Electronic Colloquium on Computational Complexity, Report No. 87 (2019)

Coin Theorems and the Fourier Expansion

Rohit Agrawal*

June 9, 2019

Abstract

In this note we compare two measures of the complexity of a class $\mathcal{F}$ of Boolean functions studied in (unconditional) pseudorandomness: $\mathcal{F}$'s ability to distinguish between biased and uniform coins (the *coin problem*), and the norms of the different levels of the Fourier expansion of functions in $\mathcal{F}$ (the *Fourier growth*). We show that for coins with low bias $\varepsilon = o(1/n)$, a function's distinguishing advantage in the coin problem is essentially equivalent to ε times the sum of its level 1 Fourier coefficients, which in particular shows that known level 1 and total influence bounds for some classes of interest (such as constant-width read-once branching programs) in fact follow as a black-box from the corresponding coin theorems, thereby simplifying the proofs of some known results in the literature. For higher levels, it is well-known that Fourier growth bounds on all levels of the Fourier spectrum imply coin theorems, even for large ε, and we discuss here the possibility of a converse.

1 Introduction

A natural question one can ask when studying a limited model of computation is how well it can solve some basic computational task, such as distinguishing between an unfair and a fair coin:

Definition 1.1 (Coin problem)**.** The *advantage* α of a Boolean function $f : \{-1,1\}^n \to \{-1,1\}$ in *distinguishing ε-biased coins from uniform coins* is defined to be

$$\alpha = \left|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\right|,$$

where X_δ^n are iid random variables over $\{-1,1\}$ with expectation δ, so that X_0^n are uniform random bits.

A set $\mathcal{F}$ of Boolean functions is said to *solve the ε-coin problem with advantage* α for

$$\alpha = \max_{f\in\mathcal{F}}\left|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\right|.$$

One can see (e.g. via the equivalence of ℓ_1 and total variation distance of probability distributions) that the unique Boolean function f achieving the greatest distinguishing advantage is of the form $f(x) = 1$ if and only if the number of 1s in x is at least k, for the smallest k such that $(1+\varepsilon)^k(1-\varepsilon)^{n-k} \geq 1$. This is simply a (symmetric) linear threshold function, and so one sees that the coin problem for a class of Boolean functions $\mathcal{F}$ is closely related to the ability of $\mathcal{F}$ to approximate threshold functions, and in particular the majority function. The study of threshold functions in limited models is extensive, with early works due to e.g. Ajtai [Ajt83] and Valiant [Val84], and early explicit consideration of the coin problem by Shaltiel and Viola [SV10], Brody and Verbin (who introduced the name) [BV10], and Aaronson [Aar10]. These results are generally stated as a *coin theorem*, giving a statement of the form $\mathcal{F}_n$ (parametrized by some parameter, e.g. the input length) cannot solve the ε-coin problem except with some advantage $\beta(n,\varepsilon)$. Subsequent work has given

*John A. Paulson School of Engineering and Applied Sciences, Harvard University, Cambridge, MA 02138, USA. Email: rohitagr@seas.harvard.edu. Supported by the Department of Defense (DoD) through the National Defense Science & Engineering Graduate Fellowship (NDSEG) Program.

ISSN 1433-8092

tight coin theorems on constant-width read-once branching programs (Steinberger [Ste13]), AC^0 (Cohen, Ganor, and Raz [CGR14]), $\mathsf{AC}^0[\oplus]$ (Limaye, Sreenivasaiah, Srinivasan, Tripathi, and Venkitesh [LSS+18]), and product tests (Lee and Viola [LV18]).

The other main object we will discuss is the Fourier expansion of f, for which we follow the notation of O'Donnell [O'D14].

Definition 1.2. The *Fourier expansion* of a function $f : \{-1,1\}^n \to \mathbb{R}$ is its unique representation as a multilinear polynomial

$$f(x) = f(x_1, \ldots, x_n) = \sum_{S \subseteq [n]} \widehat{f}(S) \prod_{i \in S} x_i \,,$$

where $[n] \overset{\text{def}}{=} \{1, 2, \ldots, n\}$ and $\widehat{f}(S)$ is called the *Fourier coefficient of f on S*. The coefficient $\widehat{f}(S)$ is said to be at *level* $|S|$, and can be expressed as

$$\widehat{f}(S) = \mathop{\mathbb{E}}_{x}\left[f(x) \prod_{i \in S} x_i \right]$$

where the expectation is taken over the uniform distribution over $\{-1,1\}^n$. In particular, $\widehat{f}(\emptyset) = \mathbb{E}_x[f(x)]$.

The *total influence of f*, denoted $\mathbf{I}[f]$, is defined as $\mathbf{I}[f] = \sum_{i=1}^n \sum_{S \ni i} \widehat{f}(S)^2 = \sum_{S \subseteq [n]} |S| \widehat{f}(S)^2$. If $f : \{-1,1\}^n \to \{-1,1\}$ is monotone, then the total influence has the simpler expression $\mathbf{I}[f] = \sum_{i=1}^n \widehat{f}(\{i\})$.

The use of Fourier analysis in the study of Boolean functions was pioneered by the work of Kahn, Kalai, and Linial [KKL88], which kicked off a long line of work, including early results analyzing DNFs and CNFs by Brandman, Orlitsky, and Hennessy [BOH90], and AC^0 by Linial, Mansour, and Nisan [LMN93]. More recently, Reingold, Steinke, and Vadhan [RSV13] introducted the concept of *Fourier growth* for use in constructions of pseudorandom generators via the iterative random restriction framework of Ajtai and Wigderson [AW89], and particularly in the sense of the later work of Gopalan, Meka, Reingold, Trevisan, and Vadhan [GMR+12].

Definition 1.3 ([RSV13])**.** Given $f : \{-1,1\}^n \to \mathbb{R}$, we define its *level k ℓ_1 norm* to be

$$\mathcal{L}_1^k(f) = \sum_{|S|=k} \left| \widehat{f}(S) \right|.$$

For a class $\mathcal{F}$ of functions, we define the *level k ℓ_1 norm of $\mathcal{F}$* to be $\mathcal{L}_1^k(\mathcal{F}) = \sup_{f \in \mathcal{F}} \mathcal{L}_1^k(f)$. $\mathcal{F}$ is said to have *Fourier growth with base t* if $\mathcal{L}_1^k(\mathcal{F}) \leq t^k$ for all k.

Fourier growth bounds were introduced by [RSV13] to capture the fact that (roughly speaking) a random restriction that keeps input bits alive with probability p reduces the level k ℓ_1 norm of a function by p^k, and so a random restriction keeping an $O(1/t)$ fraction of bits alive simplifies a function with Fourier growth with base t into one function with constant total Fourier ℓ_1 norm, which is then easily fooled by a small-bias generator (Naor and Naor [NN93]). Fourier growth bounds have been studied for classes such as AC^0 [LMN93, Hås01, Tal17], regular and constant-width read-once branching programs [RSV13, CHRT18], and product tests [Lee19].

In this work, we study implications between bounds on the advantage of a class of Boolean functions in the coin problem and bounds on the Fourier spectrum. Some connections along this line are well known, for example it is folklore (see e.g. Tal [Tal17]) that Fourier growth bounds of the form $\mathcal{L}_1^k(f) \leq t^k$ imply a strong coin theorem with bound $\beta(n, \varepsilon) = \varepsilon \cdot O(t)$ for all $\varepsilon = O(1/t)$. Recently, Tal [Tal19] (who graciously allowed the author to include his result in this note) showed that if a class of functions $\mathcal{F}$ is closed under restriction, then for $\mathcal{F}$ to satisfy such a strong coin theorem it is enough for it to merely have $\mathcal{L}_1^1(\mathcal{F}) \leq t$ rather than have Fourier growth with base t.

In this note, we give the first (to the best of our knowledge) results in the other direction, showing that coin theorems for small $\varepsilon = o(1/n)$ are *equivalent* to bounds on the sum of the level 1 Fourier coefficients, and in particular to bounds on $\mathcal{L}_1^1(\mathcal{F})$ assuming that these coefficients can be taken to be non-negative (e.g.

if $\mathcal{F}$ consists of monotone functions, or is closed under negating input variables). Thus, perhaps surprisingly, even coin theorems for only a small range of ε are sufficient to bound the level 1 spectrum of the class $\mathcal{F}$, even for $\mathcal{F}$ not closed under restriction. This allows us to give simple "black-box" proofs of existing level 1 bounds in the literature, such as the bound for constant-width read-once branching programs due to Steinke, Vadhan, and Wan [SVW17] in 2014, which was conjectured by [RSV13].

These results are summarized in Figure 1, showing the implications between bounds on coin problems and Fourier growth for a class $\mathcal{F}$, arranged from top to bottom in order of strength (under the assumption that $\mathcal{F}$ is monotone or closed under negation of input variables, but need not be closed under restriction). If $\mathcal{F}$ is additionally closed under restriction, then the bottom two layers collapse.

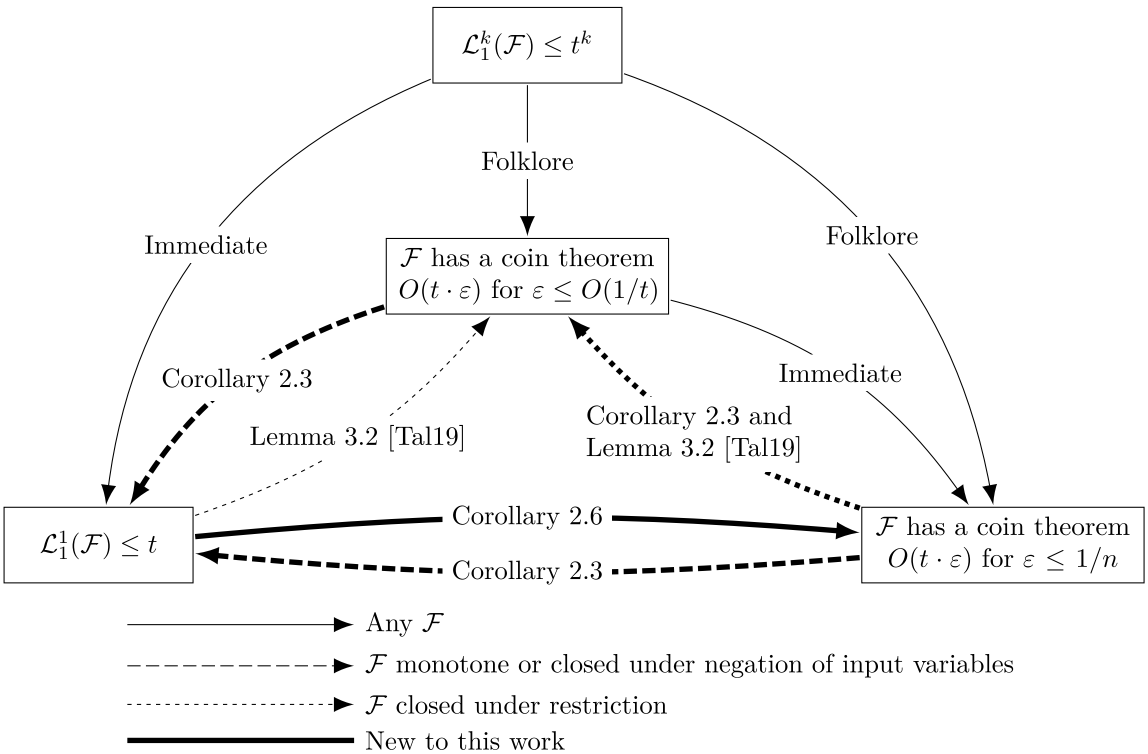

Figure 1: Implications studied in this work for a class $\mathcal{F}$ of Boolean functions, assuming $t \geq 1$

We also show (non-constructively) the existence of a class of Boolean functions $\mathcal{F}$ closed under restriction and negations which satisfies a coin theorem of the form $\varepsilon \cdot O(\log n)$ for all $\varepsilon \leq O(1/\log n)$ (and therefore has $\mathcal{L}_1^1(\mathcal{F}) \leq O(\log n)$), but yet has $\mathcal{L}_1^3(\mathcal{F}) = \Omega(\log n \cdot n)$. This result may be of interest because, intriguingly, many natural classes of Boolean functions $\mathcal{F}$ with known coin theorems or level-1 bounds are also known (or conjectured) to satisfy corresponding Fourier growth bounds (and in fact we are unaware of any natural class of Boolean functions satisfying these closure conditions and a $\mathcal{L}_1^1(\mathcal{F}) \leq t$ bound or coin theorem $\varepsilon \cdot O(t)$ which does not at least conjecturally also have Fourier growth with base $O(t)$). We hope that this result may help point the way to giving some additional constraints under which one could hope for a $\mathcal{L}_1^1$ or coin problem bound to imply a general $\mathcal{L}_1^k$ bound.

2 Low bias and level 1

The main technical result of this section is the following simple proposition.

Proposition 2.1. *For every $f : \{-1,1\}^n \to \mathbb{R}$, the rate of convergence of the limit*

$$\lim_{\varepsilon \to 0} \frac{1}{\varepsilon}\Big(\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big) = \sum_{i=1}^n \widehat{f}(\{i\})$$

can be bounded for every $|\varepsilon| \le 1/\sqrt{n}$ as

$$\left|\frac{1}{\varepsilon}\Big(\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big) - \sum_{i=1}^n \widehat{f}(\{i\})\right| \le |\varepsilon| \cdot n \cdot \sqrt{\mathrm{Var}(f(X_0^n))},$$

where in particular if $f : \{-1,1\}^n \to [-1,1]$ then the right-hand side is bounded by $|\varepsilon| \cdot n$.

In particular, bounds on the coin problem for f for small ε (e.g. $\varepsilon = o(1/n)$) are equivalent to bounds on the sum of the level 1 Fourier coefficients of f. Before giving the (straightforward) proof of Proposition 2.1 (along with some slightly tighter but more technical bounds in terms of quantities smaller than $\mathrm{Var}(f(X_0^n))$), we first note some immediate corollaries, including some simple new proofs of known results in the literature on Fourier growth.

Most basically, if we can assume that the level 1 Fourier coefficients of f are non-negative, we get upper bounds on the ℓ_1 norm of these coefficients:

Corollary 2.2. *Let $f : \{-1,1\}^n \to [-1,1]$ be such that $\widehat{f}(\{i\}) \ge 0$ for every $1 \le i \le n$ (e.g. f is monotone). Then*

$$\mathcal{L}_1^1(f) = \sum_{i=1}^n \left|\widehat{f}(\{i\})\right| \le \inf_{|\varepsilon| \le 1/\sqrt{n}} \left\{ \left|\frac{1}{\varepsilon}\Big(\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big)\right| + |\varepsilon| n \right\}$$

In particular, if f is monotone, then its total influence $\mathbf{I}[f] = \mathcal{L}_1^1(f)$ satisfies the same bound.

Beyond monotonicity, another way to establish such a bound is if f is part of a larger class of functions with basic closure properties that all simultaneously satisfy a coin theorem.

Corollary 2.3. *Let $\mathcal{F}$ be a class of functions $f : \{-1,1\}^n \to [-1,1]$ such that*

1. *$\mathcal{F}$ satisfies a coin theorem with bound $\beta(n,\varepsilon)$, meaning $|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]| \le \beta(n,\varepsilon)$ for every $f \in \mathcal{F}$.*
2. *For every $f \in \mathcal{F}$ there exists $g \in \mathcal{F}$ such that $\widehat{g}(\{i\}) = \left|\widehat{f}(\{i\})\right|$ for every $1 \le i \le n$ (e.g. $\mathcal{F}$ is closed under negation of input variables, or consists only of monotone functions).*

Then

$$\mathcal{L}_1^1(\mathcal{F}) = \sup_{f \in \mathcal{F}} \sum_{i=1}^n \left|\widehat{f}(\{i\})\right| \le \inf_{|\varepsilon| \le 1/\sqrt{n}} \left\{ \left|\frac{\beta(n,\varepsilon)}{\varepsilon}\right| + |\varepsilon| n \right\}$$

and in particular, every monotone $f \in \mathcal{F}$ has $\mathbf{I}[f] = \mathcal{L}_1^1(f)$ at most the above.

Note that taking $\varepsilon = 1/n$ in Corollary 2.3 gives the simple upper bound of $n \cdot |\beta(n, 1/n)| + 1$. To show the applicability of this result, we show how it can be used to give simple proofs of several existing results in the literature. As it is not relevant for us, we will not give formal definitions of the classes $\mathcal{F}$ involved and defer to the original papers for such details.

For constant-width read-once branching programs, Brody and Verbin [BV10] first claimed a coin theorem, which was improved by Steinberger [Ste13] to give an optimal bound. Interestingly, Steinberger also separately proved (using the same techniques) a total influence bound on monotone constant-width read-once branching programs, which was generalized (again using the same techniques) by Steinke, Vadhan, and Wan [SVW17] in 2014 to a corresponding level 1 Fourier bound for (non-necessarily monotone) constant-width read-once branching programs. Applying Corollary 2.3, we see that these latter results can in fact be derived (up to constant factors) using Steinberger's coin theorem as a black box.

Corollary 2.4 ([Ste13, SVW17]). *Let $f : \{-1,1\}^n \to \{-1,1\}$ be computable by a width-w read-once branching program. Then $\mathcal{L}_1^1(f) \le O_w(\log n)^{w-2} + O(1)$. In particular, if f is monotone then f has total influence $\mathbf{I}[f] = \mathcal{L}_1^1(f)$ satisfying the same bound.*

Proof. Steinberger's full coin theorem [Ste13, Full version, Corollary 1] states that for every integer $r \ge 1$ that

$$\Big|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big| \le \varepsilon r^{w-2} + \big(n + r^{w-2}\big)(w-2)\left(\frac{1}{2-\varepsilon}\right)^{r-1}$$

so since width-w read-once branching programs are closed under negation if input variables, Corollary 2.3 implies that for $0 < \varepsilon \le 1/\sqrt{n}$ that

$$\mathcal{L}_1^1(f) \le r^{w-2} + \frac{1}{\varepsilon}\big(n + r^{w-2}\big)(w-2)\left(\frac{1}{2-\varepsilon}\right)^{r-1} + \varepsilon n$$

so setting $\varepsilon = 1/n$ and taking $r = \lceil 4\log n\rceil + 1$ gives the result. ☐

One thing to note about the above proof is that the coin theorem we used of [Ste13] was suboptimal in the range $\varepsilon = n^{-\omega(1)}$, but still implied the optimal level 1 bound of [SVW17]. Using Proposition 2.1, we can also improve the [Ste13] coin theorem for small ε by setting $\varepsilon_0 = 1/n$ in the following corollary:

Corollary 2.5. *Let $f : \{-1,1\}^n \to [-1,1]$ satisfy a coin theorem of $|\varepsilon| \cdot B$ for all $|\varepsilon| \ge \varepsilon_0$, where $B \ge 0$ and $\varepsilon_0 \le 1/\sqrt{n}$. Then for all $|\varepsilon| < \varepsilon_0$, it holds that*

$$\Big|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big| \le |\varepsilon| \cdot \big(B + n(|\varepsilon| + \varepsilon_0)\big) \le |\varepsilon| \cdot (B + 2n \cdot \varepsilon_0).$$

In particular, f satisfies a coin theorem with bound $|\varepsilon| \cdot (B + 2n \cdot \varepsilon_0)$ for all $|\varepsilon| \le 1$.

The proof of Corollary 2.5 goes by using Proposition 2.1 applied with ε_0 to derive a bound on the sum of the level 1 Fourier coefficients of f, then applying the following converse of Corollary 2.3 to derive a coin theorem for small ε from such a bound:

Corollary 2.6. *Let $f : \{-1,1\}^n \to [-1,1]$ have $\Big|\sum_{i=1}^n \widehat{f}(\{i\})\Big| \le t$ (e.g. $\mathcal{L}_1^1(f) \le t$). Then for all $|\varepsilon| \le 1/\sqrt{n}$,*

$$\Big|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big| \le |\varepsilon| \cdot (t + |\varepsilon| \cdot n),$$

so that in particular f satisfies a coin theorem with bound $2t \cdot |\varepsilon|$ for all $|\varepsilon| \le t/n$.

Proof. The triangle inequality and Proposition 2.1 imply that

$$\begin{aligned}
|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]| &= |\varepsilon| \cdot \left|\frac{1}{\varepsilon} \cdot \Big(\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big)\right| \\
&\le |\varepsilon| \cdot \left(\left|\frac{1}{\varepsilon}\Big(\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big) - \sum_{i=1}^n \widehat{f}(\{i\})\right| + \left|\sum_{i=1}^n \widehat{f}(\{i\})\right|\right) \\
&\le |\varepsilon| \cdot (|\varepsilon| \cdot n + t)
\end{aligned}$$

as desired. ☐

Proof of Corollary 2.5. By the triangle inequality and Proposition 2.1 we have

$$\left|\sum_{i=1}^n \widehat{f}(\{i\})\right| \le \left|\sum_{i=1}^n \widehat{f}(\{i\}) - \frac{1}{\varepsilon_0}\Big(\mathbb{E}\big[f\big(X_{\varepsilon_0}^n\big)\big] - \mathbb{E}[f(X_0^n)]\Big)\right| + \left|\frac{1}{\varepsilon_0}\Big(\mathbb{E}\big[f\big(X_{\varepsilon_0}^n\big)\big] - \mathbb{E}[f(X_0^n)]\Big)\right| \le |\varepsilon_0| \cdot n + B,$$

so the result follows by applying Corollary 2.6 with $t = B + |\varepsilon_0| \cdot n$. ☐

It remains to prove Proposition 2.1, for which we will need just one simple fact about the Fourier expansion.

Lemma 2.7 (Parseval's identity)**.** *The Fourier coefficients of* $f : \{-1,1\}^n \to \mathbb{R}$ *satisfy*

$$\sum_{S\subseteq[n]} \widehat{f}(S)^2 = \mathbb{E}\Big[f(X_0^n)^2\Big].$$

In particular, $\mathrm{Var}(f(X_0^n)) = \sum_{|S|\geq 1} \widehat{f}(S)^2$.

Proof of Proposition 2.1. Let $f : \{-1,1\}^n \to \mathbb{R}$. Then by the multilinearity of the Fourier expansion, we have

$$\begin{aligned}
\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)] &= \sum_{S\subseteq[n]} \widehat{f}(S)\left(\mathop{\mathbb{E}}_{x\sim X_\varepsilon^n}\left[\prod_{i\in S} x_i\right] - \mathop{\mathbb{E}}_{x\sim X_0^n}\left[\prod_{i\in S} x_i\right]\right) \\
&= \sum_{\emptyset\neq S\subseteq[n]} \widehat{f}(S)\cdot \varepsilon^{|S|}
\end{aligned}$$

$$\frac{1}{\varepsilon}\Big(\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big) - \sum_{i=1}^n \widehat{f}(\{i\}) = \frac{1}{\varepsilon}\sum_{k=2}^n \varepsilon^k \sum_{|S|=k} \widehat{f}(S)$$

The limit claim follows since the right-hand side is a polynomial in ε with no constant term, and thus goes to 0 with ε. For an effective bound for nonzero ε, we see

$$\begin{aligned}
\left|\frac{1}{\varepsilon}\Big(\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\Big) - \sum_{i=1}^n \widehat{f}(\{i\})\right| &\leq \frac{1}{|\varepsilon|}\sum_{k=2}^n |\varepsilon|^k \sum_{|S|=k} \left|\widehat{f}(S)\right| \\
&\leq \frac{1}{|\varepsilon|}\sum_{k=2}^n |\varepsilon|^k \sqrt{\binom{n}{k}\sum_{|S|=k} \widehat{f}(S)^2} \qquad \text{(by Cauchy-Schwarz)}
\end{aligned}$$

We show two different techniques to bound this sum, in terms of either $\mathrm{Var}(f(X_0^n)) = \sum_{|S|\geq 1} \widehat{f}(S)^2$ or $\max_{k\geq 2}\sum_{|S|=k} \widehat{f}(S)^2$ (though the latter result is not needed to prove the claim, we present the simple proof here since depending on the function f it may be significantly stronger). For the former, we have

$$\begin{aligned}
&\frac{1}{|\varepsilon|}\sum_{k=2}^n |\varepsilon|^k \sqrt{\binom{n}{k}\sum_{|S|=k} \widehat{f}(S)^2} \\
&\qquad \leq \frac{1}{|\varepsilon|}\sqrt{\sum_{k=2}^n \binom{n}{k}\cdot \varepsilon^{2k}}\cdot \sqrt{\sum_{|S|\geq 2} \widehat{f}(S)^2} \qquad \text{(by Cauchy-Schwarz)} \\
&\qquad = \frac{1}{|\varepsilon|}\sqrt{(1+\varepsilon^2)^n - (1+n\varepsilon^2)}\cdot \sqrt{\mathrm{Var}(f(X_0^n)) - \sum_{i=1}^n \widehat{f}(\{i\})^2}
\end{aligned}$$

Then $(1+\varepsilon^2)^n - (1+n\varepsilon^2) \leq e^{n\varepsilon^2} - (1+n\varepsilon^2) \leq (n\varepsilon^2)^2$ for $n\varepsilon^2 \leq 1$, which gives the claim. For the other bound, we have

$$\begin{aligned}
\frac{1}{|\varepsilon|}\sum_{k=2}^{n}|\varepsilon|^k\sqrt{\binom{n}{k}\sum_{|S|=k}\widehat{f}(S)^2} &\le \frac{1}{|\varepsilon|}\cdot\sqrt{\max_{k\ge 2}\sum_{|S|=k}\widehat{f}(S)^2}\cdot\sum_{k=2}^{n}\left(|\varepsilon|\sqrt{n}\right)^k && \left(\text{since } \binom{n}{k}\le n^k\right)\\
&= \sqrt{\max_{k\ge 2}\sum_{|S|=k}\widehat{f}(S)^2}\cdot\frac{1}{|\varepsilon|}\cdot\frac{|\varepsilon|^2 n-|\varepsilon|^{n+1}\sqrt{n}^{n+1}}{1-|\varepsilon|\sqrt{n}}\\
&= \sqrt{\max_{k\ge 2}\sum_{|S|=k}\widehat{f}(S)^2}\cdot\frac{|\varepsilon| n-|\varepsilon|^{n}\sqrt{n}^{n+1}}{1-|\varepsilon|\sqrt{n}}\\
&\le \sqrt{\max_{k\ge 2}\sum_{|S|=k}\widehat{f}(S)^2}\cdot 2\cdot|\varepsilon|\cdot n && (\text{if } |\varepsilon|\le 1/(2\sqrt{n}))
\end{aligned}$$

as desired. □

3 Larger bias and beyond Level 1

The previous section demonstrated that bounds on the level 1 Fourier coefficients are essentially equivalent to coin theorems for inverse-polynomially small error $\varepsilon = o(1/n)$. This raises two natural questions: can we say anything about either coin theorems for larger ε, or about bounds on the Fourier spectrum beyond level 1?

These questions are of interest because, perhaps surprisingly, many natural classes of Boolean functions $\mathcal{F}$ for which we know level-1 bounds are also known (or conjectured) to satisfy corresponding Fourier growth bounds $\mathcal{L}_1^k(\mathcal{F}) \le O\big(\mathcal{L}_1^1(\mathcal{F})\big)^k$ for all k. For example, AC^0 (Tal [Tal17]) and the class of product tests (Lee [Lee19]) are known to have this property, and constant-width read-once branching programs (cwROBPs) are believed to (Chattopadhyay, Hatami, Reingold, and Tal [CHRT18] explicitly make this conjecture and prove almost this optimal result). Furthermore, these classes all have known corresponding coin theorems which are not only capable of proving the known $\mathcal{L}_1^1$ bound via Corollary 2.3, but are also valid for all $\varepsilon = O(1/\mathcal{L}_1^1(\mathcal{F}))$ (Cohen, Ganor, and Raz [CGR14] for AC^0, Lee and Viola [LV18] for product tests, and Steinberger [Ste13] for cwROBPs). One might therefore hope that there is a stronger relationship between Fourier growth and coin theorems.

One direction, that Fourier growth bounds of this form imply coin theorems, is well-known (see e.g. [Tal17], this can also be seen in the proof of Proposition 2.1 by replacing the first Cauchy-Schwarz step), so the goal of this section is to explore the possibility of a converse. Generally, allowing for both additive and multiplicative losses, one might ask something like the following:

Question 3.1. Is there a "natural" set of conditions $\mathcal{C}$ such that the following is true: Let $\mathcal{F} = (\mathcal{F}_n)_{n\in\mathbb{N}}$ be a class of Boolean functions $f_n : \{-1,1\}^n \to \{-1,1\}$ satisfying $\mathcal{C}$. Then if $\mathcal{F}$ satisfies a coin theorem with bound $|\varepsilon|\cdot B(n)$, meaning for all $n\in\mathbb{N}$, $f_n \in \mathcal{F}_n$ and $|\varepsilon|\le 1$ it holds that $|\mathbb{E}[f_n(X_\varepsilon^n)] - \mathbb{E}[f_n(X_0^n)]| \le |\varepsilon|\cdot B(n)$, then there exists a constant $c_{\mathcal{F}}$ such that

$$\mathcal{L}_1^k(\mathcal{F}) \le \left(c_{\mathcal{F}}\cdot(1+B(n))\right)^k$$

for all k.

Perhaps the most natural condition to impose, beyond closure under negations as considered in the previous section, is closure under *restriction*, that is, fixing parts of the input, since intuitively this has the property of "reducing the level" of any Fourier coefficient containing one of the fixed inputs. Furthermore, all the classes of Boolean functions mentioned earlier in this section are closed under restriction, and we are not aware of any natural class of Boolean functions with these properties which does not (at least conjecturally) satisfy a corresponding $\mathcal{L}_1^k$ bound. However, Tal [Tal19] recently gave evidence suggesting that this is not enough, showing that any $\mathcal{F}$ closed under restriction satisfies a coin theorem of $\varepsilon\cdot O(\mathcal{L}_1^1(\mathcal{F}))$ for

$\varepsilon = O(1/\mathcal{L}_1^1(\mathcal{F}))$, so that for such $\mathcal{F}$ there is essentially no difference between coin theorems for $\varepsilon = o(1/n)$ and $\varepsilon = O(1/\mathcal{L}_1^1(\mathcal{F}))$.

Lemma 3.2 ([Tal19][1]). *Let $\mathcal{F}$ be a class of Boolean functions which is closed under restriction and satisfies $\left|\sum_{i=1}^n \widehat{f}(\{i\})\right| \leq t$ for every $f \in \mathcal{F}$ (e.g. $\mathcal{L}_1^1(\mathcal{F}) \leq t$). Then for all $|\varepsilon| < 1$ it holds that*

$$\left|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]\right| \leq \ln\left(\frac{1}{1-\varepsilon}\right) \cdot t.$$

In particular, $\mathcal{F}$ satisfies a coin theorem of $|\varepsilon| \cdot O(t)$ for all $|\varepsilon| = \min(1/t, 0.99)$.

As an example of the power of this result, note that it implies the coin theorem for AC^0 of Cohen, Ganor, and Raz [CGR14] as a corollary of Boppana's [Bop97] bound on the total influence of that class.

Corollary 3.3 ([CGR14]). *Let $f : \{-1,1\}^n \to \{-1,1\}$ be computable by a size s, depth d Boolean circuit and $|\varepsilon| \leq 1$. Then $|\mathbb{E}[f(X_\varepsilon^n)] - \mathbb{E}[f(X_0^n)]| \leq |\varepsilon| \cdot O_d(\log^{d-1}(s))$.*

We include the proof[1] of Lemma 3.2 at the end of this section, but we will first use Tal's result to provide a simple proof that there exist classes of Boolean functions $\mathcal{F}$ which are closed under restriction and negations of input variables and satisfy a coin theorem and level 1 bound of $B(n)$, but have $\mathcal{L}_1^3(\mathcal{F}) \geq \Omega(n \cdot B(n))$, thereby showing that these properties themselves are not enough to give a positive answer to Question 3.1.

Proposition 3.4. *For every function $\sqrt{\log n} + O(1) < B(n) < \sqrt{n}$ and sufficiently large odd integer n, there is a class $\mathcal{F}_B$ of Boolean functions on at most n bits that is closed under restriction, negation of input variables, and negation of outputs such that $\mathcal{L}_1^1(\mathcal{F}) \leq B$ and $\mathcal{F}$ satisfies a coin theorem of $|\varepsilon| \cdot O(B)$ for all $\varepsilon = O(1/B)$, but $\mathcal{L}_1^3(\mathcal{F}) = \Omega(B \cdot n)$.*

The idea is that it is easy to construct such a family $\mathcal{F}$ if we consider functions $f : \{-1,1\}^n \to [-1,1]$ which are not Boolean but instead take on values inside the interval: in particular, if f takes on the values $\{\pm B(n)/\sqrt{n}\}$, then f will satisfy a coin theorem of bound $|\varepsilon| \cdot B(n)$ and a corresponding $\mathcal{L}_1^1$ bound, but need not satisfy higher $\mathcal{L}_1^k$ bounds. By randomly rounding such a function f to have Boolean outputs, the resulting function (and its closure under restriction and negation of input variables) will with high probability still satisfy a coin theorem but will keep its large $\mathcal{L}_1^k$ mass. Thus, this suggests that any positive answer to Question 3.1 will require a condition which is in some sense "not linear" and can detect such bad examples. Formally, Proposition 3.4 follows from the following lemma which shows that the above process indeed preserves the sums of Fourier coefficients with high probability.

Lemma 3.5. *Let m be a positive integer and $g : \{-1,1\}^m \to [-1,1]$ be a function. Then defining $\tilde{\boldsymbol{g}} : \{-1,1\}^m \to \{-1,1\}$ as the random function which for each $x \in \{-1,1\}^m$ independently sets $\tilde{\boldsymbol{g}}(x) \in \{-1,1\}$ to have expectation $g(x)$, it holds for every collection $\mathcal{T} \subseteq 2^{[m]}$ of subsets of $[m]$ that*

$$\Pr\left[\left|\sum_{S \in \mathcal{T}} \widehat{\tilde{\boldsymbol{g}}}(S) - \sum_{S \in \mathcal{T}} \widehat{g}(S)\right| \geq \varepsilon\right] \leq 2\exp\left(-2^{m-1}\varepsilon^2/|\mathcal{T}|\right)$$

Proof. We first write

$$\sum_{S \in \mathcal{T}} \widehat{\tilde{\boldsymbol{g}}}(S) - \sum_{S \in \mathcal{T}} \widehat{g}(S) = 2^{-m} \sum_{x \in \{-1,1\}^m} (\tilde{\boldsymbol{g}}(x) - g(x)) \cdot \left(\sum_{S \in \mathcal{T}} \prod_{i \in S} x_i\right).$$

by definition of Fourier coefficients. Then by definition of $\tilde{\boldsymbol{g}}$, the right hand side is a sum of 2^m independent mean-zero random variables, one for each $x \in \{-1,1\}^n$, bounded in a range of size $2^{-m} \cdot 2 \cdot \left|\sum_{S \in \mathcal{T}} \prod_{i \in S} x_i\right|$,

[1] We thank Avishay Tal for telling us about this result and allowing us to include it and its proof in this note.

where the last term depends on x. Thus, Hoeffding's inequality [Hoe63] implies the concentration bound

$$\begin{aligned}\Pr\left[\left|\sum_{S\in\mathcal{T}}\widehat{\tilde{\boldsymbol{g}}}(S)-\sum_{S\in\mathcal{T}}\widehat{g}(S)\right|\geq\varepsilon\right]&\leq 2\exp\left(-\frac{2\cdot\varepsilon^2}{\sum_{x\in\{-1,1\}^m}\left(2\cdot 2^{-m}\cdot\left|\sum_{S\in\mathcal{T}}\prod_{i\in S}x_i\right|\right)^2}\right)\\&=2\exp\left(-\frac{2^{m-1}\cdot\varepsilon^2}{2^{-m}\sum_{x\in\{-1,1\}^m}\left(\sum_{S\in\mathcal{T}}\prod_{i\in S}x_i\right)^2}\right)\end{aligned}$$

It remains to show that the denominator is equal to $|\mathcal{T}|$: first note that this sum can be written as $\mathbb{E}_{x\sim X_0^m}\left[\left(\sum_{S\in\mathcal{T}}\prod_{i\in S}x_i\right)^2\right]$ where the x_i are distributed as iid random signs. Note that for $S\neq\emptyset$ we have that $\prod_{i\in S}x_i$ has mean zero and is marginally distributed as a random sign, and for $S=\emptyset$ we have that $\prod_{i\in S}x_i=1$, so that if $\emptyset\in\mathcal{T}$ we can write $\mathbb{E}_{x\sim X_0^m}\left[\left(\sum_{S\in\mathcal{T}}\prod_{i\in S}x_i\right)^2\right]=1+\mathbb{E}_{x\sim X_0^m}\left[\left(\sum_{S\in\mathcal{T}\setminus\{\emptyset\}}\prod_{i\in S}x_i\right)^2\right]$ with $|\mathcal{T}\setminus\{\emptyset\}|=|\mathcal{T}|-1$, and thus it suffices to consider the case that $\mathcal{T}$ does not contain the empty set.

In this case, we have that $\mathbb{E}_{x\sim X_0^n}\left[\left(\sum_{S\in\mathcal{T}}\prod_{i\in S}x_i\right)^2\right]$ is the variance of a sum of $|\mathcal{T}|$ random variables each marginally distributed as a random sign. Since all the terms are distinct, given $S\neq S'\in\mathcal{T}$ we know there exists some j in the symmetric difference of S and S' (without loss of generality in S), and thus the covariance of $\prod_{i\in S}x_i$ and $\prod_{i\in S'}x_i$ is zero, as x_j has mean zero even conditioned on the value of $\prod_{i\in S'}x_i$. Hence, these variables are all uncorrelated, and so the variance of their sum is simply the sum of the variances, which is $|\mathcal{T}|\cdot 1=|\mathcal{T}|$ as desired. ☐

Applying Lemma 3.5 to the majority function proves Proposition 3.4.

Proof of Proposition 3.4. Let $f:\{-1,1\}^n\to\{-1,1\}$ be the majority function on n bits for n odd, and $\tilde{\boldsymbol{f}}:\{-1,1\}^n\to\{-1,1\}$ be the random function which independently for each $x\in\{-1,1\}^n$ sets $\tilde{\boldsymbol{f}}(x)$ with expectation $B/\sqrt{n}\cdot f(x)$. Then define $\tilde{\boldsymbol{\mathcal{F}}}$ to be the set of all restrictions of all functions of the form $z\mapsto\tau\cdot\tilde{\boldsymbol{f}}(z_1\sigma_1,\dots,z_n\sigma_n)$ for $\tau\in\{-1,1\}$ and $\sigma\in\{-1,1\}^n$.

We claim that with positive probability $\tilde{\boldsymbol{\mathcal{F}}}$ has the desired properties. Note that $\tilde{\boldsymbol{\mathcal{F}}}$ is closed under restriction, negation of input variables, and negation of the output by definition. To prove the coin theorem claim, by Tal's result (Lemma 3.2) it is enough to prove the level 1 bound $\mathcal{L}_1^1(\tilde{\boldsymbol{\mathcal{F}}})\leq B$. Thus, we need to show that with positive probability $\mathcal{L}_1^1(\tilde{\boldsymbol{\mathcal{F}}})\leq B$ and $\mathcal{L}_1^3(\tilde{\boldsymbol{\mathcal{F}}})\geq\Omega(B\cdot n)$ (we will in fact show an upper bound of $B+1$, which is equivalent by shifting).

Since $\mathcal{L}_1^3(f)=\Theta(n^{3/2})$ (see e.g. [O'D14, Problem 5.26]), we have $\mathcal{L}_1^3(B/\sqrt{n}\cdot f)=\Theta(B\cdot n)$, so applying Lemma 3.5 to $B/\sqrt{n}\cdot f$ and $\mathcal{T}=\{S\subseteq[n]\mid |S|=3\}$ implies that

$$\Pr\left[\mathcal{L}_1^3(\tilde{\boldsymbol{\mathcal{F}}})\geq\mathcal{L}_1^3(\tilde{\boldsymbol{f}})\geq\mathcal{L}_1^3(B/\sqrt{n}\cdot f)-n=\Omega(B\cdot n)\right]\geq 1-\exp(-\Omega(2^n/n)).$$

For the level one bound, since $\tilde{\boldsymbol{\mathcal{F}}}$ is closed under negation of input variables, it suffices to bound the sum of the level 1 Fourier coefficients of each member of $\tilde{\boldsymbol{\mathcal{F}}}$. For this, consider a fixed sign $\tau\in\{-1,1\}$, sign pattern $\sigma\in\{-1,1\}^n$, and restriction ρ of $z\mapsto\tau\cdot\tilde{\boldsymbol{f}}(z_1\sigma_1,\dots,z_n\sigma_n)$ keeping m variables alive, which we denote $\tilde{\boldsymbol{f}}|_\rho^{\sigma,\tau}$. By Parseval and Cauchy-Schwarz, the sum of the level 1 Fourier coefficients of any Boolean function on m variables is at most $\sqrt{m}$, so if $\sqrt{m}\leq B$ then $\mathcal{L}_1^1(\tilde{\boldsymbol{f}}|_\rho^{\sigma,\tau})\leq B$ with probability 1. Thus, assume without loss of generality that $m>B^2$. Define $g:\{-1,1\}^m\to\{\pm B/\sqrt{n}\}$ be given by $g(z_1,\dots,z_m)=B/\sqrt{n}\cdot\tau\cdot f(x_1,\dots,x_n)$ where x_i is equal to $\sigma_i\cdot\rho(i)$ if i is fixed by R, and equal to $\sigma_j\cdot z_j$ for j the index of i in the free coordinates otherwise. Then the sum of the singleton Fourier coefficients of the restriction $\tilde{\boldsymbol{f}}|_\rho^{\sigma,\tau}$ is distributed exactly as the sum of the Fourier coefficients $\tilde{\boldsymbol{g}}:\{-1,1\}^m\to\{-1,1\}$ where $\tilde{\boldsymbol{g}}(x)$ is set independently for each $x\in\{-1,1\}^m$ with expectation $g(x)$. Since the sum of g's singleton Fourier coefficients is at most $(B/\sqrt{n})\cdot\sqrt{m}\leq B$, by Lemma 3.5 we have

$$\Pr\left[\mathcal{L}_1^1(\tilde{\boldsymbol{f}}|_\rho^{\sigma,\tau})\geq B+1\right]\leq 2\exp\left(-2^{m-1}/m\right).$$

Now, by assumption $m \geq B^2 \geq \log n + O(\sqrt{\log n})$, so since $m \mapsto 2^m/m$ is increasing in m for $m \geq 1/\ln 2$, this probability is at most $\exp(-\omega(n))$. Thus, since there are $2^{O(n)}$ functions $\tilde{\boldsymbol{f}}|_\rho^{\sigma,\tau}$, we conclude by a union bound. $\square$

It remains to give the proof of Lemma 3.2.

Proof of Lemma 3.2 [Tal19]. By Proposition 2.1, the sum of the partial derivatives of f at zero can be bounded in terms of $\mathcal{L}_1^1(f)$. Tal [Tal19] observed that by a technique of Chattopadhyay, Hatami, Hosseini, and Lovett [CHHL18], the partial derivatives at any other point can be bounded in terms of the Fourier coefficients of appropriate restrictions of f. Formally, for $\varepsilon_0 \in [-1, 1]$ we have that there exists a distribution $\mathcal{D}^{(n)}(\varepsilon_0)$ over restrictions ρ such that for $\varepsilon \in [|\varepsilon_0| - 1, 1 - |\varepsilon_0|]$,

$$\mathbb{E}\big[f\big(X^n_{\varepsilon_0+\varepsilon}\big)\big] = \mathop{\mathbb{E}}_{\rho \sim \mathcal{D}^{(n)}(\varepsilon_0)}\Big[f|_\rho\Big(X^n_{\varepsilon/(1-|\varepsilon_0|)}\Big)\Big].$$

Therefore, letting $g(\varepsilon) = \mathbb{E}[f(X^n_\varepsilon)]$, we have for $|\varepsilon_0| < 1$ that

$$\begin{aligned}
g'(\varepsilon_0) &= \lim_{\varepsilon \to 0} \frac{g(\varepsilon_0 + \varepsilon) - g(\varepsilon_0)}{\varepsilon} \\
&= \lim_{\varepsilon \to 0} \frac{\mathbb{E}\big[f\big(X^n_{\varepsilon_0+\varepsilon}\big)\big] - \mathbb{E}\big[f\big(X^n_{\varepsilon_0+0}\big)\big]}{\varepsilon} \\
&= \lim_{\varepsilon \to 0} \mathop{\mathbb{E}}_{\rho \sim \mathcal{D}^{(n)}(\varepsilon_0)}\left[\frac{\mathbb{E}\Big[f|_\rho\Big(X^n_{\varepsilon/(1-|\varepsilon_0|)}\Big)\Big] - \mathbb{E}\Big[f|_\rho\Big(X^n_{0/(1-|\varepsilon_0|)}\Big)\Big]}{\varepsilon}\right] \\
&= \mathop{\mathbb{E}}_{\rho \sim \mathcal{D}^{(n)}(\varepsilon_0)}\left[\frac{1}{1-|\varepsilon_0|} \cdot \lim_{\delta \to 0} \frac{\mathbb{E}[f|_\rho(X^n_\delta)] - \mathbb{E}[f|_\rho(X^n_0)]}{\delta}\right] && \text{(setting } \delta = \varepsilon/(1-|\varepsilon_0|)) \\
&= \frac{1}{1-|\varepsilon_0|} \cdot \mathop{\mathbb{E}}_{\rho \sim \mathcal{D}^{(n)}(\varepsilon_0)}\left[\sum_{i=1}^n \widehat{f|_\rho}(\{i\})\right]. && \text{(by Proposition 2.1)}
\end{aligned}$$

Since $\mathcal{F}$ is closed under restriction, we have for every ρ that $\left|\sum_{i=1}^n \widehat{f|_\rho}(\{i\})\right| \leq t$, and so we can bound $|g'(x)| \leq t/(1-|x|)$. The result follows since $\mathbb{E}[f(X^n_\varepsilon)] - \mathbb{E}[f(X^n_0)] = g(\varepsilon) - g(0) = \int_0^\varepsilon g'(x)\,dx$. $\square$

4 Acknowledgements

We thank Salil Vadhan for helpful conversations and his feedback on this note, and Avishay Tal for his feedback on this note, telling us about Lemma 3.2, and allowing us to include it and its proof in this note.

References

[Aar10] S. Aaronson, "BQP and the Polynomial Hierarchy," in *Proceedings of the Forty-Second ACM Symposium on Theory of Computing*, ser. STOC '10. New York, NY, USA: ACM, 2010, pp. 141–150.

[Ajt83] M. Ajtai, "Σ_1^1-Formulae on finite structures," *Annals of Pure and Applied Logic*, vol. 24, no. 1, pp. 1–48, Jul. 1983.

[AW89] M. Ajtai and A. Wigderson, "Deterministic Simulation of Probabilistic Constant Depth Circuits," *Advances in Computing Research*, vol. 5, pp. 199–222, 1989.

[BOH90] Y. Brandman, A. Orlitsky, and J. Hennessy, "A spectral lower bound technique for the size of decision trees and two-level AND/OR circuits," *IEEE Transactions on Computers*, vol. 39, no. 2, pp. 282–287, Feb. 1990.

[Bop97] R. B. Boppana, "The average sensitivity of bounded-depth circuits," *Information Processing Letters*, vol. 63, no. 5, pp. 257–261, Sep. 1997.

[BV10] J. Brody and E. Verbin, "The Coin Problem and Pseudorandomness for Branching Programs," in *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*. Las Vegas, NV, USA: IEEE, Oct. 2010, pp. 30–39.

[CGR14] G. Cohen, A. Ganor, and R. Raz, "Two Sides of the Coin Problem," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2014)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), K. Jansen, J. D. P. Rolim, N. R. Devanur, and C. Moore, Eds., vol. 28. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2014, pp. 618–629.

[CHHL18] E. Chattopadhyay, P. Hatami, K. Hosseini, and S. Lovett, "Pseudorandom Generators from Polarizing Random Walks," *Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik GmbH, Wadern/Saarbruecken, Germany*, 2018.

[CHRT18] E. Chattopadhyay, P. Hatami, O. Reingold, and A. Tal, "Improved Pseudorandomness for Unordered Branching Programs Through Local Monotonicity," in *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, ser. STOC 2018. New York, NY, USA: ACM, 2018, pp. 363–375.

[GMR+12] P. Gopalan, R. Meka, O. Reingold, L. Trevisan, and S. Vadhan, "Better Pseudorandom Generators from Milder Pseudorandom Restrictions," in *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, Oct. 2012, pp. 120–129.

[Hås01] J. Håstad, "A Slight Sharpening of LMN," *Journal of Computer and System Sciences*, vol. 63, no. 3, pp. 498–508, Nov. 2001.

[Hoe63] W. Hoeffding, "Probability Inequalities for Sums of Bounded Random Variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963.

[KKL88] J. Kahn, G. Kalai, and N. Linial, "The influence of variables on Boolean functions," in *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, Oct. 1988, pp. 68–80.

[Lee19] C. H. Lee, "Fourier bounds and pseudorandom generators for product tests," Electronic Colloquium on Computational Complexity, Tech. Rep. 017, 2019, to appear in Computational Complexity Conference (CCC'19).

[LMN93] N. Linial, Y. Mansour, and N. Nisan, "Constant Depth Circuits, Fourier Transform, and Learnability," *J. ACM*, vol. 40, no. 3, pp. 607–620, Jul. 1993.

[LSS+18] N. Limaye, K. Sreenivasaiah, S. Srinivasan, U. Tripathi, and S. Venkitesh, "A Fixed-Depth Size-Hierarchy Theorem for $\mathrm{AC}^0[\oplus]$ via the Coin Problem," *arXiv:1809.04092 [cs]*, Sep. 2018.

[LV18] C. H. Lee and E. Viola, "The Coin Problem for Product Tests," *ACM Trans. Comput. Theory*, vol. 10, no. 3, pp. 14:1–14:10, Jun. 2018.

[NN93] J. Naor and M. Naor, "Small-Bias Probability Spaces: Efficient Constructions and Applications," *SIAM Journal on Computing*, vol. 22, no. 4, pp. 838–856, Aug. 1993.

[O'D14] R. O'Donnell, *Analysis of Boolean Functions*, 1st ed. New York, NY: Cambridge University Press, Jun. 2014.

[RSV13] O. Reingold, T. Steinke, and S. Vadhan, "Pseudorandomness for Regular Branching Programs via Fourier Analysis," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, ser. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, Aug. 2013, pp. 655–670.

[Ste13] J. Steinberger, "The Distinguishability of Product Distributions by Read-Once Branching Programs," in *2013 IEEE Conference on Computational Complexity*. Stanford, CA, USA: IEEE, Jun. 2013, pp. 248–254.

[SV10] R. Shaltiel and E. Viola, "Hardness Amplification Proofs Require Majority," *SIAM Journal on Computing*, vol. 39, no. 7, pp. 3122–3154, Jan. 2010.

[SVW17] T. Steinke, S. Vadhan, and A. Wan, "Pseudorandomness and Fourier-Growth Bounds for Width-3 Branching Programs," *Theory of Computing*, vol. 13, pp. 1–50, Oct. 2017.

[Tal17] A. Tal, "Tight Bounds on the Fourier Spectrum of AC^0," in *32nd Computational Complexity Conference (CCC 2017)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), R. O'Donnell, Ed., vol. 79. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017, pp. 15:1–15:31.

[Tal19] ——, Private Communication, 2019.

[Val84] L. G. Valiant, "Short monotone formulae for the majority function," *Journal of Algorithms*, vol. 5, no. 3, pp. 363–366, Sep. 1984.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il