Randomness buys depth for approximate counting

Emanuele Viola

Northeastern University

October 2011

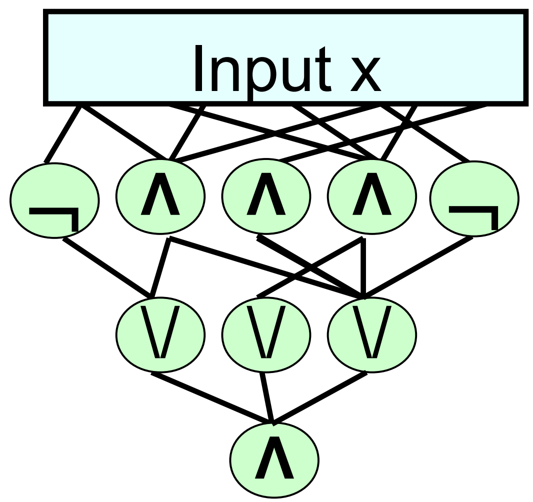
Approximate counting

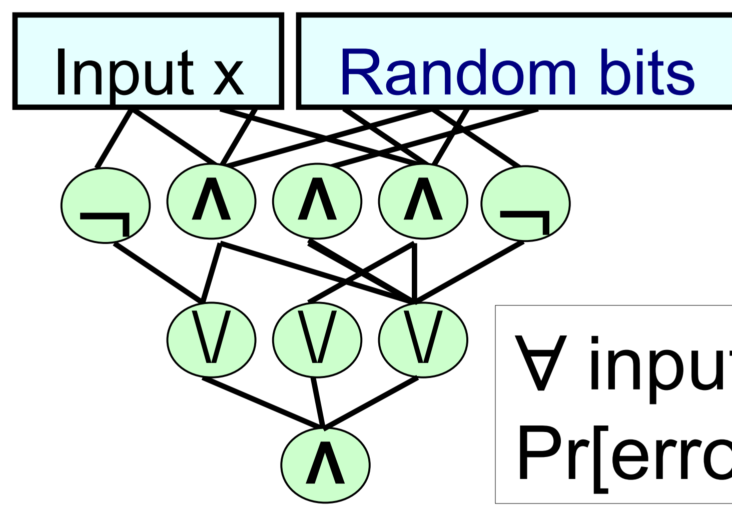
- ε–approx count (majority) distinguish weights $n(1/2 \pm \varepsilon)$

Input: $x \in \{0,1\}^n$ Output: $\begin{cases} 1 & \text{if } \sum x_i > n(1/2 + \varepsilon) \\ 0 & \text{if } \sum x_i < n(1/2 - \varepsilon) \\ 1 \text{ or } 0 & \text{otherwise} \end{cases}$

- Model: AC^0 BP AC^0

Depth d=3





$\forall$ input x,
Pr[error] < 1/3

Approx count in AC^0: surprising and useful

- [Ajtai '83] 0.1–approx count in depth 3, poly(n)-size
- [V] above, explicit
- [Sipser] [Gacs] [Lautemann] BPP $\subseteq$ PH
- [Stockmeyer] #P approximated in PH
- [Goldwasser Sipser] approx count in AM
- [Chaudhuri Radhakrishnan] $LC^0 \neq AC^0$
- ......

yet still gaps in our knowledge!

Our results

- ε–approx count : distinguish weights $n(1/2 \pm \varepsilon)$

- Theorem: For every d: ε–approx count

  in poly-size depth-d $BPAC^0$ $\Leftrightarrow$ $\varepsilon = \Omega(1/\log^{d-1} n)$;

  in poly-size depth-d AC^0 $\Leftrightarrow$ $\varepsilon = \Omega(1/\log^{d-3} n)$.

  Also, BP AC^0 circuits are explicit.

- Previously, depth estimated only within > 2.

  Could not differentiate between AC^0 and BP AC^0

Our results

- Corollary: Randomness buys depth.

- Analogy (all circuits non-uniform)

- BP Size $n^{O(1)}$ = Size $n^{O(1)}$ [Adleman]
- BP Size n^2 $=^?$ Size n^2

- BP AC^0 depth d $\subseteq$ AC^0 depth d+2 [Ajtai Ben-Or]
- BP AC^0 depth d $\not\subseteq$ AC^0 depth d+1 [This work]

Proof outline

- Theorem: For every d: ε–approx count

  in poly-size depth-d BPAC^0 $\Leftrightarrow$ $\varepsilon = \Omega(1/\log^{d-1} n)$;

  in poly-size depth-d AC^0 $\Leftrightarrow$ $\varepsilon = \Omega(1/\log^{d-3} n)$.

  Also, BP AC^0 circuits are explicit.

BP AC^0 depth d $\subseteq$ AC^0 depth d+2

[Ajtai Ben-Or]

- Not in depth-d AC^0 for $\varepsilon = o(1/\log^{d-3} n)$
- In depth-d BP AC^0 for $\varepsilon = \Omega(1/\log^{d-1} n)$

Lower bound

- Lemma: $o(1/\log^{d-3} n)$-approx count not in depth-d AC^0
- Proof by induction on d:
- Base case d = 3: [V]
- Induction step: Switching lemma [Hastad]

  Restriction: leave free 1/log n fraction variables

  multiply approximation parameter by 1/log n

  Increase depth by 1. ♦

Outline

- Lower bound
- Upper bound
- New pseudorandom generator

Upper bound

- Lemma ($\varepsilon = 1/\log^{d-1} n$)-approx count in depth-d $BPAC^0$

- [Amano 09, Brody Verbin 10]
  deterministic depth-d circuit distinguishing
  i.i.d. bits $X_1, X_2, \ldots, X_n$ $\Pr[X_i=1] = 1/2 \pm \underbrace{1/\log^{d-1} n}_{\varepsilon}$

- Right tradeoff, different setting

Upper bound

- In proof of [Amano 09, Brody Verbin 10] deterministic depth-(d-1) distinguishing i.i.d. bits $X_1, X_2, \ldots, X_n$ $\quad \Pr[X_i=1] = n^{-1}(1 \pm \boldsymbol{\varepsilon} \log n)$

- We reduce to above

- Want BP DNF (depth 2) D : $\forall$ x

  $$\sum x_i = n(1/2 \pm \boldsymbol{\varepsilon}) \Rightarrow \Pr[D(x)=1] = n^{-1}(1 \pm \boldsymbol{\varepsilon} \log n)$$

Upper bound

- Want BP DNF (depth 2) D : ∀ x

  $\sum x_i = n(1/2 \pm \boldsymbol{\varepsilon}) \Rightarrow \Pr[D(x)=1] = n^{-1}(1 \pm \boldsymbol{\varepsilon} \log n)$

- **Attempt**: AND log(n) randomly-selected bits
  Probability reduction √
  $\log^2 n$ randomness ⇒ not poly-size DNF **X**

- **Better**: AND log(n) pseudorandomly-selected bits
  O(log n) randomness ⇒ poly-size √
  Probability reduction: Non-explicit: chernoff bound.
  Explicit?

Explicit upper bound

- Need pseudorandom generator:
  - fools rectangles A x A x … x A $\subseteq [n]^{\log n}$ (A = input bits set to 1)
  - seed length O(log n)
  - error < 1/n (distinguish $n^{-1}(1 \pm \varepsilon \log n)$)

- Previous generators: seed > log n log log n

  Expander walk: [Ajtai Komlos Szemeredi]

  For space: [Nisan], [N Zuckerman], [Impagliazzo N Wigderson]

  For rectangles: [Even Goldreich Luby N Velickovic] [Armoni Saks W Zhou], [Lu]

Our pseudorandom generator

- Theorem: Pseudorandom generator:
  - fools $A \times A \times \ldots \times A \subseteq [n]^{\log n}$ $(|A| = n/2)$
  - seed length $O(\log n)$
  - error $< 1/n$

- Two-level expander walk of length $(\log n)^{1/2}$

  Simple calculations $\neq$ previous generators

  $\approx$ approx count in AC^0

- Challenge: make error $1/n^2$

Conclusion

- Theorem: For every d: ε–approx count
  in poly-size depth-d $BPAC^0$ ⟺ $\boldsymbol{\varepsilon = \Omega(1/\log^{d-1} n)}$;
  in poly-size depth-d AC^0 ⟺ $\boldsymbol{\varepsilon = \Omega(1/\log^{d-3} n)}$.

  Also, BP AC^0 circuits are explicit.

- Pseudorandom generator: fool $A \times \ldots \times A \subseteq [n]^{\log n}$
  error 1/n, seed O(log n) (|A| = n/2)

- Randomness buys depth:
  BP AC^0 depth d $\not\subseteq$ AC^0 depth d+1
- Match BP AC^0 depth d $\subseteq$ AC^0 depth d+2 [Ajtai Ben-Or]

- **ΣΠ√ ∩∪ ⊃⊇⊄⊂⊆∨∧**
- **≥≤ ∀∃ ΩΘω αβεγδ**
- **→⇓⇒⇑⇐⇔**
- **≠≈**
- **Θω**
- **∈ ∉**
- **±**
- ΣΠ√∩∉∪⊃⊇⊄⊂⊆∈⇓⇒⇑⇐⇔∨∧≥≤∀∃Ωαβεγδ→
- ≠≈TAΘ
  Recall: edit style changes ALL settings.
- Click on “line” for just the one you highlight
- To rotate, right-click, position and size
- Format->Style & Formatting allows to set default font