A Pseudorandom Generator for Polynomial Threshold Functions with Subpolynomial Seed Length

Daniel M. Kane

Department of Mathematics
Stanford University
dankane@math.stanford.edu

November 18th, 2013

Definitions

We briefly recall some basic definitions:

Definition

We call a function $f : \mathbb{R}^n \to \mathbb{R}$ a (degree-d) *Polynomial Threshold Function* (or PTF) if it is of the form $f(x) = \mathrm{sgn}(p(x))$ for p a (degree-d) polynomial in n variables.

Definition

For $p : \mathbb{R}^n \to \mathbb{R}$ and define

$$|p|_2 := \left(\mathbb{E}_{X\sim G^n}\left[|p(X)|^2\right]\right)^{1/2}.$$

Pseudorandom Generators

Definition

Given a class $\mathcal{C}$ of functions $f : \mathbb{R}^n \to \mathbb{R}$, and a probability distribution D on $\mathbb{R}^n$ we say that another distribution B on $\mathbb{R}^n$ ϵ-fools $\mathcal{C}$ with respect to D if for every $f \in \mathcal{C}$,

$$|\mathbb{E}_{X\sim D}[f(X)] - \mathbb{E}_{Y\sim B}[f(Y)]| \leq \epsilon.$$

Definition

We say that the probability distribution B is a *Pseudorandom Generator* (PRG) for $\mathcal{C}$ with respect to D if it can be produced by a polynomial time randomized algorithm using few random bits.

We will produce a small-seed PRG to ϵ-fool the class of degree-d PTFs with respect to the n-dimensional Gaussian (or Bernoulli) distribution.

PRGs from k-independence

Recall that a random variable is *k-wise independent* if any k of its coordinates are independent. There are good constructions of k-wise independent variables from small seeds, and they can be used as PRGs for PTFs.

- [Diakonikolas-Gopalan-Jaiswal-Servedio-Viola, 2010] $k = \tilde{O}(\epsilon^{-2})$-independence fools degree-1 PTFs
- [Diakonikolas-K.-Nelson 2010] $k = O(\epsilon^{-8})$-independence fools degree-2 PTFs
- [K. 2011] $k = O_d(\epsilon^{-2^{O(d)}})$-independence fools degree-d PTFs
- Best lower bound that I know: $k = \Omega(d^2\epsilon^{-2})$.
- I suspect that the lower bound is tight.

Other PRGs

- [Meka-Zuckerman 2010] $O(d \log(n) + \log(1/\epsilon))$ (Existential)
- [Meka-Zuckerman 2010] $\log(n) 2^{O(d)} \epsilon^{-8d-3}$ (Bernoulli)
- [K. 2011] $\log(n) 2^{O(d)} \epsilon^{-4.1}$ (Gaussian)
- [K. 2012] $\log(n) O_d(\epsilon^{-11.1})$ (Bernoulli)
- [K. 2012] $\log(n) O_d(\epsilon^{-2.1})$ (Gaussian)

In this talk we discuss the structure and analysis of a generator with seed length subpolynomial in the error parameter. Namely, seed length

$$\log(n) O_{c,d}(\epsilon^{-c}).$$

General Construction Idea

Basic idea for the above: Combine a bunch of independent copies of a weak PRG.

Bernoulli case:

- Split coordinates into M bins in a 2-independent fashion.
- Fill each bin using a k-independent generator.

Gaussian Case:

- Y_i are k-independent Gaussians chosen independently.
- $Y = \frac{1}{\sqrt{M}} \sum_{i=1}^{M} Y_i$.

The Replacement Method

These generators can be analyzed using Lindeberg's replacement method.

- Approximate f by smooth function g
- Show $\mathbb{E}[f(X)] \approx \mathbb{E}[g(X)] \approx \mathbb{E}[g(Y)] \approx \mathbb{E}[f(Y)]$
  - $\mathbb{E}[f(X)] \approx \mathbb{E}[g(X)]$ from anticoncentration
  - $\mathbb{E}[g(X)] \approx \mathbb{E}[g(Y)]$ from replacement

The Replacement Step

To get $\mathbb{E}[g(X)] \approx \mathbb{E}[g(Y)]$,

- $X = (X_1, \ldots, X_M)$, $Y = (Y_1, \ldots, Y_M)$
- Replace X_i by Y_i one at a time
- Show:

$$\mathbb{E}[g(Y_1, \ldots, Y_{i-1}, Y_i, X_{i+1}, \ldots, X_M)] \approx \mathbb{E}[g(Y_1, \ldots, Y_{i-1}, X_i, X_{i+1}, \ldots, X_M)].$$

- Fixing, $Y_1, \ldots, Y_{i-1}, X_{i+1}, \ldots, X_M$ Taylor expand g

$$g(Y_1, \ldots, Y_{i-1}, Z, X_{i+1}, \ldots, X_M) = \mathrm{Poly}(Z) + \mathrm{Error}.$$

- Since $Z = X_i$ and $Z = Y_i$ have same low order moments, they give similar expectations.

Anticoncentration

- To ensure $\mathbb{E}[f(X)] \approx \mathbb{E}[g(X)]$, want $f(X) = g(X)$ with high probability.
- Approximating discontinuous function by smooth one have error near locus of discontinuity.
- Need *anticoncentration* result.

For example:

Lemma (Carbery-Wright)

If p is a degree-d polynomial in n variables, X an n-dimensional Gaussian, and $\tau > 0$ then

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

Balancing Errors

- To get low anticoncentration error, need g to have sharp cutoffs
- This causes g to have large derivatives
- This causes large Taylor error
- Which forces M to be large
- Improvements can be made by shaping g to the polynomial, but probably can't beat seed length ϵ^{-2}.

New Idea

- First replacement step, show that

$$\mathbb{E}_{X,Y}\left[g\left(\sqrt{\frac{M-1}{M}}X+\frac{1}{\sqrt{M}}Y\right)\right]$$

  Is determined to small error by k-independence of Y.
- Want g smooth, so that above holds for any fixed X.
- Expectation over X provides smoothing.
- Hope to show

$$\mathbb{E}_{X,Y}\left[f\left(\sqrt{\frac{M-1}{M}}X+\frac{1}{\sqrt{M}}Y\right)\right]$$

  Is approximately determined by k-independence.
- Avoids anticoncentration error.

The Degree 1 Case

We begin by seeing how this works in the degree 1 case. Let

$$f(x) = \mathrm{sgn}(v \cdot x + \theta)$$

for some vector v with $|v| = 1$ and some $\theta \in \mathbb{R}$. For fixed Y, we have

$$\begin{aligned}
&\mathbb{E}_X \left[f\left(\sqrt{\frac{M-1}{M}} X + \frac{1}{\sqrt{M}} Y \right) \right] \\
&= \mathbb{E}_X \left[\mathrm{sgn}\left(v \cdot X + \frac{1}{\sqrt{M-1}} v \cdot Y + \sqrt{\frac{M}{M-1}} \theta \right) \right] \\
&= \mathrm{erf}\left(\frac{1}{\sqrt{M-1}} v \cdot Y + \sqrt{\frac{M}{M-1}} \theta \right) \\
&= T_k(v \cdot Y) + O(|v \cdot Y|^k (kM)^{-k/2}).
\end{aligned}$$

Expectation is determined by k-independence up to an error of $O(M^{-1})^{k/2}$.

The Degree 1 Case

Lemma

If f is a degree 1 PTF, X a random Gaussian, and Y a k-independent Gaussian (k even) and $\delta > 0$,

$$\mathbb{E}_X[f(X)] = \mathbb{E}_{X,Y}[f(\sqrt{1-\delta^2}X + \delta Y)] + O(\delta)^k.$$

For fixed Y, have another degree 1 PTF in X, so we can iterate:

$$\begin{aligned}
\mathbb{E}[f(X)] &= \mathbb{E}[f(\sqrt{1-\delta^2}X + \delta Y_1)] + O(\delta)^k \\
&= \mathbb{E}[f((1-\delta^2)X + \delta Y_1 + \delta(1-\delta^2)^{1/2}Y_2)] + 2O(\delta)^k \\
&= \dots \\
&= \mathbb{E}\left[f\left((1-\delta^2)^{\ell/2}X + \delta\sum_{i=1}^{\ell}(1-\delta^2)^{(i-1)/2}Y_i\right)\right] + \ell O(\delta)^k.
\end{aligned}$$

Getting Rid of the X

For large ℓ, the coefficient of X is small. Thus, we expect it to have little effect.
The expected difference of

$$p\left((1-\delta^2)^{\ell/2}X+\delta\sum_{i=1}^{\ell}(1-\delta^2)^{(i-1)/2}Y_i\right)$$

and

$$p\left(\frac{\sum_{i=1}^{\ell}(1-\delta^2)^{(i-1)/2}Y_i}{\sqrt{\sum_{i=1}^{\ell}(1-\delta^2)^{i-1}}}\right)$$

is about $O((1-\delta^2)^{\ell/2})$. Thus, they likely have the same sign.

Result

Theorem

Let X be a random Gaussian. Let Y_i be independently chosen from k-independent families of Gaussians. For some $\ell, \delta > 0$, let

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

Then for f any degree 1 PTF,

$$|\mathbb{E}[f(X)] - \mathbb{E}[f(Y)]| = \ell O(\delta)^k + \tilde{O}((1-\delta^2)^{\ell/2}).$$

Taking δ constant and $k, \ell = O(\log(1/\epsilon))$ gives a generator of seed length

$$s = O(\log(n)\log^2(1/\epsilon)).$$

Higher Degrees

- To get this generator to work for higher degree PTFs we need to show

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

- Show that

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

is approximated by a polynomial in Y.

Approximately Linear Polynomials

We first consider the case where p is approximately linear,

$$p(x) = (1-\delta^2)^{-1/2} x_{(1)} + \theta + q(x)$$

with $|q(x)|_2$ small. Letting $X = (X_{(1)}, X')$, we have that

$$p(\sqrt{1-\delta^2}X + \delta Y) = X_{(1)} + \theta + r(X_{(1)}, X', Y).$$

Fixing the values of X' and Y we have that

$$p = p(X_{(1)}) = X_{(1)} + \theta + R_{x',Y}(X_{(1)}).$$

With $|R|_2$ small with high probability.

Approximately Linear Polynomials

$$p = p(X_{(1)}) = X_{(1)} + \theta + R_{x',Y}(X_{(1)}).$$

For small X, p is invertible by the Inverse Function Theorem.

$$\mathbb{E}[\mathrm{sgn}(p(X_{(1)}))] \approx \mathrm{erf}(p^{-1}(0)).$$

We have $p^{-1}(0)$ smooth in coefficients of R, so Taylor expanding,

$$\mathbb{E}[\mathrm{sgn}(p(X_{(1)}))] = \mathrm{Polynomial}(R) + \tilde{O}_{d,k}(|R|_2^k).$$

Since the expectation of a degree-k polynomial in R is determined by dk-independence of Y, we have that

$$\mathbb{E}[\mathrm{sgn}(p(X))] = \mathbb{E}[\mathrm{sgn}(p(\sqrt{1-\delta^2}X + \delta Y))] + \tilde{O}_{d,k}((|q|_2 + \delta)^k).$$

Local Restrictions

- Problem: Most polynomials are not approximately linear
- Idea: A smooth function is approximately linear on small scales
  - Let $p_Z(X) = p(\sqrt{1-\delta^2}Z + \delta X)$.
  - With high probability over Z,

$$p_Z(X) = \mathrm{Const.} + \delta p'(Z) \cdot X + \tilde{O}(\delta^2)$$

  - Need linear term not too small
  - Want $|p'(Z)| > \delta^{1/2}$ with high probability

Definition

We say that p is (δ, c, N)-*non-singular* if

$$\mathrm{Pr}_Z(|p'(Z)| \leq \delta^c |p|_2) \leq \delta^N.$$

Non-Singular Polynomials

Proposition

If p is $(\delta, 1/2, k)$-non-singular, and Y is $4dk$-wise independent, then for $f(x) = sgn(p(x))$,

$$\left|\mathbb{E}[f(X)] - \mathbb{E}[f(\sqrt{1-\delta^4}X + \delta^2 Y)]\right| = \tilde{O}_{d,k}(\delta^k).$$

Proof.

- Let $\sqrt{1-\delta^4}X = \sqrt{1-\delta^2}X_1 + \delta\sqrt{1-\delta^2}X_2$
- With probability $1-\delta^k$, $p_{X_1}(-)$ is approximately linear
- When this happens,

$$|\mathbb{E}_{X_2,Y}[f(\sqrt{1-\delta^2}X_1 + \delta\sqrt{1-\delta^2}X_2 + \delta^2 Y)] - \mathbb{E}_{X_2}[f(\sqrt{1-\delta^2}X_1 + \delta X_2)]| = \tilde{O}_{d,k}(\delta^k)$$

□

Getting Non-Singular Polynomials

- Most polynomials are non-singular
- Some aren't.
  - $p(x) = L(x)^d$
  - $|p'(x)| = d|L'(x)||L(x)|^{d-1}$ often small
  - Suffices to study $L(x)$ instead
- Idea: Decompose arbitrary polynomial in terms of non-singular polynomials

Degree 2 Case

- $p(x)$ degree 2, $|p|_2 = 1$
- Diagonalize quadratic form, change variables:

$$p(x) = \sum_{i=1}^{n} a_i p_i(x_{(i)}) + \theta$$

where p_i is mean 0 and variance 1, $a_1 \geq a_2 \geq \ldots \geq a_n \geq 0$.

- $|p'(x)|^2 = \sum a_i^2 (p_i'(x_{(i)}))^2$
- p is (δ, c, N)-non-singular if:
  - $a_{3N/c} \gg \delta^{2c/3}$ (one of the first few $a_i |p_i'(x_{(i)})|$ will be big enough)
  - $\sum_{i=3N/c}^{n} a_i^2 \gg \delta^c$ (the sum of the tail terms is too well concentrated)
- Thus, p is non-singular unless all but $\delta^{c/2}$ of its L^2 norm is determined by the first $3N/c$ coordinates.

Degree 2 Case

- Either p is non-singular or
$$p(x) = q(x_{(1)}, \ldots, x_{(3N/c)}) + \delta^{c/2} p_1(x).$$
- Either p_1 is non-singular or
$$p(x) = q(x_{(1)}, \ldots, x_{(6N/c)}) + \delta^{c} p_2(x).$$
- ...
- Either:
  - $$p(x) = q(x_{(1)}, \ldots, x_{(m)}) + r(x)$$
    with $m \leq 24N^2/c^2$ and r (δ, c, N)-non-singular
  - $$p(x) = q(x_{(1)}, \ldots, x_{(m)}) + O(\delta^{4N})$$
- Need to simultaneously fool m linear functions and one non-singular quadratic function

Non-Singular Decomposition

Definition

We say that a sequence of polynomials, $(p_1, \ldots, p_m)$, is (δ, c, N)-*non-singular* if $|p_i|_2 = 1$ for all i and except for with probability δ^N

$$\begin{bmatrix} | & | & & | \\ p_1'(X) & p_2'(X) & \ldots & p_m'(X) \\ | & | & & | \end{bmatrix} \text{ has no singular value smaller than } \delta^c.$$

Definition

A degree d polynomial p has a (δ, c, N)-*non-singular decomposition of size* m if $p(x)$ can be written as

$$p(x) = Q(p_1(x), p_2(x), \ldots, p_m(x))$$

for some Q and polynomials $p_1, \ldots, p_m$ of degree at most d so that $(p_1, \ldots, p_m)$ is a (δ, c, N)-non-singular set.

The Decomposition Theorem

Theorem

For any $d, c, N > 0$ *there exists a constant* $s(d, c, N)$ *so that for any degree-*d *polynomial* p*, and any* $\delta > 0$ *sufficiently small, there exists a degree* d *polynomial* p_0 *with* $|p - p_0|_2 \leq \delta^{2dN}|p|_2$*, so that* p_0 *has a* (δ, c, N)*-non-singular decomposition of size at most* $s(d, c, N)$*.*

In particular, we may take $s(1, c, N) = 1$ *and* $s(2, c, N) = O(N^2/c^2)$*.*

Remark

The proof for $d > 2$ *is quite technical. Also the bounds on* s *are quite bad. The best I can show is* $s(d, c, N) \leq A(d + O(1), N/c)$*, where* A *is the Ackermann function.*

Using the Decomposition

Proposition

Let f be a degree d PTF. Let $M = dks(d, 1/2, k)$. Let X be a random Gaussian and Y a $2kd$-independent Gaussian. Then for $\delta > 0$

$$|\mathbb{E}[f(X)] - \mathbb{E}[f(\sqrt{1-\delta^4}X + \delta^2 Y)]| = O(M)^{O(M)}\tilde{O}(\delta^k).$$

Proof.

- $p \approx p_0$ where p_0 has a decomposition into $(p_1, \ldots, p_m)$.
- Replacing $\mathrm{sgn}(p(x))$ by $\mathrm{sgn}(p_0(x))$ introduces $O(\delta^k)$ error.
- $\mathrm{sgn}(p_0(x)) = h(p_1(x), p_2(x), \ldots, p_m(x))$.
- Evaluate at $X = \sqrt{1-\delta^2}X_1 + \delta X_2$ at random, fixed X_1
- With high probability, $p_i^{X_1}(X_2)$ approximately linear
- Change variables, $q_i(X) = X_{(i)} + O(\delta^{1/2})R(X)$

Using the Decomposition

Proof continued...

- $q_i(X) = X_{(i)} + O(\delta^{1/2})R(X)$
- Let $q(x) = (q_1(x), \ldots, q_m(x))$. $f(x) = h(q(x))$.
- Need $|\mathbb{E}[h(q(X))] - \mathbb{E}[h(q(\sqrt{1-\delta^2}X + \delta Y))]| = \tilde{O}(\delta^k)$.
- Let $X_{(0)} = (X_{(1)}, \ldots, X_{(m)})$, $X' = (X_{(m+1)}, \ldots, X_{(n)})$.
- $$\begin{aligned} q(\sqrt{1-\delta^2}X + \delta Y) &= \sqrt{1-\delta^2}(X_{(0)} + O(\delta^{1/2})R(X_{(0)}, X', Y)) \\ &= \sqrt{1-\delta^2}q_{X',Y}(X_{(0)}). \end{aligned}$$
- With high probability, $q_{X',Y}$ invertible for small $X_{(0)}$

Using the Decomposition

Proof continued...

- $$\begin{aligned}\mathbb{E}[f(\sqrt{1-\delta^2}X+\delta Y)] &= \mathbb{E}_{X',Y}[\mathbb{E}_{X_{(0)}}[g(q_{X',Y}(X_{(0)}))]] \\ &= \mathbb{E}_{X',Y}\left[\frac{1}{(2\pi)^{m/2}}\int e^{-|x|^2/2}g(q_{X',Y}(x))dx\right] \\ &= \mathbb{E}_{X',Y}\left[\frac{1}{(2\pi)^{m/2}}\int e^{-|q^{-1}(y)|^2/2}g(y)\frac{dy}{|\mathrm{Jac}(q)|}\right]\end{aligned}$$

- Taylor expand integrand

$$\begin{aligned}&= \mathbb{E}_{X',Y}\left[\mathrm{Poly}(R(X',Y)) + O(M)^{O(M)}\tilde{O}(\delta^k)\right] \\ &= \mathbb{E}[f(X)] + O(M)^{O(M)}\tilde{O}(\delta^k)\end{aligned}$$

□

Putting it Together

Theorem

For d, k positive integers and $\delta > 0$, there exists an explicit pseudorandom generator, Y of seed length $O(d^2k^2\log(n)\delta^{-1})$ so that for X an n-dimensional Gaussian, and f any degree-d polynomial threshold function in n variables, and $M = dks(d, 1/2, 3k)$

$$|\mathbb{E}[f(X)] - \mathbb{E}[f(Y)]| = O(M)^{O(M)}(\delta^k).$$

In particular, such a generator is given by letting

$$Y = \frac{\sum_{i=1}^{[\delta^{-2/3}(2d+1)k]}(1-\delta^{2/3})^{i/2}Y_i}{\sqrt{\sum_{i=1}^{[\delta^{-1}dk]}(1-\delta^{2/3})^i}}$$

Where the Y_i are independent of each other and approximate $10d(3k+3)$-independent random Gaussians.

Results

Applying this theorem, we get PRGs of error ϵ and seed length

- $O(\log(n)\log^2(1/\epsilon))$ for $d = 1$
- $\log(n)\exp(O(\log^{2/3}(1/\epsilon)\log\log^{1/3}(1/\epsilon)))$ for $d = 2$
- $\log(n)O_{c,d}(\epsilon^{-c})$ for $d > 2$

Linear Threshold Functions

We can actually do even better in the case of linear threshold functions. Meka and Zuckerman noticed in 2010 that:

- Linear Threshold Function can be approximately computed by a Read Once Branching Program (a program that gets one pass over the input and has limited memory)
- PRGs for Read Once Branching Programs also fool Linear Threshold Functions
- Seed length $O(\log(n) + \log^2(1/\epsilon))$ in the Bernoulli case.

We can beat this in the Gaussian case.

Old Generator

Our old generator set

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

With Y_i k-independent and

- $\ell O(\delta)^k \ll \epsilon$
- $(1-\delta^2)^{\ell/2} \ll \epsilon$

Note that

$$L(Y) = \sum_{i=1}^{\ell} L_i(Y_i)$$

It suffices to seed Y_i with a PRG for ROBPs.

New Generator

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

With Y_i k-independent, seeded by a PRG for ROBPs. Seed length:

$$O(k \log(n/\epsilon) + \log(\ell)\log(\ell/\epsilon)).$$

Need:

- $\ell O(\delta)^k \ll \epsilon$
- $(1-\delta^2)^{\ell/2} \ll \epsilon$

Use:

- $k = \log(1/\delta) \approx \sqrt{\log(n/\epsilon)}$
- $\ell \approx \delta^{-3}$

Seed length: $O(\log^{3/2}(n/\epsilon))$. Standard dimension reduction techniques improve this to

$$O(\log(n) + \log^{3/2}(1/\epsilon)).$$

Conclusions

We have thus made substantial improvements to the smallest known PRGs for PTFs in the Gaussian case. In particular, we have:

- Seed length $O(\log(n) + \log^{3/2}(1/\epsilon))$ for $d = 1$
- Seed length $\log(n) \exp(O(\log^{2/3}(1/\epsilon) \log \log^{1/3}(1/\epsilon)))$ for $d = 2$
- Seed length $\log(n) O_{c,d}(\epsilon^{-c})$ for $d > 2$

Future Directions

There are several directions of attack for future progress on this problem:

- Find similarly good generators in the Bernoulli context
- For $d = 1$, we are close to the optimal $O(\log(n/\epsilon))$
- For $d = 2$, the reduction step only needs to fool a bunch of linear polynomials and one non-singular quadratic. Using a better PRG for LTFs might improve seed length to $\mathrm{polylog}(n/\epsilon)$.
- For $d > 2$ the main obstacle is the potentially huge sizes of the decompositions. If, as I would conjecture, $s(d, 1/2, k) = \mathrm{Poly}(d, k)$, we would have a generator of seed length $\log(n) \exp(O(d \log(1/\epsilon)^{1-a}))$.

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) (2001), pp. 233248.

I. Diakonikolas, P. Gopalan, R. Jaiswal, R. Servedio and E. Viola, *Bounded independence fools halfspaces*, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2009.

Ilias Diakonikolas, Daniel M. Kane, Jelani Nelson, *Bounded Independence Fools Degree-2 Threshold Functions*, Foundations of Computer Science (FOCS 2010).

Daniel M. Kane *A Pseudorandom Generator for Polynomial Threshold Functions of Gaussians with Subpolynomial Seed Length*, submitted to Conference on Computational Complexity.

Daniel M. Kane, *A Small PRG for Polynomial Threshold Functions of Gaussians*, Foundations of Computer Science (FOCS 2011).

- Daniel M. Kane *A Structure Theorem for Poorly Anticoncentrated Gaussian Chaoses and Applications to the Study of Polynomial Threshold Functions*, Foundations of Computer Science (FOCS) 2012, pp. 91-100.
- Daniel M. Kane *k-Independent Gaussians Fool Polynomial Threshold Functions*, Conference on Computational Complexity (CCC 2011).
- Raghu Meka, David Zuckerman *Pseudorandom generators for polynomial threshold functions*, Proceedings of the 42nd ACM Symposium on Theory Of Computing (STOC 2010).
- Nelson *The free Markov field*, J. Func. Anal. Vol. 12 no. 2 (1973), p. 211-227