variable can be efficiently sampled with seed length $O(\log\log(n) + \log k + \log(1/\epsilon))$ [NN93]. Combining these two errors yields the claim. Again, $\mathbf{X}$ remains $\Theta(\epsilon^{2/k}/b^2)$-noticeable. □

3.1 From Fractional Generators to PRGs

Using Theorem 1.1 and Theorem 2.2, it is fairly immediate to obtain PRGs that rely only on level-k bounds. Similarly, bounds on levels up to k can be leveraged to get an improved seed length.

Theorem 3.7 (Theorem 1.2, restated)**.** *Let $\mathcal{F}$ be any class of n-variate Boolean functions that is under restrictions and negations. Suppose that $M_k(\mathcal{F}) \leq b^k$ for some $b \geq 1$ and $k > 2$. Then for any $\epsilon > 0$, there exists an explicit PRG for $\mathcal{F}$ with error ϵ with seed length*

$$s = O\left(\frac{b^{2+\frac{4}{k-2}} \cdot k \cdot \log(n) \log^{1+\frac{2}{k-2}}(n/\epsilon)}{\epsilon^{\frac{2}{k-2}}}\right). \tag{21}$$

If it further holds that $L_{1,i}(\mathcal{F}) \leq b^i$ for all $1 \leq i < k$, then the seed length can be improved to

$$s = O\left(\frac{b^{2+\frac{4}{k-2}} \cdot (\log\log n + \log k + \log(b/\epsilon)) \cdot \log^{1+\frac{2}{k-2}}(n/\epsilon)}{\epsilon^{\frac{2}{k-2}}}\right). \tag{22}$$

Proof. By Theorem 2.2, given an explicit p-noticeable fractional PRG for $\mathcal{F}$ with error δ and seed length s, one immediately obtains an explicit PRG for $\mathcal{F}$ with error $O(\delta \log(n/\delta)/p)$ and seed length $O(s \log(n/\delta)/p)$.

For the first statement, by our assumption and using the fractional PRG guaranteed by Theorem 1.1, for any $\delta > 0$, we immediately obtain an explicit PRG for $\mathcal{F}$ with error $O(b^2\delta^{1-2/k}\log(n/\delta))$ and seed length $O(b^2 k \log(n)\log(n/\delta)/\delta^{2/k})$. To get the error below ϵ, we set

$$\delta = \Theta\left(\left(\frac{\epsilon}{b^2\log(n/\epsilon)}\right)^{\frac{k}{k-2}}\right) \tag{23}$$

(the astute reader may notice we implicitly use $b \leq n$ here). This yields a PRG with error ϵ and seed length

$$s = O\left(\frac{b^{2+\frac{4}{k-2}} \cdot k \cdot \log(n)\log^{1+\frac{2}{k-2}}(n/\epsilon)}{\epsilon^{\frac{2}{k-2}}}\right). \tag{24}$$

The second statement follows in an identical manner from using the improved seed length from the second part of Theorem 1.1 in the case that one has control on the L_1 Fourier mass on the lower levels. □

Corollary 1.1 is now an immediate consequence of Theorem 3.7; for any desired $\epsilon > b\cdot\log(n)\cdot 2^{-O(k)}$, one can simply apply Theorem 3.7 using level $k = \Theta(\log(b\log(n)/\epsilon))$ to obtain a PRG for $\mathcal{F}$ with error at most ϵ with seed length

$$s = O(b^2 \cdot \log(b\log(n)/\epsilon)\cdot\log(n/\epsilon)). \tag{25}$$

Note that if $\epsilon = 1/\mathrm{poly}(n)$, then this means that one needs bounds only up to level $\Theta(\log(n))$ (again, using the fact that $b \leq n$). This also partially answers an open question of [CHLT19], which asks how many levels of Fourier bounds suffice to recover polylogarithmic dependence in $1/\varepsilon$.

Remark 3.8. *Note that this Taylor approach does not yield anything nontrivial given just level-two bounds, unlike the fractional generator in [CHLT19]. This is actually a necessary byproduct of combining this approach with the random walk gadget of [CHHL19]. Given only level-two bounds, this approach attempts to use j-wise independence for $j < k = 2$ and smallness to deal with errors on the high degree terms ($k \geq 2$). However, the trivial random variable that is $\pm\mathbf{1}$ with equal probability is trivially 1-wise independent, as each component is a uniform random bit, albeit trivially correlated. No matter how we scale them, one can show that composing arbitrarily many independent copies of this random variable via the random walk gadget will necessarily polarize to $\pm\mathbf{1}$ at termination, which clearly cannot fool nontrivial functions.*

4 Low-Degree Polynomials over $\mathbb{F}_2$

Our analysis recovers all the existing applications of [CHHL19] (among them, $\mathbf{AC}^0$ circuits, low-sensitivity functions, and read-once branching programs); indeed, all the classes considered there satisfy L_1 Fourier bounds on the entire tail. To our knowledge, our new analysis does not immediately improve the seed lengths obtained there, though it shows (i) *the seed lengths there can potentially be improved using stronger bounds on M_k*, and (ii) *the analysis would still have been valid had these Fourier bounds been known only up to some level k.*

However, the generality afforded to us by this new analysis allows us to obtain a new PRG for low-degree polynomials over $\mathbb{F}_2$, which addresses an open question of [CHHL19] by showing that this framework can handle this class. Indeed, let $\mathcal{F}$ be the set of n-variate, degree-d polynomials over $\mathbb{F}_2$. As a preliminary step towards deriving Fourier tail bounds that would imply a nontrivial PRG for this class using their framework, [CHHL19] prove the following Fourier bounds:

Proposition 4.1 (Theorem 6.1 of [CHHL19])**.** *Let $p : \mathbb{F}_2^n \to \mathbb{F}_2$ be a degree-d polynomial, and let $f(\mathbf{x}) = (-1)^{p(\mathbf{x})}$. Then $L_{1,k}(f) \leq (k \cdot 2^{3d})^k$.*

Note that this result cannot be applied to their original analysis, for they require a nontrivial bound at all levels, while this bound is trivial for $k = \Omega(\sqrt{n})$ and any d. While Theorem 2.4 can yield a nontrivial PRG by just applying the level-two bound, the dependence on $1/\epsilon$ is at least quadratic.[2] However, using our new, more flexible analysis, one can obtain a nontrivial PRG with polylogarithmic dependence on the error parameter. Our formal result is the following:

Theorem 4.2. *Let $\mathcal{F}$ be the class of degree-d polynomials over $\mathbb{F}_2$ on n variables. Then there exists an explicit pseudorandom generator for $\mathcal{F}$ with error ϵ and seed length*

$$s = O(2^{O(d)} \cdot \log^3(\log(n)/\varepsilon) \cdot \log(n/\varepsilon)). \tag{26}$$

Proof. Fix $\varepsilon > 0$ and let $k = \Theta(\log(\log(n)/\varepsilon))$. By Proposition 4.1, we have that for all $j \leq k$,

$$L_{1,j}(\mathcal{F}) \leq (\Theta(\log(\log(n)/\varepsilon) \cdot 2^{3d}))^j. \tag{27}$$

By setting $b = \Theta(\log(\log(n)/\varepsilon) \cdot 2^{3d})$, we may apply Theorem 3.7 for $\mathcal{F}$ and error ε. Note that $\varepsilon^{-\Theta(1/\log(1/\varepsilon))} = O(1)$, so plugging in this value of b, we immediately obtain the desired pseudorandom generator. □

For comparison, the best known construction by Viola [Vio09], obtained by summing d independent copies of a sufficiently good small-biased space, attains seed length $d \cdot \log(n) + O(d \cdot 2^d \log(1/\varepsilon))$, which for constant ε and d is within an additive constant of the optimal possible seed. The generator implied by our analysis recovers this polylogarithmic dependence in n/ε, although with slightly worse dependence on $\log n$ and polynomially worse dependence in $\log(1/\varepsilon)$. Neither generator can handle superlogarithmic degree. While this result clearly falls short of the state-of-the-art, we emphasize that this generator is conceptually distinct from the existing constructions, and yet belongs to this generic random walk framework.

Our analysis allows us to exploit known Fourier bounds that are too weak for the existing analyses to obtain polylogarithmic error dependence. In particular, to get a nontrivial pseudorandom generator for polynomials of superlogarithmic degree with nontrivial seed length, our work shows that the following weaker conjecture would suffice to break the logarithmic degree barrier and still achieve polylogarithmic (in n) seed length for $\epsilon = 1/\mathrm{poly}(n)$:

Conjecture 4.3. *Let $\mathcal{F}$ be the class of degree-d polynomials over $\mathbb{F}_2$ on n variables. Then*

$$M_k(\mathcal{F}) \leq (\mathrm{poly}(k, \log n) \cdot 2^{o(d)})^k \tag{28}$$

for $k \leq O(\log n)$.

In fact, we observe that to break the logarithmic degree barrier, it actually suffices that this holds just at $k = 3$, though with poor dependence on ε. Note that this is a significantly weaker conjecture than positing that the same bounds hold for $L_{1,k}(\mathcal{F})$. Moreover, as we explain in the next section, $M_k(\mathcal{F})$ can be controlled using correlation bounds, which are much better studied than L_1 Fourier bounds.

[2] By applying this Fourier bound at level-two, one can use the fractional PRG of [CHLT19] to obtain seed length $2^{O(d)}\mathrm{polylog}(n)/\epsilon^{2+o(1)}$ using the random walks framework. This gives exponentially worse error dependence compared to our approach.

5 Bounds on $M_k(\mathcal{F})$ via Correlation with Shifted Majorities

As we have seen, this analysis allows for the construction of PRGs from the weaker quantity $M_k(\mathcal{F})$. In this section, we repeat the argument of [CHH+20] to show how bounds on $M_k(\mathcal{F})$ follow from covariance bounds with certain resilient functions (in particular, shifted majorities). In their paper, they deal with the case of $k = 2$; we rather straightforwardly generalize this argument, but stress that the approach is the same as in Section 6 of their paper. To that end, for convenience and consistency with their argument, we adopt their conventions and requisite definitions just for this section. We will now consider Boolean functions written as $f : \{0,1\}^n \to \{0,1\}$. Translating to this notation, for any such Boolean function, let $e(f)(\mathbf{x}) \triangleq (-1)^{f(\mathbf{x})}$. Then, letting $F = e(f)$, we now have $\hat{F}(S) = \mathbb{E}_{\mathbf{x}}[F(\mathbf{x})e(\sum_{i\in S} x_i)]$.

Definition 5.1. The *covariance between* f *and* g, where f, g are Boolean is

$$\mathrm{cov}(f,g) \triangleq |\mathbb{E}[e(f(\mathbf{x}))e(g(\mathbf{x}))] - \mathbb{E}[e(f(\mathbf{x}))]\mathbb{E}[e(g(\mathbf{x}))]|, \tag{29}$$

while the covariance between a function f and a class $\mathcal{G}$ is defined as $\mathrm{cov}(f,\mathcal{G}) \triangleq \max_{g\in\mathcal{G}} \mathrm{cov}(f,g)$.

For any $\mathbf{x} \in \{0,1\}^n$, we write $|\mathbf{x}|$ for the Hamming weight, i.e. $\sum_{i=1}^n x_i$. For any $a \in \{0,1,\ldots,n\}$, [CHH+20] define Maj_a by

$$\mathrm{Maj}_a(\mathbf{x}) \triangleq \begin{cases} 1 & \text{if } |\mathbf{x}| > a \\ 0 & \text{else,} \end{cases} \tag{30}$$

as well as the following associated functions for any $\theta \in [n/2]$:

$$\mathrm{Thr}_\theta(x) \triangleq \begin{cases} (-1)^{\mathrm{Maj}_{n/2}(\mathbf{x})} & \text{if } \big||\mathbf{x}| - n/2\big| > \theta \\ 0 & \text{else} \end{cases} \tag{31}$$

We now show the following lemma relating $M_k(\mathcal{F})$ with covariance bounds against k-XORs of these functions:

Lemma 5.1 (Lemma 6.1 of [CHH+20], adapted)**.** *Let $\mathcal{F}$ be any family of (kn)-variate Boolean functions that is closed under relabeling variables. Further, suppose that for any $a_1,\ldots,a_k$ such that $|a_i - n/2| = O(\sqrt{kn\log n})$ for all $i \in [k]$, and all $f \in \mathcal{F}$, we have for some $t \geq 1$*

$$\mathrm{cov}(f(\mathbf{x}_1,\ldots,\mathbf{x}_k), \oplus_{i=1}^k \mathrm{Maj}_{a_i}) \leq \left(\sqrt{\frac{t}{n}}\right)^k, \tag{32}$$

where $\mathbf{x}_i \in \{0,1\}^n$ and $\oplus$ denotes the XOR *function.*

Then, it holds that

$$M_k(\mathcal{F}) \leq O(\sqrt{tk\log n})^k. \tag{33}$$

To prove this lemma, [CHH+20] use the following sequence of claims.

Fact 5.1 (Claim 6.2 in [CHH+20])**.** *For any $f \in \mathcal{F}$, let $F(\mathbf{x}_1,\ldots,\mathbf{x}_k) = e(f(\mathbf{x}_1,\ldots,\mathbf{x}_k))$. Under the hypotheses of Lemma 5.1, for any $1 \leq a_1,\ldots,a_k \leq O(\sqrt{kn\log n})$,*

$$|\mathbb{E}_{\mathbf{x}_1,\ldots,\mathbf{x}_k}[(F(\mathbf{x}_1,\ldots,\mathbf{x}_k) - \mathbb{E}[F])\prod_{i=1}^k \mathrm{Thr}_{a_i}(\mathbf{x}_i)]| \leq \left(\sqrt{\frac{t}{n}}\right)^k. \tag{34}$$

.

Fact 5.2 (Claim 6.3 of [CHH+20])**.** *For any $\mathbf{x} \in \{0,1\}^n$, $\sum_{i=1}^n e(x_i) = 2\sum_{1\leq a\leq n/2} \mathrm{Thr}_a(\mathbf{x})$.*

Fact 5.3 (Claim 6.4 of [CHH+20], adapted)**.** *For any Boolean function $f : \{0,1\}^{kn} \to \{0,1\}$, there exists a k-equipartition of $[kn]$ into disjoint sets $S_1, \dots, S_k$ such that*

$$\left| \sum_{S \subseteq [kn] : |S| = k} \hat{f}(S) \right| \leq C^k \left| \sum_{i_j \in S_j \, \forall j \in [k]} \hat{f}(\{i_1, \dots, i_k\}) \right| \tag{35}$$

for some absolute constant $C > 0$.

As this fact is not quite identical to that in [CHH+20], we give an argument here:

Proof. We (effectively) use the probabilistic method: let $\mathcal{P}$ be the set of k-equipartitions of $[kn]$. Let $T \subseteq [kn]$ of size k be arbitrary; without loss of generality, suppose $T = [k]$. Consider a uniformly random k-equipartition $P = S_1 \sqcup \dots \sqcup S_k \in \mathcal{P}$. The probability that each $i \in T$ belong to distinct S_j is easily seen to be

$$\prod_{i=1}^{k-1} \frac{(k-i) \cdot n}{kn - i} \geq \frac{(k-1)! n^{k-1}}{(kn)^{k-1}} = \frac{(k-1)!}{k^{k-1}} = e^{-O(k)}, \tag{36}$$

where the last line uses Stirling's approximation. By symmetry, let $\alpha \in \mathbb{N}$ be the number of k-equipartitions that any arbitrary subset T is in. Then we have

$$\begin{aligned}
\alpha \left| \sum_{S \subseteq [kn] : |S| = k} \hat{f}(S) \right| &= \left| \sum_{P \in \mathcal{P}} \sum_{i_j \in S_j \, \forall j \in [k]} \hat{f}(\{i_1, \dots, i_k\}) \right| && (37) \\
&\leq \sum_{P \in \mathcal{P}} \left| \sum_{i_j \in S_j \, \forall j \in [k]} \hat{f}(\{i_1, \dots, i_k\}) \right| && (38) \\
&\leq |\mathcal{P}| \max_{P \in \mathcal{P}} \left| \sum_{i_j \in S_j \, \forall j \in [k]} \hat{f}(\{i_1, \dots, i_k\}) \right|. && (39)
\end{aligned}$$

The first line follows from simple counting, while the second is the triangle inequality. Rearranging, we deduce that (writing T as a generic subset of size k)

$$\begin{aligned}
\left| \sum_{S \subseteq [kn] : |S| = k} \hat{f}(S) \right| &\leq \frac{|\mathcal{P}|}{\alpha} \max_{P \in \mathcal{P}} \left| \sum_{i_j \in S_j \, \forall j \in [k]} \hat{f}(\{i_1, \dots, i_k\}) \right| && (40) \\
&= \Pr_{P \sim \mathcal{P}}(T \in P)^{-1} \max_{P \in \mathcal{P}} \left| \sum_{i_j \in S_j \, \forall j \in [k]} \hat{f}(\{i_1, \dots, i_k\}) \right| && (41) \\
&\leq e^{O(k)} \max_{P \in \mathcal{P}} \left| \sum_{i_j \in S_j \, \forall j \in [k]} \hat{f}(\{i_1, \dots, i_k\}) \right|. && (42)
\end{aligned}$$

□

The last fact that is needed can be deduced from the Chernoff bound:

Fact 5.4 (Claim 6.5 of [CHH+20], adapted)**.** *For any $a \geq \Omega(\sqrt{kn \log n})$, $\mathbb{E}[|\mathrm{Thr}_a|] \leq O(1/n^k)$.*

With these facts, we can now prove Lemma 5.1 in an entirely analogous fashion to [CHH+20]:

Proof of Lemma 5.1. Fix $f \in \mathcal{F}$, and again write $F(\mathbf{x}_1, \dots, \mathbf{x}_k) = e(f(\mathbf{x}_1, \dots, \mathbf{x}_k))$. Let $F' = F - \mathbb{E}[F]$. Let $U_j = \{i : (j-1)n + 1 \leq i \leq jn\}$. Then, possibly after relabelling variables, we have by Fact 5.3 that

$$M_k(f) = \left| \sum_{S \subseteq [kn] : |S| = k} \hat{f}(S) \right| \leq C^k \left| \sum_{i_j \in U_j, \forall j \in [k]} \hat{f}(\{i_1, \dots, i_k\}) \right|, \tag{43}$$

so we may turn to bounding this latter term. We have

$$\begin{aligned}
\left|\sum_{i_j\in U_j,\forall j\in[k]}\hat{f}(\{i_1,\dots,i_k\})\right| &= \left|\sum_{i_j\in U_j,\forall j\in[k]}\mathbb{E}[F'(\mathbf{x}_1,\dots,\mathbf{x}_k)\prod_{j=1}^{k}e((\mathbf{x}_j)_{i_j})]\right| \\
&= \left|\mathbb{E}\left[F'(\mathbf{x}_1,\dots,\mathbf{x}_k)\prod_{j=1}^{k}\left(\sum_{i_j\in U_j}e((\mathbf{x}_j)_{i_j})\right)\right]\right| \\
&\le 2^k\sum_{1\le a_i\le n/2,\forall i\in[k]}\left|\mathbb{E}\left[F'(\mathbf{x}_1,\dots,\mathbf{x}_k)\prod_{i=1}^{k}\mathrm{Thr}_{a_i}(\mathbf{x}_i)\right]\right| \\
&\le 2^k\left(\sum_{1\le a_i\le O(\sqrt{kn\log n}),\forall i\in[k]}\left|\mathbb{E}\left[F'(\mathbf{x}_1,\dots,\mathbf{x}_k)\prod_{i=1}^{k}\mathrm{Thr}_{a_i}(\mathbf{x}_i)\right]\right| + O(1)\right) \\
&\le 2^k\cdot O\left(\sqrt{kn\log n}\right)^k\cdot\left(\sqrt{\frac{t}{n}}\right)^k \\
&= O\left(\sqrt{tk\log n}\right)^k.
\end{aligned}$$

The first inequality follows from Fact 5.2, the second from Fact 5.4, and the last by Fact 5.1. As $f\in\mathcal{F}$ was arbitrary, and by absorbing the constant C from above into the implicit constant here in this bound, we obtain the desired claim. □

6 Discussion and Open Questions

In this work, we have given a nearly complete interpolation between the PRGs obtained in the polarizing random walks framework by exploiting level-k bounds on the class of functions, thus answering an open question from [CHLT19]. We do so by exploiting an alternate Fourier analysis via Taylor's theorem and utilizing multilinearity and random restrictions. This new analysis enables us to construct PRGs from bounds on the potentially much smaller and better-understood, Fourier quantity $M_k(\mathcal{F})$, for any $k\ge 3$. By generalizing the connection established in [CHH+20], this reduces the problem of constructing PRGs in this framework to proving correlation bounds. Further, we show how to improve the seed length of the PRG if we have bounds on $L_{1,i}$, for all $i\le k$, where $k\ge 3$. A natural open question along these lines is to obtain such an improved seed length using bounds on M_i (instead of $L_{1,i}$) for all $i\le k$. Another natural question is to construct a PRG using bounds on just M_2 (recall that [CHLT19] gives such a construction using bounds on $L_{1,2}$ and our analysis only gives a non-trivial PRG from bounds on M_k when $k\ge 3$).

Finally, exploiting known level k bounds for $\mathbb{F}_2$ polynomials, our approach shows that the random walks framework can yield pseudorandom generators for the class of $\mathbb{F}_2$ polynomials that is competitive with, though falls short of, the state-of-the-art. As mentioned, we hope this paper both gives evidence that stronger Fourier control (perhaps via proving the required correlation bounds) can give better PRGs using this framework, and can also handle classes that were previously not known to be possible. In particular, we emphasize that proving Conjecture 4.3 even for the case of $k=3$ will lead to PRGs for $\mathbb{F}_2$ polynomials with degree $\omega(\log n)$, a longstanding problem in complexity theory.

References

[CHH+20] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, Shachar Lovett, and David Zuckerman. XOR lemmas for resilient functions against polynomials. In *Proceedings of the 52nd*

Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, page 234–246, New York, NY, USA, 2020. Association for Computing Machinery.

[CHHL19] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, and Shachar Lovett. Pseudorandom generators from polarizing random walks. *Theory of Computing*, 15(10):1–26, 2019.

[CHLT19] Eshan Chattopadhyay, Pooya Hatami, Shachar Lovett, and Avishay Tal. Pseudorandom Generators from the Second Fourier Level and Applications to AC0 with Parity Gates. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*, volume 124 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 22:1–22:15, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[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, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 363–375, 2018.

[GSW16] Parikshit Gopalan, Rocco A. Servedio, and Avi Wigderson. Degree and sensitivity: Tails of two distributions. In Ran Raz, editor, *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, volume 50 of *LIPIcs*, pages 13:1–13:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.

[Kel12] Nathan Keller. A simple reduction from a biased measure on the discrete cube to the uniform measure. *European Journal of Combinatorics*, 33(8):1943 – 1957, 2012.

[LMN89] Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, Fourier transform, and learnability. In *30th Annual Symposium on Foundations of Computer Science*, pages 574–579. IEEE, 1989.

[NN93] Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM Journal on Computing*, 22(4):838–856, 1993.

[O'D14] Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.

[Raz87] A. A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical notes of the Academy of Sciences of the USSR*, 41(4):333–338, Apr 1987.

[RT19] Ran Raz and Avishay Tal. Oracle separation of BQP and PH. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 13–23, New York, NY, USA, 2019. Association for Computing Machinery.

[Smo87] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, page 77–82, New York, NY, USA, 1987. Association for Computing Machinery.

[Smo93] R. Smolensky. On representations by low-degree polynomials. In *Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science*, SFCS '93, page 130–138, USA, 1993. IEEE Computer Society.

[Tal17] Avishay Tal. Tight bounds on the Fourier spectrum of AC0. In *32nd Computational Complexity Conference (CCC 2017)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

[Vad12] Salil P Vadhan. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science*, 7(1–3):1–336, 2012.

[Vio09] Emanuele Viola. The sum of d small-bias generators fools polynomials of degree d. *Computational Complexity*, 18(2):209–217, 2009.

[Wu20] Xinyu Wu. A stochastic calculus approach to the oracle separation of BQP and PH. *arXiv preprint arXiv:2007.02431*, 2020.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il