

A Pseudorandom Generator for Functions of Low-Degree Polynomial Threshold Functions

Penghui Yao^{*†} Mingnan Zhao[‡]

April 15, 2025

Abstract

Developing explicit *pseudorandom generators* (PRGs) for prominent categories of Boolean functions is a key focus in computational complexity theory. In this paper, we investigate the PRGs against the functions of degree- d *polynomial threshold functions* (PTFs) over Gaussian space. Our main result is an explicit construction of PRG with seed length $\text{poly}(k, d, 1/\epsilon) \cdot \log n$ that can fool *any* function of k degree- d PTFs with probability at least $1 - \epsilon$. More specifically, we show that the summation of L independent R -moment-matching Gaussian vectors ϵ -fools functions of k degree- d PTFs, where $L = \text{poly}(k, d, \frac{1}{\epsilon})$ and $R = O(\log \frac{kd}{\epsilon})$. The PRG is then obtained by applying an appropriate discretization to Gaussian vectors with bounded independence.

1 Introduction

In computational complexity theory, derandomization is a powerful technique that aims to reduce randomness in algorithms without sacrificing efficiency or accuracy. A versatile approach for derandomization is to design explicit *pseudorandom generators* (PRGs) for notable families of Boolean functions. A PRG for a family of Boolean functions is able to consume few random bits and produce a distribution over high-dimensional vectors, which is indistinguishable from a target distribution, such as the uniform distribution over Boolean cube, by any function in the family. In this paper, we concern ourselves with the Gaussian distribution over \mathbb{R}^n . Formally,

Definition 1.1. Let $\mathcal{F} \subseteq \{f : \mathbb{R}^n \rightarrow \{0, 1\}\}$ be a family of Boolean functions. A function $G : \{0, 1\}^r \rightarrow \mathbb{R}^n$ is a *pseudorandom generator* for \mathcal{F} with error ϵ over Gaussian distribution $\mathcal{N}(0, 1)^n$ if for any $f \in \mathcal{F}$,

$$\left| \mathbb{E}_{s \sim \mathcal{U}_{\{0,1\}^r}} [f(G(s))] - \mathbb{E}_{x \sim \mathcal{N}(0,1)^n} [f(x)] \right| \leq \epsilon .$$

We call r the *seed length* of G . We also say G ϵ -fools \mathcal{F} over the Gaussian distribution.

^{*}State Key Laboratory for Novel Software Technology, New Cornerstone Science Laboratory, Nanjing University, Nanjing 210023, China.
Email: phyao1985@gmail.com.

[†]Hefei National Laboratory, Hefei 230088, China.

[‡]State Key Laboratory for Novel Software Technology, New Cornerstone Science Laboratory, Nanjing University, Nanjing 210023, China.
Email: mingnanzh@gmail.com.

There has been a considerable amount of research developing PRGs for various Boolean function families, including halfspaces, polynomial threshold functions and intersections of halfspaces. Let $\text{sign} : \mathbb{R} \rightarrow \{0, 1\}$ be the function such that $\text{sign}(x) = 1$ iff $x \geq 0$. A *halfspace* is a Boolean function of the form $f(x) = \text{sign}(a_1x_1 + \dots + a_nx_n - b)$ for some $a_1, \dots, a_n, b \in \mathbb{R}$. Halfspaces are a fundamental class of Boolean functions which have found significant applications in machine learning, complexity theory, theory of approximation and more. A very successful series of work produced PRGs that ϵ -fools halfspaces with seed length poly-logarithmic in n and ϵ^{-1} over both Boolean space [Ser06, DGJ⁺10, MZ13, GKM18] and Gaussian space [KM15]. *Polynomial threshold functions* (PTFs) are functions of the form $f(x) = \text{sign}(p(x))$ where p is a polynomial. We call f is a degree- d PTF if p is a degree- d polynomial. PTFs are natural generalization for halfspaces since a halfspace is a degree-1 PTF. An explicit PRG that ϵ -fools PTFs over Boolean space has been achieved with seed length $(d/\epsilon)^{O(d)} \cdot \log n$ [MZ13]. As for Gaussian space, a sequence of work [DKN10, Kan11a, Kan11b, Kan12, MZ13, Kan14, Kan15, OST20, KM22] succeeds in giving a PRG with seed length polynomial in d , ϵ^{-1} and $\log n$ [OST20, KM22]. Another extension for halfspaces is *intersections* of k halfspaces which are polytopes with k facets. A line of work [GOWZ10, HKM13, ST17, CDS20, OST22] results in PRGs with seed length polynomial in $\log k$, $\log n$ and $1/\epsilon$ over Boolean space [OST22] and over Gaussian space [CDS20].

Considering the prosperity of PRGs for these functions families, we commence designing PRGs for *functions of degree- d polynomial threshold functions*.

Definition 1.2. We say a function $F : \mathbb{R}^n \rightarrow \{0, 1\}$ is a function of k degree- d PTFs if there exist k polynomials $p_1, \dots, p_k : \mathbb{R}^n \rightarrow \mathbb{R}$ of degree d and a Boolean function $f : \{0, 1\}^k \rightarrow \{0, 1\}$ such that

$$F(x) = f(\text{sign}(p_1(x)), \dots, \text{sign}(p_k(x))) \quad .$$

This family consumes all three function families we discussed above. For example, it includes intersections of halfspaces by setting $d = 1$ and $f(x) = x_1 \cdots x_k$. The research on PRGs for functions of PTFs is driven by several motivations beyond its fundamental role in derandomization tasks. For instance, the collection of satisfying assignments of an intersection of k degree-2 PTFs corresponds to the feasible solutions set of an $\{0, 1\}$ -integer quadratic programming [NW99] with k constraints. The investigation into the structure of these sets has been a central focus of extensive research in areas including learning theory, counting, optimization, and combinatorics.

In this work, we consider building explicit PRGs for functions of degree- d PTFs over Gaussian space. Before presenting our main result, we briefly revisit relevant prior work on fooling functions of halfspaces.

1.1 Prior Work

The related work is summarized in Table 1. Gopalan, O'Donnell, Wu and Zuckerman [GOWZ10] constructed PRGs for *monotone functions of halfspaces*. They modified the PRG for halfspaces in [MZ13] and showed the modified PRG ϵ -fools any monotone function of k halfspaces over a broad class of *product distributions* with seed length $O((k \log(k/\epsilon) + \log n) \cdot \log(k/\epsilon))$. When $k/\epsilon \leq \log^c n$ any $c > 0$, the seed length can be further improved to $O(k \log(k/\epsilon) + \log n)$.

Harsha, Klivans and Meka [HKM13] considered designing PRGs for intersections of *regular* halfspaces (i.e., halfspaces with low influence). A halfspace $f(x) = \text{sign}(a_1x_1 + \dots + a_nx_n - b)$ is

Table 1: Related Work on PRGs for Intersections of PTFs

Reference	Function Family	Seed length
[GOWZ10]	Monotone functions of k halfspaces	$O((k \log(k/\epsilon) + \log n) \cdot \log(k/\epsilon))$
[HKM13]	Intersections of k δ -regular halfspaces	$O(\log n \log k/\epsilon)$ for $\delta \leq \epsilon^5/(\log^{8.1} k \log(1/\epsilon))$
[ST17]	Intersections of k weight- t halfspaces	$\text{poly}(\log n, \log k, t, 1/\epsilon)$
[OST22]	Intersections of k halfspaces	$\text{polylog } m \cdot \epsilon^{-(2+\delta)} \cdot \log n$ for any absolute constant $\delta \in (0, 1)$
[CDS20]	Intersections of k halfspaces Arbitrary functions of k halfspaces	$O(\log n + \text{poly}(\log k, 1/\epsilon))$ $O(\log n + \text{poly}(k, 1/\epsilon))$
[DKN10]	Intersections of k degree-2 PTFs	$O(\log n \cdot \text{poly}(k, 1/\epsilon))$

δ -regular if $\sum_i a_i^4 \leq \delta^2 \sum_i a_i^2$. They gave an explicit PRG construction for intersections of k δ -regular halfspaces over *proper* and *hypercontractive* distributions with seed length $O(\log n \log k/\epsilon)$ when δ is no more than a threshold. Their proof is based on developing an invariance principle for intersections of regular halfspaces via a generalization of the well-known Lindeberg method [Lin22] and an anti-concentration result of polytopes in Gaussian space from [KOS08].

By extending the approach of [HKM13] and combining the results on bounded independence fooling CNF formulas [Baz09, Raz09], Servedio and Tan [ST17] designed an explicit PRG that ϵ -fools intersections of k weight- t halfspaces over Boolean space with $\text{poly}(\log n, \log k, t, 1/\epsilon)$ seed length. A halfspace $f(x) = \text{sign}(a_1 x_1 + \dots + a_n x_n - b)$ is said to be weight- t if each a_i is an integer in $[-t, t]$.

As for intersections of k general halfspaces, O’Donnell, Servedio and Tan [OST22] gave a PRG construction over Boolean space with a polylogarithmic seed length dependence on k and n . Their proof involves a novel invariance principle for intersections of arbitrary halfspaces and a Littlewood–Offord style anticoncentration inequality for polytopes over Boolean space.

Concurrently, Chattopadhyay, De and Servedio [CDS20] proposed a simple PRG that ϵ -fools intersections of k general halfspaces over Gaussian space, building upon the concept of *Johnson-Lindenstrauss transform* [JLS86, KMN11]. The seed length is $O(\log n + \text{poly}(\log k, 1/\epsilon))$. Additionally, they show that the same PRG with seed length $O(\log n + \text{poly}(k, 1/\epsilon))$ is able to fool arbitrary functions of k halfspaces.

Speaking of fooling functions of PTFs, the study by Diakonikolas, Kane and Nelson [DKN10] stands out as the sole work that constructs a PRG for intersections of k degree-2 PTFs. Their PRG is specific to degree $d \leq 2$ with a $O(\log n \cdot \text{poly}(k, 1/\epsilon))$ seed length.

1.2 Main Result

In this work, we investigate the PRGs fooling any function of low-degree PTFs. The main result is the following.

Theorem 1.3. (Informal version of [Theorem 4.2](#)) *There exists an explicit PRG ϵ -fools any function of k degree- d PTFs over Gaussian space with seed length $\text{poly}(k, d, 1/\epsilon) \cdot \log n$.*

The proof is inspired by the PRG proposed in [\[Kan11b\]](#) and the work [\[KM22\]](#). This theorem follows from two components.

(1) Bounded independence fools functions of k degree- d PTFs. Consider the continuous random vector $Y = \frac{1}{\sqrt{L}} \sum_{i=1}^L Y_i$ where Y_i is a R -wise independent standard Gaussian vector of length n . Every $Y_{i,j}$ is a standard Gaussian variable and for any degree- R polynomial f , $\mathbb{E}[f(Y_i)] = \mathbb{E}_{y \sim \mathcal{N}(0,1)^n}[f(y)]$. We will prove that

Theorem 1.4. (Informal version of [Theorem 3.1](#)) *With $R = O(\log \frac{kd}{\epsilon})$ and $L = \text{poly}(k, d, \frac{1}{\epsilon})$, the distribution of Y ϵ -fools any function of k degree- d PTFs over Gaussian space.*

The prior work [\[KM22\]](#) shows that bounded independence fools a single low-degree polynomial threshold function. This generalizes their work to the case of functions of k low-degree PTFs.

(2) Discretization of bounded independence Gaussians. An explicit PRG construction requires a discrete approximation to Gaussian vectors with bounded independence. The idea is to use a finite entropy random variable X to approximate Y . Previous work [\[Kan11b\]](#) uses the idea that a single Gaussian variable can be produced by two uniform random variables in $[0, 1]$ through the Box–Muller transform [\[BM58\]](#). Therefore bounded independence Gaussian variables Y_i can be generated by using bounded independence uniform random variables. Then by truncating these uniform $[0, 1]$ random variables to a sufficient precision, we obtain vectors X_i that serve as a discrete approximation of Y_i . We prove that X also fools functions of k degree- d PTFs as long as X is a good approximation to Y .

Lemma 1.5. (Informal version of [Lemma 4.1](#)) *If $X_{i,j}$ and $Y_{i,j}$ are sufficiently close with high probability, then X also fools functions of k degree- d PTFs.*

Acknowledgment. PY and MZ were supported by National Natural Science Foundation of China (Grant No. 62332009 and 12347104), Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302901), NSFC/RGC Joint Research Scheme (Grant No. 12461160276), Natural Science Foundation of Jiangsu Province (Grant No. BK20243060), and the New Cornerstone Science Foundation.

2 Preliminary

Basic Notation. For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, 2, \dots, n\}$. For $\alpha \in \mathbb{R}^n$ and $i \in [n]$, α_i denotes the i -th coordinate of α , $|\alpha| = \sum_{i=1}^n |\alpha_i|$ and $\|\alpha\|_\infty = \max_{1 \leq i \leq n} |\alpha_i|$. For $\alpha, \beta \in \mathbb{R}^n$, $\alpha - \beta$ denotes the vector v such that $v_i = \alpha_i - \beta_i$ for all $i \in [n]$, and $\alpha^\beta = \prod_{i=1}^n \alpha_i^{\beta_i}$. For $\alpha \in \mathbb{N}^n$, $\alpha! = \prod_{i=1}^n \alpha_i!$. When it is clear from the context, we will use both subscript and superscript as indices.

Derivatives and Multidimensional Taylor Expansion. For a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ and $\alpha \in \mathbb{N}^n$, we use $\partial^\alpha f$ to denote the partial derivative taken α_i times in the i -th coordinate and define $\|\nabla^t f(x)\| = \sqrt{\sum_{\alpha \in \mathbb{N}^n, |\alpha|=t} (\partial^\alpha f(x))^2}$. For $f(a, b) : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ and $\alpha, \beta \in \mathbb{N}^n$, we use $\partial_a^\alpha \partial_b^\beta f$ to denote the partial derivative taken α_i times in a_i and β_i times in b_i . Using these notations, one has:

Theorem 2.1 (Multidimensional Taylor's Theorem). *Let $d \in \mathbb{N}$ and $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$ be a C^{d+1} function. Then for all $x, y \in \mathbb{R}^n$,*

$$f(y) = \sum_{\alpha \in \mathbb{N}^n, |\alpha| \leq d} \frac{\partial^\alpha f(x)}{\alpha!} (y-x)^\alpha + \sum_{\alpha \in \mathbb{N}^n, |\alpha|=d+1} \frac{\partial^\alpha f(z)}{\alpha!} (y-x)^\alpha$$

where $z = cx + (1-c)y$ for some $c \in (0, 1)$.

Bump Function. Consider the bump function $\Psi : \mathbb{R} \rightarrow \mathbb{R}$ defined by $\Psi(x) = \begin{cases} e^{\frac{1}{x^2-1}}, & \text{if } |x| < 1, \\ 0, & \text{if } |x| \geq 1. \end{cases}$ It is well known that this function is infinitely differentiable and the derivatives are bounded.

Fact 2.2. For all $t \in \mathbb{N}$, $|\Psi^{(t)}(x)| \leq t^{(3+o(1))t}$.

Let ρ be the smooth univariate function defined by $\rho(x) = \begin{cases} 1, & \text{for } x \geq 1, \\ e \cdot e^{\frac{1}{(x-1)^2-1}} & \text{for } 0 < x < 1, \\ 0, & \text{for } x \leq 0. \end{cases}$

It is easy to see ρ is obtained from Ψ via translation, stretch, and concatenation. We have

Fact 2.3. For all $t \in \mathbb{N}$, $|\rho^{(t)}(x)| \leq t^{(3+o(1))t}$.

Fact 2.4. Let $r(u, v) := \rho(\log u - \log v + c)$ for some constant c . Then we have that for all $n, m \in \mathbb{N}$, $\left| \frac{\partial^n \partial^m r(u, v)}{\partial u^n \partial v^m} \right| \leq \frac{(n+m)^{6(n+m)}}{|u|^n |v|^m}$.

We include the proof for the above three facts in [Appendix A](#) for self-containment.

Gaussian Space and the Gaussian Noise Operator We denote by $y \sim \mathcal{N}(0, 1)^n$ that $y = (y_1, \dots, y_n) \in \mathbb{R}^n$ is a random vector whose components are independent standard Gaussian variables (i.e., with mean 0 and variance 1). We say a random vector $Y \in \mathbb{R}^n$ is a k -wise independent standard Gaussian vector if every component of Y is a standard Gaussian variable and $\mathbb{E}[p(Y)] = \mathbb{E}_{y \sim \mathcal{N}(0, 1)^n}[p(y)]$ for all polynomials $p : \mathbb{R}^n \rightarrow \mathbb{R}$ with degree at most k . For a function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ on Gaussian space and $1 \leq p \leq \infty$, the p -norm is denoted by $\|f\|_p = (\mathbb{E}_{y \sim \mathcal{N}(0, 1)^n}[|f(y)|^p])^{1/p}$. For $\rho \in [0, 1]$, the *Gaussian noise operator* U_ρ is the operator on the space of functions $f : \mathbb{R}^n \rightarrow \mathbb{R}$ defined by $U_\rho f(x) = \mathbb{E}_{y \sim \mathcal{N}(0, 1)^n} [f(\rho x + \sqrt{1-\rho^2}y)]$.

The *probabilists' Hermite polynomials* [O'D14, Section 11] $\{H_j\}_{j \in \mathbb{N}}$ are defined by

$$H_j(y) = \frac{(-1)^j}{\varphi(y)} \cdot \frac{d^j \varphi(y)}{d y^j}$$

where $\varphi(y) = \frac{1}{\sqrt{2\pi}} e^{-\frac{y^2}{2}}$. The *univariate Hermite polynomials* $\{h_j\}_{j \in \mathbb{N}}$ are defined by normalization: $h_j = \frac{1}{\sqrt{j!}} H_j$. For a multi-index $\alpha \in \mathbb{N}^n$, the *(multivariate) Hermite polynomial* $h_\alpha : \mathbb{R}^n \rightarrow \mathbb{R}$ is

$$h_\alpha(y) = \prod_{j=1}^n h_{\alpha_j}(y_j) .$$

The degree of h_α is $|\alpha|$. The Hermite polynomials $\{h_\alpha\}_{\alpha \in \mathbb{N}^n}$ form an orthonormal basis for the functions over Gaussian space: $\mathbb{E}_{y \sim \mathcal{N}(0,1)^n} [h_\alpha(y) h_\beta(y)] = 1$ iff $\alpha = \beta$, and every degree- d polynomial $f : \mathbb{R}^n \rightarrow \mathbb{R}$ can be uniquely expanded as

$$f(y) = \sum_{\alpha \in \mathbb{N}^n, |\alpha| \leq d} \widehat{f}(\alpha) h_\alpha(y) .$$

We can also expand the function $f(x + \sqrt{\lambda}y)$ in the Hermite basis in a manner similar to Taylor expansion.

Lemma 2.5 (Lemma 16 in [KM22]). *Suppose $f(y) = \sum_{\alpha \in \mathbb{N}^n} \widehat{f}(\alpha) h_\alpha(y)$, we have*

$$f(x + \sqrt{\lambda}y) = \sum_{\alpha \in \mathbb{N}^n} \frac{\partial^\alpha \phi(x)}{\sqrt{\alpha!}} \lambda^{|\alpha|/2} h_\alpha(y) ,$$

where $\phi(x) = U_{\sqrt{1-\lambda}} f\left(\frac{x}{\sqrt{1-\lambda}}\right)$.

The function $U_\rho f$ has the following expansion:

$$U_\rho f(y) = \sum_{\alpha \in \mathbb{N}^n, |\alpha| \leq d} \rho^{|\alpha|} \widehat{f}(\alpha) h_\alpha(y) .$$

The definition of U_ρ can be extended to $\rho > 1$ by its action on the Hermite polynomials: $U_\rho h_\alpha(y) = \rho^{|\alpha|} h_\alpha(y)$. We will use the following hypercontractive inequality:

Theorem 2.6. *Let $f : \mathbb{R}^n \rightarrow \mathbb{R}$ and $2 \leq p \leq \infty$, $\|f\|_p \leq \|U_{\sqrt{p-1}} f\|_2$.*

For more details on analysis over Gaussian space, readers may refer to [O'D14].

Low-Degree Polynomials. Low-degree polynomials are extensively studied in the literature. We list some results used in this paper. It is well-known that low-degree polynomials have the following anti-concentration property:

Lemma 2.7 (Theorem 8 in [CW01]). *Let $p : \mathbb{R}^n \rightarrow \mathbb{R}$ be a polynomial of degree d with $\|p\|_2 = 1$. Then*

$$\Pr_{x \sim \mathcal{N}(0,1)^n} [|p(x)| \leq \epsilon] = O(d\epsilon^{1/d}) .$$

Suppose p is a low-degree polynomial, the following gives an estimation on the deviation of $p(x)$ caused by a small perturbation.

Lemma 2.8 (Lemma 22 in [Kan11b]). *Let $p : \mathbb{R}^n \rightarrow \mathbb{R}$ be a polynomial of degree d with $\|p\|_2 = 1$. Suppose $x \in \mathbb{R}^n$ be a vector with $\|x\|_\infty \leq B$ ($B > 1$). Let x' be another vector such that $\|x - x'\|_\infty \leq \delta < 1$. Then*

$$|p(x) - p(x')| \leq \delta n^{d/2} O(B)^d .$$

The magnitudes of the derivatives of a low-degree polynomial are likely to grow at a moderate rate with high probability. Formally,

Lemma 2.9 (Lemma 6 in [KM22]). *Let $p : \mathbb{R}^n \rightarrow \mathbb{R}$ be an arbitrary polynomial of degree d and $y \sim \mathcal{N}(0, 1)^n$, the following holds with probability at least $1 - \epsilon d^3$:*

$$\|\nabla^t p(y)\| \leq O\left(\frac{1}{\epsilon}\right) \|\nabla^{t-1} p(y)\| \text{ for all } 1 \leq t \leq d.$$

The following lemma gives quantitative bounds on how much the derivatives $\nabla^t p(x + \sqrt{\lambda}y)$ are concentrated around those of $\phi(x) = \mathbb{E}_{y \sim \mathcal{N}(0,1)^n} [p(x + \sqrt{\lambda}y)]$ when $y \sim \mathcal{N}(0, 1)^n$.

Lemma 2.10 (Lemma 23 in [KM22]). *Let $0 \leq \lambda < 1$ and $p : \mathbb{R}^n \rightarrow \mathbb{R}$ be an arbitrary polynomial of degree d and $\phi(x) = U_{\sqrt{1-\lambda}} p\left(\frac{x}{\sqrt{1-\lambda}}\right) = \mathbb{E}_{y \sim \mathcal{N}(0,1)^n} [p(x + \sqrt{\lambda}y)]$. For $0 \leq t \leq d$ and $y \sim \mathcal{N}(0, 1)^n$,*

$$\left(\mathbb{E}_{y \sim \mathcal{N}(0,1)^n} \left[\left\| \nabla^t p(x + \sqrt{\lambda}y) - \nabla^t \phi(x) \right\|^R \right] \right)^{\frac{1}{R}} \leq \sqrt{\sum_{j=t+1}^d (\lambda d R)^{j-t} \|\nabla^j \phi(x)\|^2} .$$

3 Fooling the Functions of PTFs via Bounded Independence

In this section, we show that a random Gaussian vector matching certain moments fools *any* function of low-degree polynomial threshold functions. Formally, we prove

Theorem 3.1. *Fix a small constant $0 < \epsilon < 1$ and let $R \in \mathbb{N}$ be an integer. Let $p_1, \dots, p_k : \mathbb{R}^n \rightarrow \mathbb{R}$ be arbitrary polynomials of degree d and $f : \{0, 1\}^k \rightarrow \{0, 1\}$ be an arbitrary Boolean function. Define function*

$$F(x) := f(\text{sign}(p_1(x)), \dots, \text{sign}(p_k(x)))$$

Let $Y = \frac{1}{\sqrt{L}} \sum_{i=1}^L Y_i$ where Y_i is a $2dR$ -wise independent standard Gaussian vector of length n and $L = \Omega\left(\frac{k^2 d^3 R^{15}}{\epsilon^2}\right)$. Then, we have

$$\left| \mathbb{E}_Y[F(Y)] - \mathbb{E}_{y \sim \mathcal{N}(0,1)^n}[F(y)] \right| = O(\epsilon k d^3) + k d L \cdot 2^{-\Omega(R)} .$$

The key idea in the proof of [Theorem 3.1](#) is to analyze the derivatives of the disturbed function $\phi_i(x) = \mathbb{E}_{y \sim \mathcal{N}(0,1)^n} [p_i(x + \sqrt{\lambda}y)]$. We will see that once the derivatives of ϕ_i are well-controlled by its preceding order derivative at x , $\nabla^t p_i(x + \sqrt{\lambda}y)$ is concentrated around $\nabla^t \phi_i(x)$ for a random y , and $p_i(x + \sqrt{\lambda}y)$ and $\phi_i(x)$ share the same sign with high probability. Starting from this point, we use the mollifier introduced in [KM22]

$$G(x) := \prod_{i=1}^k \prod_{t=0}^{d-1} \rho \left(\log \left(\frac{\|\nabla^t p_i(x)\|^2}{16\epsilon^2 \|\nabla^{t+1} p_i(x)\|^2} \right) \right) \quad (1)$$

to judge whether the derivatives are all well-controlled for all k polynomials. $G(x) = 0$ as long as a certain order of derivative that is not controlled by its preceding order derivative. Our proof consists of following steps:

- **Approximation using the mollifier G :** We first establish that

$$\left| \mathbb{E}_Y[F(Y)] - \mathbb{E}_y[F(y)] \right| \approx \left| \mathbb{E}_Y[F(Y)G(Y)] - \mathbb{E}_y[F(y)G(y)] \right|.$$

This approximation enables us to focus primarily on the analysis of $F(y)G(y)$ in the subsequent steps.

- **Hybrid argument:** Let $\lambda = L^{-1}$, $y = \sqrt{\lambda} \sum_{i=1}^L y_i$ where $y_i \sim \mathcal{N}(0, 1)^n$ and $Z^i = \sqrt{\lambda}(y_1 + \dots + y_{i-1} + Y_{i+1} + \dots + Y_L)$. We will show

$$\mathbb{E} \left[F(Z^i + \sqrt{\lambda}Y_i)G(Z^i + \sqrt{\lambda}Y_i) \right] \approx \mathbb{E} \left[F(Z^i + \sqrt{\lambda}y_i)G(Z^i + \sqrt{\lambda}y_i) \right]. \quad (2)$$

Therefore by the triangle inequality, we have

$$\begin{aligned} \mathbb{E}_Y[F(Y)G(Y)] &= \mathbb{E} \left[F(Z^1 + \sqrt{\lambda}Y_1)G(Z^1 + \sqrt{\lambda}Y_1) \right] \\ &\approx \mathbb{E} \left[F(Z^1 + \sqrt{\lambda}y_1)G(Z^1 + \sqrt{\lambda}y_1) \right] = \mathbb{E} \left[F(Z^2 + \sqrt{\lambda}Y_2)G(Z^2 + \sqrt{\lambda}Y_2) \right] \\ &\approx \dots \approx \mathbb{E} \left[F(Z^L + \sqrt{\lambda}Y_L)G(Z^L + \sqrt{\lambda}Y_L) \right] = \mathbb{E}[F(y)G(y)] \quad . \end{aligned}$$

To prove (2), we show for any fixed x ,

$$\mathbb{E} \left[F(x + \sqrt{\lambda}Y_i)G(x + \sqrt{\lambda}Y_i) \right] \approx \mathbb{E} \left[F(x + \sqrt{\lambda}y_i)G(x + \sqrt{\lambda}y_i) \right].$$

This is done by a case analysis:

- The derivatives of all k polynomials $\phi_j(x)$ are well-controlled at point x . In this case, all $p_j(x + \sqrt{\lambda}Y_i)$ and $p_j(x + \sqrt{\lambda}y_i)$ share the same sign with high probability. Thus, it is highly likely that $F(x + \sqrt{\lambda}Y_i)$ and $F(x + \sqrt{\lambda}y_i)$ are nearly the same constant. It suffices to show Y_i fools the mollifier function $G(x + \sqrt{\lambda}Y_i)$.
- At least one derivative is not controlled. In this case, we will show that $G(x + \sqrt{\lambda}Y_i)$ and $G(x + \sqrt{\lambda}y_i)$ are 0 with high probability. This implies that $F(x + \sqrt{\lambda}Y_i)G(x + \sqrt{\lambda}Y_i) = F(x + \sqrt{\lambda}y_i)G(x + \sqrt{\lambda}y_i) = 0$ with overwhelming probability.

In the subsequent sections, [Section 3.1](#) first demonstrates that Y_i is able to fool the mollifier function G when x is a well-behaved point. [Section 3.2](#) shows the closeness of a single step in the hybrid argument. Lastly, we prove [Theorem 3.1](#) using approximation and the hybrid argument in [Section 3.3](#).

3.1 Fooling the Mollifier G

We begin with proving that a $2dR$ -wise independent standard Gaussian vector Y fools the mollifier function $G(x + \sqrt{\lambda}y)$. To achieve this, we utilize the Taylor expansion to expand the mollifier function $G(x + \sqrt{\lambda}y)$ up to a specified order. As a result, $G(x + \sqrt{\lambda}y)$ is decomposed into two parts: a degree- $d(R - 1)$ polynomial $l(y)$ and a remainder term $\Delta(y)$. We mainly show that $\mathbb{E}[\Delta]$ is negligible under both pseudorandom distribution and true Gaussian distribution. This leads us to the conclusion that $\mathbb{E}[G(x + \sqrt{\lambda}y)] \approx \mathbb{E}[l(y)]$ and $\mathbb{E}[G(x + \sqrt{\lambda}Y)] \approx \mathbb{E}[l(Y)]$. Furthermore, since $l(y)$ has degree at most dR , it follows that $\mathbb{E}[l(y)] = \mathbb{E}[l(Y)]$. Thus, we conclude that $\mathbb{E}[G(x + \sqrt{\lambda}y)] \approx \mathbb{E}[G(x + \sqrt{\lambda}Y)]$.

Lemma 3.2. *Fix a small constant $0 < \epsilon < 1$ and let $R \in \mathbb{N}$ be an integer. Let $p_1, \dots, p_k : \mathbb{R}^n \rightarrow \mathbb{R}$ be arbitrary polynomials of degree d . Define $\phi_i(x) := U_{\sqrt{1-\lambda}} p_i\left(\frac{x}{\sqrt{1-\lambda}}\right) = \mathbb{E}_{y \sim \mathcal{N}(0,1)^n} [p_i(x + \sqrt{\lambda}y)]$ for all p_i . Suppose that a fix point $x \in \mathbb{R}^n$ satisfies $\|\nabla^{t+1}\phi_i(x)\| \leq \frac{1}{\epsilon} \|\nabla^t\phi_i(x)\|$ for any $1 \leq i \leq k$ and $0 \leq t \leq d - 1$. Let Y be a $2dR$ -wise independent standard Gaussian vector of length n . For $\lambda = O(k^{-2}d^{-3}R^{-15}\epsilon^2)$, we have*

$$\left| \mathbb{E}_Y [G(x + \sqrt{\lambda}Y)] - \mathbb{E}_{y \sim \mathcal{N}(0,1)^n} [G(x + \sqrt{\lambda}y)] \right| = kd \cdot 2^{-\Omega(R)},$$

where G is defined in (1).

Proof. **TOPROVE 0** □

3.2 A Single Step in the Hybrids

In this section, we analyze one single step in the entire hybrid argument. We will show that for any x , we have that $\mathbb{E}_Y[F(x + \sqrt{\lambda}Y)G(x + \sqrt{\lambda}Y)] \approx \mathbb{E}_y[F(x + \sqrt{\lambda}y)G(x + \sqrt{\lambda}y)]$ for $2dR$ -wise independent Gaussian Y and true Gaussian y .

Let $\phi_i(x) = U_{\sqrt{1-\lambda}} p_i\left(\frac{x}{\sqrt{1-\lambda}}\right) = \mathbb{E}_y[p_i(x + \sqrt{\lambda}y)]$. The proof proceeds through a case analysis based on the behavior of ϕ_i at the fixed point x . Specifically, we define x as well-behaved if $\|\nabla^{t+1}\phi_i(x)\| \leq \frac{1}{\epsilon} \|\nabla^t\phi_i(x)\|$ for all $t \in [d]$ and $i \in [k]$. In other words, for each function ϕ_i , its t -th order derivatives are controlled by its $(t - 1)$ -th order derivatives.

- In the scenario where x is not well-behaved, we can identify an i_0 and a t_0 such that with at least probability $1 - 2^{-R+1}$,

$$\left\| \nabla^{t_0+1} p_{i_0}(x + \sqrt{\lambda}y) \right\| > \frac{1}{4\epsilon} \left\| \nabla^{t_0} p_{i_0}(x + \sqrt{\lambda}y) \right\|.$$

Thus, it is highly probable that the mollifier function $G(x + \sqrt{\lambda}y) = 0$. So, the expectation of $F(x + \sqrt{\lambda}y)G(x + \sqrt{\lambda}y)$ is no more than 2^{-R+1} . The same argument works for Y as well.

- For the case that x is well-behaved, we will show that for all p_i , $p_i(x + \sqrt{\lambda}y)$ and $p_i(x + \sqrt{\lambda}Y)$ are nearly the same constant. This implies $F(x + \sqrt{\lambda}y)$ and $F(x + \sqrt{\lambda}Y)$ are equal in most situations. Then it suffices to show Y fools the mollifier, as discussed in the previous section.

Lemma 3.3. Fix a small constant $0 < \epsilon < 1$ and let $R \in \mathbb{N}$ be an integer. Let $p_1, \dots, p_k : \mathbb{R}^n \rightarrow \mathbb{R}$ be arbitrary polynomials of degree d and $f : \{0, 1\}^k \rightarrow \{0, 1\}$ be an arbitrary Boolean function. Define function

$$F(x) := f(\text{sign}(p_1(x)), \dots, \text{sign}(p_k(x))) .$$

Let Y be a $2dR$ -wise independent standard Gaussian vector of length n . For any $x \in \mathbb{R}^n$ and $\lambda = O(k^{-2}d^{-3}R^{-15}\epsilon^2)$

$$\left| \mathbb{E}_Y \left[F(x + \sqrt{\lambda}Y) G(x + \sqrt{\lambda}Y) \right] - \mathbb{E}_{y \sim \mathcal{N}(0,1)^n} \left[F(x + \sqrt{\lambda}y) G(x + \sqrt{\lambda}y) \right] \right| = kd2^{-\Omega(R)} ,$$

where G is defined in (1).

Proof. **TOPROVE 1** □

3.3 Proof of Theorem 3.1

Proof. **TOPROVE 2** □

4 Discretization

To give an explicit construction of a PRG, we need a discretization of R -wise independent Gaussian distributions. In this section, we show an algorithm which outputs L vectors $\{X_i\}_{1 \leq i \leq L}$ approximating Y_i , that is, $|X_{i,j} - Y_{i,j}|$ is sufficiently small. Before that, we first prove that if X and Y are close enough, then X also fools any function of low-degree polynomial threshold functions.

Lemma 4.1. Let $0 < \epsilon, \delta < 1$, and $R \in \mathbb{N}$ be an integer. Let $Y = \frac{1}{\sqrt{L}} \sum_{i=1}^L Y_i$ where Y_i is an R -wise independent Gaussian vector of length n for $1 \leq i \leq L$. Let $p_1, \dots, p_k : \mathbb{R}^n \rightarrow \mathbb{R}$ be arbitrary polynomials of degree d and $f : \{0, 1\}^k \rightarrow \{0, 1\}$ be an arbitrary Boolean function. Define functions

$$F(x) := f(\text{sign}(p_1(x)), \dots, \text{sign}(p_k(x)))$$

Suppose that for any such function F ,

$$\left| \mathbb{E}_Y [F(Y)] - \mathbb{E}_{y \sim \mathcal{N}(0,1)^n} [F(y)] \right| \leq \epsilon .$$

Suppose that $\{X_i\}_{1 \leq i \leq L}$ are random vectors of length n and there is a joint distribution over X and Y such that for each $1 \leq i \leq L, 1 \leq j \leq n, \Pr[|X_{i,j} - Y_{i,j}| \leq \delta] \geq 1 - \delta$.

Let $X = \frac{1}{\sqrt{L}} \sum_{i=1}^L X_i$ and we have that for any such function F

$$\left| \mathbb{E}_X [F(X)] - \mathbb{E}_{y \sim \mathcal{N}(0,1)^n} [F(y)] \right| \leq \epsilon + k2^{2k}d\delta^{1/d}\sqrt{nL} \log \frac{1}{\delta} + O(2^{2k}nL\delta) .$$

Proof. **TOPROVE 3** □

We now prove the main theorem for constructing an explicit pseudorandom generator. The idea is that a standard Gaussian variable can be generated using two uniform $[0, 1]$ random variables through the Box–Muller transform [BM58]. Let $Y_{i,j} = \sqrt{-2 \log u_{i,j}} \cos(2\pi v_{i,j})$ where $u_{i,j}$ and $v_{i,j}$ are uniform in $[0, 1]$. Then $Y_{i,j}$ is a Gaussian variable. Thus, if we truncate $u_{i,j}$ and $v_{i,j}$ to a certain precision and produce $X_{i,j}$ in a similar manner, X approximates Y with high probability.

Theorem 4.2. *There exists an explicit PRG which ϵ -fools any k degree- d polynomial threshold functions over $\mathcal{N}(0, 1)^n$ with seed length $O\left(\frac{k^5 d^{11}}{\epsilon^2} \log \frac{kd n}{\epsilon}\right)$.*

Proof. **TOPROVE 4**

□

References

- [Baz09] Louay M. J. Bazzi. Polylogarithmic independence can fool DNF formulas. *SIAM Journal on Computing*, 38(6):2220–2272, 2009. [3](#)
- [BM58] G. E. P. Box and Mervin E. Muller. A note on the generation of random normal deviates. *The Annals of Mathematical Statistics*, 29(2):610 – 611, 1958. [4](#), [11](#)
- [CDS20] Eshan Chattopadhyay, Anindya De, and Rocco A. Servedio. Simple and efficient pseudorandom generators from Gaussian processes. In *Proceedings of the 34th Computational Complexity Conference*, Dagstuhl, DEU, 2020. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. [2](#), [3](#)
- [CW01] Anthony Carbery and James Wright. Distributional and L^q norm inequalities for polynomials over convex bodies in \mathbb{R}^n . *Mathematical Research Letters*, 8:233–248, 2001. [6](#)
- [DGJ⁺10] Ilias Diakonikolas, Parikshit Gopalan, Ragesh Jaiswal, Rocco A. Servedio, and Emanuele Viola. Bounded independence fools halfspaces. *SIAM Journal on Computing*, 39(8):3441–3462, 2010. [2](#)
- [DKN10] Ilias Diakonikolas, Daniel M. Kane, and Jelani Nelson. Bounded independence fools degree-2 threshold functions. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 11–20, 2010. [2](#), [3](#)
- [GKM18] Parikshit Gopalan, Daniel M. Kane, and Raghu Meka. Pseudorandomness via the discrete fourier transform. *SIAM Journal on Computing*, 47(6):2451–2487, 2018. [2](#)
- [GOWZ10] Parikshit Gopalan, Ryan O’Donnell, Yi Wu, and David Zuckerman. Fooling functions of halfspaces under product distributions. In *2010 IEEE 25th Annual Conference on Computational Complexity*, pages 223–234, 2010. [2](#), [3](#)
- [HKM13] Prahladh Harsha, Adam Klivans, and Raghu Meka. An invariance principle for polytopes. *J. ACM*, 59(6), 2013. [2](#), [3](#)
- [JLS86] William B Johnson, Joram Lindenstrauss, and Gideon Schechtman. Extensions of Lipschitz maps into Banach spaces. *Israel Journal of Mathematics*, 54(2):129–138, 1986. [3](#)
- [Kan11a] Daniel M. Kane. k -independent Gaussians fool polynomial threshold functions. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 252–261, 2011. [2](#)
- [Kan11b] Daniel M. Kane. A small PRG for polynomial threshold functions of Gaussians. In *Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, page 257–266, USA, 2011. IEEE Computer Society. [2](#), [4](#), [7](#)
- [Kan12] Daniel M. Kane. A structure theorem for poorly anticoncentrated Gaussian chaoses and applications to the study of polynomial threshold functions. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 91–100, 2012. [2](#)

- [Kan14] Daniel M. Kane. A pseudorandom generator for polynomial threshold functions of Gaussian with subpolynomial seed length. In *2014 IEEE 29th Conference on Computational Complexity*, pages 217–228, 2014. [2](#)
- [Kan15] Daniel M. Kane. A Polylogarithmic PRG for Degree 2 Threshold Functions in the Gaussian Setting. In David Zuckerman, editor, *30th Conference on Computational Complexity (CCC 2015)*, volume 33 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 567–581, Dagstuhl, Germany, 2015. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. [2](#)
- [KM15] Pravesh K. Kothari and Raghu Meka. Almost optimal pseudorandom generators for spherical caps: extended abstract. In *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, page 247–256, New York, NY, USA, 2015. Association for Computing Machinery. [2](#)
- [KM22] Zander Kelley and Raghu Meka. Random restrictions and PRGs for PTFs in Gaussian space. In Shachar Lovett, editor, *37th Computational Complexity Conference (CCC 2022)*, volume 234 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 21:1–21:24, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. [2](#), [4](#), [6](#), [7](#)
- [KMN11] Daniel Kane, Raghu Meka, and Jelani Nelson. Almost optimal explicit johnson-lindenstrauss families. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 628–639, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg. [3](#)
- [KOS08] Adam R. Klivans, Ryan O’Donnell, and Rocco A. Servedio. Learning geometric concepts via Gaussian surface area. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 541–550, 2008. [3](#)
- [Lin22] J. W. Lindeberg. Eine neue herleitung des exponentialgesetzes in der wahrscheinlichkeitsrechnung. *Mathematische Zeitschrift*, 15:211–225, 1922. [3](#)
- [MZ13] Raghu Meka and David Zuckerman. Pseudorandom generators for polynomial threshold functions. *SIAM Journal on Computing*, 42(3):1275–1301, 2013. [2](#)
- [NW99] Jorge Nocedal and Stephen J. Wright, editors. *Quadratic Programming*, pages 438–486. Springer New York, New York, NY, 1999. [2](#)
- [O’D14] Ryan O’Donnell. *Analysis of boolean functions*. Cambridge University Press, 2014. [5](#), [6](#)
- [OST20] Ryan O’Donnell, Rocco A. Servedio, and Li-Yang Tan. Fooling Gaussian PTFs via local hyperconcentration. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, page 1170–1183, New York, NY, USA, 2020. Association for Computing Machinery. [2](#)
- [OST22] Ryan O’Donnell, Rocco A. Servedio, and Li-Yang Tan. Fooling polytopes. *J. ACM*, 69(2), jan 2022. [2](#), [3](#)

- [Raz09] Alexander Razborov. A simple proof of Bazzi’s theorem. *ACM Trans. Comput. Theory*, 1(1), feb 2009. [3](#)
- [Ser06] Rocco A. Servedio. Every linear threshold function has a low-weight approximator. In *21st Annual IEEE Conference on Computational Complexity (CCC’06)*, pages 18–32, 2006. [2](#)
- [ST17] R. A. Servedio and L. Tan. Fooling intersections of low-weight halfspaces. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 824–835, Los Alamitos, CA, USA, oct 2017. IEEE Computer Society. [2](#), [3](#)

A Facts about Bump Function

Fact 2.2. For all $t \in \mathbb{N}$, $|\Psi^{(t)}(x)| \leq t^{(3+o(1))t}$.

Proof. **TOPROVE 5** □

Fact 2.3. For all $t \in \mathbb{N}$, $|\rho^{(t)}(x)| \leq t^{(3+o(1))t}$.

Proof. **TOPROVE 6** □

Fact 2.4. Let $r(u, v) := \rho(\log u - \log v + c)$ for some constant c . Then we have that for all $n, m \in \mathbb{N}$,
$$\left| \frac{\partial^n \partial^m r(u, v)}{\partial u^n \partial v^m} \right| \leq \frac{(n+m)^{6(n+m)}}{|u|^n |v|^m}.$$

Proof. **TOPROVE 7** □