Almost Optimal Pseudorandom Generators for Spherical Caps

Pravesh K. Kothari
UT Austin

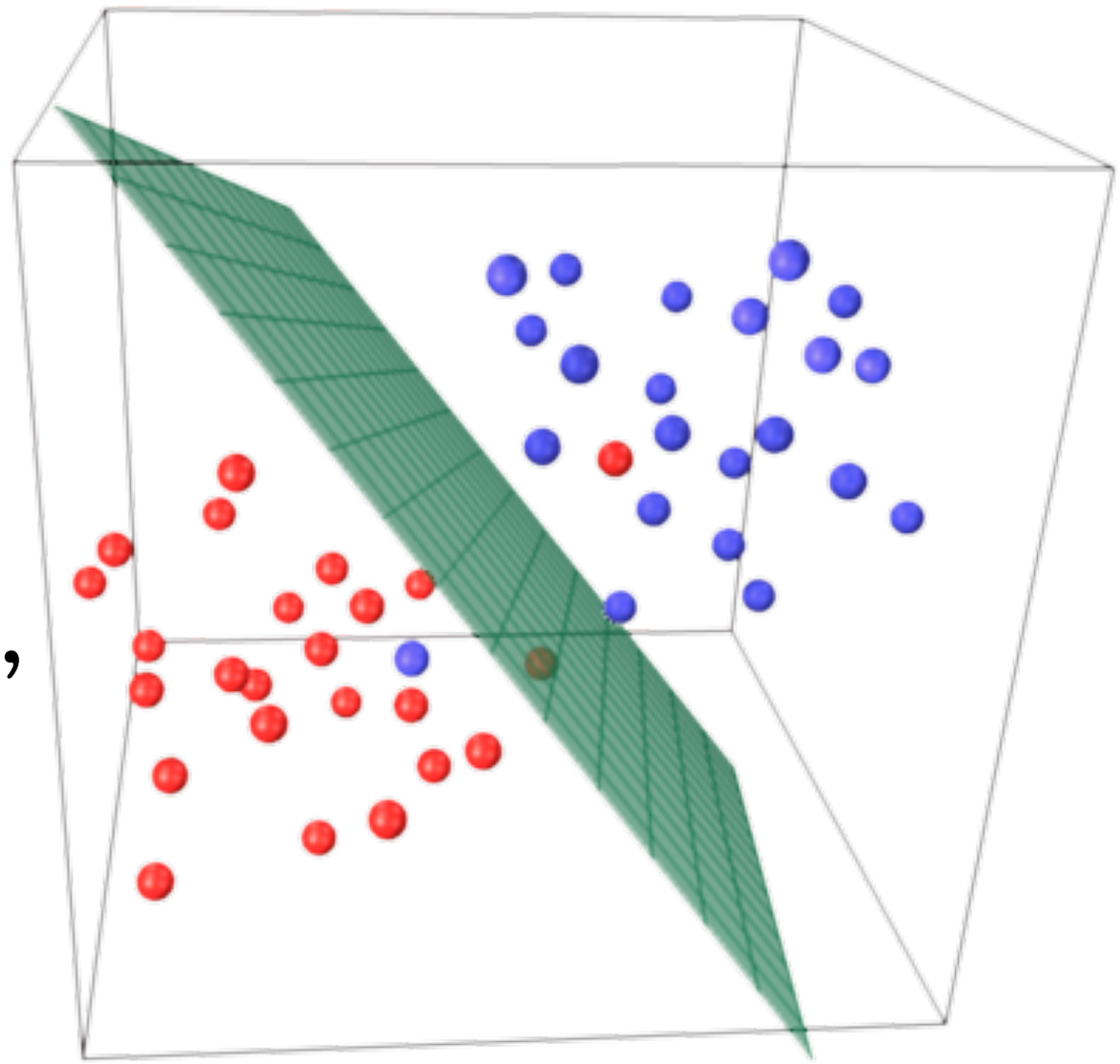
Raghu Meka
UCLA

Halfspaces

$$f : \mathbb{R}^n \to \{-1, 1\}$$

$$f(x) = \mathsf{sign}(\langle w, x \rangle - \theta)$$

Applications: Perceptrons, Boosting, Support Vector Machines, Voting, Social Choice



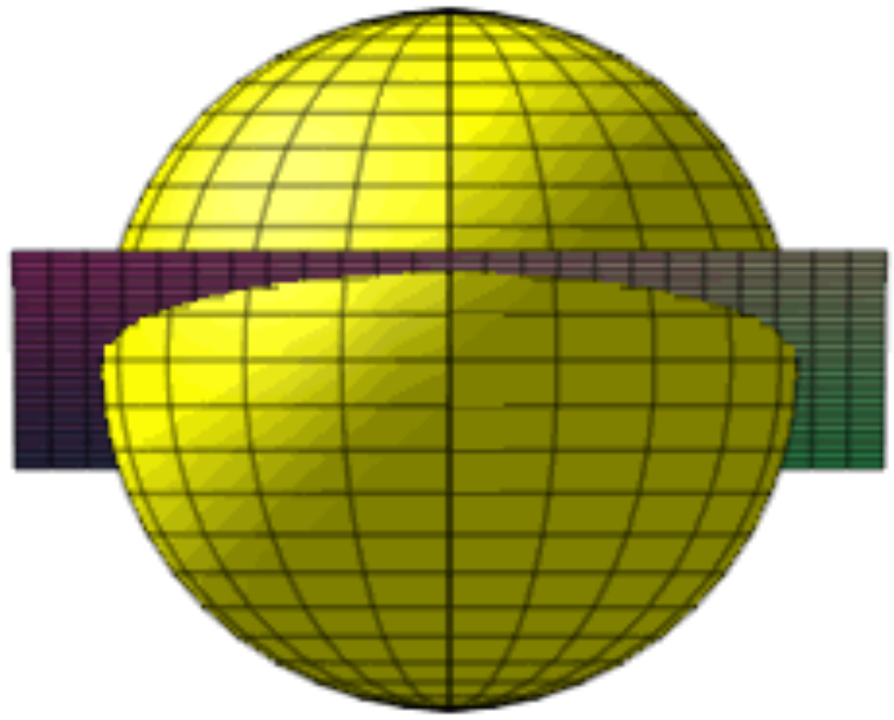
Spherical Caps

halfspaces on the sphere

$\mathbb{S}^{n-1}$:unit sphere $\subseteq \mathbb{R}^n$

$$f : \mathbb{S}^{n-1} \to \{-1, 1\}$$

$$f(x) = \mathsf{sign}(\langle w, x \rangle - \theta)$$



Applications: Perceptrons, Boosting, Support Vector Machines, Voting, Social Choice

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

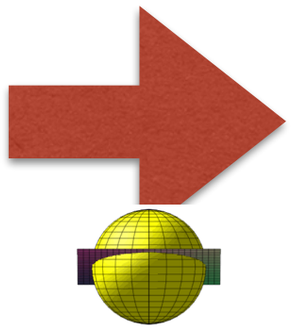
PRGs for Spherical Caps/Halfspaces?

efficiently samplable prob. dist.

1) “looks” uniform on the sphere to **every** halfspace.

2) needs only **a few** purely random bits to sample.

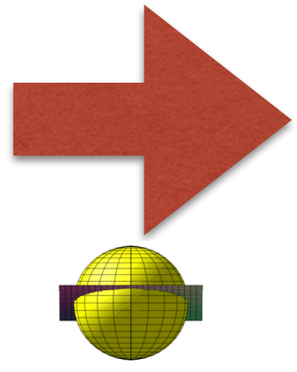
“small set with low spherical cap discrepancy”



PRGs for Spherical Caps/Halfspaces?

1. natural problem in pseudorandomness
2. derandomization of Goemans-Williamson
3. deterministic estimation of accuracy of halfspaces classifiers.

PRGs for Spherical Caps

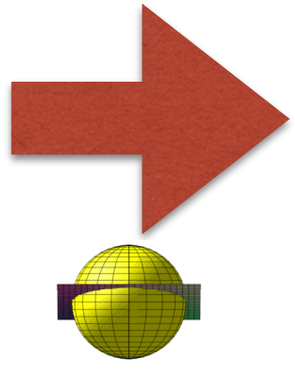


efficiently computable $G : \{0,1\}^r \to \mathbb{S}^{n-1}$

for all spherical caps $f : \mathbb{S}^{n-1} \to \{-1,1\}$

$$\left|\mathbb{E}_{x\sim\mathbb{S}^{n-1}}[f(x)] - \mathbb{E}_{y\sim\{0,1\}^r}[f(G(y))]\right| \leq \varepsilon$$

PRGs for Spherical Caps



efficiently c

for all s

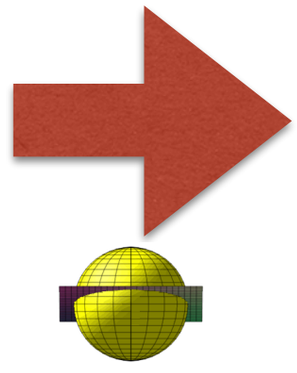
$$G : \{0,1\}^r \to \mathbb{S}^{n-1}$$

$$\mathbb{S}^{n-1} \to \{-1,1\}$$

bias on uniform distribution on the sphere

$$\left|\mathbb{E}_{x \sim \mathbb{S}^{n-1}}[f(x)] - \mathbb{E}_{y \sim \{0,1\}^r}[f(G(y))]\right| \leq \varepsilon$$

PRGs for Spherical Caps



efficiently computable

for all spherical caps

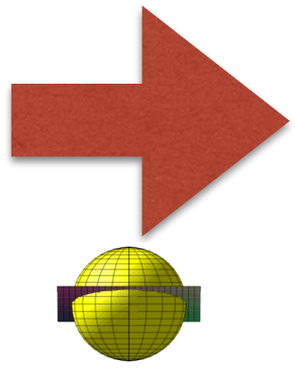
$$G : \{$$

$$f : \mathbb{S}$$

bias on output of G on uniform seed bits

$$\left|\mathbb{E}_{x\sim\mathbb{S}^{n-1}}[f(x)] - \mathbb{E}_{y\sim\{0,1\}^r}[f(G(y))]\right| \leq \varepsilon$$

PRGs for Spherical Caps



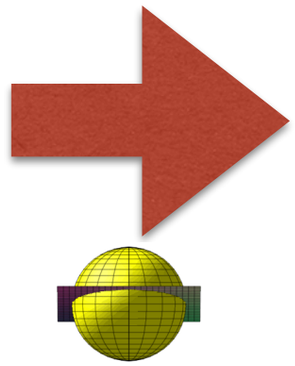
efficiently computable $G : \{0,1\}^r \to \mathbb{S}^{n-1}$

for all spherical caps $f : \mathbb{S}^{n-1} \to \{-1$

error

$$\left|\mathbb{E}_{x\sim\mathbb{S}^{n-1}}[f(x)] - \mathbb{E}_{y\sim\{0,1\}^r}[f(G(y))]\right| \leq \varepsilon$$

PRGs for Spherical Caps



seed length

efficiently computable $G : \{0,1\}^r \to \mathbb{S}^{n-1}$

for all spherical caps $f : \mathbb{S}^{n-1} \to \{-1,1\}$

$$\left|\mathbb{E}_{x\sim\mathbb{S}^{n-1}}[f(x)] - \mathbb{E}_{y\sim\{0,1\}^r}[f(G(y))]\right| \leq \varepsilon$$

PRGs for Spherical Caps

efficiently computable $G : \{0,1\}^r \to \mathbb{S}^{n-1}$

for all spherical caps $f : \mathbb{S}^{n-1} \to \{-1, 1\}$

$$\left|\mathbb{E}_{x \sim \mathbb{S}^{n-1}}[f(x)] - \mathbb{E}_{y \sim \{0,1\}^r}[f(G(y))]\right| \leq \varepsilon$$

Goal: To have a small seed length.

Probabilistic Method: $2\log(n) + 2\log(1/\epsilon) + O(1)$

PRGs for Spherical Caps

Probabilistic Method: $2\log(n) + 2\log(1/\epsilon) + O(1)$

Reference	Class/Distribution	Seed Length
LPS87	3 Dimensional Spherical Caps	$3 \cdot \log(1/\epsilon) + O(1)$
DGJSV10	Halfspaces/Uniform on the hypercube	$O(\log(n)/\epsilon^2)$
KRS12	Spherical Caps	$O(\log(n) + \log^2(1/\epsilon))$
Kan14	Spherical Caps	$O(\log(n) + \log^{3/2}(1/\epsilon))$

PRGs for Spherical Caps

Probabilistic Method: $2\log(n) + 2\log(1/\epsilon) + O(1)$

Reference	Class/Distribution	Seed Length
LPS87	3 Dimensional Spherical Caps	$3 \cdot \log(1/\epsilon) + O(1)$
DGJSV10	Halfspaces/Uniform on the hypercube	$O(\log(n)/\epsilon^2)$
KRS12	Spherical Caps	$O(\log(n) + \log^2(1/\epsilon))$
Kan14	Spherical Caps	$O(\log(n) + \log^{3/2}(1/\epsilon))$

For $\varepsilon \sim 1/\mathrm{poly}(n)$ best previous result $\Omega(\log^{1.5}(n))$

PRGs for Spherical Caps

Probabilistic Method: $2\log(n) + 2\log(1/\epsilon) + O(1)$

Reference	Class/Distribution	Seed Length
LPS87	3 Dimensional Spherical Caps	$3 \cdot \log(1/\epsilon) + O(1)$
DGJSV10	Halfspaces/Uniform on the hypercube	$O(\log(n)/\epsilon^2)$
KRS12	Spherical Caps	$O(\log(n) + \log^2(1/\epsilon))$
Kan14	Spherical Caps	$O(\log(n) + \log^{3/2}(1/\epsilon))$
This Work	**Spherical Caps**	$O(\log(n)) + \tilde{O}(\log(1/\epsilon))$

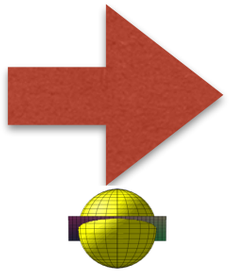
PRGs for Spherical Caps

Probabilistic Method: $2\log(n) + 2\log(1/\epsilon) + O(1)$

Reference	Class/Distribution	Seed Length
LPS87	3 Dimensional Spherical Caps	$3 \cdot \log(1/\epsilon) + O(1)$
DGJSV10	Halfspaces/Uniform on the hypercube	$O(\log(n)/\epsilon^2)$
KRS12	Spherical Caps	$O(\log(n) + \log^2(1/\epsilon))$
Kan14	Spherical Caps	$O(\log(n) + \log^{3/2}(1/\epsilon))$
This Work	**Spherical Caps**	$O(\log(n)) + \tilde{O}(\log(1/\epsilon))$

optimal up to a factor of $\log\log(n)$ for inverse poly error!

Main Result



PRG for spherical caps with seed length

$$O(\log(n) + \log(1/\varepsilon) \log\log(1/\varepsilon))$$

optimal up to a factor of $\log\log(n)$ for inverse poly error!

similar result for spherical Gaussian distribution.

General Techniques

Iterated Dimension Reduction

[Kane-Meka-Nelson11, Celis,Reingold,Segev,Wieder11]

General Techniques

Iterated Dimension Reduction

[Kane-Meka-Nelson11, Celis,Reingold,Segev,Wieder11]

Strong quantitative bounds for the **truncated moment problem** for "mixtures of smooth random variables".

General Techniques

Iterated Dimension Reduction

[Kane-Meka-Nelson11, Celis,Reingold,Segev,Wieder11]

Strong quantitative bounds for the **truncated moment problem** for "mixtures of smooth random variables".

how many moments of a random variable must we match to approximate it?

Order r moment of X: $\mathbb{E}[X^r]$

General Techniques

Iterated Dimension Reduction

[Kane-Meka-Nelson11, Celis,Reingold,Segev,Wieder13]

Strong quantitative bounds for the **truncated moment problem** for “mixtures of smooth random variables”.

Pseudorandom Projection Matrices from **orthogonal designs**.

Proof Sketch

Outline

1. Iterative Dimension Reduction

2. Pseudorandom Projections to Moment Matching

3. Moment Matching

4. Pseudorandom Projections from Orthogonal Designs

Outline

1. Iterative Dimension Reduction

2. Pseudorandom Projections to Moment Matching

3. Moment Matching

4. Pseudorandom Projections from Orthogonal Designs

Goal

A generator G such that:

$w \in \mathbb{R}^n$ unit coeff. vector of a half space

$x \sim \mathbb{S}^{n-1}$ uniform point from the unit sphere

$y \sim \{0,1\}^r$ uniformly random r bits.

$$\langle w, x \rangle \quad \sim_{\varepsilon}^{CDF} \quad \langle w, G(y) \rangle$$

CDF Dist (X,Y) = $\sup_t |\Pr[X \leq t] - \Pr[Y \leq t]|$

Goal

A generator G such that:

$w \in \mathbb{R}^n$ unit coeff. vector of a half space

$x \sim \mathbb{S}^{n-1}$ uniform point from the unit sphere

$y \sim \{0,1\}^r$ uniformly random r bits.

$$\langle w, x \rangle \quad \sim_{\varepsilon}^{CDF} \quad \langle w, G(y) \rangle$$

$\varepsilon \sim 1/\mathsf{poly}(n)$

Goal

A generator G such that:

$w \in \mathbb{R}^n$ unit coeff. vector of a half space

$x \sim \mathbb{S}^{n-1}$ uniform point from the unit sphere

$y \sim \{0,1\}$ n r bits.

random projection of w on to dim 1

$$\langle w, x \rangle \sim_{\varepsilon}^{CDF} \langle w, G(y) \rangle$$

$\varepsilon \sim 1/\mathsf{poly}(n)$

Two Step Dimension Reduction

$w \in \mathbb{R}^n$

$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$Q_1 w$

$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$

$\langle Q_1 w, x_1 \rangle$

Q_1:a uniformly random projection matrix.

Two Step Dimension Reduction

$w \in \mathbb{R}^n$

derandomize the first step

$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

niformly random projection matrix.

$Q_1 w$

$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$

$\langle Q_1 w, x_1 \rangle$

Two Step Generator

$w \in \mathbb{R}^n$

$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$Q_1 w$

$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$

$\langle Q_1 w, x_1 \rangle$

$w \in \mathbb{R}^n$

$P_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$P_1 w$

Two Step Generator

$w \in \mathbb{R}^n$

$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$w \in \mathbb{R}^n$

$P_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

P_1 :"Pseudorandom Projection"
can be sampled using $\sim$log n random bits.

$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$

$\langle Q_1 w, x_1 \rangle$

Two Step Generator

$$w \in \mathbb{R}^n$$

$$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

$$Q_1 w$$

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

$$\langle Q_1 w, x_1 \rangle \quad \sim_{\varepsilon}^{CDF}$$

$$w \in \mathbb{R}^n$$

$$P_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

$$P_1 w$$

$$\langle P_1 w, x_1 \rangle$$

Two Step Generator

$$Q_1 w \qquad\qquad P_1 w$$

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

$$\langle Q_1 w, x_1 \rangle \qquad \sim_{\varepsilon}^{CDF} \qquad \langle P_1 w, x_1 \rangle$$

reduction to a $\sqrt{n}$ dimensional problem!

$w \in \mathbb{R}^n$

$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$Q_1 w$

$Q_2 : \mathbb{R}^{\sqrt{n}} \to \mathbb{R}^{n^{1/4}}$

$Q_2 Q_1 w$

w_t

$\langle w_t, x \rangle$

recurse!

$t \sim \log\log(n)$ steps

$x_t \sim \mathbb{S}^{\sim \log(n)}$

$w \in \mathbb{R}^n$

$P_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$P_1 w$

$P_2 : \mathbb{R}^{\sqrt{n}} \to \mathbb{R}^{n^{1/4}}$

$P_2 P_1 w$

v_t

$\langle v_t, x \rangle$

$w \in \mathbb{R}^n$

$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$Q_1 w$

$Q_2 : \mathbb{R}^{\sqrt{n}} \to \mathbb{R}^{n^{1/4}}$

w_t

$\langle w_t, x \rangle$

$w \in \mathbb{R}^n$

$P_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$P_1 w$

$P_2 : \mathbb{R}^{\sqrt{n}} \to \mathbb{R}^{n^{1/4}}$

v_t

$\langle v_t, x \rangle$

P_i :"Pseudorandom Projection"
can be sampled using $\sim$log n random bits.

$t \sim \log\log(n)$ steps

$x_t \sim \mathbb{S}^{\sim \log(n)}$

$w \in \mathbb{R}^n$

$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$Q_1 w$

$Q_2 : \mathbb{R}^{\sqrt{n}} \to \mathbb{R}^{n^{1/4}}$

$Q_2 Q_1 w$

w_t

$\langle w_t, x \rangle$

$w \in \mathbb{R}^n$

$P_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$

$P_1 w$

$P_2 : \mathbb{R}^{\sqrt{n}} \to \mathbb{R}^{n^{1/4}}$

$P_2 P_1 w$

v_t

$\langle v_t, x \rangle$

$t \sim \log\log(n)$ steps

$x_t \sim \mathbb{S}^{\sim \log(n)}$

$\sim_{\varepsilon}^{CDF}$

Outline

1. Iterative Dimension Reduction

2. Pseudorandom Projections from Moment Matching

3. Moment Matching

4. Pseudorandom Projections from Orthogonal Designs

Two Step Generator

$$w \in \mathbb{R}^n$$

$$Q_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

$$Q_1 w$$

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

$$\langle Q_1 w, x_1 \rangle \quad \sim_{\varepsilon}^{CDF}$$

$$w \in \mathbb{R}^n$$

$$P_1 : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

$$P_1 w$$

$$\langle P_1 w, x_1 \rangle$$

Pseudorandom Projection

A distribution on projections

$$P : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

such that for

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

- **P can be sampled with log n random bits.**
- $$\langle Qw, x_1 \rangle \sim_{\varepsilon}^{CDF} \langle Pw, x_1 \rangle$$

Q: uniformly random projection

w: arbitrary unit vector

Pseudorandom Projection

A distribution on projections

$$P : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

such that for

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

- **P can be sampled with log n random bits.**
- $\langle Qw, x_1 \rangle$ **and** $\langle Pw, x_1 \rangle$ **have approx. equal low order moments.**

Q: uniformly random projection

Pseudorandom Projection

A distribution on projections

$$P : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

such that for

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

"Moment Matching Projections"

- **P can be sampled with log n random bits.**
- $\langle Qw, x_1 \rangle$ **and** $\langle Pw, x_1 \rangle$ **have approx. equal low order moments.**

Q: uniformly random projection

Pseudorandom Projection

A distribution on projections

$$P : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

such that for

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

- **P can be sampled with l… its.**
- $\langle Qx$… **… equal lo…**

How many moments to match?

Q: uniformly random projection

Outline

1. Iterative Dimension Reduction

2. Pseudorandom Projections to Moment Matching

3. Moment Matching

4. Pseudorandom Projections from Orthogonal Designs

Truncated Moment Problem

Order r moment of X: $\mathbb{E}[X^r]$

Suppose $\forall d \leq r \ , \mathbb{E}[X^r] = \mathbb{E}[Y^r]$

How large is DCDF(X,Y)?

extensively studied in probability

[Akhiezer1965], [Klebanov-Mkrtcjan1980],[Lasserre 2012]

Our Setting

Order r moment of X: $\mathbb{E}[X^r]$

Suppose $\forall d \leq r \ , \mathbb{E}[X^r] = \mathbb{E}[Y^r]$

How large is DCDF(X,Y)?

For us:

$X = \langle Qw, x_1 \rangle, Y = \langle Pw, x_1 \rangle, \ \ x_1 \sim \mathbb{S}^{\sqrt{n}-1}$

Our Setting

Suppose $\forall d \leq r \ , \mathbb{E}[X^r] = \mathbb{E}[Y^r]$

How large is DCDF(X,Y)?

For us:

$$X = \langle Qw, x_1 \rangle, Y = \langle Pw, x_1 \rangle, \ \ x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

[Klebanov-Mkrtchyan80]

r = $\left(\frac{1}{\varepsilon}\right)^C$ for ε CDF distance bound.

Our Setting

For us:

$$X = \langle Qw, x_1 \rangle, Y = \langle Pw, x_1 \rangle, \quad x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

Only $||Qw||_2$ and $||Pw||_2$ matter.

Our Setting

For us:

$$X = \langle Qw, x_1 \rangle, Y = \langle Pw, x_1 \rangle, \ x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

$$M = ||Qw||_2 \qquad N = ||Pw||_2$$

$$(z_1, z_2, \ldots) \sim \mathbb{S}^{\sqrt{n}-1}$$

Our Setting

For us:

$$X = \langle Qw, x_1 \rangle, Y = \langle Pw, x_1 \rangle, \ x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

$$M = ||Qw||_2 \qquad N = ||Pw||_2$$

$$(z_1, z_2, \ldots) \sim \mathbb{S}^{\sqrt{n}-1}$$

$$\langle Qw, x_1 \rangle \sim M \cdot z_1 \qquad \langle Pw, x_1 \rangle \sim M \cdot z_1$$

"mixtures of different scalings of z_1"

This Work

Matching $\sim \frac{\log(1/\varepsilon)}{\log(n)}$ **moments enough!**

For random variables of the form

$$M \cdot Z \, , \, N \cdot Z$$

Approximately match moments of M and N!

This Work

Matching $\sim \dfrac{\log(1/\varepsilon)}{\log(n)}$ **moments enough!**

For random variables of the form

$$M \cdot Z \,,\; N \cdot Z$$

1. $\forall d \leq r,\, \mathbb{E}[M^d] \sim \mathbb{E}[N^d]$

This Work

Matching $\sim \frac{\log(1/\varepsilon)}{\log(n)}$ **moments enough!**

For random variables of the form

$$M \cdot Z \,,\, N \cdot Z$$

1. $\forall d \leq r,\, \mathbb{E}[M^d] \sim \mathbb{E}[N^d]$
2. **Moments of M don't grow too fast.**

This Work

Matching $\sim \frac{\log(1/\varepsilon)}{\log(n)}$ **moments enough!**

For random variables of the form

$$M \cdot Z \,,\, N \cdot Z$$

1. $\forall d \leq r,\, \mathbb{E}[M^d] \sim \mathbb{E}[N^d]$
2. **Moments of M don't grow too fast.**
3. **Z has symmetric, infinitely differentiable CDF**

This Work

Matching $\sim \frac{\log(1/\varepsilon)}{\log(n)}$ **moments enough!**

For random variables of the form

$$M \cdot Z \,,\, N \cdot Z$$

1. $\forall d \leq r,\ \mathbb{E}[M^d] \sim \mathbb{E}[N^d]$
2. [illegible]
3. [illegible] **CDF**

Crucially uses the smoothening effect of Z.

This Work

Matching $\sim \frac{\log(1/\varepsilon)}{\log(n)}$ **moments enough!**

For random variables of the form

$$M \cdot Z \,,\, N \cdot Z$$

1. $\forall d \leq r,\, \mathbb{E}[M^d] \sim \mathbb{E}[N^d]$
2. **Moments of M don't grow too fast.**
3. **Z has symmetric, infinitely differentiable CDF**

structure of random variables+plus moment matching:

[Anandkumar,Hsu,Kakade12], [Daskalakis,Papadimitriou13]

Outline

1. Iterative Dimension Reduction

2. Pseudorandom Projections to Moment Matching

3. Moment Matching

4. Pseudorandom Projections from Orthogonal Designs

Pseudorandom Projection

A distribution on projections

$$P : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

such that for

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

"Moment Matching Projections"

- **P can be sampled with log n random bits.**
- $\langle Qw, x_1 \rangle$ **and** $\langle Pw, x_1 \rangle$ **have approx. equal low order moments.**

Q: uniformly random projection

Pseudorandom Projection

A distribution on projections

$$P : \mathbb{R}^n \to \mathbb{R}^{\sqrt{n}}$$

such that for

$$x_1 \sim \mathbb{S}^{\sqrt{n}-1}$$

"Moment Matching Projections"

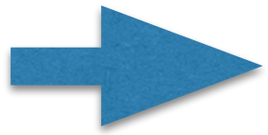
- **P can be sampled with log n random bits.**
- $\langle Qw, x$ **ox. equal low order moments.**

Construction?

Q: uniformly random projection

Approximate Orthogonal Designs

t-wise independence



fools degree t polys on hypercube.

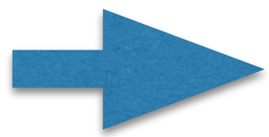
Approximate Orthogonal Designs

t-wise independence → fools degree t polys on hypercube.

orthogonal t-design → fools degree t polys on "**rotation matrices**".

Approximate Orthogonal Designs

orthogonal t-design



fools
degree t polys
on "**rotation matrices**".

A distribution D on a subset of rotation matrices:

For every degree t Polynomial $p : \mathsf{SO}(n) \to \mathbb{R}$

$$|\mathbb{E}_D[p] - \mathbb{E}_{\mathcal{H}}[p]| \leq \epsilon$$

ε **approximate, orthogonal t-design**

Approximate Orthogonal Designs

orthogonal t-design

fools
degree t polys
on "**rotation matrices**".

A distribution D on a subset of matrices:

For every degree t Polyn $\to \mathbb{R}$

Haar measure on SO(n)

$$|\mathbb{E}_D[p] - \mathbb{E}_{\mathcal{H}}[p]| \leq \epsilon$$

ε approximate, orthogonal t-design

Approximate Orthogonal Designs

orthogonal t-design

fools
degree t
on "**rotat**

magnitudes of coeffs sum to 1.

A distribution D on a subset of rot s:

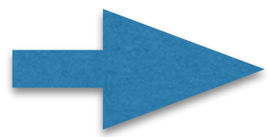
For every degree t Polynomial $p : \mathsf{SO}(n) \to \mathbb{R}$

$$|\mathbb{E}_D[p] - \mathbb{E}_{\mathcal{H}}[p]| \leq \epsilon$$

ε approximate, orthogonal t-design

Approximate Orthogonal Designs

orthogonal t-design



fools
degree t polys
on "**rotation matrices**".

A distribution D on a subset of rotation matrices:

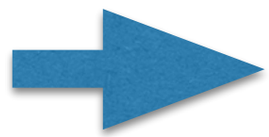
For every degree t Polynomial $p : \mathsf{SO}(n) \to \mathbb{R}$

$$|\mathbb{E}_D[p] - \mathbb{E}_{\mathcal{H}}[p]| \leq \epsilon$$

"fool" low degree polynomials in the entries of the matrices.

Approximate Orthogonal Designs

orthogonal t-design



fools
degree t polys
on "**rotation matrices**".

A distribution D on a subset of rotation matrices:

For every degree t Polynomial $p : \mathsf{SO}(n) \to \mathbb{R}$

$$|\mathbb{E}_D[p] - \mathbb{E}_{\mathcal{H}}[p]| \leq \epsilon$$

real analogs of unitary designs studied in quantum computing

[Seymour-Zaslavsky84, Harrow-Low09,Ambainis-Bouda-Winter09, Brandao-Harrow-Horodecki12]

Approximate Orthogonal Designs

A distribution D on a subset of rotation matrices:

For every degree t Polynomial $p : \mathsf{SO}(n) \to \mathbb{R}$

$$|\mathbb{E}_D[p] - \mathbb{E}_{\mathcal{H}}[p]| \leq \epsilon$$

need explicit construction!

[Brandao-Harrow-Horodecki12]

based on **[Bourgain-Gamburd12]**
"expander walks on Lie Groups"

Approximate Orthogonal Designs

A distribution D on a subset of rotation matrices:

For every degree t Polynomial $p : \mathsf{SO}(n) \to \mathbb{R}$

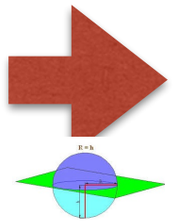
$$|\mathbb{E}_D[p] - \mathbb{E}_{\mathcal{H}}[p]| \leq \epsilon$$

Pseudorandom Projection

1. Draw R according to D.

2. P = first $\sqrt{n}$ rows of R.

Summary



PRG for spherical caps with seed length

$$O(\log(n) + \log(1/\varepsilon) \log\log(1/\varepsilon))$$

- stronger bounds for truncated moment problem.

- pseudorandom projections via the moment method using orthogonal designs.