A Pseudorandom Generator for Functions of Low-Degree PTFs

Penghui Yao[1, 2] **Mingnan Zhao**[1]

[1] *State Key Laboratory for Novel Software Technology, New Cornerstone Science Laboratory, Nanjing University*

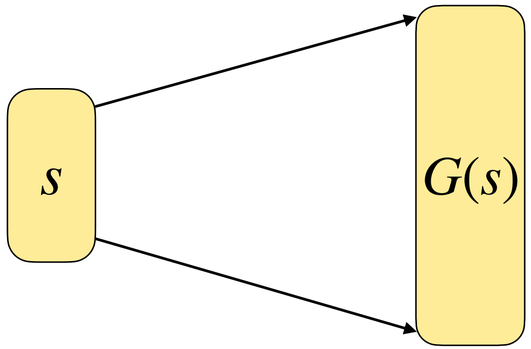
[2] *Hefei National Laboratory*

July 8, 2025 @ ICALP 2025, Aarhus, Denmark

Pseudorandom Generator

$G : \{0,1\}^r \to \mathbb{R}^n$

$\mathscr{F} \subseteq \{f : \mathbb{R}^n \to \mathbb{R}\}$: a family of functions



short seed **long** output

looks random to any *statistical test* in $\mathscr{F}$

Pseudorandom Generator

$G : \{0,1\}^r \to \mathbb{R}^n$ $\mathcal{F} \subseteq \{f : \mathbb{R}^n \to \mathbb{R}\}$: a family of functions

A function G is a ***pseudorandom generator*** (PRG) for $\mathcal{F}$ with error ε over distribution $\mathcal{D}$ if for any $f \in \mathcal{F}$,

$$\left| \mathop{\mathbb{E}}_{s \sim \{0,1\}^r} \left[f(G(s)) \right] - \mathop{\mathbb{E}}_{x \sim \mathcal{D}} \left[f(x) \right] \right| \leq \varepsilon$$

"G ε-fools $\mathcal{F}$ over $\mathcal{D}$" **r : seed length of G**

Applications: complexity theory, learning theory, derandomization…

E.g. a PRG with $\log(n)$ seed length for $\mathcal{F} = \{\text{all poly}(n)\text{-sized Boolean circuit}\}$ over uniform distribution $\mathcal{D}$

"Randomness doesn't add power to polynomial-time computation."

Linear Threshold Functions

LTFs (Halfspaces): $h(x) = \mathrm{sign}(a_0 + a_1 x_1 + \cdots + a_n x_n)$ for some $a_0, a_1, \ldots, a_n \in \mathbb{R}$

E.g. AND, OR, majority, dictators

Boolean space ($\mathscr{D}$ = uniform distribution over $\{0,1\}^n$)

- $r = O(\log n \cdot \log^2(1/\varepsilon)/\varepsilon^2)$ [DGJ+10]
  - by showing that *bounded independence fools halfspaces*
- $r = O(\log n + \log^2(1/\varepsilon))$ [MZ13]
  - using *invariance principles* to get PRG
  - introducing *monotone ROBP*
- $r = O(\log(n/\varepsilon) \cdot (\log\log(n/\varepsilon))^2)$ [GKM18]
  - a PRG that fools the *discrete Fourier transforms of linear functions*

Gaussian space ($\mathscr{D} = \mathscr{N}(0,1)^n$ over $\mathbb{R}^n$)

- $r = O(\log n + \log(1/\varepsilon) \cdot \log\log(1/\varepsilon))$ [KM15]

Extensions of LTFs I: Functions of LTFs

Functions of LTFs: $F(x) = f(h_1(x), h_2(x), \ldots, h_k(x))$ where each $h_i(x)$ is an LTF

E.g. intersection of halfspaces (polytopes)

Ref.	Function family $\mathscr{F}$	Target distribution $\mathscr{D}$	Seed length
[GOWZ13]	***arbitrary*** functions of k LTFs	product distributions	$\mathrm{poly}(k, 1/\varepsilon) \cdot \log n$
[CDS20]	***arbitrary*** functions of k LTFs	Gaussian	$\mathrm{poly}(k, 1/\varepsilon) + \log n$
[HKM13]	***intersections*** of k ***δ-regular*** LTFs	Boolean	$\mathrm{poly}(\log k, 1/\varepsilon) \cdot \log n$ for some δ
[ST17]	***intersections*** of k ***weight-t*** LTFs	Boolean	$\mathrm{poly}(\log k, 1/\varepsilon, \log n, t)$
[CDS20]	***intersections*** of k LTFs	Gaussian	$\mathrm{poly}(\log k, 1/\varepsilon) + \log n$
[OST22]	***intersections*** of k LTFs	Boolean	$\mathrm{poly}(\log k, 1/\varepsilon) \cdot \log n$

Extensions of LTFs II: Polynomial Threshold Functions

degree-d PTFs: $h(x) = \mathrm{sign}(p(x))$ where $p(x)$ is a degree-d polynomial

E.g. A halfspace is a degree-1 PTF.

Ref.	Target distribution $\mathscr{D}$	Seed length
[DKN10]	Boolean	$\tilde{O}(\varepsilon^{-9}) \cdot \log n$ for $d = 2$
[MZ13]	Boolean	$(d/\varepsilon)^{O(d)} \cdot \log n$
[Kan11a]	Gaussian	$O_d(\varepsilon^{-2^{O(d)}}) \cdot \log n$
[Kan11b]	Gaussian	$2^{O(d)} \cdot \mathrm{poly}(1/\varepsilon) \cdot \log n$
[Kan12, Kan14]	Gaussian	$A(d,1/c) \cdot (1/\varepsilon)^c \cdot \log n$ for any $c > 0$
[OST20, OSTK21]	Gaussian	$(d/\varepsilon)^{O(\log d)} \cdot \log n \longrightarrow \mathrm{poly}(d/\varepsilon) \cdot \log n$
[KM22]	Gaussian	$\mathrm{poly}(d/\varepsilon) \cdot \log n$

Our Results: Functions of PTFs

Functions of PTFs:

$$F(x) = f(\mathrm{sign}(p_1(x)), \mathrm{sign}(p_2(x)), \ldots, \mathrm{sign}(p_k(x)))$$

where each $p_i(x)$ is a degree-d polynomial.

E.g. polynomial programing

Theorem.

There exists an explicit PRG ε-fools ***arbitrary functions*** of k degree-d PTFs over ***Gaussian space*** with seed length $\mathrm{poly}(k, d, 1/\varepsilon) \cdot \log n$.

Ref.	Function family $\mathscr{F}$	Seed length
[OSTK21, KM22]	degree-d PTFs	$\mathrm{poly}(d/\varepsilon) \cdot \log n$
[CDS20]	***arbitrary*** functions of k LTFs	$\mathrm{poly}(k, 1/\varepsilon) + \log n$
[GKM18]	***intersections*** of k ***degree-***2 PTFs	$\mathrm{poly}(k, 1/\varepsilon) \cdot \log n$

probabilistic method: $k + d \log n + \log 1/\varepsilon$

The PRG Framework

$$Y = \frac{1}{\sqrt{L}} \sum_{i=1}^{L} Y_i$$

where each Y_i is ***R-wise independent*** n-dimensional Gaussians

$$\mathbb{E}[f(Y_i)] = \mathop{\mathbb{E}}_{y \sim \mathcal{N}(0,1)^n}[f(y)]$$ **for any degree-R polynomial f**

Used in [Kan11b, OST20, OSTK21, KM22] to design PRGs for PTFs.

Theorem.

With $R = O(\log(kd/\varepsilon))$ and $L = \mathrm{poly}(k, d, 1/\varepsilon)$, the distribution of Y ε-fools arbitrary functions of k degree-d PTFs over Gaussian space.

Lemma.

A discretization of Y (via *the Box–Muller transform*) also fools functions of k degree-d PTFs.

Discretization of Y

$$Y = 1/\sqrt{L}\left(Y_1 + Y_2 + \cdots + Y_{L-1} + Y_L\right)$$

$$\begin{bmatrix} Y_{1,1} & Y_{2,1} & \cdots & Y_{L,1} \\ Y_{1,2} & Y_{2,2} & \cdots & Y_{L,2} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{1,n} & Y_{2,n} & \cdots & Y_{L,n} \end{bmatrix}$$

R-wise independent

Box-Muller transform

Given $u, v \sim \mathrm{U}(0,1)$, $\sqrt{-2\ln u}\cos(2\pi v) \sim \mathcal{N}(0,1)$.

$$Y_{i,j} = \sqrt{-2\ln u_{i,j}}\cos(2\pi v_{i,j})$$

$$\begin{bmatrix} u_{1,1} & u_{2,1} & \cdots & u_{L,1} \\ u_{1,2} & u_{2,2} & \cdots & u_{L,2} \\ \vdots & \vdots & \ddots & \vdots \\ u_{1,n} & u_{2,n} & \cdots & u_{L,n} \end{bmatrix} \quad \begin{bmatrix} v_{1,1} & v_{2,1} & \cdots & v_{L,1} \\ v_{1,2} & v_{2,2} & \cdots & v_{L,2} \\ \vdots & \vdots & \ddots & \vdots \\ v_{1,n} & v_{2,n} & \cdots & v_{L,n} \end{bmatrix}$$

R-wise independent

$M = O(kd\log(kdn/\epsilon))$ approximation of $\mathrm{U}(0,1)$

seed length: $2 \cdot L \cdot R \cdot M = \mathrm{poly}(k, d, 1/\varepsilon) \cdot \log n$

Open Questions

- Improve the seed length? *Ideal*: $k + d \log n + \log 1/\varepsilon$
- Design PRGs against functions of PTFs over Boolean space?
- Fooling intersections of PTFs?

Thank you!