Poly-logarithmic independence fools AC^0

K Dinesh
CS11M019

IIT Madras

April 18, 2012

Outline

Outline

1. Introduction
2. Main Theorem

Outline

Outline

Outline

Outline

Motivation

- AC^0 circuits have been identified to have limitations in computation ability.
- Natural question : Can we generate pseudorandom distributions that "looks random" ?
- In general : No answer !

Motivation

- AC^0 circuits have been identified to have limitations in computation ability.
- Natural question : Can we generate pseudorandom distributions that "looks random" ?
- In general : No answer !
- Let us focus on circuits and ask this question.
- Say a circuit uses a set of random bits (gets as input) for computation.

Motivation

- AC^0 circuits have been identified to have limitations in computation ability.
- Natural question : Can we generate pseudorandom distributions that "looks random" ?
- In general : No answer !
- Let us focus on circuits and ask this question.
- Say a circuit uses a set of random bits (gets as input) for computation.

Question

Are there prob. distributions which circuit cannot distinguish, i.e. the circuit will compute the same value on expectation ?

Definition and Notations

For a boolean function $F : \{0,1\}^n \to \{0,1\}$, distribution $\mu : \{0,1\}^n \to$ R, we denote

Notations

- $E_\mu[F]$: Expected value of F when inputs are drawn according to μ.
- $\mu(X)$: Probability of event X under μ.
- $E[F]$: Expected value of F when inputs are drawn uniformly.
- $Pr(X)$: Probability of event X under uniform distribution.

Definition and Notations

For a boolean function $F : \{0,1\}^n \to \{0,1\}$, distribution $\mu : \{0,1\}^n \to$ R, we denote

Notations

- $E_\mu[F]$: Expected value of F when inputs are drawn according to μ.
- $\mu(X)$: Probability of event X under μ.
- $E[F]$: Expected value of F when inputs are drawn uniformly.
- $Pr(X)$: Probability of event X under uniform distribution.

r-independence

A probability distribution μ defined on $\{0,1\}^n$ is said to be r-independent for $(r \leq n)$ if, $\forall I \subseteq [n], |I| = r$, $i_j \in I$,

$$\mu(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) = U(x_{i_1}, x_{i_2}, \ldots, x_{i_r}) = \frac{1}{2^r}$$

Definition

ϵ-fooling

A distribution μ is said to ϵ-fool a circuit C computing a boolean function F if,

$$|E_\mu(F) - E(F)| < \epsilon$$

ℓ_2 Norm

For a boolean function $F : \{0,1\}^n \to \{0,1\}$ is defined as,

$$||F||_2^2 = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} |F(x)|^2$$

Problem statement

Problem

Given a AC^0 circuit of size m depth d computing F, for every r-independent distribution μ on $\{0,1\}^n$, can μ ϵ-fool C ?

Problem statement

Problem

Given a AC^0 circuit of size m depth d computing F, for every r-independent distribution μ on $\{0,1\}^n$, can μ ϵ-fool C ? How large r has to be ?

Problem statement

Problem

Given a AC^0 circuit of size m depth d computing F, for every r-independent distribution μ on $\{0,1\}^n$, can μ ϵ-fool C ? How large r has to be ?

- First asked by Linial and Nisan in 1990. Conjectured that polylogarithmic independence suffices.
- Shown to be possible for depth to AC^0 circuits (of size m) by Louay Bazzi in 2007 where $r = O(\log^2 \frac{m}{\epsilon})$ for DNF formulas.
- The conjucture has been finally proved

Problem statement

Problem

Given a AC^0 circuit of size m depth d computing F, for every r-independent distribution μ on $\{0,1\}^n$, can μ ϵ-fool C ? How large r has to be ?

- First asked by Linial and Nisan in 1990. Conjectured that polylogarithmic independence suffices.
- Shown to be possible for depth to AC^0 circuits (of size m) by Louay Bazzi in 2007 where $r = O(\log^2 \frac{m}{\epsilon})$ for DNF formulas.
- The conjucture has been finally proved in this paper !

Outline

1. Introduction
2. Main Theorem
   - Proof Outline
   - Construction of approximation polynomial
3. Proof of Theorem

Braverman's Theorem

Theorem

For any AC^0 circuit C of size m and depth d computing F, any r-independent circuit ϵ-fools C where.

$$r = \left(\log\left(\frac{m}{\epsilon}\right)\right)^{O(d^2)}$$

Proof Techniques used :

- Razbarov-Smolensky method of approximation of boolean functions by low degree polynomial.

Braverman's Theorem

Theorem

For any AC^0 circuit C of size m and depth d computing F, any r-independent circuit ϵ-fools C where.

$$r = \left(\log\left(\frac{m}{\epsilon}\right)\right)^{O(d^2)}$$

Proof Techniques used :

- Razbarov-Smolensky method of approximation of boolean functions by low degree polynomial.
- Linial-Mansoor-Nisan [LMN] result that gives low degree approximation for functions computable in AC^0.

Braverman's Theorem

Theorem

For any AC^0 circuit C of size m and depth d computing F, any r-independent circuit ϵ-fools C where.

$$r = \left(\log\left(\frac{m}{\epsilon}\right)\right)^{O(d^2)}$$

Proof Techniques used :

- Razbarov-Smolensky method of approximation of boolean functions by low degree polynomial.
- Linial-Mansoor-Nisan [LMN] result that gives low degree approximation for functions computable in AC^0.
- Linear of Expectation.

Outline

Proof Outline

Fix F to be the function computed by the circuit and f to be its approximation.

- Raz-Smol. method gives us an approximating polynomial that agree on all but a small fraction of inputs.

Proof Outline

Fix F to be the function computed by the circuit and f to be its approximation.

- Raz-Smol. method gives us an approximating polynomial that agree on all but a small fraction of inputs.
- Does not guarentee anything about their expected values : can be highly varying on non-agreeing points.

Proof Outline

Fix F to be the function computed by the circuit and f to be its approximation.

- Raz-Smol. method gives us an approximating polynomial that agree on all but a small fraction of inputs.
- Does not guarentee anything about their expected values : can be highly varying on non-agreeing points.
- Key observation : The error indicator function $\mathcal{E} = 0$ if $F = f$, 1 if $F \neq f$ can be computed by an AC^0 circuit.

Proof Outline

Fix F to be the function computed by the circuit and f to be its approximation.

- Raz-Smol. method gives us an approximating polynomial that agree on all but a small fraction of inputs.
- Does not guarentee anything about their expected values : can be highly varying on non-agreeing points.
- Key observation : The error indicator function $\mathcal{E} = 0$ if $F = f$, 1 if $F \neq f$ can be computed by an AC^0 circuit.
- Now apply LMN, get an approximation $\tilde{\mathcal{E}}$ for $\mathcal{E}$.
- Define $f' = f(1 - \tilde{\mathcal{E}})$.

Proof Outline

Fix F to be the function computed by the circuit and f to be its approximation.

- Raz-Smol. method gives us an approximating polynomial that agree on all but a small fraction of inputs.
- Does not guarentee anything about their expected values : can be highly varying on non-agreeing points.
- Key observation : The error indicator function $\mathcal{E} = 0$ if $F = f$, 1 if $F \neq f$ can be computed by an AC^0 circuit.
- Now apply LMN, get an approximation $\tilde{\mathcal{E}}$ for $\mathcal{E}$.
- Define $f' = f(1 - \tilde{\mathcal{E}})$.
- Then argue that $||F - f'||_2^2$ is small for both uniform distribution and r-independent distribution μ.

Outline

Construction of approximation polynomial

Lemma

Let μ be any probability distribution on $\{0,1\}^n$. Let F be a boolean function computed by a circuit of depth d and size m. Then for any parameter s,

Construction of approximation polynomial

Lemma

Let μ be any probability distribution on $\{0,1\}^n$. Let F be a boolean function computed by a circuit of depth d and size m. Then for any parameter s,

- there is a degree $r = (s \cdot \log m)^d$ polynomial f.

Construction of approximation polynomial

Lemma

Let μ be any probability distribution on $\{0,1\}^n$. Let F be a boolean function computed by a circuit of depth d and size m. Then for any parameter s,

- there is a degree $r = (s \cdot \log m)^d$ polynomial f.
- error function $\mu(\mathcal{E}(x) = 1) < (0.82)^s m$
- $\mathcal{E}(x) = 0 \implies f(x) = F(x)$.

Construction of approximation polynomial

Lemma

Let μ be any probability distribution on $\{0,1\}^n$. Let F be a boolean function computed by a circuit of depth d and size m. Then for any parameter s,

- there is a degree $r = (s \cdot \log m)^d$ polynomial f.
- error function $\mu(\mathcal{E}(x) = 1) < (0.82)^s m$
- $\mathcal{E}(x) = 0 \implies f(x) = F(x)$.
- $\mathcal{E}$ can computed by a depth $(d+3)$ circuit.

Construction of approximation polynomial

Lemma

Let μ be any probability distribution on $\{0,1\}^n$. Let F be a boolean function computed by a circuit of depth d and size m. Then for any parameter s,

- there is a degree $r = (s \cdot \log m)^d$ polynomial f.
- error function $\mu(\mathcal{E}(x) = 1) < (0.82)^s m$
- $\mathcal{E}(x) = 0 \implies f(x) = F(x)$.
- $\mathcal{E}$ can computed by a depth $(d+3)$ circuit.

Base case : $x_i \to x_i$, $\overline{x_i} \to 1 - x_i$.

Construction of approximation polynomial

Lemma

Let μ be any probability distribution on $\{0,1\}^n$. Let F be a boolean function computed by a circuit of depth d and size m. Then for any parameter s,

- there is a degree $r = (s \cdot \log m)^d$ polynomial f.
- error function $\mu(\mathcal{E}(x) = 1) < (0.82)^s m$
- $\mathcal{E}(x) = 0 \implies f(x) = F(x)$.
- $\mathcal{E}$ can computed by a depth $(d+3)$ circuit.

Base case : $x_i \to x_i$, $\overline{x_i} \to 1 - x_i$.

- Induction case : (AND case, OR is symmetric)
  Let $G = G_1 \wedge \mathrm{G}_2 \ldots \wedge G_k$ and their approximations $g_1, g_2, \ldots, g_k$ for $k < m$.

Construction of approximation polynomial

Lemma

Let μ be any probability distribution on $\{0,1\}^n$. Let F be a boolean function computed by a circuit of depth d and size m. Then for any parameter s,

- there is a degree $r = (s \cdot \log m)^d$ polynomial f.
- error function $\mu(\mathcal{E}(x) = 1) < (0.82)^s m$
- $\mathcal{E}(x) = 0 \implies f(x) = F(x)$.
- $\mathcal{E}$ can computed by a depth $(d+3)$ circuit.

Base case : $x_i \to x_i$, $\overline{x_i} \to 1 - x_i$.

- Induction case : (AND case, OR is symmetric)
  Let $G = G_1 \wedge G_2 \ldots \wedge G_k$ and their approximations $g_1, g_2, \ldots, g_k$ for $k < m$.
- Assume $k = 2^l$.
- Pick l subsets from $\{1, 2, \ldots, k\}$, i^{th} set is picked with probability 2^{-i}.

Construction of approximation polynomial (Cont...)

- Repeat this s times (independently) to get $t = sl = s \log k$ subsets.
- The approximation polynomial for the AND gate is

$$f = \prod_{i=1}^{t} \left(\sum_{j \in S_i} g_j - |S_i| + 1 \right)$$

.

- Need to bound $P[F \neq f]$.
- Fix $G_1(x), G_2(x), \ldots, G_k(x)$.

What is error probability for a random choice of set S_i ?

- $G(x) = 1 \implies$ No error since all $G_j(x) = 1$.
- $G(x) = 0 \implies$ At least one $G_j(x) = 0$.

Construction of approximation polynomial (Cont...)

- Repeat this s times (independently) to get $t = sl = s \log k$ subsets.
- The approximation polynomial for the AND gate is

$$f = \prod_{i=1}^{t} \left(\sum_{j \in S_i} g_j - |S_i| + 1 \right)$$

.

- Need to bound $P[F \neq f]$.
- Fix $G_1(x), G_2(x), \ldots, G_k(x)$.

What is error probability for a random choice of set S_i ?

- $G(x) = 1 \implies$ No error since all $G_j(x) = 1$.
- $G(x) = 0 \implies$ At least one $G_j(x) = 0$. We ask : when will

$$\prod_{i=1}^{t} \left(\sum_{j \in S_i} G_j(x) - |S_i| + 1 \right) = 0$$

Construction of approximation polynomial (Cont...)

- At least one set S_i such that

$$\sum_{j \in S_i} G_j = |S| - 1$$

Construction of approximation polynomial (Cont...)

- At least one set S_i such that

$$\sum_{j \in S_i} G_j = |S| - 1$$

- Let there be $1 \leq z \leq k$ zeros in $G_1, \ldots, G_k$. Hence S_i must be looking at exactly 1 zero.

Construction of approximation polynomial (Cont...)

- At least one set S_i such that

$$\sum_{j \in S_i} G_j = |S| - 1$$

- Let there be $1 \leq z \leq k$ zeros in $G_1, \ldots, G_k$. Hence S_i must be looking at exactly 1 zero.
- Let $2^{\alpha} \leq z < 2^{\alpha+1}$. Let S be a set picked with probability $2^{-\alpha-1}$.

- At least one set S_i such that

$$\sum_{j \in S_i} G_j = |S| - 1$$

- Let there be $1 \leq z \leq k$ zeros in $G_1, \ldots, G_k$. Hence S_i must be looking at exactly 1 zero.
- Let $2^\alpha \leq z < 2^{\alpha+1}$. Let S be a set picked with probability $2^{-\alpha-1}$.
- $Prob[\text{Exactly one zero}] = z \cdot p \cdot (1-p)^{z-1} \geq \frac{1}{2} \cdot (1-p)^{1/p-1} > 0.18$.

Construction of approximation polynomial (Cont...)

- At least one set S_i such that

$$\sum_{j \in S_i} G_j = |S| - 1$$

- Let there be $1 \leq z \leq k$ zeros in $G_1, \ldots, G_k$. Hence S_i must be looking at exactly 1 zero.
- Let $2^\alpha \leq z < 2^{\alpha+1}$. Let S be a set picked with probability $2^{-\alpha-1}$.
- $Prob[\text{Exactly one zero}] = z \cdot p \cdot (1-p)^{z-1} \geq \frac{1}{2} \cdot (1-p)^{1/p-1} > 0.18$.
- $Prob[\text{Making error in one iteration for an AND gate}] \leq 0.82$. In s iterations - $(0.82)^s$.
- $Prob[\text{Atleast one AND makes error}] \leq m(0.82)^s$.

Construction of approximation polynomial (Cont...)

- At least one set S_i such that

$$\sum_{j \in S_i} G_j = |S| - 1$$

- Let there be $1 \leq z \leq k$ zeros in $G_1, \ldots, G_k$. Hence S_i must be looking at exactly 1 zero.
- Let $2^\alpha \leq z < 2^{\alpha+1}$. Let S be a set picked with probability $2^{-\alpha-1}$.
- $Prob$[Exactly one zero] $= z \cdot p \cdot (1-p)^{z-1} \geq \frac{1}{2} \cdot (1-p)^{1/p-1} > 0.18$.
- $Prob$[Making error in one iteration for an AND gate] ≤ 0.82. In s iterations - $(0.82)^s$.
- $Prob$[Atleast one AND makes error] $\leq m(0.82)^s$.

Circuit computing $\mathcal{E}$

- No error if the random sets picked have at least one set that looks at exactly one zero.

Circuit computing $\mathcal{E}$

- No error if the random sets picked have at least one set that looks at exactly one zero.
- Can decide $F \neq f$, by looking at $\leq ts$ sets and check if no sets contains exactly one zero.

Circuit computing $\mathcal{E}$

- No error if the random sets picked have at least one set that looks at exactly one zero.
- Can decide $F \neq f$, by looking at $\leq ts$ sets and check if no sets contains exactly one zero.
- Resultant circuit has depth $< (d + 3)$.

Outline

Results used

Proposition

For any $f : \mathrm{R}^n \to \mathrm{R}$ that is a degree r polynomial, let μ be an r-independent distribution. Then, f is completely fooled by μ.

$$E_\mu[f] = E[f]$$

LMN Theorem

Let $F : \{0,1\}^n \to \{0,1\}$ be a boolean function computed by depth d circuit of size m, then for any t there is a degree t polynomial such that,

$$||F - \tilde{f}||_2^2 = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} |F(x) - \tilde{f}|^2 \leq 2m \cdot 2^{-t^{1/d}}/20$$

Thank You!