A Polylogarithmic PRG for Degree 2 Threshold Functions in the Gaussian Setting

Daniel M. Kane

University of California, San Diego
Department of Computer Science and Engineering / Department of Mathematics
9500 Gilman Drive #0404
La Jolla, CA 92023, USA
dakane@ucsd.edu

Abstract

We construct and analyze a new pseudorandom generator for degree 2 polynomial threshold functions with respect to the Gaussian measure. In particular, we obtain one whose seed length is polylogarithmic in both the dimension and the desired error, a substantial improvement over existing constructions.

Our generator is obtained as an appropriate weighted average of pseudorandom generators against read once branching programs. The analysis requires a number of ideas including a hybrid argument and a structural result that allows us to treat our degree 2 threshold function as a function of a number of linear polynomials and one approximately linear polynomial.

1998 ACM Subject Classification G.3 Probability and Statistics

Keywords and phrases polynomial threshold function, pseudorandom generator, Gaussian distribution

Digital Object Identifier 10.4230/LIPIcs.CCC.2015.567

1 Introduction

We say that a function $f : \mathbb{R}^n \to \{+1, -1\}$ is a (degree-d) *polynomial threshold function* (PTF) if it is of the form $f(x) = \mathrm{sgn}(p(x))$ for p some (degree-d) polynomial in n variables. Polynomial threshold functions make up a natural class of Boolean functions and have applications to a number of fields of computer science such as circuit complexity [1], communication complexity [14] and learning theory [11].

In this paper, we study the question of pseudorandom generators (PRGs) for polynomial threshold functions of Gaussians (and in particular for $d = 2$). In other words, we wish to find explicit functions $F : \{0,1\}^s \to \mathbb{R}^n$ so that for any degree-2 polynomial threshold function f

$$\left|\mathbb{E}_{x\sim_u\{0,1\}^s}[f(F(x))] - \mathbb{E}_{X\sim\mathcal{G}^n}[f(X)]\right| < \epsilon.$$

We say that such an F is a pseudorandom generator of seed length s that fools degree-d polynomial threshold functions with respect to the Gaussian distribution to within ϵ. In this paper, we develop a generator with s polylogarithmic in n and ϵ in the case when $d = 2$.

1.1 Previous Work

There have been a number of papers dealing with the question of finding pseudorandom generators for polynomial threshold functions with respect to the Gaussian distribution or the Bernoulli distribution (i.e. uniform over $\{-1, 1\}^n$). Several early works in this area showed that polynomial threshold functions of various degrees could be fooled by arbitrary

30th Conference on Computational Complexity (CCC'15).
Editor: David Zuckerman; pp. 567–581

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Table 1 Generators Based on Limited Independence.

Paper	Bernoulli/Gaussian	d	k
Diakonikolas, Gopalan, Jaiswal, Servedio, Viola [3]	Bernoulli	1	$O(\epsilon^{-2}\log^2(\epsilon^{-1}))$
Diakonikolas, Kane, Nelson [4]	Gaussian	1	$O(\epsilon^{-2})$
Diakonikolas, Kane, Nelson [4]	Both	2	$O(\epsilon^{-8})$[1]
Kane [7]	Both	d	$O_d\left(\epsilon^{-2^{O(d)}}\right)$

k-wise independent families of Gaussian or Bernoulli random variables. It should be noted that a k-wise independent family of Bernoulli random variables can be generated from a seed of length $O(k\log(n))$. Although, any k-wise independent family of Gaussians will necessarily have infinite entropy, it is not hard to show that a simple discretization of these random variables leads to a generator of comparable seed length. These results on fooling polynomial threshold functions with k-independence are summarized in Table 1.

Unfortunately, it is not hard to exhibit k-wise independent families of Bernoulli or Gaussian random variables that fail to ϵ-fool the class of degree-d polynomial threshold functions for $k = \Omega(d^2\epsilon^{-2})$, putting a limit on what can be obtained through mere k-independence.

There have also been a number of attempts to produce pseudorandom generators by using more structure than limited independence. In [12], Meka and Zuckerman develop a couple of such generators in the Bernoulli case. Firstly, they make use of pseudorandom generators against space bounded computation to produce a generator of seed length $O(\log(n)+\log^2(\epsilon^{-1}))$ in the special case where $d = 1$. By piecing together several k-wise independent families, they produce a generator for arbitrary degree PTFs of seed length $2^{O(d)}\log(n)\epsilon^{-8d-3}$. In [10], the author develops an improved analysis of this generator allowing for a seed length as small as $O_{c,d}(\log(n)\epsilon^{-11-c})$. For the Gaussian case, the author developed a generator of seed length $2^{O_c(d)}\log(n)\epsilon^{-4-c}$ in [9]. This generator was given essentially as an average several random variables each picked independently from a k-wise independent family of Gaussians. The analysis of this generator was also improved in [10], obtaining a seed length of $O_{c,d}(\log(n)\epsilon^{-2-c})$. Finally, in [8] it was shown that this could be improved further by taking an average with unequal weights, given seed length $O_{c,d}(\epsilon^{-c})$ for arbitrary degree and $\log(n)\exp(O(\log(1/\epsilon)^{2/3}\log\log(1/\epsilon)^{1/3}))$ for degree 2. For a summary of these results, see Table 2.

The bound in [8] came from showing that for Y a weak pseudorandom generator (and in particular one that fools low degree moments) that

$$\left|\mathbb{E}[f(X)] - \mathbb{E}[f(\sqrt{1-\epsilon^2}X + \epsilon Y)]\right| \ll \epsilon^k \tag{1}$$

for any k. This followed from an important structure theorem that said that any polynomial p could be decomposed in terms of other polynomials, q_i so that when the q_i were localized near a random location then with high probability they would all be approximately linear polynomials. It was then shown that a moment matching random variable could fool such functions of approximately linear polynomials with high fidelity.

The bottleneck in this analysis comes in the size of the decomposition described above. On the one hand, for $d > 2$ the size of the decomposition described above could potentially

[1] The bound in [4] for the Bernoulli case is actually $\tilde{O}(\epsilon^{-9})$, but this can be easily improved to $O(\epsilon^{-8})$ using technology from [10].

Table 2 Other Generators.

Paper	Bernoulli/Gaussian	d	s
Meka, Zuckerman [12]	Bernoulli	1	$O(\log(n)+\log^2(1/\epsilon))$
Kane [8]	Gaussian	1	$O(\log(n)+\log^{3/2}(1/\epsilon))$
Meka, Zuckerman [12]	Bernoulli	d	$\log(n)2^{O(d)}\epsilon^{-8d-3}$
Kane [9]	Gaussian	d	$\log(n)2^{O(d)}\epsilon^{-4.1}$
Kane [10]	Gaussian	d	$\log(n)O_d(\epsilon^{-2.1})$
Kane [10]	Bernoulli	d	$\log(n)O_d(\epsilon^{-11.1})$
Kane [8]	Gaussian	2	$\log(n)\exp(O(\log(1/\epsilon)^{2/3}\log\log(1/\epsilon)^{1/3}))$
Kane [8]	Gaussian	d	$\log(n)O_{c,d}(\epsilon^{-c})$
Kane, this paper	Gaussian	2	$O(\log^6(\epsilon)\log(n)\log\log(n/\epsilon))$

be quite large, though for $d=2$, it can be handled explicitly. On the other hand, the implied constant in the approximation above depends exponentially on the size of this decomposition. While, we still do not know how to solve the former problem when $d>2$, we can solve the latter in the case of degree-2 polynomial threshold functions.

In the special case of degree 2 functions, we end up with a decomposition of our quadratic polynomial as a function of a single approximately linear quadratic and several other linear polynomials. Fortunately, as discovered by Meka and Zuckerman, pseudorandom generators against read once branching programs are excellent at fooling linear polynomials (or even small numbers of them). As such generators also approximately fool the expectation of low degree polynomials (which is required for dealing with the approximately linear quadratic), they will actually be much better suited as our Y above. In fact, we can produce a pseudorandom generator for degree 2 polynomial threshold functions with polylogarithmic seed length. In particular, given an appropriate notion of a discretized Gaussian (the δ-approximate Gaussian defined in Section 3), we have the following Theorem:

▶ **Theorem 1.1.** *Let $\epsilon>0$ and n a positive integer. For sufficiently large constant C, let $\delta=\log(\epsilon)/C$ and ℓ an integer at least $\delta^{-3}\log(\epsilon)$. For $1\le i\le\ell$ let Y_i be a family of n $\exp(-\delta^{-1}\log(n/\delta))$-approximate Gaussians seeded by a pseudorandom generator that fools read once branching programs of width $\delta^{-2}\log(n/\delta)$ to within error $\exp(-\delta^{-1}\log(n/\delta))$. Let*

$$Y=\frac{\sum_{i=1}^{\ell}(1-\delta^3)^{(\ell-1)/2}Y_i}{\sqrt{\sum_{i=1}^{\ell}(1-\delta^3)^{\ell-1}}},$$

and let X be an n dimensional standard Gaussian. Then for any degree 2 polynomial threshold function f in n variables,

$$|\mathbb{E}[f(X)]-\mathbb{E}[f(Y)]|\le\epsilon.$$

Furthermore, such Y can be constructed from generators of seed length of at most $O(\log(\epsilon)^6\log(n)\log\log(n/\epsilon))$.

In Section 2, we will go over some basic notation and results. In Section 3, we introduce the concept of an approximate Gaussian, and show that families of them seeded by a PRG for read once branching programs will fool certain functions depending on a finite numbers of linear threshold functions and polynomials of low degree. In Section 4, we will prove our generalization of Equation (1). Finally, in Section 5, we will use this result to finish up our analysis and prove Theorem 1.1.

2 Background Information

2.1 Conventions

Throughout the paper we will use $X, X_i, \ldots$ as standard Gaussian random variables. We will usually use $Y, Y_i, \ldots$ to denote some sort of pseudorandom Gaussian.

2.2 Distribution of Values of Polynomials

Given a polynomial, p, we will need to know some basic information about how its values at random Gaussian inputs are distributed. Perhaps the most basic measure of such distribution is the average size of $p(X)$. In order to keep track this, we will make use of the L^t (and especially L^2) norms. In particular, recall:

▶ **Definition 2.1.** If $p : \mathbb{R}^n \to \mathbb{R}$ and $t \geq 1$ then

$$|p|_t := \left(\mathbb{E}[|p(X)|^t]\right)^{1/t}$$

where X is a standard Gaussian.

We will also need an anticoncentration result. That is a result telling us that the value of $p(X)$ is unlikely to lie in any small neighborhood. In particular, we have:

▶ **Lemma 2.2** (Carbery and Wright, [2])**.** *If p is a degree-d polynomial then*

$$Pr(|p(X)| \leq \epsilon |p|_2) = O(d\epsilon^{1/d}).$$

Where the probability is over X, a standard n-dimensional Gaussian.

We will also need a concentration result for the values. To obtain one, we make use of the hypercontractive inequality below. The proof follows from Theorem 2 of [13].

▶ **Lemma 2.3.** *If p is a degree-d polynomial and $t > 2$, then*

$$|p|_t \leq \sqrt{t-1}^d |p|_2.$$

This bound on higher moments allows us to prove a concentration bound on the distribution of $p(X)$. The following result is a well-known consequence that can be found, for example, in [6].

▶ **Corollary 2.4.** *If p is a degree-d polynomial and $N > 0$, then*

$$Pr_X(|p(X)| > N|p|_2) = O\left(2^{-(N/2)^{2/d}}\right).$$

Proof. Apply the Markov inequality and Lemma 2.3 with $t = (N/2)^{2/d}$. ◀

2.3 Hermite Polynomials

Recall that the Hermite polynomials h_a are an orthogonal set of polynomials with respect to the Gaussian distribution obtained by taking products of univariate Hermite polynomials in different coordinates. In particular,

$$\mathbb{E}[h_a(X)h_b(X)] = \delta_{a,b}.$$

We will need to make use of a few standard facts about the Hermite polynomials:

- Any degree-d polynomial, p, can be written as a linear combination of Hermite polynomials of degree at most d so that the sum of the squares of the coefficients is $|p|_2^2$ (and thus, the sum of the absolute values of the coefficients is at most $n^d|p|_2$).
- A Hermite polynomial of degree d depends on at most d coordinates of its input. In fact it can be written as a product of one variable polynomials on these inputs.
- The sum of the absolute values of the coefficients of a Hermite polynomial of degree d is $O(1)^d$.

These properties are all easy to verify given basic facts about univariate Hermite polynomials.

3 Approximate Gaussians and Read Once Branching Programs

In order to produce a pseudorandom generator supported on a discrete set, we will first need to come up with a discrete version of the single variable Gaussian distribution. We will make use of the following notation:

▶ **Definition 3.1.** We say that a random variable Y is a δ-*approximate Gaussian*, if there is a (correlated) standard (1-dimensional) Gaussian variable X so that

$$\Pr(|X - Y| > \delta) < \delta,$$

and $|Y| = O(\log(\delta))$ with probability 1.

In particular, it is not difficult to generate a random variable with this property.

▶ **Lemma 3.2.** *There exists an explicit δ-approximate Gaussian random variable that can be generated from a seed of length $O(\log(\delta))$.*

Proof. We assume that δ is sufficiently small since otherwise there is nothing to prove. Let $N = \lfloor \delta^{-3} \rfloor$. Note that the random variable

$$X := \sqrt{-2\log(z)}\cos(2\pi\theta)$$

is a random Gaussian if z and θ independent uniform $(0, 1)$ random variables. Let z' and θ' be the roundings of z and θ to the nearest half-integer multiple of $1/N$, and let

$$Y := \sqrt{-2\log(z')}\cos(2\pi\theta').$$

Note that $|z - z'|, |\theta - \theta'| \leq N^{-1}$. From this it follows that

$$|X - Y| = O\left(\frac{1}{N\min(z, z', 1 - z, 1 - z')}\right).$$

Thus, $|X - Y| < \delta$ with probability at least $1 - \delta$.

On the other hand, z' and θ' are discrete uniform variables with $O(\log(N)) = O(\log(\delta))$ bits of entropy each. Thus, Y can be generated from a seed of length $O(\log(\delta))$. ◀

We will also need to recall the concept of a read once branching program. An (M, D, n)-branching program is a program that is allowed to take only a single pass over an input consisting of n D-bit blocks that is only allowed to save M-bits of memory between blocks. We will sometimes refer to this as a read once branching program of memory M (with n and D usually implicit). We note that there are small seed-length generators to fool such programs. In particular, we note the following theorem of [5]:

▶ **Theorem 3.3.** *There exists an explicit pseudorandom generator G with seed length $O(M + d + \log(n/\epsilon)\log(n))$ so that if f is any Boolean function computed by an (M, D, n)-branching program, then*

$$|\mathbb{E}_{X\sim_u\{\{0,1\}^D\}^n}[f(X)] - \mathbb{E}[f(G)]| \leq \epsilon.$$

As shown in [12], using pseudorandom generators for read once branching programs is a good way to fool linear threshold functions, or by extension, things that depend on a small number of linear functions of the input. They will also fool the expectations of polynomials of low degree. An important building block for our construction will be families of approximate Gaussians seeded with a pseudorandom generator which fools read once branching programs. These, it turns out will simultaneously fool functions of a small number of linear functions and expectations of low degree polynomials in the following sense:

▶ **Proposition 3.4.** *Let s be a quadratic polynomial in n variables whose value depends on at most r linear polynomials. Let $g(x)$ be the indicator function of the event that $s(x)$ lies in I for some interval I. Let $q(x)$ be a degree d polynomial in n variables. Let X be a standard Gaussian and let Y be a family on n δ_1-approximate Gaussians seeded by a PRG that fools read once branching programs of length n and memory $M = O((d + r)\log(n/\delta_1))$ to error at most δ_2. Then*

$$|\mathbb{E}[g(X)q(X)] - \mathbb{E}[g(Y)q(Y)]| \leq O(\log(\delta_1))^{d+1}(\delta_2 + n\delta_1^{1/4})n^d|q|_2.$$

First, we will need the following Lemma:

▶ **Lemma 3.5.** *Let s be a quadratic polynomial in n variables whose value depends on at most r linear polynomials. Let $g(x)$ be the indicator function of the event that $s(x)$ lies in I for some interval I. Let $h(x)$ be a Hermite polynomial of degree d. Let X and Y be as given in Proposition 3.4. Then*

$$|\mathbb{E}[g(X)h(X)] - \mathbb{E}[g(Y)h(Y)]| \leq O(\log(\delta_1))^{d+1}(\delta_2 + n\delta_1^{1/4}).$$

Proof. We prove this in two steps. First, show that for Y' a family of n independent approximate Gaussians that $\mathbb{E}[g(X)h(X)] \approx \mathbb{E}[g(Y')h(Y')]$. This is because by correlating X and Y' appropriately, we can guarantee that X and Y' are close with high probability. This will mean that $g(X) = g(Y')$ with high probability that $h(X) \approx h(Y')$ with high probability. Next, we will need to show that $\mathbb{E}[g(Y')h(Y')] \approx \mathbb{E}[g(Y)h(Y)]$. This will hold because we can construct a read once branching program of small memory that computes approximations to the linear functions upon which s depends and the values of the (at most d) coordinates upon which h depends.

We may assume that $|s|_2 = 1$. We begin by letting Y' be a family of independent δ_1-approximate Gaussians. We can pick correlated copies of X and Y' so that with probability at least $1 - n\delta_1$ each coordinate of X is within δ_1 of the corresponding coordinate of Y'. If this is the case, then $|s(X) - s(Y')| = O(n\log(\delta_1)\delta_1)$. By Lemma 2.2, $s(X)$ is only within this distance of an endpoint of I with probability $O(n^{1/2}\delta_1^{1/2}\log^d(\delta_1))$. Thus, neglecting an event with this probability, $g(X) = g(Y')$. Let E be the event that $g(X) \neq g(Y')$, or that some coordinate of X and Y' differs by more than δ_1. The contribution to $\mathbb{E}[|g(X)h(X) - g(Y')h(Y')|]$ coming from times when E holds is at most

$$\mathbb{E}[\mathbf{1}_E(|h(X)| + |h(Y')|)],$$

which by Cauchy-Schwartz is at most

$$O((n^{1/4}\delta_1^{1/4}\log^{d/2}(\delta_1))\sqrt{\mathbb{E}[h(X)^2 + h(Y')^2]}) = O(n^{1/4}\delta_1^{1/4}\log^{d+1}(\delta_1)).$$

On the other hand $\mathbb{E}[|h(X) - h(Y')|]$ when X and Y' agree to within δ_1 in each coordinate is $O(n \log^d(\delta_1)\delta_1)$. Thus,

$$|\mathbb{E}[g(X)h(X)] - \mathbb{E}[g(Y')h(Y')]| \leq O(\log^{d+1}(\delta_1)n\delta_1^{1/4}).$$

We now need to show that seeding Y' by a read once branching programs with M memory fools this expectation to within small error. Notice that a read once branching program with $O((d+r)\log(n/\delta_1))$ memory can keep track of an approximation to within $n^{-1}\delta_1^3$ of each of the r normalized linear functions that s depends on, and compute h to precision δ_1. The latter is accomplished by writing h as $\prod_{i=1}^n h_{a_i}(x_i)$ and keeping track of a running product $\prod_{i=1}^m h_{a_i}(x_i)$ to relative precision $\delta_1 O(\log(\delta_1))^{-d}(m/n)$. This allows the program to compute the values of s and h to within an error of at most δ_1.

Thus, $\Pr(h(Y')g(Y') \geq c)$ is at most

$$\Pr(h(Y)g(Y) \geq c - \delta_1) + \Pr(s(Y') \text{ is within } \delta_1 \text{ of an endpoint of } I) + \delta_2.$$

Note that except for an event of probability $n\delta_1$, the difference between $s(X)$ and $s(Y')$ is at most $O(n\log(\delta_1)\delta_1)$ and the former is this close to an endpoint of I with probability at most $O(\log(\delta_1)\sqrt{n\delta_1})$. Thus, with probability $1 - O(\log(\delta_1)\sqrt{n\delta_1} + n\delta_1)$, $s(Y')$ is not within δ_1 of a boundary of I. Thus for any c,

$$\Pr(h(Y)g(Y) \geq c) \leq \Pr(h(Y')g(Y') \geq c - \delta_1) + O(\delta_2 + \log(\delta_1)n^{1/2}\delta_1^{1/2} + n\delta_1).$$

Integrating this over all $|c| \leq O(\log(\delta_1))^d$ (which is the full range of values of $h(Y')$ and $h(Y)$), we find that

$$\mathbb{E}[g(Y)h(Y)] \leq \mathbb{E}[g(Y')h(Y')] + \delta_1 + O(\log(\delta_1))^{d+1}(\delta_2 + n\delta_1^{1/2}).$$

The lower bound follows similarly, and this completes the proof. ◀

Proof of Proposition 3.4. Note that we can write q as a linear combination of degree d hermite polynomials, where the sum of the absolute values of the coefficients is at most $O(n^d|q|_2)$. Our result follows from applying Lemma 3.5 to each term separately. ◀

We also note the following corollary when $r = 0$:

▶ **Corollary 3.6.** *Let X and Y be as in Proposition 3.4. Let q be a polynomial of degree at most d then*

$$|\mathbb{E}[q(X)] - \mathbb{E}[q(Y)]| \leq O(\log(\delta_1))^{d+1}(\delta_2 + n\delta_1^{1/4})n^d|q|_2.$$

4 The Key Result

Our analysis will depend heavily upon the following Proposition:

▶ **Proposition 4.1.** *Let $\delta > 0$ and n a positive integer. Let C be a sufficiently large constant, and let Y be a family of n $\exp(-C\delta^{-1}\log(n/\delta))$-approximate Gaussians seeded by a pseudorandom generator that fools read once branching programs of memory $C\delta^{-2}\log(n/\delta)$ to within error $\exp(-C\delta^{-1}\log(n/\delta))$. Let X be an n dimensional standard Gaussian. Then for any degree-2 polynomial threshold function f in n variables, we have that*

$$\left|\mathbb{E}[f(X)] - \mathbb{E}[f(\sqrt{1-\delta^3}X + \delta^{3/2}Y)]\right| = \exp(-\Omega(\delta^{-1})).$$

We first will need to show that this result holds for a certain class of quadratic polynomials. In particular, we define:

▶ **Definition 4.2.** A degree 2 polynomial $p : \mathbb{R}^n \to \mathbb{R}$ is called (r, δ)-*approximately linear* if it can be written in the form

$$p(x) = p_0(x \cdot v_1, \ldots, x \cdot v_r) + x \cdot v + q(x)$$

for some vectors $v_1, \ldots, v_k, v$ with v orthogonal to v_i, and some degree-2 polynomials p_0 and q so that $|q|_2 < \delta |v|_2$.

We now show an analogue of Proposition 4.1 for approximately linear polynomials:

▶ **Lemma 4.3.** *Let $k, r > 0$ be integers and $\delta, \delta_1, \delta_2 > 0$ real numbers. Let p be an $(r, \sqrt{\delta})$-approximately linear polynomial in n variables with f the corresponding threshold function. Let X be an n-dimensional standard Gaussian, and Y a family on n δ_1-approximate Gaussians seeded by a PRG that fools read once branching programs of length n and memory $M = C(k + r)\log(n/(\delta\delta_1\delta_2))$, for sufficiently large C, to error at most δ_2. Then*

$$\left|\mathbb{E}[f(X)] - \mathbb{E}[f(\sqrt{1-\delta^2}X + \delta Y)]\right|$$

is at most

$$\leq \exp(-\Omega(\delta^{-1}))4^k + O(\log^{5k}(\delta_1)(\delta_2 + n\delta_1^{1/4}))O(nk)^{4k} + O(\delta k)^{2k} + O(2^{-k/2}).$$

The basic idea of the proof is as follows. First, we bin based on the approximate value of p_0. We are reduced to considering the expectation of the threshold function of a polynomial $C + x \cdot v + q(x)$ times the indicator function of the event that p_0 (a polynomial depending on a bounded number of linear functions) lies in a small interval. To deal with the threshold function, we note that averaging over possible values of $X \cdot v$ smooths it out, and we may approximate it by its Taylor polynomial. Thus, we only need Y to fool the expectation of an indicator function of p_0 lying in a small interval, times a low degree polynomial. This should hold by Proposition 3.4. The proof is as follows.

Proof. Since p is $(r, \sqrt{\delta})$-approximately linear, after rescaling we may assume that for some orthonormal set of vectors $v, v_1, \ldots, v_k$ that

$$p(x) = p_0(x \cdot v_1, \ldots, x \cdot v_r) + x \cdot v + q(x)$$

for some quadratic polynomials p_0 and q with $|q|_2 < \sqrt{\delta}$. We may assume that $\delta \ll 1$, for otherwise there is nothing to prove.

Let $N = 2^k/|p|_2$. Let $I_n(x) := \mathbf{1}_{p_0(x) \in [n/N, (n+1)/N)}$ and let $f_n(x) := I_n(x)f(x)$. Let

$$f_n^+(x) = I_n(x)\mathrm{sgn}(x \cdot v + q(x) + (n+1)/N), \quad \text{and} \quad f_n^-(x) = I_n(x)\mathrm{sgn}(x \cdot v + q(x) + (n)/N).$$

Note that $f(x) = \sum_{n \in \mathbb{Z}} f_n(x)$. Note also that $f_n^+(x) \geq f_n(x) \geq f_n^-(x)$ for all x, n. We note that $f_n^{\pm}(x)$ is actually a very close approximation to $f_n(x)$. In particular, by Lemma 2.2 if X is a random Gaussian then

$$\sum_{n \in \mathbb{Z}} \mathbb{E}[f_n^+(X) - f_n^-(X)] \leq \Pr(|p(X)| \leq 1/N) = O(2^{-k/2}).$$

Thus, it suffices to show that $f_n^{\pm}(X)$ and $f_n^{\pm}(\sqrt{1-\delta^2}X+\delta Y)$ have similar expectations for each n. To analyze this, let X_v be the component of X in the v direction, and X' be the component in the orthogonal directions. Let

$$\begin{aligned} &g_n^{\pm}(X',Y) \\ &\quad := \mathbb{E}_{X_v}[f_n^{\pm}(\sqrt{1-\delta^2}X+\delta Y)] \\ &\quad = I_n(X',Y)\mathbb{E}_{X_v}[\mathrm{sgn}(C(X')+q_0(X',Y)+X_v(1+q_1'(X')+q_1''(Y)))+X_v^2q_2)] \end{aligned} \tag{2}$$

where $C(X')$ is a polynomial in X' and q_0, q_1', q_1'' and q_2 are polynomials (of degree at most 2,1,1 and 0 respectively) of L^2 norms at most $|q_0|_2 = O(\delta)$, $|q_1'|_2 = O(\sqrt{\delta})$, $|q_1''|_2 = O(\delta)$, and $|q_2|_2 = O(\sqrt{\delta})$. We may also assume that q_0 is at most linear in the variables of X', and that if we write $q_0(X',Y) = \delta v \cdot Y + q_0'(X',Y)$, then $|q_0'(X',Y)|_2 = O(\delta^{3/2})$. We claim that with probability $1-\exp(-\Omega(\delta^{-1}))$ over the choice of X' that the following hold:

1. $\mathbb{E}_Y[q_0(X',Y)^2] = O(\delta^2)$.
2. $|q_1'(X')| < 1/3$.

The first holds by Corollary 2.4 since $\mathbb{E}_Y[q_0'(X',Y)^2]$ is a degree 2 polynomial in X' with L^2 norm $O(\delta^3)$. Thus, with the desired probability $\mathbb{E}_Y[q_0'(X',Y)^2] = O(\delta^2)$, which implies the desired bound. The second holds by Corollary 2.4 since q_1' is a degree 1 polynomial with L^2 norm $O(\sqrt{\delta})$. For the next part of the argument we will assume that we have fixed a value of X' so that the above holds.

Let $q_1(X',Y) := q_1'(X') + q_1''(Y)$. Note that if $|q_0(X',Y)|, |q_1(X',Y)| < 2/3$, then the polynomial $C+q_0+x(1+q_1)+x^2q_2$ cannot have more than one root with absolute value less than $\Omega(\delta^{-1/2})$. Since X_v cannot be larger than this except with probability $\exp(-\Omega(\delta^{-1}))$, the expectation above is $\mathrm{erf}(R)+\exp(-\Omega(\delta^{-1}))$, where R is the smaller root of that quadratic. Furthermore, there will be no such root R unless $|C| \ll \delta^{-1/2}$. In such a case, by the quadratic formula, this root is

$$\begin{aligned} R &= \frac{-1-q_1+\sqrt{1+2q_1+q_1^2-4q_2(C+q_0)}}{2q_2} \\ &= (1+q_1)\frac{\sqrt{1-4q_2(C+q_0)/(1+q_1)^2}-1}{2q_2} = \frac{C+q_0}{1+q_1}+O(1). \end{aligned} \tag{3}$$

Thus, in the range $|q_0|, |q_1| < 2/3$ and $|C| \ll \delta^{-1/2}$ we have that the expectation in (2) is

$$\mathrm{erf}(R)+\exp(-\Omega(\delta^{-1})).$$

Note that even for complex values of q_0 and q_1 with absolute value at most $2/3$, the $\mathrm{erf}(R)$ (with R given by Equation (3)) is complex analytic with absolute value uniformly bounded. Therefore, by Taylor expanding about $q_0 = 0$ and $q_1 = q_1'$, we can find a polynomial P of degree at most $2k$ (depending on q, C and X') so that $\mathrm{erf}(R)$ is

$$\begin{aligned} &P(q_0(X',Y), q_1(X',Y)-q_1'(X'))+O(q_0(X',Y))^{2k}+O(q_1(X',Y)-q_1'(Y))^{2k} \\ &= P(q_0(X',Y), q_1''(Y))+O(q_0(X',Y))^{2k}+O(q_1''(Y))^{2k}. \end{aligned}$$

Furthermore, the coefficients of P are all $O(1)^k$. The above must hold when $|q_0|, |q_1''|$ are not at most $1/3$. On the other hand, this means that even when $|q_0|, |q_1''|$ are larger than $1/3$, we have that $P(q_0(X',Y), q_1''(X',Y)) \pm 1 = O(q_0(X',Y))^{2k} + O(q_1(X',Y))^{2k}$. This means that the above formula holds for all values of q_0 and q_1''. Thus, $g_n^{\pm}(X',Y)$ is

$$G(X',Y) := \mathbf{1}_{s(X',Y)\in I}(P(q_0(X',Y), q_1''(Y))+O(q_0(X',Y))^{2k}+O(q_1''(Y))^{2k})+\exp(-\Omega(\delta^{-1}))$$

where s is some quadratic that depends on at most r linear functions, I is an interval. Thus, $g(X', Y)$ will be approximately the product of an indicator function of something that depends on only a limited number linear functions of Y and a polynomial of bounded degree. Our proposition will hold essentially because PRGs for read once branching programs fool such functions as show in Proposition 3.4.

Note that $P(q_0(Y), q_1''(Y))$ can be written as a polynomial of degree at most $4k$ and L^2 norm at most $O(k)^{4k}$. Letting $G_0(y)$ be

$$G_0(y) := \mathbb{E}_X\left[\mathbf{1}_{s(X,y)\in I} P(q_0(X,y), q_1''(y))\right]$$

we have by Proposition 3.4 that

$$|\mathbb{E}[G_0(X)] - \mathbb{E}[G_0(Y)]| \leq O(\log^{5k}(\delta_1)(\delta_2 + n\delta_1^{1/4}))O(nk)^{4k}.$$

Similarly, if

$$G_1(y) := \mathbb{E}_X\left[\mathbf{1}_{s(X,y)\in I}(q_0(X,y)^{2k} + q_1''(X,y)^{2k})\right]$$

then

$$|\mathbb{E}[G_1(X)] - \mathbb{E}[G_1(Y)]| \leq O(\log^{5k}(\delta_1)(\delta_2 + n\delta_1^{1/4}))O(nk)^{4k}.$$

Also,

$$\mathbb{E}[G_1(X)] \leq O(\delta k)^{2k}$$

by Lemma 2.3. Therefore, we have that the difference in expectations between $g_n^{\pm}(X', Y)$ and $g_n^{\pm}(X', Z)$ where Z is an independent standard Gaussian, is at most

$$\exp(-\Omega(\delta^{-1})) + O(\log^{5k}(\delta_1)(\delta_2 + n\delta_1^{1/4}))O(nk)^{4k} + O(\delta k)^{2k}.$$

Thus,

$$\begin{aligned}&\left|\mathbb{E}[f_n^{\pm}(X)] - \mathbb{E}[f_n^{\pm}(\sqrt{1-\delta^2}X + \delta Y)]\right| \\ &\qquad \leq \exp(-\Omega(\delta^{-1})) + O(\log^{5k}(\delta_1)(\delta_2 + n\delta_1^{1/4}))O(nk)^{4k} + O(\delta k)^{2k}.\end{aligned}$$

Therefore, we have that

$$\begin{aligned}&\sum_{|n|\leq 4^k}\left|\mathbb{E}[f_n(X)] - \mathbb{E}[f_n(\sqrt{1-\delta^2}X + \delta Y)]\right| \\ &\qquad \leq \exp(-\Omega(\delta^{-1}))4^k + O(\log^{5k}(\delta_1)(\delta_2 + n\delta_1^{1/4}))O(nk)^{4k}\delta^{-k} + O(\delta k)^k \\ &\qquad\qquad + \sum_n \left|\mathbb{E}[f_n^+(X) - f_n^-(X)]\right| \\ &\qquad \leq \exp(-\Omega(\delta^{-1}))4^k + O(\log^{5k}(\delta_1)(\delta_2 + n\delta_1^{1/4}))O(nk)^{4k}\delta^{-k} + O(\delta k)^k + O(2^{-k/2}).\end{aligned}$$

On the other hand,

$$\sum_{|n|\geq 4^k}\left|\mathbb{E}[f_n(X)] - \mathbb{E}[f_n(\sqrt{1-\delta^2}X + \delta Y)]\right|$$

is at most the probability that either $|p_0(X)|$ or $|p_0(\sqrt{1-\delta^2}X + \delta Y)|$ is more than 2^k times the L^2 norm of p, which is $O(2^{-k})$ by the Markov bound and Corollary 3.6. Thus,

$$\begin{aligned}&\left|\mathbb{E}[f(X)] - \mathbb{E}[f(\sqrt{1-\delta^2}X + \delta Y)]\right| \\ &\qquad \leq \sum_{|n|\in\mathbb{Z}}\left|\mathbb{E}[f_n(X)] - \mathbb{E}[f_n(\sqrt{1-\delta^2}X + \delta Y)]\right| \\ &\qquad \leq \exp(-\Omega(\delta^{-1}))4^k + O(\log^{5k}(\delta_1)(\delta_2 + n\delta_1^{1/4}))O(nk)^{4k} + O(\delta k)^{2k} + O(2^{-k/2}).\end{aligned}$$

As desired. ◀

We would like to reduce Proposition 4.1 to this case. Fortunately, it can be shown that after an appropriate random restriction that any quadratic polynomial can be made to be approximately linear with high probability.

▶ **Lemma 4.4.** *Let p be a degree 2 polynomial, $\delta > 0$ and r a non-negative integer. Let X be a Gaussian random variable and $p^{(X)}$ be the polynomial*

$$p^{(X)}(x) := p(\sqrt{1-\delta^2}X + \delta x).$$

Then with probability at least $1 - \exp(-\Omega(r))$ over the choice of X, $p^{(X)}$ is $(r, O(\delta))$-approximately linear.

Proof. For any polynomial q, let $q^{(X)}$ be the polynomial

$$q^{(X)}(x) := q(\sqrt{1-\delta^2}X + \delta x).$$

After diagonalizing the quadratic part of p and making an orthonormal change of variables we may write

$$p(x) = \sum_{i=1}^{n} p_i(x_i)$$

where p_i is a quadratic polynomial in one variable. Furthermore, we may assume that the quadratic term of $p_i(x)$ is $a_i x^2$ with $|a_i|$ decreasing in i. Note that

$$p^{(X)}(x) = \sum_{i=1}^{n} p_i^{(X_i)}(x_i).$$

We may write $p_i^{(X_i)}(x)$ as $\delta^2\sqrt{2}a_i h_2(x) + C_{i,1}(X_i)x + C_{i,0}(X_i)$ where $h_2(x) = (x^2-1)/\sqrt{2}$ is the second Hermite polynomial, and $C_{i,1}$ and $C_{i,0}$ are appropriate constants depending on X_i. Note furthermore, that unless X_i lies within a small constant of the global maximum or minimum of p_i that $|C_{i,1}(X_i)| = \Omega(\delta|a_i|)$. Thus, with probability at least $2/3$, independently for each i, we have that $|C_{i,1}(X_i)| = \Omega(\delta|a_i|)$. Let I_i be the indicator random variable for the event that this happens.

From this it is easy to show that with probability $1-\exp(-\Omega(r))$ we have that $\sum_{i=1}^{m} I_i \geq m/2 - r$ for all m (in fact the expected number of m for which this fails is exponentially small). We claim that if this occurs, then $p^{(X)}$ is $(r, O(\delta))$-approximately linear. To show this, let S be the set of the r smallest indices i for which $I_i = 0$. We may write

$$p^{(X)}(x) = \left(\sum_{i\in S} p_i^{(X_i)}(x_i) + \sum_{i\notin S} C_{i,0}(X_i)\right) + \left(\sum_{i\notin S} C_{i,1}(X_i)e_i\right)\cdot X + \left(\sum_{i\notin S}\delta^2\sqrt{2}a_i h_2(x_i)\right).$$

We claim that letting

$$p_0(x) = \sum_{i\in S} p_i^{(X_i)}(x_i) + \sum_{i\notin S} C_{i,0}(X_i), \quad v = \sum_{i\notin S} C_{i,1}(X_i)e_i, \quad q(x) = \sum_{i\notin S}\delta^2\sqrt{2}a_i h_2(x_i)$$

shows that $p^{(X)}$ is $(r, O(\delta))$-approximately linear.

It is clear that p_0 depends on only the r linear functions $x\cdot e_i$ for $i\in S$, that v is orthogonal to these e_i, and that $p^{(X)}$ is the sum of $p_0, x\cdot v$ and q. We have only to verify that $|q|_2 = O(\delta)|v|$. It is clear that $|q|_2 = O(\delta^2)\sqrt{\sum_{i\notin S} a_i^2}$. On the other hand, we have that

$$|v|_2 = \sqrt{\sum_{i\notin S} C_{i,1}^2(X_i)} \geq \Omega\left(\delta\sqrt{\sum_{i\notin S} I_i a_i^2}\right).$$

Thus, it suffices to show that

$$\sum_{i \notin S} I_i a_i^2 \geq \frac{1}{2} \sum_{i \notin S} a_i^2.$$

We can show this by Abel summation. In particular, for $i \notin S$ let i' be the value of the next smallest integer not in S and let $a_{n+1} = 0$. We have that

$$\sum_{i \notin S} a_i^2 = \sum_{i \notin S} \sum_{j \notin S, j \geq i} a_j^2 - a_{j'}^2 = \sum_{j \notin S} (a_j^2 - a_{j'}^2) \left(\sum_{i \notin S, i \leq j} 1 \right).$$

Similarly,

$$\sum_{i \notin S} I_i a_i^2 = \sum_{i \notin S} I_i \sum_{j \notin S, j \geq i} I_i (a_j^2 - a_{j'}^2) = \sum_{j \notin S} (a_j^2 - a_{j'}^2) \left(\sum_{i \notin S, i \leq j} I_i \right).$$

On the other hand, for any j we have that

$$\sum_{i \notin S, i \leq j} I_i \geq \frac{1}{2} \sum_{i \notin S, i \leq j} 1.$$

Substituting into the above we find that

$$\sum_{i \notin S} I_i a_i^2 \geq \frac{1}{2} \sum_{i \notin S} a_i^2$$

and our result follows. ◀

Proposition 4.1 now follows easily by using Lemma 4.4 to reduce us to the case handled by Lemma 4.3.

Proof. Let $f(x) = \operatorname{sgn}(p(x))$ for some degree 2 polynomial p.

Let X_1 and X_2 be independent standard Gaussians. Note that

$$\mathbb{E}[f(\sqrt{1-\delta^3} X + \delta^{3/2} Y)] = \mathbb{E}[f(\sqrt{1-\delta} X_1 + \sqrt{\delta}(\sqrt{1-\delta^2} X_2 + \delta Y))].$$

Let $p^{(X_1)}$ be the polynomial given by

$$p^{(X_1)}(x) := p(\sqrt{1-\delta} X_1 + \sqrt{\delta} x)$$

and let $f^{(X_1)}(x) := \operatorname{sgn}(p^{(X_1)})(x)$. Note that

$$\mathbb{E}[f(\sqrt{1-\delta^3} X + \delta^{3/2} Y)] = \mathbb{E}_{X_1}[\mathbb{E}_{X_2, Y}[f^{(X_1)}(\sqrt{1-\delta^2} X_2 + \delta Y)]].$$

By Lemma 4.4, we have with probability $1 - \exp(-\Omega(\delta^{-1}))$ over the choice of X_1 that $p^{(X_1)}$ is $(\delta^{-1}, O(\sqrt{\delta}))$-approximately linear. If this is the case, then by applying Lemma 4.3 with k a sufficiently small multiple of δ^{-1}, we find that

$$\mathbb{E}_{X_2, Y}[f^{(X_1)}(\sqrt{1-\delta^2} X_2 + \delta Y)] = \mathbb{E}[f^{(X_1)}(X)] + \exp(-\Omega(\delta^{-1})).$$

Putting these together, we find that

$$\begin{aligned} \mathbb{E}[f(\sqrt{1-\delta^3} X + \delta^{3/2} Y)] &= \mathbb{E}_{X_1}[\mathbb{E}[f^{(X_1)}(X)]] + \exp(-\Omega(\delta^{-1})) \\ &= \mathbb{E}[f(\sqrt{1-\delta} X_1 + \sqrt{\delta} X)] + \exp(-\Omega(\delta^{-1})) \\ &= \mathbb{E}[f(X)] + \exp(-\Omega(\delta^{-1})). \end{aligned}$$

◀

5 Cleanup

It is not difficult to complete the analysis of our generator given Proposition 4.1. We begin by applying Proposition 4.1 iteratively to obtain:

▶ **Lemma 5.1.** *Let $\delta > 0$ and n, ℓ be positive integers. Let C be a sufficiently large constant. For $1 \leq i \leq \ell$ let Y_i be an independent copy of a family of n $\exp(-C\delta^{-1}\log(n/\delta))$-approximate Gaussians seeded by a pseudorandom generator that fools read once branching programs of memory $C\delta^{-2}\log(n/\delta)$ to within error $\exp(-C\delta^{-1}\log(n/\delta))$. Let X be an n dimensional standard Gaussian. Then for any degree 2 polynomial threshold function f in n variables, we have that*

$$\left|\mathbb{E}[f(X)] - \mathbb{E}\left[f\left((1-\delta^3)^{\ell/2}X + \delta^{3/2}\sum_{i=1}^{\ell}(1-\delta^3)^{(\ell-1)/2}Y_i\right)\right]\right| \leq \ell\exp(-\Omega(\delta^{-1})).$$

Proof. The proof is by induction on ℓ. The case of $\ell = 0$ is trivial. Assuming that our Lemma holds for ℓ, applying Proposition 4.1 to the threshold function

$$g(x) := f\left((1-\delta^3)^{\ell/2}x + \delta^{3/2}\sum_{i=1}^{\ell}(1-\delta^3)^{(\ell-1)/2}Y_i\right),$$

we find that

$$\begin{aligned}
&\mathbb{E}\left[f\left((1-\delta^3)^{(\ell+1)/2}X + \delta^{3/2}\sum_{i=1}^{\ell+1}(1-\delta^4)^{(\ell-1)/2}Y_i\right)\right] \\
&\quad = \mathbb{E}\left[f\left((1-\delta^3)^{\ell/2}X + \delta^{3/2}\sum_{i=1}^{\ell}(1-\delta^4)^{(\ell-1)/2}Y_i\right)\right] + \exp(-\Omega(\delta^{-1})) \\
&\quad = \mathbb{E}[f(X)] + (\ell+1)\exp(-\Omega(\delta^{-1})).
\end{aligned}$$

This completes the proof. ◀

Next, we note that when ℓ is large, the coefficient of X above is small enough that it should have negligible probability of affecting the sign of the polynomial in question.

▶ **Lemma 5.2.** *Let $\delta > 0$ and n, ℓ be positive integers. Let C be a sufficiently large constant. For $1 \leq i \leq \ell$ let Y_i be an independent copy of a family of n $\exp(-C\delta^{-1}\log(n/\delta))$-approximate Gaussians seeded by a pseudorandom generator that fools read once branching programs of memory $C\delta^{-2}\log(n/\delta)$ to within error $\exp(-C\delta^{-1}\log(n/\delta))$. Let X be an n dimensional standard Gaussian. Then for any degree 2 polynomial threshold function f in n variables, we have that*

$$\left|\mathbb{E}[f(X)] - \mathbb{E}\left[f\left(\frac{\sum_{i=1}^{\ell}(1-\delta^3)^{(\ell-1)/2}Y_i}{\sqrt{\sum_{i=1}^{\ell}(1-\delta^3)^{\ell-1}}}\right)\right]\right| \leq \ell\exp(-\Omega(\delta^{-1})) + O((1-\delta^3)^{\ell/18}).$$

Proof. Let

$$Y := \frac{\sum_{i=1}^{\ell}(1-\delta^3)^{(\ell-1)/2}Y_i}{\sqrt{\sum_{i=1}^{\ell}(1-\delta^3)^{\ell-1}}},$$

and

$$Y' = (1-\delta^3)^{\ell/2}X + \sqrt{1-(1-\delta^3)^{\ell}}Y.$$

By Lemma 5.1, it suffices to compare $\mathbb{E}[f(Y)]$ with $\mathbb{E}[f(Y')]$. To do this, let p be the degree-2 polynomial defining the threshold function f. Consider

$$\mathbb{E}\left[\left(p(Y) - p(Y')\right)^2\right].$$

We may write this as $\mathbb{E}[q(X, Y_1, \ldots, Y_\ell)^2]$ for an appropriate quadratic polynomial q. Letting $X_1, \ldots, X_\ell$ be independent standard Gaussians, we have by repeated use of Corollary 3.6 that

$$\begin{aligned}
\mathbb{E}[q(X, Y_1, \ldots, Y_\ell)^2] &\leq (1+\delta^5)\mathbb{E}[q(X, X_1, Y_2, \ldots, Y_\ell)^2] \\
&\leq (1+\delta^5)^2\mathbb{E}[q(X, X_1, X_2, Y_3, \ldots, Y_\ell)^2] \\
&\leq \ldots \\
&\leq (1+\delta^5)^\ell\mathbb{E}[q(X, X_1, \ldots, X_\ell)^2] \\
&= (1+\delta^5)^\ell\mathbb{E}\left[\left(p(X) - p\left((1-\delta^3)^{\ell/2}X_1 + \sqrt{1-(1-\delta^3)^\ell}X\right)\right)^2\right] \\
&= O((1-\delta^3)^{\ell/3})|p|_2^2.
\end{aligned}$$

The factors of $(1+\delta^5)$ are showing up as a very loose approximation to the truth, and are obtained by noting that

$$\begin{aligned}
&\left|\mathbb{E}[q(X, X_1, \ldots, X_i, Y_{i+1}, \ldots, Y_\ell)^2] - \mathbb{E}[q(X, X_1, \ldots, X_{i-1}, Y_i, \ldots, Y_\ell)^2]\right| \\
&\quad\leq \exp(-\Omega(\delta^{-1}))\mathbb{E}_{X, X_j, Y_j, j\neq i}[\mathbb{E}[q(X, X_1, \ldots, X_i, Y_{i+1}, \ldots, Y_\ell)^4]^{1/2}] \\
&\quad\leq \delta^5\mathbb{E}[q(X, X_1, \ldots, X_i, Y_{i+1}, \ldots, Y_\ell)^2].
\end{aligned}$$

Let $K = (1-\delta^3)^{\ell/9}|p|_2$. By Markov's inequality we have that $|q(X, Y_i)| \leq K$ except with probability at most $O((1-\delta^3)^{\ell/18})$. Let $f_\pm(x) = \operatorname{sgn}(p(x) \pm K)$. By Lemma 2.2, we have that $|\mathbb{E}[f_+(X)] - \mathbb{E}[f_-(X)]| \leq O(K^{1/2}) = O((1-\delta^3)^{\ell/18})$. By Lemma 5.1, $|\mathbb{E}[f_\pm(X)] - \mathbb{E}[f_\pm(Y')]| \leq \ell\exp(-\Omega(\delta^{-1}))$. On the other hand, with high probability $|p(Y) - p(Y')| \leq K$ and thus with high probability

$$f_+(Y') \geq f(Y) \geq f_-(Y').$$

Therefore,

$$\begin{aligned}
\mathbb{E}[f(Y)] &\leq \mathbb{E}[f_+(Y')] + O((1-\delta^3)^{\ell/18}) \\
&\leq \mathbb{E}[f_+(X)] + O((1-\delta^3)^{\ell/18}) + \ell\exp(-\Omega(\delta^{-1})) \\
&\leq \mathbb{E}[f(X)] + O((1-\delta^3)^{\ell/18}) + \ell\exp(-\Omega(\delta^{-1})).
\end{aligned}$$

The lower bound follows similarly, and this completes the proof. ◀

Theorem 1.1 now follows immediately.

Proof. The result follows immediately from Lemma 5.2. We can obtain the stated seed length by using the generators from Lemma 3.2 and Theorem 3.3. ◀

Acknowledgements. This research was done with the support of an NSF postdoctoral fellowship.

References

1. Richard Beigel *The polynomial method in circuit complexity*, Proc. of 8th Annual Structure in Complexity Theory Conference (1993), pp. 82–95.
2. A. Carbery, J. Wright *Distributional and L^q norm inequalities for polynomials over convex bodies in $\mathbb{R}^n$* Mathematical Research Letters, Vol. 8(3), pp. 233–248, 2001.
3. I. Diakonikolas, P. Gopalan, R. Jaiswal, R. Servedio, E. Viola, *Bounded Independence Fools Halfspaces* SIAM Journal on Computing, Vol. 39(8), pp. 3441–3462, 2010.
4. Ilias Diakonikolas, Daniel M. Kane, Jelani Nelson, *Bounded Independence Fools Degree-2 Threshold Functions*, Foundations of Computer Science (FOCS), 2010.
5. Russell Impagliazzo, Noam Nisan, Avi Wigderson *Pseudorandomness for network algorithms*, STOC (1994), pp. 356–364.
6. Svante Janson *Gaussian Hilbert Spaces*, Cambridge University Press, 1997.
7. Daniel M. Kane *k-Independent Gaussians Fool Polynomial Threshold Functions*, Conference on Computational Complexity (CCC), 2011.
8. Daniel M. Kane *A Pseudorandom Generator for Polynomial Threshold Functions of Gaussians with Subpolynomial Seed Length*, Conference on Computational Complexity (CCC) 2014.
9. Daniel M. Kane *A Small PRG for Polynomial Threshold Functions of Gaussians* Symposium on the Foundations Of Computer Science (FOCS), 2011.
10. Daniel M. Kane *A Structure Theorem for Poorly Anticoncentrated Gaussian Chaoses and Applications to the Study of Polynomial Threshold Functions*, manuscript `http://arxiv.org/abs/1204.0543`.
11. Adam R. Klivans, Rocco A. Servedio *Learning DNF in time* $2^{O(n^{1/3})}$, J. Computer and System Sciences Vol. 68 (2004), pp. 303–318.
12. Raghu Meka, David Zuckerman *Pseudorandom generators for polynomial threshold functions*, Proceedings of the 42nd ACM Symposium on Theory Of Computing (STOC 2010).
13. Nelson *The free Markov field*, J. Func. Anal. Vol. 12(2), pp. 211–227, 1973.
14. Alexander A. Sherstov *Separating AC0 from depth-2 majority circuits*, SIAM J. Computing Vol. 38 (2009), pp. 2113–2129.