Pseudorandom generators from polarizing random walks

Kaave Hosseini (UC San Diego)

Eshan Chattopadhyay (Cornell)

Pooya Hatami (UT Austin → Ohio State)

Shachar Lovett (UC San Diego)

Outline

Introduce Pseudorandom generators (PRGs)

New approach to construct PRGs

Open problems

Introduce Pseudorandom generators(PRGs)

General formulation:

Introduce Pseudorandom generators(PRGs)

General formulation:

$\mathcal{F} = \{f : \mathcal{D} \longrightarrow \mathbb{R}\}$ family of functions : tests

Introduce Pseudorandom generators(PRGs)

General formulation:

$\mathcal{F} = \{f : \mathcal{D} \longrightarrow \mathbb{R}\}$ family of functions : tests

U : Random variable uniform over $\mathcal{D}$: truly random object

Introduce Pseudorandom generators(PRGs)

General formulation:

$\mathcal{F} = \{f : \mathcal{D} \longrightarrow \mathbb{R}\}$ family of functions : tests

U : Random variable uniform over $\mathcal{D}$: truly random object

A random variable X over $\mathcal{D}$

Introduce Pseudorandom generators(PRGs)

General formulation:

$\mathcal{F} = \{f : \mathcal{D} \longrightarrow \mathbb{R}\}$ family of functions : tests

U : Random variable uniform over $\mathcal{D}$: truly random object

A random variable X over $\mathcal{D}$ is ε-pseudorandom for $\mathcal{F}$ (X ε-fools $\mathcal{F}$) if

$$|\mathbb{E}f(X) - \mathbb{E}f(U)| \leq \varepsilon \qquad \forall f \in \mathcal{F}$$

Introduce Pseudorandom generators(PRGs)

General formulation:

$\mathcal{F} = \{f: \mathcal{D} \longrightarrow \mathbb{R}\}$ family of functions : tests

U : Random variable uniform over $\mathcal{D}$: truly random object

A random variable X over $\mathcal{D}$ is ε-pseudorandom for $\mathcal{F}$ (X ε-fools $\mathcal{F}$) if

$$|\mathbb{E}f(X) - \mathbb{E}f(U)| \leq \varepsilon \qquad \forall f \in \mathcal{F}$$

Usually dealing with functions $f: \{-1,1\}^n \to \{-1,1\}$

So we take $\mathcal{D} = \{-1,1\}^n$

Introducing Pseudorandom generators(PRGs)

Goal: Construct random variable X:

Introducing Pseudorandom generators(PRGs)

Goal: Construct random variable X:

An algorithm to sample random variable $X \in \{-1,1\}^n$

Introducing Pseudorandom generators(PRGs)

Goal: Construct random variable X:

An algorithm to sample random variable $X \in \{-1,1\}^n$

Use few coin flips in the construction.

Algorithm should be "explicit"/ "easy to compute"

Introducing Pseudorandom generators(PRGs)

Goal: Construct random variable X:

An algorithm to sample random variable $X \in \{-1,1\}^n$

Use few coin flips in the construction.

Algorithm should be “explicit”/ ”easy to compute”

$$G: \{-1,1\}^s \longrightarrow \{-1,1\}^n$$

Introducing Pseudorandom generators(PRGs)

Goal: Construct random variable X:

An algorithm to sample random variable $X \in \{-1,1\}^n$

Use few coin flips in the construction.

Algorithm should be "explicit"/ "easy to compute"

$G: \{-1,1\}^s \longrightarrow \{-1,1\}^n$

$X = G(U_s)$ *where* U_s is uniform over $\{-1,1\}^s$

Introducing Pseudorandom generators(PRGs)

Goal: Construct random variable X:

An algorithm to sample random variable $X \in \{-1,1\}^n$

Use few coin flips in the construction.

Algorithm should be "explicit"/ "easy to compute"

$G: \{-1,1\}^s \longrightarrow \{-1,1\}^n$

$X = G(U_s)$ *where* U_s is uniform over $\{-1,1\}^s$

s *is called seed length*

Example

Example 1: Tests: $\mathbb{F}_2^n$ characters

$$\mathcal{F} = \{f(x) = \prod_{i \in S} x_i \quad : \quad S \subseteq [n]\}$$

X : ε-bias random variable

- PRGs with optimal seed length $O(\log(n/\varepsilon))$ are known.

Some known approaches to construct PRGs

- Use basic PRGs:

Viola[09]: sum of a d many ε-biased PRGs fools degree-d $\mathbb{F}_2$-polynomials.

Some known approaches to construct PRGs

- Pseudorandom restriction:

Ajtai-Wigderson85, Ajt93, CR96, AAI+01, GMR+12, IMP12, GMR13, TX13, GW14, HT17, ST18, …

Step 1: show $\mathcal{F}$ simplifies under random restriction.

Some known approaches to construct PRGs

- Pseudorandom restriction:

Ajtai-Wigderson85, Ajt93, CR96, AAI+01, GMR+12, IMP12, GMR13, TX13, GW14, HT17, ST18, …

Step 1: show $\mathcal{F}$ simplifies under random restriction.

Step 2: derandomize the above statement:

Some known approaches to construct PRGs

- Pseudorandom restriction:

Ajtai-Wigderson85, Ajt93, CR96, AAI+01, GMR+12, IMP12, GMR13, TX13, GW14, HT17, ST18, …

Step 1: show $\mathcal{F}$ simplifies under random restriction.

Step 2: derandomize the above statement:

show $\mathcal{F}$ simplifies under pseudorandom restriction as well.

Some known approaches to construct PRGs

- Pseudorandom restriction:

Ajtai-Wigderson85, Ajt93, CR96, AAI+01, GMR+12, IMP12, GMR13, TX13, GW14, HT17, ST18, …

Step 1: show $\mathcal{F}$ simplifies under random restriction.

Step 2: derandomize the above statement:

show $\mathcal{F}$ simplifies under pseudorandom restriction as well.

Examples of $\mathcal{F}$: AC^0, CNFs, Combinatorial rectangles, Branching programs, …

Some known approaches to construct PRGs

- Pseudorandom restriction:

Ajtai-Wigderson85, Ajt93, CR96, AAI+01, GMR+12, IMP12, GMR13, TX13, GW14, HT17, ST18, …

Step 1: show $\mathcal{F}$ simplifies under random restriction.

Step 2: derandomize the above statement:

show $\mathcal{F}$ simplifies under pseudorandom restriction as well.

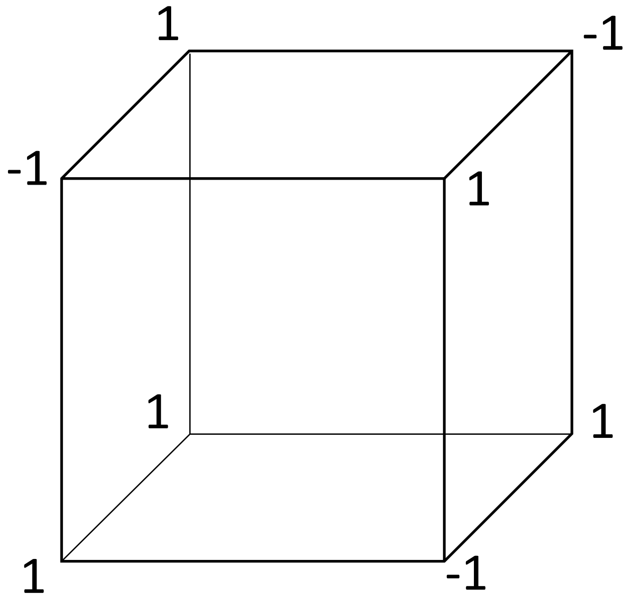
Examples of $\mathcal{F}$: AC^0, CNFs, Combinatorial rectangles, Branching programs, …

- Consequence of this work:

Generic method to do step 2 for arbitrary $\mathcal{F}$.

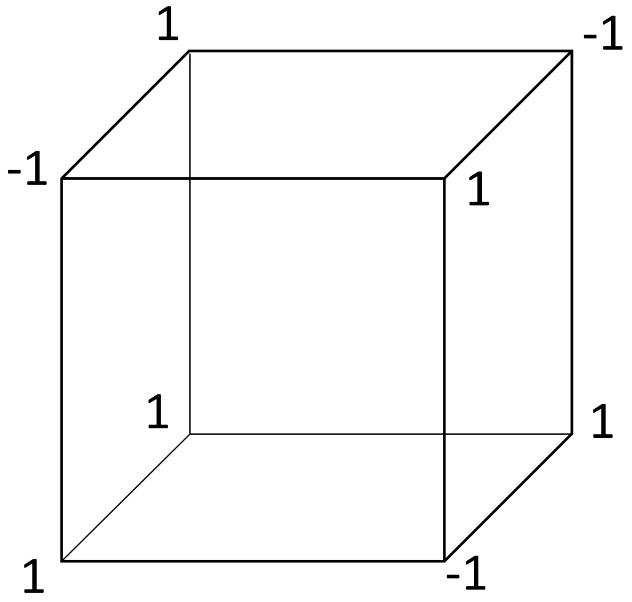
Fractional PRGs

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



Fractional PRGs

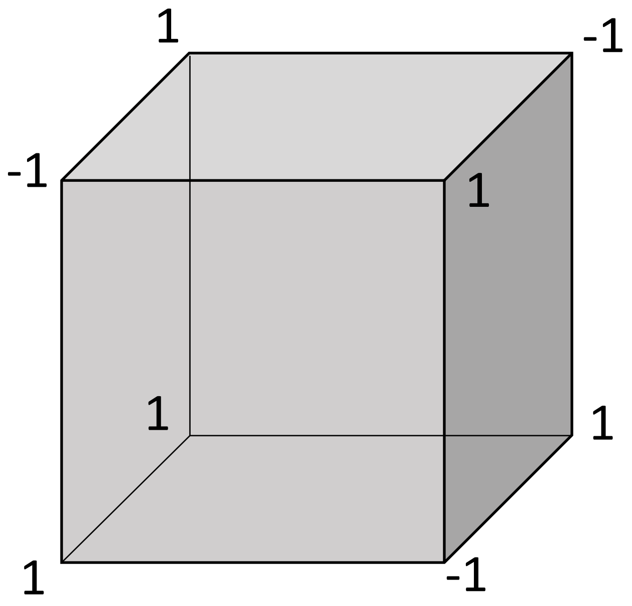
$f : \{-1,1\}^n \to \{-1,1\} \xrightarrow{\text{multi-linear extension}} f : \mathbb{R}^n \to \mathbb{R}$



Fractional PRGs

$f: \{-1,1\}^n \to \{-1,1\} \xrightarrow{\text{multi-linear extension}} f: \mathbb{R}^n \to \mathbb{R}$

Only consider points in $[-1,1]^n$ so $f: [-1,1]^n \to [-1,1]$

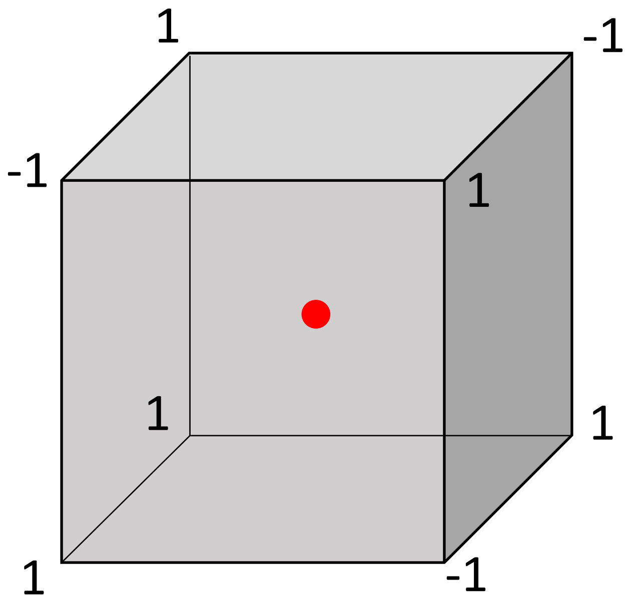


Fractional PRGs

Equivalent definition of PRG:

$X \in \{-1,1\}^n$ ε-fools $\mathcal{F}$ if

$$|\mathbb{E}f(X) - f(0)| \leq \varepsilon, \ \ \forall f \in \mathcal{F}$$



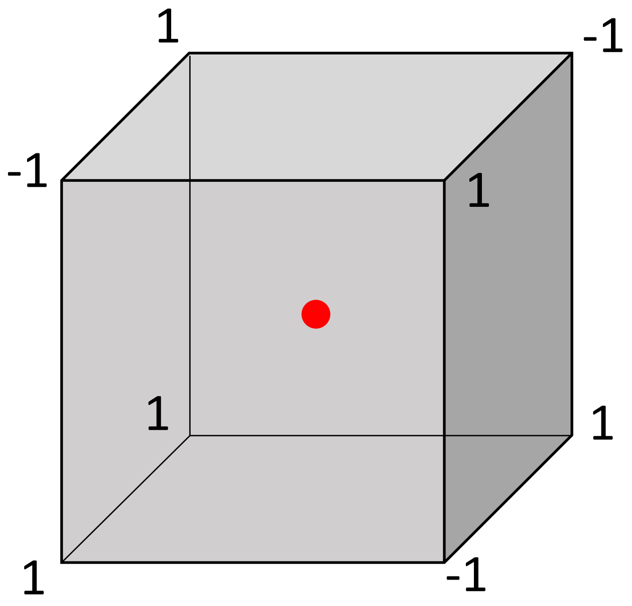
Fractional PRGs

Equivalent definition of PRG:

$X \in \{-1,1\}^n$ ε-fools $\mathcal{F}$ if

$$|\mathbb{E}f(X) - f(0)| \leq \varepsilon, \quad \forall f \in \mathcal{F}$$

because $\mathbb{E}f(U_n) = f(\mathbb{E}U_n) = f(0)$



Fractional PRGs

PRG: random variable $X \in \{-1,1\}^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Fractional PRGs

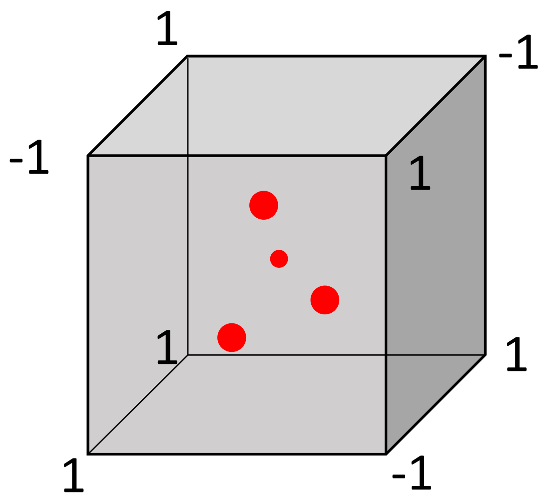
PRG: random variable $X \in \{-1,1\}^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Fractional PRG (f-PRG): random variable $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Fractional PRGs

PRG: random variable $X \in \{-1,1\}^n$ where $|\mathbb{E}f(X) - f(0)| \le \varepsilon$

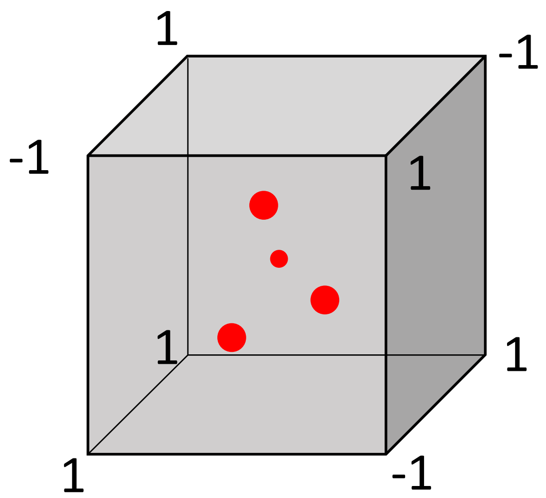
Fractional PRG (f-PRG): random variable $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \le \varepsilon$



Fractional PRGs

PRG: random variable $X \in \{-1,1\}^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Fractional PRG (f-PRG): random variable $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

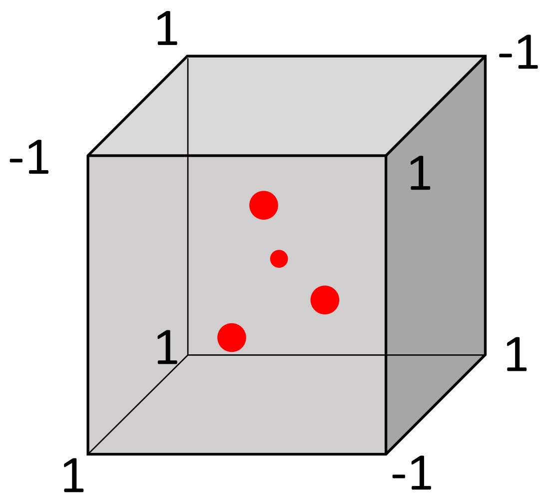


Trivial f-PRG: $X \equiv 0$; we will rule it out later.

Fractional PRGs

PRG: random variable $X \in \{-1,1\}^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Fractional PRG (f-PRG): random variable $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$



Trivial f-PRG: $X \equiv 0$; we will rule it out later.

Question. Are f-PRGs easier to construct than PRGs?

Can f-PRGs be used to construct PRGs?

Fractional PRGs

How to convert $X \in [-1,1]^n$ to $X' \in \{-1,1\}^n$?

Fractional PRGs

How to convert $X \in [-1,1]^n$ to $X' \in \{-1,1\}^n$?

Main idea: do a random walk that converges to $\{-1,1\}^n$

Fractional PRGs

How to convert $X \in [-1,1]^n$ to $X' \in \{-1,1\}^n$?

Main idea: do a random walk that converges to $\{-1,1\}^n$

the steps of the random walk are from X

Fractional PRGs

How to convert $X \in [-1,1]^n$ to $X' \in \{-1,1\}^n$?

Main idea: do a random walk that converges to $\{-1,1\}^n$

the steps of the random walk are from X

Recall: f-PRG is $X = (X_1, \cdots, X_n) \in [-1,1]^n$ where $|\mathbb{E}\, f(X) - f(0)| \leq \varepsilon$

Trivial solution: $X \equiv 0$

Fractional PRGs

How to convert $X \in [-1,1]^n$ to $X' \in \{-1,1\}^n$?

Main idea: do a random walk that converges to $\{-1,1\}^n$

the steps of the random walk are from X

Recall: f-PRG is $X = (X_1, \cdots, X_n) \in [-1,1]^n$ where $|\mathbb{E}\, f(X) - f(0)| \leq \varepsilon$

Trivial solution: $X \equiv 0$

Need to enforce non-triviality: require $\mathbb{E}\, |X_i|^2 \geq p$ for all $i = 1, \ldots, n$

Constructing PRGs from f-PRGs

<u>Main theorem:</u>

Suppose:

$\mathcal{F}$: class of n-variate Boolean functions, closed under restrictions

Constructing PRGs from f-PRGs

<u>Main theorem:</u>

Suppose:

$\mathcal{F}$: class of n-variate Boolean functions, closed under restrictions

$X \in [-1,1]^n$: $\quad |\mathbb{E}f(X) - f(0)| \leq \varepsilon \qquad \forall f \in \mathcal{F}$

Constructing PRGs from f-PRGs

<u>Main theorem:</u>

Suppose:

$\mathcal{F}$: class of n-variate Boolean functions, closed under restrictions

$X \in [-1,1]^n$: $\quad |\mathbb{E}f(X) - f(0)| \leq \varepsilon \qquad \forall f \in \mathcal{F}$

$\mathbb{E}\,|X_i|^2 \geq p$ for all $i = 1, \ldots, n$

Constructing PRGs from f-PRGs

<u>Main theorem:</u>

Suppose:

$\mathcal{F}$: class of n-variate Boolean functions, closed under restrictions

$X \in [-1,1]^n$: $\quad |\mathbb{E}f(X) - f(0)| \leq \varepsilon \qquad \forall f \in \mathcal{F}$

$\mathbb{E}\,|X_i|^2 \geq p$ for all $i = 1, \dots, n$

Then there is $X' = G(X^1, \dots, X^t)$ such that $X^1, \dots, X^t$ are independent copies of X,

Constructing PRGs from f-PRGs

<u>**Main theorem:**</u>

Suppose:

$\mathcal{F}$: class of n-variate Boolean functions, closed under restrictions

$X \in [-1,1]^n$: $\quad |\mathbb{E}f(X) - f(0)| \le \varepsilon \qquad \forall f \in \mathcal{F}$

$\mathbb{E}\,|X_i|^2 \ge p$ for all $i = 1, \ldots, n$

Then there is $X' = G(X^1, \ldots, X^t)$ such that $X^1, \ldots, X^t$ are independent copies of X,

$$X' \in \{-1,1\}^n: \; |\mathbb{E}f(X') - f(0)| \le \varepsilon t \quad \forall f \in \mathcal{F}$$

Constructing PRGs from f-PRGs

<u>Main theorem:</u>

Suppose:

$\mathcal{F}$: class of n-variate Boolean functions, closed under restrictions

$X \in [-1,1]^n$: $\quad |\mathbb{E}f(X) - f(0)| \leq \varepsilon \qquad \forall f \in \mathcal{F}$

$\mathbb{E}\,|X_i|^2 \geq p$ for all $i = 1, \ldots, n$

Then there is $X' = G(X^1, \ldots, X^t)$ such that $X^1, \ldots, X^t$ are independent copies of X,

$$X' \in \{-1,1\}^n: \; |\mathbb{E}f(X') - f(0)| \leq \varepsilon t \quad \forall f \in \mathcal{F}$$

$$t = O\left(\frac{1}{p}\log\left(\frac{n}{\varepsilon}\right)\right)$$

Constructing PRGs from f-PRGs

<u>Main theorem:</u>

Suppose:

$\mathcal{F}$: class of n-variate Boolean functions, closed under restrictions

$X \in [-1,1]^n$: $\quad |\mathbb{E}f(X) - f(0)| \leq \varepsilon \qquad \forall f \in \mathcal{F}$

$\mathbb{E}\,|X_i|^2 \geq p$ for all $i = 1, \dots, n$

Then there is $X' = G(X^1, \dots, X^t)$ such that $X^1, \dots, X^t$ are independent copies of X,

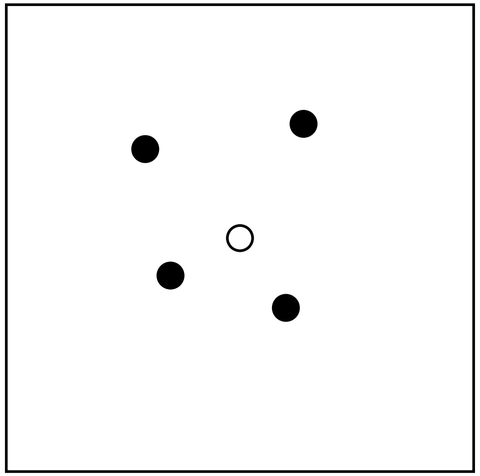
$$X' \in \{-1,1\}^n: \ |\mathbb{E}f(X') - f(0)| \leq \varepsilon t \quad \forall f \in \mathcal{F}$$

$$t = O\left(\frac{1}{p}\log\left(\frac{n}{\varepsilon}\right)\right)$$

- If X has seed length s then X' has seed length ts

Random walk PRG: First step

Goal: use the f-PRG to define a random walk

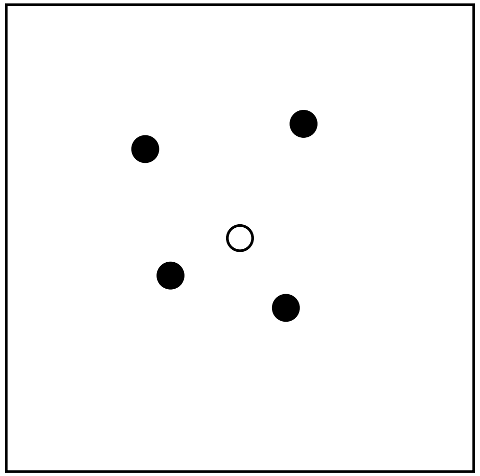


Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1st step from 0

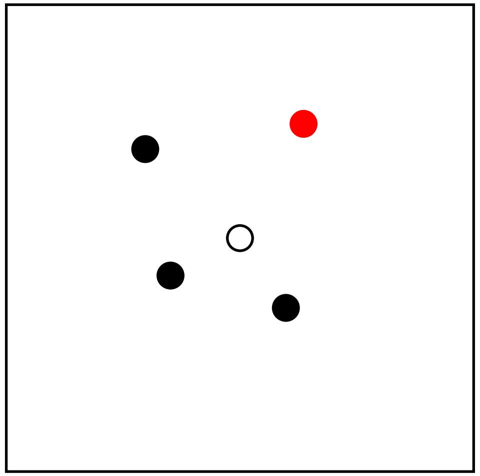


Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1st step from 0

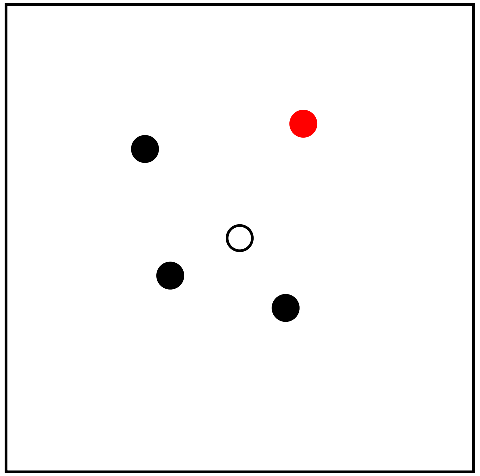


Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1^{st} step from 0



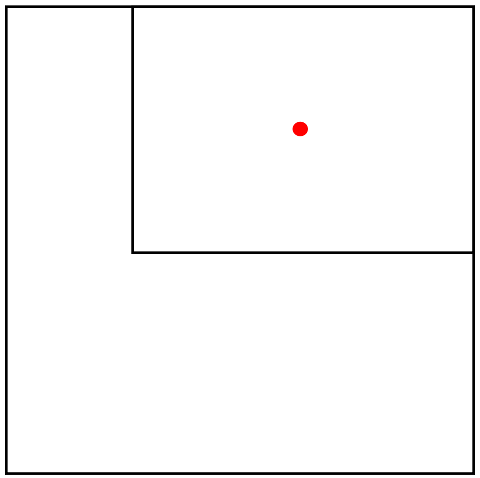
Question: what about the 2^{nd} step?

Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E} f(X) - f(0)| \leq \varepsilon$

Equivalently: 1st step from 0



Question: what about the 2nd step?

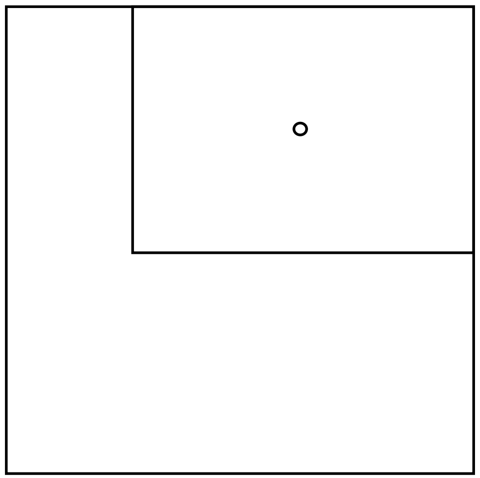
Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1^{st} step from 0

Question: what about the 2^{nd} step?



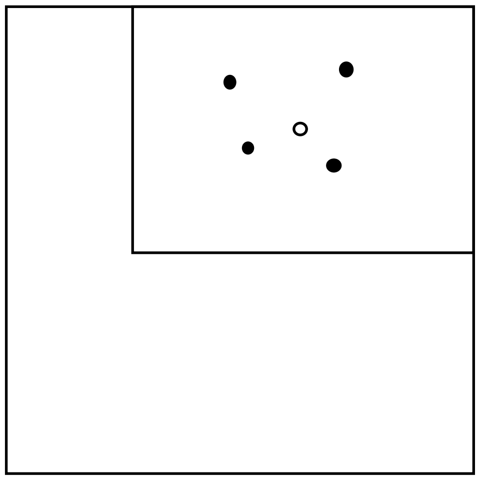
Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1st step from 0

Question: what about the 2nd step?

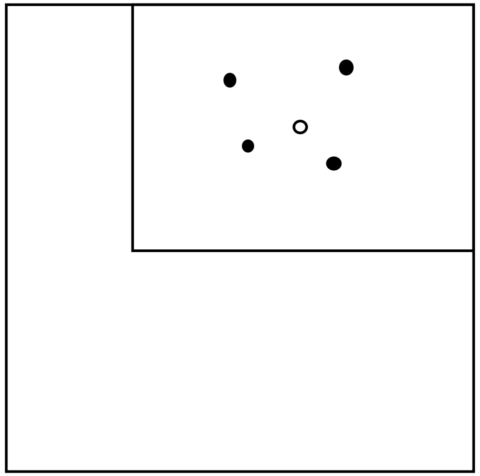


Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1^{st} step from 0



Question: what about the 2^{nd} step?

We have to assume the class is closed under restriction.

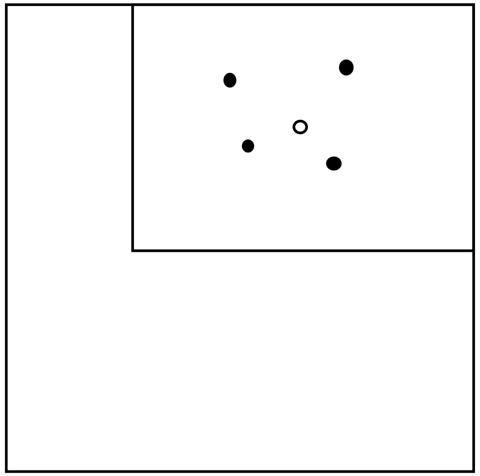
Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1^{st} step from 0

Question: what about the 2^{nd} step?



We have to assume the class is closed under restriction.

Lemma: In second step error is still $\leq \varepsilon$: because function in scaled cube is in the convex hull of restrictions of f.

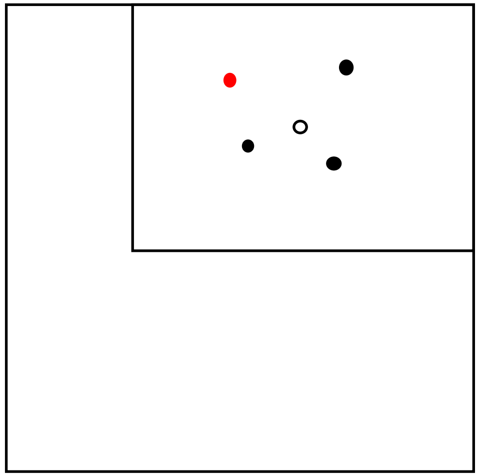
Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1^{st} step from 0

Question: what about the 2^{nd} step?



We have to assume the class is closed under restriction.

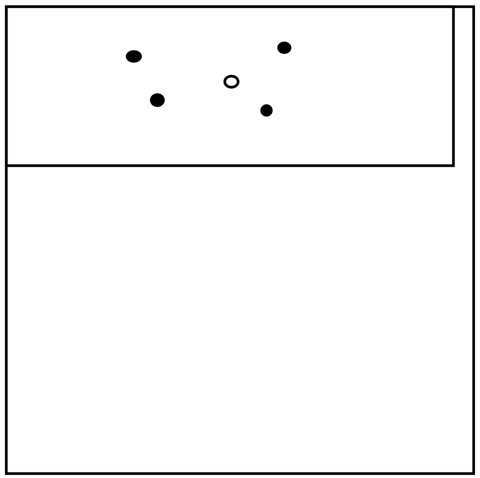
Lemma: In second step error is still $\leq \varepsilon$: because function in scaled cube is in the convex hull of restrictions of f.

Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1st step from 0



Question: what about the 2nd step?

We have to assume the class is closed under restriction.

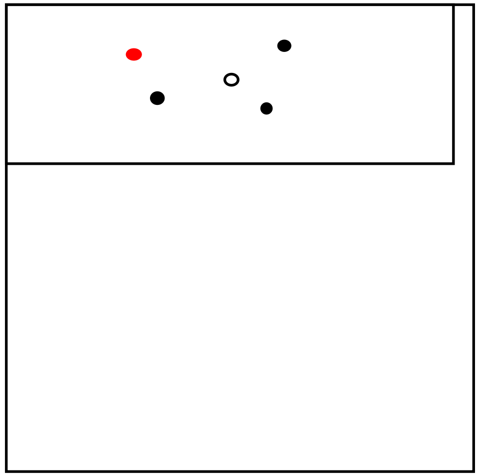
Lemma: In second step error is still $\leq \varepsilon$: because function in scaled cube is in the convex hull of restrictions of f.

Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1st step from 0



Question: what about the 2nd step?

We have to assume the class is closed under restriction.

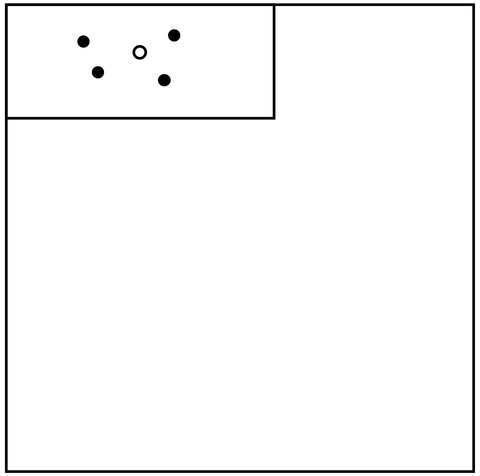
Lemma: In second step error is still $\leq \varepsilon$: because function in scaled cube is in the convex hull of restrictions of f.

Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1st step from 0



Question: what about the 2nd step?

We have to assume the class is closed under restriction.

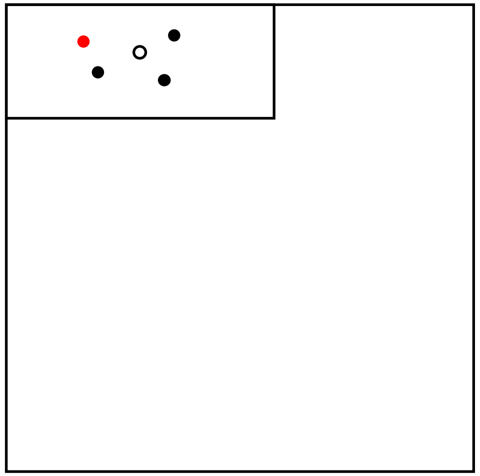
Lemma: In second step error is still $\leq \varepsilon$: because function in scaled cube is in the convex hull of restrictions of f.

Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \le \varepsilon$

Equivalently: 1st step from 0



Question: what about the 2nd step?

We have to assume the class is closed under restriction.

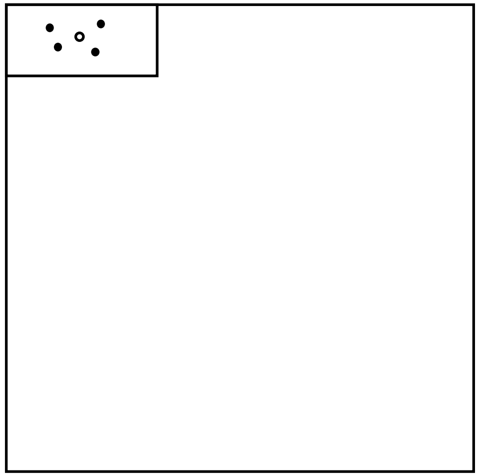
Lemma: In second step error is still $\le \varepsilon$: because function in scaled cube is in the convex hull of restrictions of f.

Random walk PRG: First step

Goal: use the f-PRG to define a random walk

f-PRG: $X \in [-1,1]^n$ where $|\mathbb{E}f(X) - f(0)| \leq \varepsilon$

Equivalently: 1st step from 0



Question: what about the 2nd step?

We have to assume the class is closed under restriction.

Lemma: In second step error is still $\leq \varepsilon$: because function in scaled cube is in the convex hull of restrictions of f.

Proof of main theorem: fast convergence

It’s enough to prove it for one dimension: so let X be a r.v. on $[-1,1]$

Proof of main theorem: fast convergence

It’s enough to prove it for one dimension: so let X be a r.v. on $[-1,1]$

Lemma: Let $Y_0 = 0$, $Y_t = Y_{t-1} + (1 - |Y_{t-1}|)X_t$ be a random walk with $\mathbb{E}X_i = 0$.

Proof of main theorem: fast convergence

It's enough to prove it for one dimension: so let X be a r.v. on $[-1,1]$

Lemma: Let $Y_0 = 0\,, Y_t = Y_{t-1} + (1 - |Y_{t-1}|)X_t$ be a random walk with $\mathbb{E}X_i = 0$.

Then after $O\left(\frac{1}{\mathbb{E}|X|^2}\log\left(\frac{1}{\varepsilon}\right)\right)$ steps, w.h.p $1 - |Y_t| \leq \varepsilon$

Proof of main theorem: fast convergence

It's enough to prove it for one dimension: so let X be a r.v. on $[-1,1]$

Lemma: Let $Y_0 = 0\,, Y_t = Y_{t-1} + (1 - |Y_{t-1}|)X_t$ be a random walk with $\mathbb{E}X_i = 0$.

Then after $O\left(\frac{1}{\mathbb{E}|X|^2}\log\left(\frac{1}{\varepsilon}\right)\right)$ steps, w.h.p $1 - |Y_t| \leq \varepsilon$

Proof: always we have $1 - |Y_i| \quad < \; (1 - \; |Y_{i-1}|)(1 - \; X_i)$

Proof of main theorem: fast convergence

It's enough to prove it for one dimension: so let X be a r.v. on $[-1,1]$

Lemma: Let $Y_0 = 0\,, Y_t = Y_{t-1} + (1 - |Y_{t-1}|)X_t$ be a random walk with $\mathbb{E}X_i = 0$.

Then after $O\left(\frac{1}{\mathbb{E}|X|^2}\log\left(\frac{1}{\varepsilon}\right)\right)$ steps, w.h.p $1 - |Y_t| \leq \varepsilon$

Proof: always we have

$$1 - |Y_i| < (1 - |Y_{i-1}|)(1 - X_i)$$

$$\mathbb{E}(1 - |Y_i|) < \mathbb{E}(1 - |Y_{i-1}|)\mathbb{E}(1 - X_i)$$

Proof of main theorem: fast convergence

It's enough to prove it for one dimension: so let X be a r.v. on $[-1,1]$

Lemma: Let $Y_0 = 0$, $Y_t = Y_{t-1} + (1 - |Y_{t-1}|)X_t$ be a random walk with $\mathbb{E}X_i = 0$.

Then after $O\left(\frac{1}{\mathbb{E}|X|^2}\log\left(\frac{1}{\varepsilon}\right)\right)$ steps, w.h.p $1 - |Y_t| \le \varepsilon$

Proof: always we have

$$1 - |Y_i| < (1 - |Y_{i-1}|)(1 - X_i)$$

$$\mathbb{E}(1 - |Y_i|) < \mathbb{E}(1 - |Y_{i-1}|)\mathbb{E}(1 - X_i)$$

$\mathbb{E}(1 - X_i) = 1$, however, $\mathbb{E}\sqrt{(1 - X_i)} < 1 - \frac{\mathbb{E}X_i^2}{8} = 1 - c$

Proof of main theorem: fast convergence

It's enough to prove it for one dimension: so let X be a r.v. on $[-1,1]$

Lemma: Let $Y_0 = 0\,, Y_t = Y_{t-1} + (1 - |Y_{t-1}|)X_t$ be a random walk with $\mathbb{E}X_i = 0$.

Then after $O\left(\frac{1}{\mathbb{E}|X|^2}\log\left(\frac{1}{\varepsilon}\right)\right)$ steps, w.h.p $1 - |Y_t| \leq \varepsilon$

Proof: always we have

$$1 - |Y_i| < (1 - |Y_{i-1}|)(1 - X_i)$$

$$\mathbb{E}(1 - |Y_i|) < \mathbb{E}(1 - |Y_{i-1}|)\mathbb{E}(1 - X_i)$$

$\mathbb{E}(1 - X_i) = 1$, however, $\mathbb{E}\sqrt{(1 - X_i)} < 1 - \frac{\mathbb{E}X_i^2}{8} = 1 - c$

$$\mathbb{E}\sqrt{1 - |Y_i|} < \mathbb{E}\sqrt{(1 - |Y_{i-1}|)}\,(1 - c) < (1 - c)^i \qquad \blacksquare$$

Proof of main theorem: fast convergence

It's enough to prove it for one dimension: so let X be a r.v. on $[-1,1]$

Lemma: Let $Y_0 = 0\,, Y_t = Y_{t-1} + (1 - |Y_{t-1}|)X_t$ be a random walk with $\mathbb{E}X_i = 0$.

Then after $O\left(\frac{1}{\mathbb{E}|X|^2}\log\left(\frac{1}{\varepsilon}\right)\right)$ steps, w.h.p $1 - |Y_t| \le \varepsilon$

Proof: always we have

$$1 - |Y_i| < (1 - |Y_{i-1}|)(1 - X_i)$$

$$\mathbb{E}(1 - |Y_i|) < \mathbb{E}(1 - |Y_{i-1}|)\mathbb{E}(1 - X_i)$$

$\mathbb{E}(1 - X_i) = 1$, however, $\mathbb{E}\sqrt{(1 - X_i)} < 1 - \frac{\mathbb{E}X_i^2}{8} = 1 - c$

$$\mathbb{E}\sqrt{1 - |Y_i|} < \mathbb{E}\sqrt{(1 - |Y_{i-1}|)}\,(1 - c) < (1 - c)^i \qquad \blacksquare$$

Round to sign$\{Y_t\}$ once the random walk is close enough to the boundary

Construction of fractional PRGs

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

Fourier coefficients: $\hat{f}(S) = \mathbb{E}\, f(x) \prod_{i \in S} x_i$, $S \subseteq [n]$

Construction of fractional PRGs

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

Fourier coefficients: $\hat{f}(S) = \mathbb{E}\, f(x) \prod_{i \in S} x_i$, $S \subseteq [n]$

f has bounded Fourier growth if

$$\sum_{S:|S|=k} |\hat{f}(S)| \le c^k \quad \forall k \ge 1$$

$\mathrm{c} = n$ is a trivial bound.

Construction of fractional PRGs

- $f:\{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \leq c^k \qquad \forall k \geq 1$

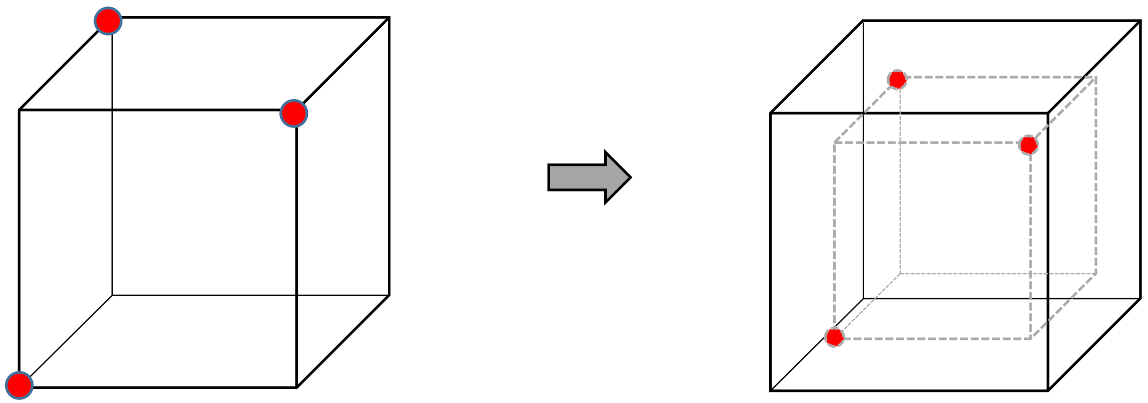
Construction of fractional PRGs

- $f:\{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \le c^k \qquad \forall k \ge 1$

- Let $Y \in \{-1,1\}^n$ be a ε-bias r.v. : $|\mathbb{E} \prod_{i \in S} Y_i| < \varepsilon$, $\forall S \subseteq [n]\,, S \neq \phi$

Construction of fractional PRGs

- $f:\{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \le c^k \qquad \forall k \ge 1$
- Let $Y \in \{-1,1\}^n$ be a ε-bias r.v. : $|\mathbb{E} \prod_{i \in S} Y_i| < \varepsilon$, $\forall S \subseteq [n]\,, S \neq \phi$
- Construction: $X = \frac{1}{2c} Y$, note: $X \in \left\{-\frac{1}{2c}, \frac{1}{2c}\right\}^n$



Construction of fractional PRGs

Proof :

$f\colon\{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \le c^k \qquad \forall k \ge 1$

Construction: $X = \frac{1}{2c}Y$, $Y \in \{-1,1\}^n$ is ε-bias r.v: $|\mathbb{E}\prod_{i\in S} Y_i| < \varepsilon$, $\forall S \subseteq [n]$,

Construction of fractional PRGs

Proof :

$f: \{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \le c^k \qquad \forall k \ge 1$

Construction: $X = \frac{1}{2c} Y$, $Y \in \{-1,1\}^n$ is ε-bias r.v: $|\mathbb{E} \prod_{i \in S} Y_i| < \varepsilon$, $\forall S \subseteq [n]$,

$$|\mathbb{E} f(X) - f(0)| = \left|\sum_{S \neq \emptyset} \hat{f}(S) \cdot \mathbb{E} \prod_{i \in S} X_i\right|$$

Construction of fractional PRGs

Proof :

$f:\{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \leq c^k \qquad \forall k \geq 1$

Construction: $X = \frac{1}{2c}Y$, $Y \in \{-1,1\}^n$ is ε-bias r.v: $|\mathbb{E}\prod_{i\in S} Y_i| < \varepsilon$, $\forall S \subseteq [n]$,

$$|\mathbb{E}f(X) - f(0)| = \left|\sum_{S\neq\emptyset} \hat{f}(S) \cdot \mathbb{E}\prod_{i\in S} X_i\right|$$
$$\leq \sum_{S\neq\emptyset} \left|\hat{f}(S)\right| |\mathbb{E}\prod_{i\in S} X_i|$$

Construction of fractional PRGs

Proof :

$f: \{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \leq c^k \qquad \forall k \geq 1$

Construction: $X = \frac{1}{2c} Y$, $Y \in \{-1,1\}^n$ is ε-bias r.v: $|\mathbb{E} \prod_{i \in S} Y_i| < \varepsilon$, $\forall S \subseteq [n]$,

$$
\begin{aligned}
|\mathbb{E} f(X) - f(0)| &= \left|\sum_{S \neq \emptyset} \hat{f}(S) \cdot \mathbb{E} \prod_{i \in S} X_i\right| \\
&\leq \sum_{S \neq \emptyset} \left|\hat{f}(S)\right| |\mathbb{E} \prod_{i \in S} X_i| \\
&\leq \sum_{S \neq \emptyset} \left|\hat{f}(S)\right| \left(\frac{1}{2c}\right)^{|S|} |\mathbb{E} \prod_{i \in S} Y_i|
\end{aligned}
$$

Construction of fractional PRGs

Proof :

$f:\{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \le c^k \qquad \forall k \ge 1$

Construction: $X = \frac{1}{2c} Y$, $Y \in \{-1,1\}^n$ is ε-bias r.v: $|\mathbb{E} \prod_{i\in S} Y_i| < \varepsilon$, $\forall S \subseteq [n]$,

$$
\begin{aligned}
|\mathbb{E} f(X) - f(0)| &= \left|\sum_{S\neq\emptyset} \hat{f}(S) \cdot \mathbb{E} \prod_{i\in S} X_i\right| \\
&\le \sum_{S\neq\emptyset} \left|\hat{f}(S)\right| |\mathbb{E} \prod_{i\in S} X_i| \\
&\le \sum_{S\neq\emptyset} \left|\hat{f}(S)\right| \left(\frac{1}{2c}\right)^{|S|} |\mathbb{E} \prod_{i\in S} Y_i| \\
&\le \sum_{S\neq\emptyset} \left|\hat{f}(S)\right| \left(\frac{1}{2c}\right)^{|S|} \varepsilon
\end{aligned}
$$

Construction of fractional PRGs

Proof :

$f: \{-1,1\}^n \to \{-1,1\}$ with $\sum_{S:|S|=k} |\hat{f}(S)| \le c^k \qquad \forall k \ge 1$

Construction: $X = \frac{1}{2c} Y$, $Y \in \{-1,1\}^n$ is ε-bias r.v: $|\mathbb{E} \prod_{i \in S} Y_i \,| < \varepsilon$, $\forall S \subseteq [n]$,

$$
\begin{aligned}
|\mathbb{E} f(X) - f(0)| &= \left| \sum_{S \neq \emptyset} \hat{f}(S) \cdot \mathbb{E} \prod_{i \in S} X_i \right| \\
&\le \sum_{S \neq \emptyset} \left| \hat{f}(S) \right| |\mathbb{E} \prod_{i \in S} X_i| \\
&\le \sum_{S \neq \emptyset} \left| \hat{f}(S) \right| \left(\frac{1}{2c} \right)^{|S|} |\mathbb{E} \prod_{i \in S} Y_i| \\
&\le \sum_{S \neq \emptyset} \left| \hat{f}(S) \right| \left(\frac{1}{2c} \right)^{|S|} \varepsilon \\
&\le \sum_{k \ge 1} c^k \left(\frac{1}{2c} \right)^{k} \varepsilon
\end{aligned}
$$

Construction of fractional PRGs

$\sum_{S:|S|=k} |\hat{f}(S)| \leq c^k \quad \forall k \geq 1,$

seed length = $c^2 \log\left(\frac{n}{\epsilon}\right)\left(\log\log n + \log\left(\frac{1}{\epsilon}\right)\right)$

Functions with sensitivity s:

Gopalan-Servedio-Wigderson'16: $c = s$

Prev. seed-length:

$2^{\sqrt{s}} \log n$ [Hatami-Tal 17]

Construction of fractional PRGs

$\sum_{S:|S|=k} |\hat{f}(S)| \leq c^k \quad \forall k \geq 1,$

seed length = $c^2 \log\left(\frac{n}{\epsilon}\right)\left(\log\log n + \log\left(\frac{1}{\epsilon}\right)\right)$

Functions with sensitivity s:

Gopalan-Servedio-Wigderson'16: $c = s$

Permutation branching programs of width w:

Reingold-Steinke-Vadhan'13: $c = w^2$

Prev. seed-length:

$2^{\sqrt{s}} \log n$ [Hatami-Tal 17]

Construction of fractional PRGs

$\sum_{S:|S|=k} |\hat{f}(S)| \leq c^k \quad \forall k \geq 1,$

seed length = $c^2 \log\left(\frac{n}{\epsilon}\right)\left(\log\log n + \log\left(\frac{1}{\epsilon}\right)\right)$

Functions with sensitivity s:

Gopalan-Servedio-Wigderson'16: $c = s$

Permutation branching programs of width w:

Reingold-Steinke-Vadhan'13: $c = w^2$

Read once branching programs of width w:

Chattopadhyay-Hatami-Reingold-Tal'18: $c = \log^w n$

Prev. seed-length:

$2^{\sqrt{s}} \log n$ [Hatami-Tal 17]

Construction of fractional PRGs

$\sum_{S:|S|=k} |\hat{f}(S)| \leq c^k \quad \forall k \geq 1,$

seed length = $c^2 \log\left(\frac{n}{\epsilon}\right)\left(\log\log n + \log\left(\frac{1}{\epsilon}\right)\right)$

Functions with sensitivity s:

Gopalan-Servedio-Wigderson'16: $c = s$

Permutation branching programs of width w:

Reingold-Steinke-Vadhan'13: $c = w^2$

Read once branching programs of width w:

Chattopadhyay-Hatami-Reingold-Tal'18: $c = \log^w n$

Circuits of depth d:

Tal'17: $c = \log^d s$

Prev. seed-length:

$2^{\sqrt{s}} \log n$ [Hatami-Tal 17]

Questions

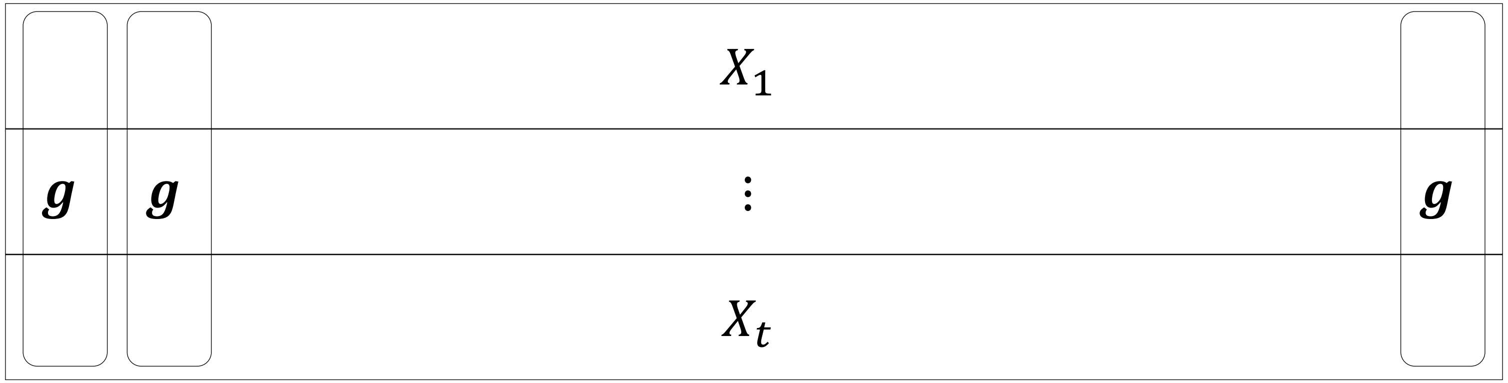
- One way to view our construction is as follows

X_1
$\vdots$
X_t

- Put the f-PRGs as rows of a $t \times n$ matrix

Questions

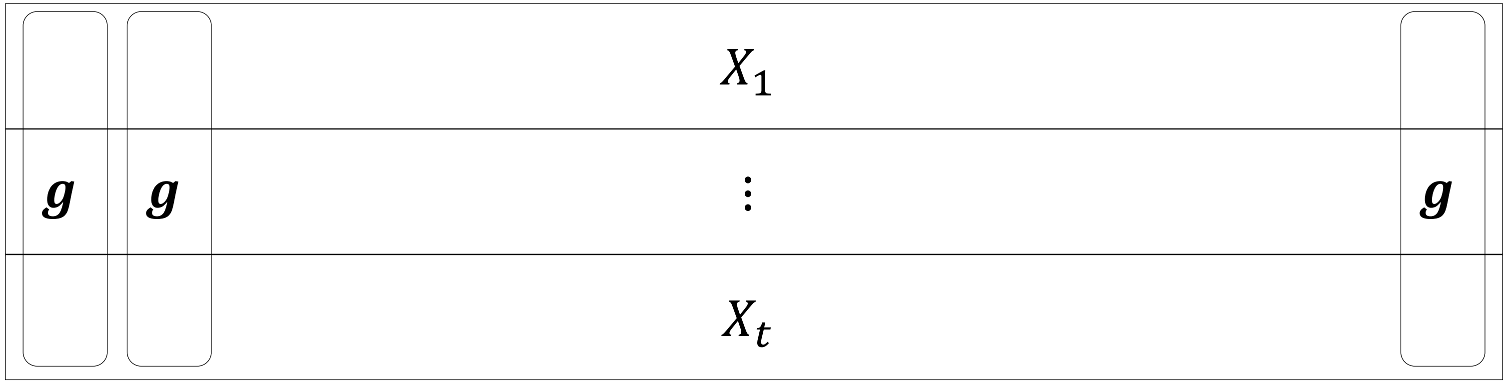
- One way to view our construction is as follows



- Put the f-PRGs as rows of a $t \times n$ matrix
- Apply a “random walk gadget” g on each column: $g: [-1,1]^t \to \{-1,1\}$

Questions

- One way to view our construction is as follows



- Put the f-PRGs as rows of a $t \times n$ matrix
- Apply a "random walk gadget" g on each column: $g: [-1,1]^t \to \{-1,1\}$

$$G(X_1, \dots, X_t) = \left(g(X_{1,1}, \dots, X_{t,1}), \dots, g(X_{1,n}, \dots, X_{t,n})\right)$$

Questions

- If function class $\mathcal{F}$ is “simple”, can we terminate the random walk earlier?

Questions

- If function class $\mathcal{F}$ is “simple”, can we terminate the random walk earlier?
- Can we construct hitting sets this way?

Thank you!