Electronic Colloquium on Computational Complexity, Report No. 12 (2018)

Nisan-Wigderson Pseudorandom Generators for Circuits with Polynomial Threshold Gates

Valentine Kabanets* Zhenjian Lu†

January 20, 2018

Abstract

We show how the classical Nisan-Wigderson (NW) generator [NW94] yields a nontrivial pseudorandom generator (PRG) for circuits with sublinearly many polynomial threshold function (PTF) gates. For the special case of a single PTF of degree d on n inputs, our PRG for error ϵ has the seed size

$$\exp\left(O\left(\sqrt{d \cdot \log n \cdot \log\log(n/\epsilon)}\right)\right);$$

this can give a super-polynomial stretch even for a sub-exponentially small error parameter $\epsilon = \exp(-n^{\gamma})$, for any $\gamma = o(1)$. In contrast, the best known PRGs for PTFs of [MZ13, Kan12] cannot achieve such a small error, although they do have a much shorter seed size for any constant error ϵ.

For the case of circuits with degree-d PTF gates on n inputs, our PRG can fool circuits with at most $n^{\alpha/d}$ gates with error $\exp(-n^{\alpha/d})$ and seed length $n^{O(\sqrt{\alpha})}$, for any $\alpha > 1$.

While a similar NW PRG construction was observed by Lovett and Srinivasan [LS11] to work for the case of constant-depth (AC^0) circuits with few PTF gates, the application of the NW generator to the case of general (unbounded depth) circuits consisting of a sublinear number of PTF gates does not seem to have been explicitly stated before. We do so in this note.

*School of Computing Science, Simon Fraser University, Burnaby, BC, Canada; kabanets@sfu.ca
†School of Computing Science, Simon Fraser University, Burnaby, BC, Canada; zla54@sfu.ca

ISSN 1433-8092

1 Introduction

Constructing pseudorandom generators (PRGs) for various computationally bounded classes of boolean functions is an important task in complexity theory. A PRG for a class $\mathcal{C}$ of boolean functions f is an efficiently deterministically computable function G mapping short binary strings (seeds) to longer binary strings so that every $f \in \mathcal{C}$ accepts G's output on a uniformly random seed with about the same probability as an actual uniformly random string. More precisely, we say that a generator $G\colon \{0,1\}^r \to \{0,1\}^n$ is ϵ-fooling for a class $\mathcal{C}$ of boolean functions $f\colon \{0,1\}^n \to \{0,1\}$ if

$$|\mathbf{Pr}[f(G(x)) = 1] - \mathbf{Pr}[f(y) = 1]| \leq \epsilon,$$

for uniformly random $x \in \{0,1\}^r$ and $y \in \{0,1\}^n$.

The holy grail in derandomization is to construct an explicit PRG fooling the class of all boolean functions computable by polynomial-size circuits (a PRG for the class $\mathsf{P/poly}$). Currently, only conditional constructions of such PRGs are known, assuming that boolean functions of superpolynomial circuit complexity are computable in deterministic exponential time [NW94, BFNW93, IW97, STV01, Uma03]; moreover, constructing such PRGs is known to be equivalent to proving circuit lower bounds for boolean functions computable in exponential time (see, e.g., [ISW99]).

Unconditional constructions of PRGs (of varying strength) are known for certain sub-classes of $\mathsf{P/poly}$, e.g., for

- constant-depth circuits of polynomially many AND, OR, and NOT gates of unbounded fan-in (AC^0) [AW85, Nis91, Bra10, TX13, Tal14, HS16],
- read-once oblivious branching programs [AKS87, BNS92, Nis92, NZ96, INW94],
- small de Morgan formulas [IMZ12],
- polynomials over the binary finite field $\mathbb{F}_2$ [NN93, LVW93, BV10, Lov09, Vio09],
- polynomial threshold functions (PTFs) [MZ13, Kan12].

The focus of the present paper is on circuits whose gates are polynomial threshold functions. Recall that an n-variate polynomial threshold function of degree d is defined as the sign[1] $\operatorname{sgn}(p)$ of a degree d polynomial $p\colon \{0,1\}^n \to \mathbb{R}$. Our main result is a construction of the PRG for the class of circuits with few PTF gates.

Theorem 1.1. *For any $\alpha > 1$, there exists a PRG $G\colon \{0,1\}^r \to \{0,1\}^n$, computable in deterministic time $\mathsf{poly}(n)$, that $\exp(-n^{\alpha/d})$-fools n-input circuits with at most $n^{\alpha/d}$ degree-d PTF gates, with the seed length*

$$r = n^{O(\sqrt{\alpha})}.$$

For the special case of a single PTF gate, we get the following PRG.

Theorem 1.2 (PRG for PTFs)**.** *There exists a PRG $G\colon \{0,1\}^r \to \{0,1\}^n$, computable in deterministic time $\mathsf{poly}(n)$, that ϵ-fools degree-d PTFs on n variables with the seed length*

$$r = \exp\left(O\left(\sqrt{d \cdot \log n \cdot \log\log(n/\epsilon)}\right)\right).$$

[1] Here we define the sign function $\operatorname{sgn}(\rho)$ to be 1 on $\rho > 0$, and 0 on $\rho < 0$.

1.1 Our construction

Our PRG is based on the celebrated Nisan-Wigderson "hardness-based" generator (NW PRG) [NW94]. To fool a class $\mathcal{C}$ of boolean functions f, the NW PRG construction requires a "hard function" h that cannot be computed correctly on significantly more than a half of all possible inputs by any boolean function g in a related class $\tilde{\mathcal{C}}$ of "slightly more powerful" functions than those in $\mathcal{C}$. Thus, sufficiently strong average-case lower bounds against the class $\tilde{\mathcal{C}}$ can be used to build a PRG fooling the class $\mathcal{C}$.

In our case, the class $\mathcal{C}$ contains all those n-variate boolean functions that are computable by constant depth D circuits with at most $s \ll n$ PTF gates of degree d. Our main observation is that the corresponding class $\tilde{\mathcal{C}}$ (for which we require average-case lower bounds) is the class of boolean functions computable by constant depth D circuits with at most s PTF gates of degree $d' = d \cdot a$, for some parameter $a \geq 1$ that we can control (and which will determine the seed size of our PRG). That is, the class $\tilde{\mathcal{C}}$ is the same as $\mathcal{C}$, except for a somewhat higher degree d' of the allowed PTF gates.

To illustrate the idea of our analysis of the NW PRG for PTF circuits, we consider the special case of a single n-variate PTF f of degree d. That is, $f = \mathrm{sgn}(p(x_1, \ldots, x_n))$ for some degree-d multilinear polynomial $p\colon \{0,1\}^n \to \mathbb{R}$. Suppose that the NW generator based on some "hard" boolean function h failed to ϵ-fool this PTF f.

First, the standard NW analysis shows that the function $h(z)$ can be computed, with probability at least $1/2 + \epsilon/n$, by (possibly the negation of) the function

$$g(z) = f(h_1(z), h_2(z), \ldots, h_i(z), b_{i+1}, \ldots, b_n), \tag{1}$$

for some $1 \leq i \leq n$, fixed bits $b_{i+1}, \ldots, b_n$, and boolean functions $h_1, \ldots, h_i$, where each $h_j(z)$ depends on at most some a bits in z, for a parameter $a \geq 1$ coming from the NW construction (the maximum overlap between pairs of sets in the NW design; see the next section for details).

It is well known that every boolean function on a inputs can be written as a multilinear polynomial of degree a over the reals. Plugging in these polynomials for the function h_j's in Equation (1), we get that $g(z)$ is a PTF of degree at most $d' = d \cdot a$.

Hence, to ensure that this NW generator based on h is indeed ϵ-fooling for degree d PTFs, we just need h to be such that no PTF of degree $d \cdot a$ can compute $h(z)$ on more than $1/2 + \epsilon/n$ of inputs z. Such hard functions h turn out to be easy to construct and analyze.

For example, we show that the generalized multiplexer function $A(x, i)$ outputting the ith bit of the encoding of x with an appropriate binary (list-decodable) error-correcting code is such a hard function for PTFs. A slightly more complicated function (generalized Andreev function) $A'(x, i)$, outputting the jth bit of the codeword encoding x for j obtained from i using a certain (seedless) extractor, is a hard function for constant-depth PTF circuits with a sublinear number of PTF gates.

The parameters of our PRG $G\colon \{0,1\}^r \to \{0,1\}^n$ (its error ϵ and seed length r) depend on the strength of the average-case lower bound for the hard function h. To get a short seed r, one needs to maximize the aforementioned parameter a, ideally setting $a = \log n$ (as is the case for a standard application of the NW construction). However, we also need to prove (average-case) lower bounds against PTFs of degree $d \cdot a$, where virtually nothing is known for the degree $\log n$. Thus we are forced to set $a \ll \log n$, which limits the stretch of our PRG to be at most only superpolynomial. On the other hand, for such small a, our hard function h has exponentially small correlation with degree (da) PTFs, thereby allowing our PRG to have an exponentially small error ϵ.

1.2 Comparison with the related work

Among the known PRG constructions for various circuit models mentioned earlier, some are NW-style "hardness-based" generators, while others are *ad hoc* constructions (often using such standard pseudorandomness tools as hashing, limited-wise independence, expander graphs, etc.) The previous PRGs for PTFs due to [MZ13, Kan12] are of the latter kind. The construction uses hashing and limited-wise independence. The analysis is quite involved, and depends on a number of analytic tools for polynomials (concentration and anti-concentration results, the invariance principle, hypercontractivity, regularization, etc.).

In contrast, our PRG for PTFs (of Theorem 1.2) is the NW-style construction, whose analysis is simple, assuming an average-case lower bound for an appropriate class of functions. It turns out that for PTFs, it is very easy to prove a required correlation bound (and we give a full proof below). Using the similar method, we can also obtain a correlation bound for PTF circuits with few gates.

For constant degree d PTFs and constant error ϵ, the PRG of [MZ13, Kan12] has exponential stretch (mapping a seed of length $O(\log n)$ to an n-bit string fooling n-input PTFs). Our PRG cannot achieve such exponentially long stretch. However, it can achieve even exponentially small error ϵ with a non-trivial (sublinear) seed size, which is impossible for the PRGs of [MZ13, Kan12].

In their work studying correlation bounds for AC^0 circuits with few symmetric gates [LS11], Lovett and Srinivasan obtained an average-case hard function for constant depth poly-size AC^0 circuits with few LTF gates and used it to construct a PRG fooling such circuits with polynomial stretch and exponentially small error, also based on the generic construction of Nisan and Wigderson. Since a PTF can be viewed as a depth-2 circuit computing an LTF of ANDs, such a PRG also fools small PTF circuits. While the PRG in [LS11] can fool a more general model, which is constant depth AC^0 circuits augmented with LTF gates, our work here focuses on circuits with only PTF gates and our PRG can fool PTF circuits regardless of the depth as long as the number of gates is small.

Remainder of the paper. We prove our Theorem 1.2 in Section 2, and Theorem 1.1 in Section 3. We give some concluding remarks in Section 4.

2 PRG for PTFs

We first give a PRG construction for a single polynomial threshold function. We start with the definition of a generalized multiplexer function, which we will show to be average-case hard for low-degree PTFs. Then we use this hard function in the NW PRG construction.[2]

2.1 Hard function for PTFs

Recall that a (ζ, L)-list-decodable binary code is a function $\mathrm{Enc}\colon \{0,1\}^k \to \{0,1\}^n$ that maps k-bit messages to n-bit codewords so that, for each codeword $y \in \{0,1\}^n$, there are at most L codewords in the range of Enc that have relative hamming distance at most ζ from y. We will use the following list-decodable code (see, e.g., [CKK+15] for its construction).

[2]The parity function is also known to be average-case for PTFs; however, the correlation bound between the n-bit parity and degree d PTFs is only $O(d/\sqrt{n})$, and this is tight [ABFR94]. For our purposes, we require hard functions for PTFs with the correlation $1/n^{\omega(1)}$.

Theorem 2.1 ([CKK+15]). *For any given $0 < \gamma < 1$, there exists a binary code* Enc *mapping $3n$-bit message to a codeword of length 2^{n^γ}, such that* Enc *is (ζ, L)-list-decodable for $\zeta = 1/2 - O\left(2^{-n^\gamma/4}\right)$ and $L \leq O\left(2^{n^\gamma/2}\right)$. Furthermore, there is a polynomial-time algorithm for computing* $\mathrm{Enc}(x)$ *in position i, for any inputs $x \in \{0,1\}^{3n}$ and $i \in [2^{n^\gamma}]$.*

Recall that a multiplexer is a function that on inputs x and $i \in [|x|]$ outputs the ith bit x_i of x. Our generalized multiplexer will output the ith bit of the encoding of the input string x with the error-correcting code of Theorem 2.1.

Definition 2.2 (Generalized Multiplexer). *Let $0 < \gamma < 0$. Define $A_{n,\gamma} \colon \{0,1\}^{3n+n^\gamma} \to \{0,1\}$ as follows:*

$$A_{n,\gamma}(x_1, \ldots, x_{3n}, y_1, \ldots, y_{n^\gamma}) = \mathrm{Enc}(x_1, \ldots, x_{3n})_{\mathrm{index}(y_1,\ldots,y_{n^\gamma})},$$

where Enc *is the code from Theorem 2.1 that maps $3n$ bits to 2^{n^γ} bits, and* $\mathrm{index}(y_1, \ldots, y_{n^\gamma})$ *gives an integer in $[2^{n^\gamma}]$ whose binary representation is $y_1, \ldots, y_{n^\gamma}$.*

Note that the function A defined above is polynomial-time computable since we can compute $\mathrm{Enc}(x)$ in position i in polynomial time. We will show that this function A is average-case for low-degree PTFs. We will need the following fact about PTFs that easily follows from the generalization of Chow's theorem [Cho61] from LTFs to PTFs, which says that a degree-d PTF on n variables is completely determined by its Fourier coefficients of degree at most d.

Theorem 2.3 ([Cho61]). *The number of distinct degree-d n-variate PTFs is at most $2^{n^{d+1}+O(n)}$.*

Corollary 2.4. *The number of distinct n-variate circuits with at most s degree-d PTF gates is at most*

$$O\left((n+s)^{d+2}\right)$$

Proof. To specify a gate g in such a circuit, we first need at most $(n+s)$ bits to specify the variables and gates which g reads from. Then by Theorem 2.3 we need at most $(n+s)^{d+1} + O(n+s)$ bits to describe g. Therefore, we need at most $O\left((n+s)^{d+1}\right)$ bits to specify one gate in the circuit, and we have s such gates. □

We also need the following simple fact saying that most n-bit strings are incompressible. Let $K(\cdot)$ denote the Kolmogorov complexity of a binary string.

Claim 2.5. *For any $0 < \alpha < 1$, $\mathbf{Pr}_{x \sim \{0,1\}^n}[K(x) < \alpha n] \leq 2^{-(1-\alpha)n}$.*

We are now ready to show that the generalized multiplexer function A from Definition 2.2 is very hard on average for degree d PTFs.

Lemma 2.6 (Hard function for PTFs). *For any $d \geq 1$, let $\gamma = 1/(d+1)$. Then, for any degree-d PTF $f \colon \{0,1\}^{3n+n^\gamma} \to \{0,1\}$, we have that*

$$\mathbf{Pr}_{x \sim \{0,1\}^{3n+n^\gamma}}[f(x) = A_{n,\gamma}(x)] \leq \frac{1}{2} + \exp\left(-\Omega(n^\gamma)\right).$$

Proof. We have

$$\begin{aligned}
&\mathbf{Pr}_{\substack{y\sim\{0,1\}^{3n}\\ z\sim\{0,1\}^{n^\gamma}}}[f(y,z) = A_{n,\gamma}(y,z)] \\
&= \mathbf{Pr}_{y,z}[f(y,z) = A_{n,\gamma}(y,z) \mid K(y) \geq 2n] \cdot \mathbf{Pr}_y[K(y) \geq 2n] \\
&\quad + \mathbf{Pr}_{y,z}[f(y,z) = A_{n,\gamma}(y,z) \mid K(y) < 2n] \cdot \mathbf{Pr}_y[K(y) < 2n] \\
&\leq \mathbf{Pr}_{y,z}[f(y,z) = A_{n,\gamma}(y,z) \mid K(y) \geq 2n] + 2^{-n/3}. \qquad \text{(Claim 2.5)}
\end{aligned}$$

Consider any fixed string a with $K(a) \geq 2n$. Towards a contradiction, suppose that the restricted function $A'(z) = A_{n,\gamma}(a,z)$ is computed by the restricted PTF $f'(z) = f(a,z)$ with probability at least $1/2 + \nu$, for some $\nu = \exp(n^\gamma)$. Then the truth table of f' agrees with the codeword $\mathrm{Enc}(a)$ in at least $1/2+\nu$ fraction of positions. By the list-decodability of Enc (Theorem 2.1), there are at most $L \leq \exp(n^\gamma)$ codewords that have such agreement with the truth table of f'. Thus, we can uniquely specify the codeword $\mathrm{Enc}(a)$, and hence also a, by the description of f' plus at most $\log L < o(n)$ bits to specify a particular element on the list. By Theorem 2.3, the degree d PTF f' on n^γ variables can be described using $n^{\gamma(d+1)} + O(n^\gamma) < (1.1) \cdot n$ bits. We conclude that the string a can be described using fewer than $2n$ bits, contradicting the fact that $K(a) \geq 2n$. □

2.2 NW PRG for PTFs

Next we apply the Nisan-Wigderson construction to the hard function A of Lemma 2.6. We will use the following (standard) combinatorial designs.

Claim 2.7 (NW Designs [NW94])**.** *For any integers $a, n > 0$, there exists an efficiently computable family of sets $S_1, \ldots, S_n$ such that*

1. *$S_i \subset [r]$, $\forall i \in [n]$, where $r = n^{2/(a+1)}$,*
2. *$|S_i| = \ell = n^{1/(a+1)}$, $\forall i \in [n]$, and*
3. *$|S_i \cap S_j| \leq a$, $\forall i, j \in [n]$ such that $i \neq j$.*

Proof. We view the set $[r]$ as the set of pairs $\mathbb{F}(\ell) \times \mathbb{F}(\ell)$, for a finite field $\mathbb{F}_\ell$ of size ℓ. Let $e_1, \ldots, e_\ell$ be the elements in $\mathbb{F}(\ell)$, and $p_1, \ldots, p_n$ all univariate degree-a polynomials over $\mathbb{F}(\ell)$. For each $i \in [n]$, define $S_i = \{(e_1, p_i(a_1)), \ldots, (e_\ell, p_i(e_\ell))\}$. The third condition follows from the fact that a non-zero univariate polynomial of degree a has at most a roots. □

We will prove the following result that implies Theorem 1.2 (once we express a in terms of the stated error ϵ).

Theorem 2.8. *There exists a constant $B > 0$ such that for any integers $a, d > 0$, there exists a polynomial-time computable PRG $G\colon \{0,1\}^r \to \{0,1\}^n$ ϵ-fooling n-variate degree d PTFs, with the seed length $r = n^{2/(a+1)}$ and the error*

$$\epsilon \leq n \cdot \exp\left(-\frac{1}{B} \cdot n^{\frac{1}{(ad+1)(a+1)}}\right).$$

Proof. Let $C = \mathrm{sgn}(p)$ be an arbitrary degree-d PTF on n variables. For $\ell = n^{1/(a+1)}$, let $A\colon \{0,1\}^\ell \to \{0,1\}$ be the generalized multiplexer function from Definition 2.2, with $\gamma = 1/(ad+1)$. By Lemma 2.6, we have, for any degree-(ad) PTF g, that

$$\mathbf{Pr}_{z\sim\{0,1\}^\ell}[g(z) = A(z)] \le \frac{1}{2} + \exp\left(-\Omega\left(n^{\frac{1}{(ad+1)(a+1)}}\right)\right). \tag{2}$$

Let $S_1, \ldots, S_n$ be the sets from Claim 2.7. Define the generator $G_{a,d}\colon \{0,1\}^r \to \{0,1\}^n$ as follows:

$$G_{a,d}(y) = A(y|_{S_1}), \ldots, A(y|_{S_n}),$$

where, for $i \in [n]$, $y|_{S_i}$ denotes the substring of y indexed by the set S_i.

Toward a contradiction, suppose

$$|\mathbf{Pr}_{x\sim\{0,1\}^n}[C(x) = 1] - \mathbf{Pr}_{y\sim\{0,1\}^r}[C(G_{a,d}(y)) = 1]| > \epsilon. \tag{3}$$

By a standard argument via "reduction from distinguishing to predicting" as in [NW94], Equation (3) implies that there exist an $i \in [n]$, and bits $b_{i+1}, \ldots, b_n \in \{0,1\}$, such that

$$\mathbf{Pr}_{z\sim\{0,1\}^\ell}[C'(h_1(z), \ldots, h_i(z), b_{i+1}, \ldots, b_n) = A(z)] > 1/2 + \epsilon/n, \tag{4}$$

where

1. $C' = C$ or $C' = \neg C$, and
2. $h_1, \ldots, h_i$ are boolean functions such that each depends on at most a bits of its input z.

First, note that C' is always a PTF of degree at most d, since for $C = \mathrm{sgn}(p)$, we have $\neg C = \mathrm{sgn}(-p)$. Let $C' = \mathrm{sgn}(p')$ for a degree d multilinear polynomial p' (where $p' = p$ or $p' = -p$).

Next, observe that every boolean function that depends on at most a variables can be computed by a multilinear polynomial of degree at most a over the reals. Replacing our functions $h_1, \ldots, h_i$ with such degree a polynomials $p_1, \ldots, p_i$ inside C', we get

$$C'(p_1(z), \ldots, p_i(z), b_{i+1}, \ldots, b_n) = \mathrm{sgn}(p'(p_1(z), \ldots, p_i(z), b_{i+1}, \ldots, b_n)),$$

which is a new PTF C'' on ℓ variables of degree at most $d \cdot a$. By Equation (4), this PTF C'' computes the function $A(z)$ with probability greater than $1/2 + \epsilon/n$. Applying Equation (2) yields the required bound on ϵ. □

3 PRG for PTF circuits

In this section, we describe our PRGs for circuits with few low-degree PTF gates. We prove the following result that implies Theorem 1.1.

Theorem 3.1. *There exist constants $B, E > 0$ such that for any integers $a, d > 0$ and any circuit C on n variables with at most $s = n^{\frac{1}{(ad+2)(a+1)}}/B$ degree-d PTF gates, there exists a polynomial-time computable PRG $G\colon \{0,1\}^r \to \{0,1\}^n$ ϵ-fooling C, with the seed length $r = n^{2/(a+1)}$ and the error*

$$\epsilon \le n \cdot \exp\left(-\frac{1}{E} \cdot n^{\frac{1}{(ad+2)(a+1)}}\right).$$

Our PRG will be an NW PRG with the following hard function.

Lemma 3.2 (Hard function for PTF Circuits)**.** *There exists a constant $B > 0$ such that the following holds. For any $d \geq 1$, let γ be such that $n^\gamma = \frac{1}{B} \cdot n^{1/(d+2)}$. Then for any circuit C on n inputs with at most $s = n^\gamma$ degree-d PTF gates, we have that*

$$\mathbf{Pr}_{x \sim \{0,1\}^{2n+n^\gamma}}[f(x) = A_{n,\gamma}(x)] \leq \frac{1}{2} + \exp\left(-\Omega(n^\gamma)\right).$$

Proof. We have

$$\begin{aligned}
&\mathbf{Pr}_{\substack{y \sim \{0,1\}^{2n} \\ z \sim \{0,1\}^{n^\gamma}}}[C(y,z) = A_{n,\gamma}(y,z)] \\
&= \mathbf{Pr}_{y,z}[C(y,z) = A_{n,\gamma}(y,z) \mid K(y) \geq n] \cdot \mathbf{Pr}_y[K(y) \geq n] \\
&\quad + \mathbf{Pr}_{y,z}[C(y,z) = A_{n,\gamma}(y,z) \mid K(y) < n] \cdot \mathbf{Pr}_y[K(y) < n] \\
&\leq \mathbf{Pr}_{y,z}[C(y,z) = A_{n,\gamma}(y,z) \mid K(y) \geq 2n] + 2^{-n/2}. \qquad \text{(Claim 2.5)}
\end{aligned}$$

Consider any fixed string a with $K(a) \geq n$. Towards a contradiction, suppose that the restricted function $A'(z) = A_{n,\gamma}(a,z)$ is computed by the restricted PTF circuit $C'(z) = f(a,z)$ with probability at least $1/2 + \nu$, for some $\nu = \exp(n^\gamma)$. Then the truth table of C' agrees with the codeword $\mathrm{Enc}(a)$ in at least $1/2 + \nu$ fraction of positions. By the list-decodability of Enc (Theorem 2.1), there are at most $L \leq \exp(n^\gamma)$ codewords that have such agreement with the truth table of C'. Thus, we can uniquely specify the codeword $\mathrm{Enc}(a)$, and hence also a, by the description of f' plus at most $\log L < o(n)$ bits to specify a particular element on the list. By Corollary 2.4, the circuit C' on n^γ variables with at most $s = n^\gamma$ gates can be described using $O\left((2n^\gamma)^{d+2}\right) < 0.5n$ bits, when B is a sufficiently large constant. We conclude that the string a can be described using fewer than n bits, contradicting the fact that $K(a) \geq n$. □

Proof of Theorem 3.1. We use the function in Lemma 3.2 as the hard function in the Nisan-Wigderson construction, to obtain a PRG that ϵ-fools the circuits described in Theorem 3.1. The analysis is similar to that in the single PTF case in the previous section, except that in the step of "reducing from distinguishing to predicting", instead of merging the h_i's, which are polynomials of degree a over reals, into a single PTF, here we merge them into every PTF gate in the circuit that reads from them. This yields a new circuit with *exactly the same* number of gates, and of degree at most (ad), that computes the hard function with probability at least $1/2 + \epsilon/n$, which leads to the required upper bound on ϵ. □

4 Concluding remarks

We showed that the NW construction can be applied to the case of PTF circuits, yielding PRGs with nontrivial parameters. For the case of a single PTF gate, our PRG can ϵ-fool PTFs even for a sub-exponentially small error ϵ, with super-polynomial seed stretch.

An obvious open question is to get PRGs for PTFs and for PTF circuits with better relationship between the error ϵ and the seed size. In particular, since our PRG for PTFs turns out to be so simple to analyze, perhaps it is possible to get better parameters by combining the ideas of our construction with those from the previous constructions of [MZ13, Kan12].

Acknowledgements. This work was done while the authors were visiting Simons Institute for the Theory of Computing at UC Berkeley for the special program on pseudorandomness in the spring of 2017. We thank Daniel Kane and Sankeerth Rao for encouraging us to write this note.

References

[ABFR94] James Aspnes, Richard Beigel, Merrick L. Furst, and Steven Rudich. The expressive power of voting polynomials. *Combinatorica*, 14(2):135–148, 1994. 3

[AKS87] Miklós Ajtai, János Komlós, and Endre Szemerédi. Deterministic simulation in LOGSPACE. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 132–140. ACM, 1987. 1

[AW85] Miklós Ajtai and Avi Wigderson. Deterministic simulation of probabilistic constant depth circuits (preliminary version). In *26th Annual Symposium on Foundations of Computer Science, Portland, Oregon, USA, 21-23 October 1985*, pages 11–19. IEEE Computer Society, 1985. 1

[BFNW93] László Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Computational Complexity*, 3:307–318, 1993. 1

[BNS92] László Babai, Noam Nisan, and Mario Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. Comput. Syst. Sci.*, 45(2):204–232, 1992. 1

[Bra10] Mark Braverman. Polylogarithmic independence fools AC^0 circuits. *J. ACM*, 57(5):28:1–28:10, 2010. 1

[BV10] Andrej Bogdanov and Emanuele Viola. Pseudorandom bits for polynomials. *SIAM J. Comput.*, 39(6):2464–2486, 2010. 1

[Cho61] Chao-Kong Chow. On the characterization of threshold functions. In *Proceedings of the 2nd Annual Symposium on Switching Circuit Theory and Logical Design (FOCS)*, pages 34–38, 1961. 4

[CKK+15] Ruiwen Chen, Valentine Kabanets, Antonina Kolokolova, Ronen Shaltiel, and David Zuckerman. Mining circuit lower bound proofs for meta-algorithms. *Computational Complexity*, 24(2):333–392, 2015. 3, 4

[HS16] Prahladh Harsha and Srikanth Srinivasan. On polynomial approximations to AC^0. In Klaus Jansen, Claire Mathieu, José D. P. Rolim, and Chris Umans, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2016, September 7-9, 2016, Paris, France*, volume 60 of *LIPIcs*, pages 32:1–32:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. 1

[IMZ12] Russell Impagliazzo, Raghu Meka, and David Zuckerman. Pseudorandomness from shrinkage. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 111–119, 2012. 1

[INW94] Russell Impagliazzo, Noam Nisan, and Avi Wigderson. Pseudorandomness for network algorithms. In Frank Thomson Leighton and Michael T. Goodrich, editors, *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, 23-25 May 1994, Montréal, Québec, Canada*, pages 356–364. ACM, 1994. 1

[ISW99] Russell Impagliazzo, Ronen Shaltiel, and Avi Wigderson. Near-optimal conversion of hardness into pseudo-randomness. In *40th Annual Symposium on Foundations of Computer Science, FOCS '99, 17-18 October, 1999, New York, NY, USA*, pages 181–190. IEEE Computer Society, 1999. 1

[IW97] Russell Impagliazzo and Avi Wigderson. $P = BPP$ if E requires exponential circuits: Derandomizing the XOR lemma. In Frank Thomson Leighton and Peter W. Shor, editors, *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El Paso, Texas, USA, May 4-6, 1997*, pages 220–229. ACM, 1997. 1

[Kan12] Daniel M. Kane. A structure theorem for poorly anticoncentrated gaussian chaoses and applications to the study of polynomial threshold functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 91–100, 2012. i, 1, 3, 7

[Lov09] Shachar Lovett. Unconditional pseudorandom generators for low degree polynomials. *Theory of Computing*, 5(1):69–82, 2009. 1

[LS11] Shachar Lovett and Srikanth Srinivasan. Correlation bounds for poly-size AC^0 circuits with $n^{1-o(1)}$ symmetric gates. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 14th International Workshop, APPROX 2011, and 15th International Workshop, RANDOM 2011, Princeton, NJ, USA, August 17-19, 2011. Proceedings*, pages 640–651, 2011. i, 3

[LVW93] Michael Luby, Boban Velickovic, and Avi Wigderson. Deterministic approximate counting of depth-2 circuits. In *Second Israel Symposium on Theory of Computing Systems, ISTCS 1993, Natanya, Israel, June 7-9, 1993, Proceedings*, pages 18–24. IEEE Computer Society, 1993. 1

[MZ13] Raghu Meka and David Zuckerman. Pseudorandom generators for polynomial threshold functions. *SIAM J. Comput.*, 42(3):1275–1301, 2013. i, 1, 3, 7

[Nis91] Noam Nisan. Pseudorandom bits for constant depth circuits. *Combinatorica*, 11(1):63–70, 1991. 1

[Nis92] Noam Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992. 1

[NN93] Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM J. Comput.*, 22(4):838–856, 1993. 1

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *J. Comput. Syst. Sci.*, 49(2):149–167, 1994. i, 1, 2, 5, 6

[NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *J. Comput. Syst. Sci.*, 52(1):43–52, 1996. 1

[STV01] Madhu Sudan, Luca Trevisan, and Salil P. Vadhan. Pseudorandom generators without the XOR lemma. *J. Comput. Syst. Sci.*, 62(2):236–266, 2001. 1

[Tal14] Avishay Tal. Tight bounds on the Fourier spectrum of AC^0. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:174, 2014. 1

[TX13] Luca Trevisan and Tongke Xue. A derandomized switching lemma and an improved derandomization of AC^0. In *Proceedings of the 28th Conference on Computational Complexity, CCC 2013, Palo Alto, California, USA, 5-7 June, 2013*, pages 242–247. IEEE Computer Society, 2013. 1

[Uma03] Christopher Umans. Pseudo-random generators for all hardnesses. *J. Comput. Syst. Sci.*, 67(2):419–440, 2003. 1

[Vio09] Emanuele Viola. The sum of D small-bias generators fools polynomials of degree D. *Computational Complexity*, 18(2):209–217, 2009. 1

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il