THEORY OF COMPUTING, Volume 5 (2009), pp. 69–82
www.theoryofcomputing.org

Unconditional Pseudorandom Generators for Low-Degree Polynomials

Shachar Lovett*

Received: July 14, 2008; published: May 27, 2008.

Abstract: We give an explicit construction of a pseudorandom generator against low-degree polynomials over finite fields. Pseudorandom generators against linear polynomials, known as *small-bias generators*, were first introduced by Naor and Naor (STOC 1990). We show that the sum of 2^d independent small-bias generators with error $\varepsilon^{2^{O(d)}}$ is a pseudorandom generator against degree-d polynomials with error ε. This gives a generator with seed length $2^{O(d)} \log(n/\varepsilon)$ against degree-d polynomails. Our construction follows the breakthrough result of Bogdanov and Viola (FOCS 2007). Their work shows that the sum of d small-bias generators is a pseudo-random generator against degree-d polynomials, assuming a conjecture in additive combinatorics, known as *the inverse conjecture for the Gowers norm*. However, this conjecture was proven only for $d = 2,3$. The main advantage of this work is that it does not rely on any unproven conjectures.

Subsequently, the inverse conjecture for the Gowers norm was shown to be false for $d \geq 4$ by Green and Tao (2008) and independently by the author, Roy Meshulam, and Alex Samorodnitsky (STOC 2008). A revised version of the conjecture was proved by Bergelson, Tao, and Ziegler (2009). Additionally, Viola (CCC 2008) showed the original construction of Bogdanov and Viola to hold unconditionally.

ACM Classification: F.2.1, F.1.3, F.2.2, G.2, G.3

AMS Classification: 68Q10, 68Q17, 12Y05, 60C05

Key words and phrases: pseudorandom, explicit constructions, polynomials, low degree

*Research supported by the Israel Science Foundation (grant 1300/05)

DOI: 10.4086/toc.2009.v005a003

1 Introduction

We are interested in explicitly constructing pseudorandom generators (PRG) against low-degree polynomials over small finite fields. A pseudorandom generator against a family $\mathbb{T}$ of tests is a function G mapping a small domain into a (much) larger one, such that any test $T \in \mathbb{T}$ cannot distinguish, with noticeable probability, a random element in the large domain from an application of G to a random element in the small domain. We say a PRG requires R random bits if the size of the small domain is 2^R.

In our case, $\mathbb{F}$ is a finite field and a test is a polynomial $p(x_1,\dots,x_n)$ over $\mathbb{F}$. The image of the PRG is a small subset of $\mathbb{F}^n$, and it is pseudorandom against $p(x_1,\dots,x_n)$ if the distribution of the outcome of p, when applied to a random element in the small subset, is close to the distribution of the outcome of p, when applied to a uniform element in $\mathbb{F}^n$. We say the PRG has error ε against p if the statistical distance between the two distributions is at most ε. We are interested in PRGs that are pseudorandom against all degree-d polynomials with error ε, and use as few random bits as possible.

The case of pseudorandom generators against linear polynomials, usually called *small-bias generators* (or *epsilon-biased generators*, a term we do not use in this paper to avoid confusion), was first studied (over $\mathbb{F} = \mathbb{F}_2$) by Naor and Naor [14] and later by Alon, Goldreich, Håstad and Peralta [1]. They and others gave explicit constructions, which were later generalized to arbitrary finite fields. These constructions have a seed length which is optimal up to a constant multiplicative factor. The construction of small-bias generators is a major tool in derandomization, PCPs and lower bounds (see [4] and the references within for details regarding small-bias generators).

The generalization of the problem to constant-degree polynomials was first studied by Luby, Velickovic, and Wigderson [13]. Their results apply, in fact, to the more general model of constant depth circuits. In the context of constant degree polynomials, they give an explicit construction of PRG requiring $\exp(O(\sqrt{\log n/\varepsilon}))$ random bits.

Bogdanov [6] gave a construction of a PRG in large fields. The minimum field size required for his construction is polynomial in the degree, the required error and the log of the number of variables. In these settings, his construction is optimal up to polynomial factors. The proof of his result uses techniques and results from algebraic geometry and computational algebra.

Recently, Bogdanov and Viola [7] presented a novel approach for constructing a PRG for low-degree polynomials over small fields. Their construction is the sum of d independent small-bias generators. They showed that, if a conjecture in additive combinatorics called the *inverse conjecture for the Gowers norm* holds, then their construction is a PRG for degree-d polynomials. At the time, the inverse conjecture for the Gowers norm was known to hold only for degrees 2 and 3, and was conjectured to hold for all constant degrees. Thus, their construction was known to be correct only for quadratic and cubic polynomials.

Our work [11] was inspired by the work of Bogdanov and Viola, with the goal of making their construction unconditional, i. e., not relying on any unproven conjectures. We prove that the sum of 2^d independent small-bias generators is pseudorandom against degree-d polynomials, without relying on any unproven conjectures. Our main theorem is:

Theorem 1.1. *There exists a global constant $c > 0$ such that the following holds. Let G be a small-bias generator with error $\varepsilon^{2^{cd}}$. Then the sum of 2^d independent copies of G is pseudorandom against degree-d polynomials with error ε. In particular, this gives a pseudorandom generator for degree-d polynomials* *with error ε using $2^{cd}\log(|\mathbb{F}|n/\varepsilon)$ random bits for the seed.*

1.1 Overview of proof method

This work is inspired by the recent result of Bogdanov and Viola [7]. We begin by providing a high level description of it, since several ideas used in [7] are also used in our work.

The analysis of [7] crucially depended on the inverse conjecture for the Gowers norm. Although we do not use this conjecture in our proof, we now briefly present and discuss it. The Gowers norm, first defined by Gowers in his new proof for Szemerédi's theorem [8], is a norm measuring the local correlation of a function to low-degree polynomials. Let $\mathbb{F} = \mathbb{F}_q$ be a prime finite field, and assume $f(\mathbf{x}) : \mathbb{F}^n \to \mathbb{F}$ is a function. The directional derivative of f in direction $\mathbf{y} \in \mathbb{F}^n$ is defined to be

$$f_{\mathbf{y}}(\mathbf{x}) = f(\mathbf{x}+\mathbf{y}) - f(\mathbf{x}).$$

Notice that if f is a degree-d polynomial, then $f_{\mathbf{y}}$ is a polynomial of degree at most $d-1$, hence the term derivative relates to the more common definition of analytical derivative. We define also iterated derivatives: $f_{\mathbf{y}_1,\ldots,\mathbf{y}_k}(x)$ is defined recursively, by taking the k derivatives in directions $y_1,\ldots,y_k$. Opening brackets, this gives

$$f_{\mathbf{y}_1,\ldots,\mathbf{y}_k}(\mathbf{x}) = \sum_{S\subset\{1,\ldots,k\}} (-1)^{k-|S|} f(\mathbf{x}+\sum_{i\in S}\mathbf{y}_i).$$

The d-th Gowers norm of f is defined as

$$U_d(f) = \left(\mathbb{E}_{\mathbf{x},\mathbf{y}_1,\ldots\mathbf{y}_d\in\mathbb{F}_q^n}\left[\omega_q^{f_{\mathbf{y}_1,\ldots,\mathbf{y}_d}(\mathbf{x})}\right]\right)^{\frac{1}{2^d}},$$

where $\omega_q = e^{\frac{2\pi i}{q}}$ is a root of unity of order q. It was proved to be a norm on functions (for $d \ge 2$) by Gowers [8].

Assume f is a degree-$(d-1)$ polynomial. Taking d derivatives results in the zero polynomial, so $f_{\mathbf{y}_1,\ldots,\mathbf{y}_d} \equiv 0$ for any choice of $\mathbf{y}_1,\ldots,\mathbf{y}_d$ and consequently $U_d(f) = 1$. It is relatively easy to see that the converse also holds, that is, $U_d(f) = 1$ iff f is a polynomial of degree at most $d-1$. Alon et al. [2] proved a robust version of this equivalence: the d-th Gowers norm of f is very close to 1 iff the function f is very close to a degree-$(d-1)$ polynomial.

The inverse conjecture for the Gowers norm studies the realm of functions with only a noticeable Gowers norm, that is $U_d(f) \ge \delta$ for some $\delta > 0$. Gowers [8] showed that if f is only somewhat close to a degree-$(d-1)$ polynomial, that is $\Pr_{\mathbf{x}}[f(\mathbf{x}) = p(\mathbf{x})] \ge 1/q + \varepsilon$ for some degree-$(d-1)$ polynomial $p(\mathbf{x})$, then f has a noticeable d-th Gowers norm, $U_d(f) \ge \varepsilon'$, where $\varepsilon' = \Omega(\varepsilon)$.

The converse of this claim is known as the inverse conjecture for the Gowers norm: if $U_d(f) \ge \varepsilon$, then there exists a degree-$(d-1)$ polynomial p such that $\Pr_{\mathbf{x}}[f(\mathbf{x}) = p(\mathbf{x})] \ge 1/q + \varepsilon'$, for some $\varepsilon' > 0$ depending on ε. The case of $d = 2$ can be proven using standard Fourier analysis tools [3]. The case of $d = 3$ was proven by Green and Tao [10] and independently by Samorodnitsy [15]. Both works conjectured this to hold for any constant degree.

Returning to the argument of [7], Bogdanov and Viola analyze the Gowers norm of a degree-d polynomial $p(\mathbf{x})$, and present a win-win argument, depending on whether the Gowers norm is either small or large. In the first case, when the Gowers norm is small, they show that the sum of d small-bias generators is pseudorandom against $p(\mathbf{x})$, by relating the distribution of $p(\mathbf{x}_1+\cdots+\mathbf{x}_d)$ to the Gowers norm of p. In the latter case, when the Gowers norm is large, and assuming the inverse conjecture for the Gowers norm holds, $p(\mathbf{x})$ is correlated to some degree-$(d-1)$ polynomial $q(\mathbf{x})$. They use $q(\mathbf{x})$ in order to construct a circuit that computes $p(\mathbf{x})$ for almost all values of x. The inputs to this circuit are all degree-$(d-1)$ polynomials; thus they show that a PRG for degree-$(d-1)$ polynomials with small enough error is also pseudorandom against $p(\mathbf{x})$.

Our construction follows similar lines; however, instead of analyzing the Gowers norm of $p(\mathbf{x})$, we analyze its Fourier coefficients. We also divide our treatment into two cases: when p has some large Fourier coefficient, and when all the Fourier coefficients of p are small.

In the first case, when $p(\mathbf{x})$ has no large Fourier coefficients, we consider inputs to p of the form $\mathbf{x}+\mathbf{y}$, where $\mathbf{x}$ and $\mathbf{y}$ are independent. We consider the polynomial

$$\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}'') = p(\mathbf{x}'+\mathbf{y}') - p(\mathbf{x}'+\mathbf{y}'') - p(\mathbf{x}''+\mathbf{y}') + p(\mathbf{x}''+\mathbf{y}'')\,.$$

We prove that it is enough to be pseudorandom against Δp in order to be pseudorandom against $p(\mathbf{x}+\mathbf{y})$, and also that it is sufficient to have $\mathbf{x}$, $\mathbf{x}'$, $\mathbf{x}''$, $\mathbf{y}$, $\mathbf{y}'$ and $\mathbf{y}''$ come from a PRG that is pseudorandom against degree-$(d-1)$ polynomials. The reason is that Δp contains no degree-d terms in just one of $\mathbf{x}'$, $\mathbf{x}''$, $\mathbf{y}'$ or $\mathbf{y}''$. In the second case, when there is some large Fourier coefficient, we know that $p(\mathbf{x})$ is correlated to some linear function. Similarly to the second case in [7], we also show in that case, or more generally when $p(\mathbf{x})$ is correlated to some lower degree polynomial, a PRG for degree-$(d-1)$ polynomials with small enough error is also pseudorandom against $p(\mathbf{x})$. However, our proof technique is more direct than the one used in [7], which results in better parameters and simpler analysis.

1.2 Subsequent work

This paper is a more polished version of the extended abstract of this work [11], first presented at STOC 2008. Subsequently, there were advances on two fronts.

First, the inverse conjecture for the Gowers norm was shown to be false for degrees ≥ 4 by Green and Tao [9] and independently by Lovett, Meshulam, and Samorodnitsky [12]. A revised inverse conjecture for the Gowers norm was proved by Bergelson, Tao and Ziegler [5, 17].

Additionally, Viola [18] proved the correctness of the construction of [7] without using the inverse conjecture for the Gowers norm, or any other unproven conjectures, thus making the original construction of [7] unconditionally correct. His proof method also follows similar lines to the works of [7] and [11]. He considers $p(\mathbf{x}+\mathbf{y})$, where $\mathbf{x}$ comes from a distribution which is pseudorandom against degree-$(d-1)$ polynomials, and $\mathbf{y}$ is a small-bias generator (i. e., pseudorandom against linear polynomials). He also uses a win-win analysis, based on the *bias* of the polynomial p, and proves that indeed the sum $\mathbf{x}+\mathbf{y}$ fools all degree-d polynomials.

The result presented here can thus be seen as an intermediate step in a sequence of works. The proof of Viola uses some of the techniques developed in this work, in addition to some of the original techniques introduced in [7] and some clever new ideas.

2 Preliminaries

We work over an arbitrary finite field $\mathbb{F}$. Let $U = U_n$ be the uniform distribution over $\mathbb{F}^n$. We fix $e : \mathbb{F} \to \mathbb{C}$ to be any non-trivial additive character. For example, in a prime field $\mathbb{F}_q$ we can have $e(x) = \omega_q^x$ where $\omega_q = 2^{\frac{2\pi i}{q}}$ is a root of unity of order q. When we refer to the degree of a multivariate polynomial, we always mean its total degree. We denote elements of $\mathbb{F}^n$ by $\mathbf{x} = (x_1, \ldots, x_n)$.

Definition 2.1. A distribution D over $\mathbb{F}^n$ is said to be pseudorandom against a polynomial $p(x_1, \ldots, x_n)$ with error ε if

$$\left| \mathbb{E}_{\mathbf{x} \in D} \left[e(p(\mathbf{x})) \right] - \mathbb{E}_{\mathbf{x} \in U} \left[e(p(\mathbf{x})) \right] \right| < \varepsilon .$$

Definition 2.2. A distribution D is said to be pseudorandom against degree-d polynomials with error ε if for every degree-d polynomial $p(x_1, \ldots, x_n)$, D is pseudorandom against p with error ε.

We study explicit constructions for pseudorandom generators against degree-d polynomials.

Definition 2.3. A function $G : \{0,1\}^r \to \mathbb{F}^n$ is said to be a pseudorandom-generator (PRG) against degree-d polynomials if the distribution obtained by applying G to a uniform element in $\{0,1\}^r$ is a pseudorandom distribution against degree-d polynomials. The value in $\{0,1\}^r$ is called the *seed* of G, and r is the *seed length* of G.

The notion of pseudorandomness we use is different from more standard notions of pseudorandomness. However, since we are working over small fields, they are tightly related. For example, the following Lemma from [7] connects it with the common notion of pseudorandomness in statistical distance (The proof in [7] is stated just for prime fields, but it remains correct over arbitrary fields):

Lemma 2.4 (Lemma 33 in [7])**.** *Let D be a distribution that is pseudorandom against degree-d polynomials with error ε. Let $p(x_1, \ldots, x_n)$ be a polynomial of degree at most d. Let $p(D)$ be the distribution, taking values in $\mathbb{F}$, obtained by applying p to an input chosen according to D, and similarly $p(U)$ be the distribution of applying p to a uniformly chosen input in $\mathbb{F}^n$. Then the variation (statistical) distance between $p(D)$ and $p(U)$ is bounded by $\frac{1}{2}\varepsilon\sqrt{|\mathbb{F}|-1}$.*

Remark 2.5. Definition 2.2 does not depend on which non-trivial character is used in Definition 2.1; since we require pseudorandomness for all degree-d polynomials, we can multiply polynomials by any non-zero constant, thus effectively achieving pseudorandomness for all non-trivial characters.

We use the Cauchy-Schwarz inequality over the complex numbers in the following form several times in the proof.

Claim 2.6. *Let Z be a random variable taking values in $\mathbb{C}$, then*

$$\left| \mathbb{E}[Z] \right|^2 \le \mathbb{E}\left[|Z|^2 \right] .$$

Fourier analysis plays a central role in our proof. In the following we define Fourier coefficients, and discuss several properties of them required in the proof. We refer to the first chapter of [16] for a more in-depth introduction to Fourier analysis.

Definition 2.7. The Fourier coefficients of a function $f : \mathbb{F}^n \to \mathbb{C}$ are defined to be

$$\hat{f}_\alpha = \mathbb{E}_{\mathbf{x}\in U}\left[f(\mathbf{x})e(-\langle\alpha,\mathbf{x}\rangle)\right],$$

where $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{F}^n$ and $\langle\alpha,\mathbf{x}\rangle = \alpha_1 x_1 + \cdots + \alpha_n x_n$ is the inner product of α and $\mathbf{x}$.

The set of functions $\{e(\langle\alpha,\mathbf{x}\rangle) : \alpha \in \mathbb{F}^n\}$ is an orthonormal basis of the Hermitian space of functions $\mathbb{F}^n \to \mathbb{C}$ under the inner product

$$f \cdot g = \frac{1}{|\mathbb{F}^n|}\sum_{\mathbf{x}\in\mathbb{F}^n}\overline{f(\mathbf{x})}g(\mathbf{x}).$$

Therefore f can be expressed as

$$f(\mathbf{x}) = \sum_{\alpha\in\mathbb{F}^n}\hat{f}_\alpha e(\langle\alpha,\mathbf{x}\rangle).$$

For a polynomial $p(\mathbf{x}) \in \mathbb{F}[x_1,\ldots,x_n]$ we define $\hat{p}_\alpha$ to be the α Fourier coefficient of the function $e(p(\mathbf{x}))$, i. e.,

$$\hat{p}_\alpha = \mathbb{E}_{\mathbf{x}\in U}\left[e(p(\mathbf{x}) - \langle\alpha,\mathbf{x}\rangle)\right].$$

We will need the following simple fact, which follows from Parseval's identity and the fact that $|e(p(\mathbf{x}))| = 1$ for all $\mathbf{x} \in \mathbb{F}^n$:

Fact 2.8. $\sum_{\alpha\in\mathbb{F}^n}|\hat{p}_\alpha|^2 = 1.$

The basis elements of our analysis are PRGs for degree-1 polynomials. PRGs for this family have been studied extensively, and are usually referred to as small-bias (or epsilon-biased) generators or distributions. Formally we define:

Definition 2.9. A distribution D is called a *small-bias distribution* over $\mathbb{F}^n$ with error δ if for all linear polynomials $p(\mathbf{x}) = a_1x_1 + \cdots + a_nx_n$ we have

$$\left|\mathbb{E}_{\mathbf{x}\in D}\left[e(p(\mathbf{x}))\right] - \mathbb{E}_{\mathbf{x}\in U}\left[e(p(\mathbf{x}))\right]\right| < \delta. \tag{2.1}$$

Constructions of small-bias distributions were first studied by Naor and Naor over $\mathbb{F}_2$ in [14], and optimal up to constant constructions were later given by Alon, Goldreich, Håstad, and Peralta [1] over general fields. Such constructions can be achieved by explicit pseudorandom generators with seed length $O(\log(|\mathbb{F}|n/\varepsilon))$.

3 Main theorem

We restate our main theorem with explicit constants:

Theorem 3.1. *Let $G : \{0,1\}^r \to \mathbb{F}^n$ be a small-bias generator over $\mathbb{F}^n$ with error $(\varepsilon/10)^{4^d}$. Then the sum of 2^d independent copies of G is pseudorandom against degree-d polynomials with error ε. That is, $G' : \{0,1\}^{r\cdot 2^d} \to \mathbb{F}^n$ defined as*

$$G'(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_{2^d}) = G(\boldsymbol{x}_1) + \ldots + G(\boldsymbol{x}_{2^d})$$

is a PRG against degree-d polynomials with error ε.

Our proof is divided into two cases, based on whether p has some large Fourier coefficient, or does not have any large Fourier coefficients. We show that when a degree-d polynomial $p(\mathbf{x})$ has some large Fourier coefficient, then a PRG for degree-$(d-1)$ polynomials, with better error, is also pseudorandom against p. On the other hand, if p has no large Fourier coefficients, it is "pseudorandom" in a sense, and then the sum of two PRGs for degree-$(d-1)$ is pseudorandom against p.

We divide the proof into two technical lemmas, dealing with the cases of whether p has some large Fourier coefficient, or it does not.

Lemma 3.2. *Let $p(x_1,\dots,x_n)$ be a degree-d polynomial over $\mathbb{F}^n$, such that for all $\alpha \in \mathbb{F}^n$, $|\hat{p}_\alpha| < \varepsilon^2/10$. Let D be a distribution that is pseudorandom against degree-$(d-1)$ polynomials with error $\varepsilon^4/400$. Then $\boldsymbol{x}+\boldsymbol{y}$, where $\boldsymbol{x}$, $\boldsymbol{y}$ are independently chosen from D, is pseudorandom against p with error ε.*

Lemma 3.3. *Let $p(x_1,\dots,x_n)$ be a degree-d polynomial over $\mathbb{F}^n$, such that $|\hat{p}_\alpha| \geq \varepsilon^2/10$ for some $\alpha \in \mathbb{F}^n$. Let D be a distribution that is pseudorandom against degree-$(d-1)$ polynomials with error $\varepsilon^3/10$. Then D is pseudorandom against $p(\boldsymbol{x})$ with error ε.*

Assuming these two lemmas, our main theorem now follows directly, by also using the following simple observation. This observation allows us to add "extra" small-bias distributions without harming our PRG construction.

Observation 3.4. *Let D be a distribution that is pseudorandom against degree-d polynomials with error ε. Let D' be any other independent distribution. Then the distribution of $\boldsymbol{x}+\boldsymbol{y}$, where $\boldsymbol{x} \in D$ and $\boldsymbol{y} \in D'$ is also pseudorandom against degree-d polynomials with error ε.*

We now prove Theorem 3.1, assuming Lemmas 3.2 and 3.3 and Observation 3.4:

Proof. We prove, by induction on d, that the sum of 2^d independent small-bias generators with error $(\varepsilon/10)^{4^d}$ is pseudorandom against degree-d polynomials with error ε. For $d=1$ this is clear. For $d>1$, let D' be the distribution of sum of the first 2^{d-1} small-bias generators, which is also the distribution of the sum of the last 2^{d-1} small-bias generators. Observe that by the inductive hypothesis, D' is pseudorandom against degree-$(d-1)$ polynomials with error $(\varepsilon/10)^4 < \min(\varepsilon^4/400, \varepsilon^3/10)$. Let $p(x)$ be any degree-d polynomial. Consider first the case that all the Fourier coefficients of p are at most $\varepsilon^2/10$. By Lemma 3.2, we know that the distribution of $\mathbf{x}+\mathbf{y}$, where $\mathbf{x}$ and $\mathbf{y}$ are chosen independently according to D', is pseudorandom against p with error ε. Alternatively, consider the case that there exists some Fourier coefficient of p of absolute value at least $\varepsilon^2/10$. By Lemma 3.3, D' is pseudorandom against p, and by Observation 3.4 so is the distribution of $\mathbf{x}+\mathbf{y}$, where $\mathbf{x}$ and $\mathbf{y}$ are chosen independently according to D'. □

The remainder of the paper is organized as follows: Lemma 3.2 is proven in Section 4 and Lemma 3.3 in Section 5.

4 Case I: No large Fourier coefficients

In this section we prove Lemma 3.2. We assume throughout this section that all the Fourier coefficients of $e(p(\mathbf{x}))$ are small, i. e., $|\hat{p}_\alpha| < \varepsilon^2/10$ for all $\alpha \in \mathbb{F}^n$.

We start by defining a derivation polynomial.

Definition 4.1. Let $p(\mathbf{x}) : \mathbb{F}^n \to \mathbb{F}$ be a polynomial. We define its derivation polynomial $\Delta p : (\mathbb{F}^n)^4 \to \mathbb{F}$ as

$$\Delta p(\mathbf{x}', \mathbf{x}'', \mathbf{y}', \mathbf{y}'') = p(\mathbf{x}' + \mathbf{y}') - p(\mathbf{x}'' + \mathbf{y}') - p(\mathbf{x}' + \mathbf{y}'') + p(\mathbf{x}'' + \mathbf{y}'') .$$

The following lemma is crucial to our analysis, and is a variation of a lemma proven in [7]. We relate the distribution of evaluating p on the sum of two independent inputs to that of Δp.

Lemma 4.2. *Let $p : \mathbb{F}^n \to \mathbb{F}$. Let D be a distribution over $\mathbb{F}^n$. Let $\boldsymbol{x}$, $\boldsymbol{y}$ be independently chosen from D, then*

$$\left|\mathbb{E}_{\boldsymbol{x},\boldsymbol{y} \in D}[e(p(\boldsymbol{x}+\boldsymbol{y}))]\right|^4 \le \mathbb{E}_{\boldsymbol{x}',\boldsymbol{x}'',\boldsymbol{y}',\boldsymbol{y}'' \in D}[e(\Delta p(\boldsymbol{x}',\boldsymbol{x}'',\boldsymbol{y}',\boldsymbol{y}''))] ,$$

where $\boldsymbol{x}', \boldsymbol{x}'', \boldsymbol{y}', \boldsymbol{y}''$ are also independent.

Proof. The proof is essentially applying the Cauchy-Schwarz inequality twice. We start by showing

$$\left|\mathbb{E}_{\mathbf{x},\mathbf{y} \in D}[e(p(\mathbf{x}+\mathbf{y}))]\right|^2 \le \mathbb{E}_{\mathbf{x},\mathbf{y}',\mathbf{y}'' \in D}[e(p(\mathbf{x}+\mathbf{y}') - p(\mathbf{x}+\mathbf{y}''))] ,$$

and then continue to show

$$\left|\mathbb{E}_{\mathbf{x},\mathbf{y} \in D}[e(p(\mathbf{x}+\mathbf{y}))]\right|^4 \le \mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}'' \in D}[e(p(\mathbf{x}'+\mathbf{y}') - p(\mathbf{x}''+\mathbf{y}') - p(\mathbf{x}'+\mathbf{y}'') + p(\mathbf{x}''+\mathbf{y}''))] ,$$

which is what we want to prove, by the definition of Δp. We prove the first part by applying the Cauchy-Schwarz inequality

$$\begin{aligned}
&\left|\mathbb{E}_{\mathbf{x},\mathbf{y} \in D}[e(p(\mathbf{x}+\mathbf{y}))]\right|^2 \le \mathbb{E}_{\mathbf{x} \in D}\left|\mathbb{E}_{\mathbf{y} \in D}[e(p(\mathbf{x}+\mathbf{y}))]\right|^2 = \\
&\mathbb{E}_{\mathbf{x} \in D}\left[\mathbb{E}_{\mathbf{y}' \in D}[e(p(\mathbf{x}+\mathbf{y}'))]\, \overline{\mathbb{E}_{\mathbf{y}'' \in D}[e(p(\mathbf{x}+\mathbf{y}''))]}\right] = \\
&\mathbb{E}_{\mathbf{x},\mathbf{y}',\mathbf{y}'' \in D}[e(p(\mathbf{x}+\mathbf{y}') - p(\mathbf{x}+\mathbf{y}''))] .
\end{aligned}$$

We prove the second part by applying the Cauchy-Schwarz inequality again

$$\begin{aligned}
&\left|\mathbb{E}_{\mathbf{x},\mathbf{y} \in D}[e(p(\mathbf{x}+\mathbf{y}))]\right|^4 \le \\
&\left|\mathbb{E}_{\mathbf{x},\mathbf{y}',\mathbf{y}'' \in D}[e(p(\mathbf{x}+\mathbf{y}') - p(\mathbf{x}+\mathbf{y}''))]\right|^2 \le \\
&\mathbb{E}_{\mathbf{y}',\mathbf{y}'' \in D}\left|\mathbb{E}_{\mathbf{x} \in D}[e(p(\mathbf{x}+\mathbf{y}') - p(\mathbf{x}+\mathbf{y}''))]\right|^2 = \\
&\mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}'' \in D}\left[e(p(\mathbf{x}'+\mathbf{y}') - p(\mathbf{x}'+\mathbf{y}'') - p(\mathbf{x}''+\mathbf{y}') + p(\mathbf{x}''+\mathbf{y}''))\right] .
\end{aligned}$$

□

In particular the following corollary follows:

Corollary 4.3. $\mathbb{E}_{\boldsymbol{x}',\boldsymbol{x}'',\boldsymbol{y}',\boldsymbol{y}'' \in D}\left[e(\Delta p(\boldsymbol{x}',\boldsymbol{x}'',\boldsymbol{y}',\boldsymbol{y}''))\right] \ge 0$.

We analyze the expression $\mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}'' \in D}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right]$, in two cases: when $D = U$ is the uniform distribution and when D is a PRG for degree-$(d-1)$ polynomials. We show that in both cases it is at most $\varepsilon/2$. Combining this with Lemma 4.2 yields the required result. We start our analysis in the uniform case.

We begin by showing the (well-known) connection between the average value of Δp and the Fourier coefficients of p, regarding Δp as an affinity-test for p. A similar analysis, carried in more depth, can be found in [3].

Lemma 4.4.

$$\mathbb{E}_{\boldsymbol{x}',\boldsymbol{x}'',\boldsymbol{y}',\boldsymbol{y}''\in U}\left[e(p(\mathbf{x}'+\mathbf{y}')-p(\mathbf{x}'+\mathbf{y}'')-p(\mathbf{x}''+\mathbf{y}')+p(\mathbf{x}''+\mathbf{y}''))\right] = \sum_{\alpha\in\mathbb{F}^n}|\hat{p}_\alpha|^4 .$$

Proof. We can write $e(p(\mathbf{x}))$ in the Fourier basis as

$$e(p(\mathbf{x})) = \sum_{\alpha\in\mathbb{F}^n}\hat{p}_\alpha e(\langle\alpha,\mathbf{x}\rangle) .$$

Notice that

$$e(-p(\mathbf{x})) = \overline{e(p(\mathbf{x}))} = \sum_{\alpha\in\mathbb{F}^n}\overline{\hat{p}_\alpha}e(-\langle\alpha,\mathbf{x}\rangle) .$$

We now expand all four terms of p in

$$e(p(\mathbf{x}'+\mathbf{y}')-p(\mathbf{x}'+\mathbf{y}'')-p(\mathbf{x}''+\mathbf{y}')+p(\mathbf{x}''+\mathbf{y}'')) .$$

This is equal to

$$\sum_{\alpha_1,\alpha_2,\alpha_3,\alpha_4\in\mathbb{F}^n}\hat{p}_{\alpha_1}e(\langle\alpha_1,\mathbf{x}'+\mathbf{y}'\rangle)\,\overline{\hat{p}_{\alpha_2}}e(-\langle\alpha_2,\mathbf{x}'+\mathbf{y}''\rangle)\,\overline{\hat{p}_{\alpha_3}}e(-\langle\alpha_3,\mathbf{x}''+\mathbf{y}'\rangle)\,\hat{p}_{\alpha_4}e(\langle\alpha_4,\mathbf{x}''+\mathbf{y}''\rangle) .$$

Remember that we are interested in the expected value over uniform $\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in\mathbb{F}^n$, i. e., in

$$\mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in U}\left[e(p(\mathbf{x}'+\mathbf{y}')-p(\mathbf{x}'+\mathbf{y}'')-p(\mathbf{x}''+\mathbf{y}')+p(\mathbf{x}''+\mathbf{y}''))\right] .$$

We now use the Fourier expansion and group elements by their related values. After doing so, the above expectation is equal to

$$\sum_{\alpha_1,\alpha_2,\alpha_3,\alpha_4\in\mathbb{F}^n}\hat{p}_{\alpha_1}\overline{\hat{p}_{\alpha_2}\hat{p}_{\alpha_3}}\hat{p}_{\alpha_4}\,\mathbb{E}_{x'\in U}\left[e(\langle\alpha_1-\alpha_2,\mathbf{x}'\rangle)\right]\mathbb{E}_{x''\in U}\left[e(\langle\alpha_4-\alpha_3,\mathbf{x}''\rangle)\right]$$
$$\mathbb{E}_{y'\in U}\left[e(\langle\alpha_1-\alpha_3,\mathbf{y}'\rangle)\right]\mathbb{E}_{y''\in U}\left[e(\langle\alpha_4-\alpha_2,\mathbf{y}''\rangle)\right] .$$

The term inside the sum for $\alpha_1,\dots,\alpha_4$ is zero unless $\alpha_1=\alpha_2=\alpha_3=\alpha_4=\alpha$, and in that case its contribution is $|\hat{p}_\alpha|^4$. This finishes the proof of the lemma. □

We now use this relation between Δp and the Fourier coefficients of p to show that the expected value of Δp is small.

Lemma 4.5. $\left|\mathbb{E}_{\boldsymbol{x}',\boldsymbol{x}'',\boldsymbol{y}',\boldsymbol{y}''\in U}\left[e(\Delta p(\boldsymbol{x}',\boldsymbol{x}'',\boldsymbol{y}',\boldsymbol{y}''))\right]\right| < \varepsilon^4/100.$

Proof. We use Lemma 4.4. We have

$$\mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in U}\left[e(p(\mathbf{x}'+\mathbf{y}')-p(\mathbf{x}'+\mathbf{y}'')-p(\mathbf{x}''+\mathbf{y}')+p(\mathbf{x}''+\mathbf{y}''))\right] = \sum_{\alpha\in\mathbb{F}^n}|\hat{p}_\alpha|^4 .$$

We now combine the fact that $\sum_{\alpha\in\mathbb{F}^n}|\hat{p}_\alpha|^2=1$ and our assumption that $|\hat{p}_\alpha|<\varepsilon^2/10$ for all $\alpha\in\mathbb{F}^n$, to yield the required bound. □

Combining Lemmas 4.2 and 4.5 we get that

$$\left|\mathbb{E}_{\mathbf{x},\mathbf{y}\in U}[e(p(\mathbf{x}+\mathbf{y}))]\right| < \left(\frac{\varepsilon^4}{100}\right)^{1/4} < \frac{\varepsilon}{2}\,.$$

We now move on to handle the pseudorandom case. We start with the following observation:

Observation 4.6. *The polynomial $\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}'')$ has total degree-d, but has no degree-d terms which have variables from only one of $\mathbf{x}'$, $\mathbf{x}''$, $\mathbf{y}'$, $\mathbf{y}''$. Therefore, the total degree of variables from $\mathbf{x}'$ in each term is at most $d-1$. The same is true for also $\mathbf{x}''$, $\mathbf{y}'$ and $\mathbf{y}''$.*

We now show that if D is a distribution that is pseudorandom against degree-$(d-1)$ polynomials, then it is also pseudorandom against Δp. We use a hybrid argument similar to the one in [7].

Lemma 4.7. *Let D be a distribution that is pseudorandom against degree-$(d-1)$ polynomials with error δ. Then*

$$\left|\mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in D}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right] - \mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in U}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right]\right| < 4\delta\,.$$

Proof. We change the inputs $\mathbf{x}',\mathbf{x}'',\mathbf{y}'$ and $\mathbf{y}''$ from U to D, one at a time. We prove that the expected value of $e(\Delta p)$ changes by at most δ in each step, accumulating to a total of at most 4δ. Formally, let H_k $(k=0,\dots,4)$ be the joint distribution of $\mathbf{x}'$, $\mathbf{x}''$, $\mathbf{y}'$, $\mathbf{y}''$, when the first k are taken from D and the last $4-k$ are taken from U. For example, H_1 is the distribution where $\mathbf{x}'\in D$ and $\mathbf{x}''$, $\mathbf{y}'$, $\mathbf{y}''\in U$, where $\mathbf{x}'$, $\mathbf{x}''$, $\mathbf{y}'$, $\mathbf{y}''$ are independent.

We prove that the distance between $e(\Delta p)$ under H_{k-1} and H_k is at most δ, for all $k=1,2,3,4$. For the sake of clarity, we focus on the proof for $k=1$. The proof for the other three cases is essentially identical.

For $k=1$, we want to show that

$$\left|\mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in U}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right] - \mathbb{E}_{\mathbf{x}'\in D,\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in U}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right]\right| < \delta\,.$$

The joint distribution of $\mathbf{x}'',\mathbf{y}',\mathbf{y}''$ is identical in both terms, so we have

$$\left|\mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in U}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right] - \mathbb{E}_{\mathbf{x}'\in D,\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in U}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right]\right| \le$$
$$\mathbb{E}_{\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in U}\left|\mathbb{E}_{\mathbf{x}'\in U}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right] - \mathbb{E}_{\mathbf{x}'\in D}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right]\right|.$$

Now, for any fixing of values for $\mathbf{x}''=a$, $\mathbf{y}'=b$, $\mathbf{y}''=c$, $\Delta p(\mathbf{x}',a,b,c)$ is a polynomial just in $\mathbf{x}'$. Observation 4.6 tells us that it is a polynomial of degree at most $d-1$. Since D is pseudorandom against degree-$(d-1)$ polynomials, the inequality follows for every fixing of $\mathbf{x}''$, $\mathbf{y}'$, $\mathbf{y}''$. Hence, it also follows for the expected value. □

If we take D to be a PRG against degree-$(d-1)$ polynomials with error $\varepsilon^4/400$ and combine this with Lemmas 4.2 and 4.5, we get that

$$\left|\mathbb{E}_{\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''\in D}\left[e(\Delta p(\mathbf{x}',\mathbf{x}'',\mathbf{y}',\mathbf{y}''))\right]\right| < \frac{\varepsilon^4}{100} + 4\frac{\varepsilon^4}{400} = \frac{\varepsilon^4}{50}\,,$$

and so using Lemma 4.2 we get that

$$\left|\mathbb{E}_{\mathbf{x},\mathbf{y}\in D}[e(p(\mathbf{x}+\mathbf{y}))]\right| < \left(\frac{\varepsilon^4}{50}\right)^{1/4} < \frac{\varepsilon}{2}.$$

This finishes the proof of Lemma 3.2.

5 Case II: Some large Fourier coefficient exists

In this section we prove Lemma 3.3. We assume throughout this section that p has some large Fourier coefficient. To be precise, there exists some $\alpha \in \mathbb{F}^n$ such that

$$|\hat{p}_\alpha| \geq \frac{\varepsilon^2}{10}.$$

Let $\ell(\mathbf{x})$ be the corresponding linear function, i. e., $\ell(\mathbf{x}) = \langle \mathbf{x}, \alpha \rangle$. Define

$$\eta = \overline{\hat{p}_\alpha} = \mathbb{E}_{\mathbf{x}\in U}\left[e(\ell(\mathbf{x}) - p(\mathbf{x}))\right].$$

η is a measure for the approximation of $p(\mathbf{x})$ by $\ell(\mathbf{x})$. By our assumption on $\hat{p}_\alpha$, we know that $|\eta| \geq \varepsilon^2/10$. For any constant $\mathbf{a} \in \mathbb{F}^n$ define the polynomial

$$q_{\mathbf{a}}(\mathbf{x}) = p(\mathbf{x}) - p(\mathbf{x}+\mathbf{a}) + \ell(\mathbf{x}+\mathbf{a}).$$

Notice that $q_{\mathbf{a}}(\mathbf{x})$ has degree at most $d-1$, because $\ell(\mathbf{x}+\mathbf{a})$ is linear (and so of degree less than d), and the degree-d terms in $p(\mathbf{x})$ and $p(\mathbf{x}+\mathbf{a})$ cancel out.

We can think of $q_{\mathbf{a}}(\mathbf{x})$ as using $\ell(\mathbf{x})$, which approximates $p(\mathbf{x})$ non-uniformly, and the derivative of $p(\mathbf{x})$ in a random direction $\mathbf{a}$, to build a random degree-$(d-1)$ polynomial which approximates $p(\mathbf{x})$ uniformly. In order to show this formally, we define

$$\nu_{\mathbf{x}}(\mathbf{a}) = \frac{1}{\eta} e(q_{\mathbf{a}}(\mathbf{x})),$$

and prove that $\nu_{\mathbf{x}}(\mathbf{a})$, taken on a random $\mathbf{a} \in \mathbb{F}^n$ value, is exactly $e(p(\mathbf{x}))$.

Lemma 5.1. *For every $\boldsymbol{x} \in \mathbb{F}^n$, $\mathbb{E}_{\boldsymbol{a}\in U}[\nu_{\boldsymbol{x}}(\boldsymbol{a})] = e(p(\boldsymbol{x}))$.*

Proof. $\mathbb{E}_{\mathbf{a}\in U}[\nu_{\mathbf{x}}(\mathbf{a})] = \frac{1}{\eta} e(p(\mathbf{x}))\,\mathbb{E}_{\mathbf{a}\in U}[e(\ell(\mathbf{x}+\mathbf{a}) - p(\mathbf{x}+\mathbf{a}))] = e(p(\mathbf{x}))$. □

Effectively, we have shown that $p(\mathbf{x})$ can be approximated uniformly by a (random) degree-$(d-1)$ polynomial $q_{\mathbf{a}}(\mathbf{x})$. We can now use this to show that a distribution that is pseudorandom against degree-$(d-1)$ polynomials is also pseudorandom against p. First, we prove the following lemma:

Lemma 5.2. *Let D be a distribution that is pseudorandom against degree-$(d-1)$ polynomials with error δ. For every $\boldsymbol{a} \in \mathbb{F}^n$*

$$\left|\mathbb{E}_{\boldsymbol{x}\in D}[\nu_{\boldsymbol{x}}(\boldsymbol{a})] - \mathbb{E}_{\boldsymbol{x}\in U}[\nu_{\boldsymbol{x}}(\boldsymbol{a})]\right| < \frac{\delta}{|\eta|}.$$

Proof. We have

$$\left|\mathbb{E}_{\mathbf{x}\in D}[\nu_{\mathbf{x}}(\mathbf{a})] - \mathbb{E}_{\mathbf{x}\in U}[\nu_{\mathbf{x}}(\mathbf{a})]\right| = \frac{1}{|\eta|}\left|\mathbb{E}_{\mathbf{x}\in D}[e(q_{\mathbf{a}}(\mathbf{x}))] - \mathbb{E}_{\mathbf{x}\in U}[e(q_{\mathbf{a}}(\mathbf{x}))]\right| < \frac{\delta}{|\eta|},$$

where we use the fact that $q_{\mathbf{a}}$ is a polynomial of degree at most $d-1$ and so D is pseudorandom against $q_{\mathbf{a}}$ with error δ. □

We now conclude by proving Lemma 3.3.

Proof of Lemma 3.3. Let D be a distribution that is pseudorandom against degree-$(d-1)$ polynomials with error $\varepsilon^3/10$. Then

$$\begin{aligned}\left|\mathbb{E}_{\mathbf{x}\in D}[e(p(\mathbf{x}))] - \mathbb{E}_{\mathbf{x}\in U}[e(p(\mathbf{x}))]\right| &= \left|\mathbb{E}_{\mathbf{x}\in D}\,\mathbb{E}_{\mathbf{a}\in U}[\nu_{\mathbf{x}}(\mathbf{a})] - \mathbb{E}_{\mathbf{x}\in U}\,\mathbb{E}_{\mathbf{a}\in U}[\nu_{\mathbf{x}}(\mathbf{a})]\right| \\ &\le \mathbb{E}_{\mathbf{a}\in U}\left|\mathbb{E}_{\mathbf{x}\in D}[\nu_{\mathbf{x}}(\mathbf{a})] - \mathbb{E}_{\mathbf{x}\in U}[\nu_{\mathbf{x}}(\mathbf{a})]\right| < \frac{\varepsilon^3/10}{|\eta|} \le \varepsilon\,.\end{aligned}$$

□

Acknowledgements I thank my supervisor, Omer Reingold, for his constant interest and encouragement. I thank Andrej Bogdanov and Emanuele Viola for making an early version of their paper available and for insightful comments. In particular I thank Bogdanov for an observation that somewhat simplifies the analysis in the case where all the Fourier coefficients are small, which allowed the reduction of the number of small-bias terms from 3^d to 2^d. I thank Zeev Dvir, Dana Moshkovitz and Ariel Gabizon for helpful discussions. I also thank the anonymous reviewers for their useful comments.

References

[1] N. ALON, O. GOLDREICH, J. HÅSTAD, AND R. PERALTA: Simple construction of almost k-wise independent random variables. *Random Structures Algorithms*, 3(3):289–304, 1992. [doi:10.1002/rsa.3240030308]. 70, 74

[2] N. ALON, T. KAUFMAN, M. KRIVELEVICH, S. LITSYN, AND D. RON: Testing low-degree polynomials over $GF(2)$. In *RANDOM-APPROX 2003*, volume 2764 of *Lecture Notes in Computer Science*, pp. 188–199. Springer, 2003. [doi:10.1007/b11961]. 71

[3] M. BELLARE, D. COPPERSMITH, J. HÅSTAD, M. KIWI, AND M. SUDAN: Linearity testing in characteristic two. *IEEE Trans. Inform. Theory*, 42(6):1781–1795, 1996. [doi:10.1109/18.556674]. 71, 76

[4] E. BEN-SASSON, M. SUDAN, S. VADHAN, AND A. WIGDERSON: Randomness-efficient low degree tests and short PCPs via epsilon-biased sets. In *Proc. 35th STOC*, pp. 612–621. ACM Press, 2003. [doi:10.1145/780542.780631]. 70

[5] V. BERGELSON, T. TAO, AND T. ZIEGLER: An inverse theorem for the uniformity seminorms associated with the action of $\mathbb{F}_p^\infty$, 2009. [arXiv:0901.2602]. 72

[6] A. BOGDANOV: Pseudorandom generators for low degree polynomials. In *Proc. 37th STOC*, pp. 21–30. ACM Press, 2005. [doi:10.1145/1060590.1060594]. 70

[7] A. BOGDANOV AND E. VIOLA: Pseudorandom bits for polynomials. In *Proc. 48th FOCS*, pp. 41–51. IEEE Comp. Soc. Press, 2007. [doi:10.1109/FOCS.2007.42]. 70, 71, 72, 73, 76, 78

[8] W. T. GOWERS: A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001. [doi:10.1007/s00039-001-0332-9]. 71

[9] B. GREEN AND T. TAO: The distribution of polynomials over finite fields, with applications to the Gowers norms, 2007. [arXiv:0711.3191]. 72

[10] B. GREEN AND T. TAO: An inverse theorem for the Gowers $U^3(G)$ norm. *Proc. Edinburgh Math. Soc. (Ser. 2)*, 51(1):73–153, 2008. [doi:10.1017/S0013091505000325]. 71

[11] S. LOVETT: Unconditional pseudorandom generators for low degree polynomials. In *Proc. 40th STOC*, pp. 557–562. ACM Press, 2008. [doi:10.1145/1374376.1374455]. 70, 72

[12] S. LOVETT, R. MESHULAM, AND A. SAMORODNITSKY: Inverse conjecture for the Gowers norm is false. In *Proc. 40th STOC*, pp. 547–556. ACM Press, 2008. [doi:10.1145/1374376.1374454]. 72

[13] M. LUBY, B. VELICKOVIC, AND A. WIGDERSON: Deterministic approximate counting of depth-2 circuits. In *Proc. of the 2nd Israeli Symposium on Theoretical Computer Science (ISTCS'93)*, pp. 18–24. IEEE Comp. Soc. Press, 1993. 70

[14] J. NAOR AND M. NAOR: Small-bias probability spaces: Efficient constructions and applications. In *Proc. 22nd STOC*, pp. 213–223. ACM Press, 1990. [doi:10.1145/100216.100244]. 70, 74

[15] A. SAMORODNITSKY: Low-degree tests at large distances. In *Proc. 39th STOC*, pp. 506–515. ACM Press, 2007. [doi:10.1145/1250790.1250864]. 71

[16] D. ŠTEFANKOVIČ: Fourier transforms in computer science. Master's thesis, University of Chicago, Department of Computer Science, 2000. `http://www.cs.rochester.edu/~stefanko/Publications/Fourier.ps`. 73

[17] T. TAO AND T. ZIEGLER: The inverse conjecture for the Gowers norm over finite fields via the correspondence principle, 2008. [arXiv:0810.5527]. 72

[18] E. VIOLA: The sum of d small-bias generators fools polynomials of degree d. In *Proc. 23rd IEEE Conf. on Computational Complexity (CCC)*, pp. 124–127. IEEE Comp. Soc. Press, 2008. [doi:10.1109/CCC.2008.16]. 72

AUTHOR

Shachar Lovett
graduate student
Weizmann Institute of Science
Rehovot 76100, Israel
shachar.lovett@gmail.com
www.wisdom.weizmann.ac.il/~shalov

ABOUT THE AUTHOR

SHACHAR LOVETT is a Ph. D. student at the Weizmann Institute of Science under the guidance of Omer Reingold. His research interests include pseudorandomness, explicit constructions, and polynomials over finite fields.