Extractors for circuit sources

Emanuele Viola

Northeastern University

April 22 2011

Randomness

- Randomness useful in computation, crucial in crypto

- Sources of randomness in nature
  (various statistics, quantum effects, human brain, ...)
  appear to exhibit correlations, biases

- Want: turn such weak source into
  good source of randomness : close to uniform

Randomness extractors

- Extractor : $\{0,1\}^n \rightarrow \{0,1\}^m$ for sources (distributions) S

  $\forall$ D $\in$ S, Extractor(D) ε-close to uniform

- Determinisitic (no seed) [Von Neumann '51, Santha Vazirani ...]

- Randomized (seed) [Nisan Zuckerman '93, Trevisan, …, Guruswami Umans Vadhan]

- Recent interest in deterministic (also for cryptography) [Trevisan Vadhan '00, Dodis, …]

Deterministic extractors for:

- Independent-blocks source: [Chor Goldreich 88, Barak Bourgain Impagliazzo Kindler Rao Raz Shaltiel Sudakov Wigderson ...]

- Bit-fixing source: some bits uniform & indep., others fixed [Chor Friedman Goldreich Hastad Rudich Smolensky '85, Cohen Wigderson, Kamp Zuckerman, …]

- Small-space: output of one-way, space-bounded algorithm [Blum '86, Vazirani, Koenig Maurer, Kamp Rao Vadhan Zuckerman]

- Affine: uniform over affine space [BKSSW, Bourgain, Rao, Ben-Sasson Kopparty, …]

- This work: first extractor for circuit sources: local, NC^0, AC^0

Outline of talk

- Extractors and the complexity of distributions
- Extractors for local sources
- Extractors for bounded-depth circuits (AC^0)
- Other results

Trevisan Vadhan [2000]

- Sources D with min-entropy k : $\Pr[D = a] < 2^{-k}$ $\forall$ a,
  sampled (or generated) by small circuit
  C: $\{0,1\}^* \to \{0,1\}^n$ given random bits.

- Extractor $\Rightarrow$ Circuit lower bound
  (even 1 bit
  from k=n-1)

- Extractor $\Leftarrow$ $\mathrm{Time}(2^{O(n)}) \not\subseteq$ Σ_5-circuits of size $2^{o(n)}$

This work

- Extractor $\Leftrightarrow$ Circuit lower bound for sampling
  (1 bit from k=n-1) [V 2010]

- Balanced $f : \{0,1\}^n \rightarrow \{0,1\}$ extractor $\Leftrightarrow$
  small circuits cannot sample $f^{-1}(0)$ given random bits

  I.e., $\forall$ small circuit $C: \{0,1\}^* \rightarrow \{0,1\}^n$
  output distribution $C(X)$ not uniform over $\{y : f(y) = 0\}$

The complexity of distributions

- Study of sampling lower bounds advocated in [V 2010]

  Surprising power of "restricted" models

  E.g.: AC^0 samples (Y, Majority(Y)) with error 2^{-n}

- First sampling lower bounds in [V, Lovett V]

  E.g.: NC^0 cannot sample (Y, Majority(Y)) with error o(1)

  $\Downarrow$

  extract 1 bit error < 1 from n-bit entropy $k = n-1$ NC^0 source

Outline of talk

- Extractors and the complexity of distributions

- Extractors for local sources

- Extractors for bounded-depth circuits (AC^0)

- Other results

Extractors for local functions

- $f : \{0,1\}^* \to \{0,1\}^n$ d-local : each output bit depends on d input bits

- Theorem From d-local n-bit source with min-entropy k:
  Let T := k poly(k/nd)
  Extract T bits, error exp(-T)

- E.g. extract $T=k^c$ bits from entropy $k=n^{1-c}$ locality $d=n^c$

- Note: any entropy-k source is k-local: always need k>d

Extractors for local functions

- Theorem From d-local n-bit source with min-entropy k:

  Let T := k poly(k/nd)

  Extract T bits, error exp(-T)

- d = O(1) ⇒ extract from NC^0 sources

  [Independently obtained by De & Watson]

- Theorem later used for AC^0

- Various values of poly(k/nd)

High-level proof

- Theorem d-local n-bit min-entropy k source ($T := k$ poly(k/nd))

  Is convex combination of bit-block source

  block-size = dn/k, entropy T, error $\exp(-T)$

- Bit-block source with entropy T:

  $(0, 1, X_1, 1- X_5, X_3, X_3, 1- X_2, 0, X_7, 1- X_8, 1, X_1)$

  $X_1, X_2, \ldots, X_T \in \{0,1\}$

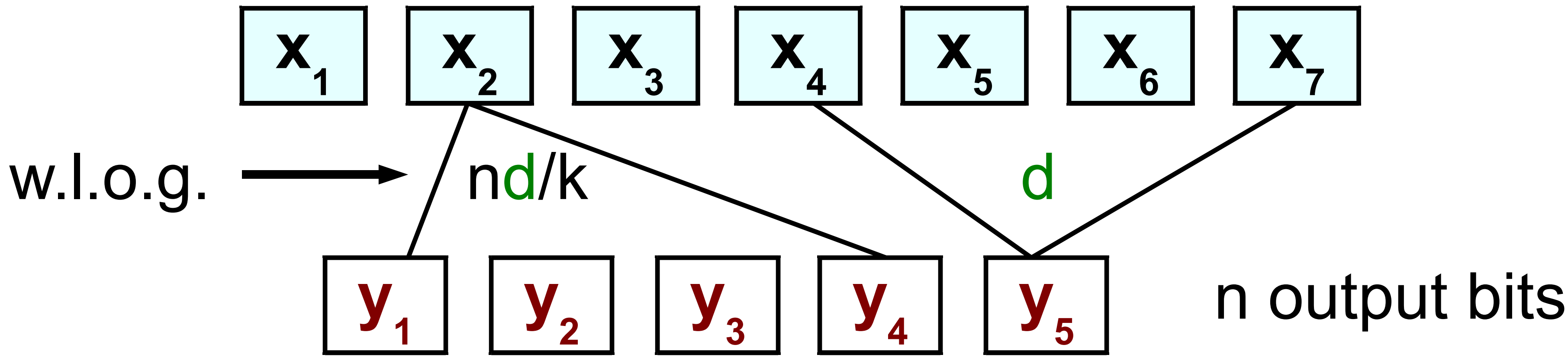
  $0 <$ occurrences of $X_i <$ block-size $= dn/k$

- Special case of low-weight affine sources

  Use extractor by Rao '09

Proof

- d-local n-bit source min-entropy k: convex combo bit-block



- Output entropy > k $\Rightarrow \exists\, \mathbf{y}_i$ with variance > k/n
- Isoperimetry $\Rightarrow \exists\, \mathbf{x}_j$ with influence > k/nd
- Set uniformly $N(N(\mathbf{x}_j)) \setminus \{\mathbf{x}_j\}$ (N(v) = neighbors of v)

  with prob. > k/nd, $N(\mathbf{x}_j)$ non-constant block of size nd/k
- Repeat $k \,/\, |N(N(\mathbf{x}_j))| = k\, k/nd^2$ times, expect $k\, k^2/n^2d^3$ blocks

Qed

Outline of talk

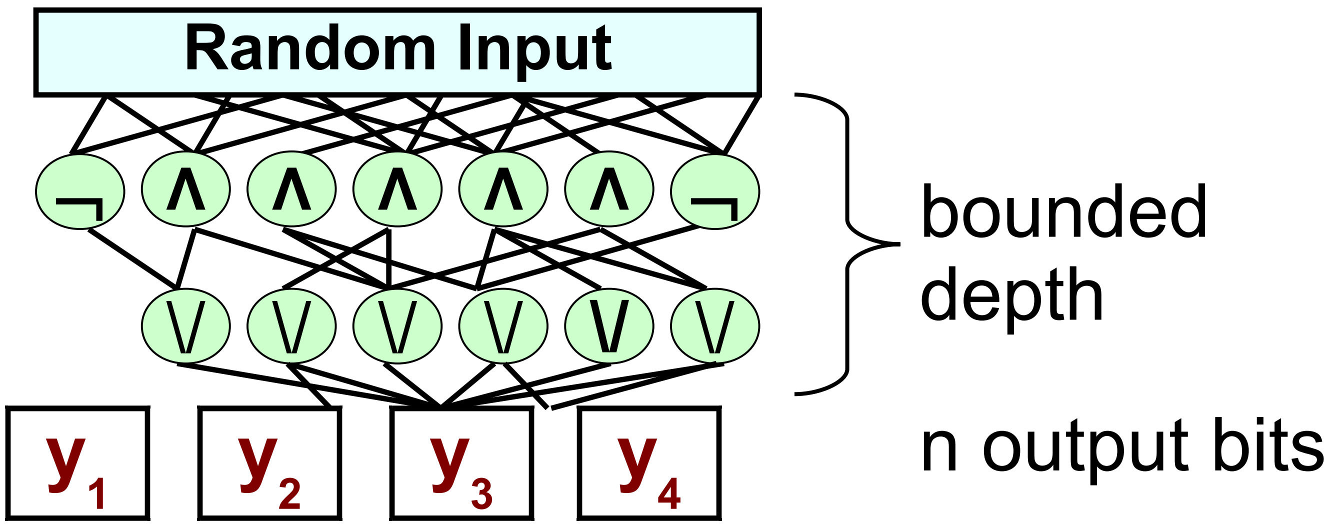
- Extractors and the complexity of distributions

- Extractors for local sources

- Extractors for bounded-depth circuits (AC^0)

- Other results

Bounded-depth circuits (AC^0)



$\bigvee$ = or
$\bigwedge$ = and
$\neg$ = not

- Theorem From AC^0 n-bit source with min-entropy k:

  Extract $k \,\mathrm{poly}\left(k / n^{1.001}\right)$ bits, error $1/n^{\omega(1)}$

High-level proof

- Apply random restriction [Furst Saxe Sipser, Ajtai, Yao, Hastad]

- Switching lemma: Circuit collapses to $d=n^{\varepsilon}$-local
  apply previous extractor for local sources

- Problem: fix 1-o(1) input variables, entropy?

The effect of restrictions on entropy

- Theorem $f : \{0,1\}^* \to \{0,1\}^n$ $f(X)$ min-entropy k

  Let R be random restriction with $\Pr[*] = p$

  With high probability, $f|_R(X)$ has min-entropy pk

- Parameters: $k = \mathrm{poly}(n)$, $p = 1/\sqrt{k}$

- After restriction both circuit collapsed

  and min-entropy $pk = \sqrt{k}$ still poly(n)

Proof idea

- Theorem $f : \{0,1\}^* \to \{0,1\}^n$ $f(X)$ min-entropy k

  Let R be random restriction with Pr[*] = p

  With high probability, $f|_R(X)$ has min-entropy pk

- Proof: Builds on [Lovett V]
- Isoperimetric inequality for noise: $\forall A \subseteq \{0,1\}^L$ of density α

  random m, m' obtained flipping bits w/ probability p :

  $$\alpha^2 \leq \Pr[\text{both } m \in A \text{ and } m' \in A] \leq \alpha^{1/(1-p)}$$

- Bound collision probability $\Pr[\, f|_R(X) = f|_R(Y)\,]$ Qed

Outline of talk

- Extractors and the complexity of distributions

- Extractors for local sources

- Extractors for bounded-depth circuits (AC^0)

- Other results

The complexity of distributions

- Theorem Explicit $b : \{0,1\}^n \to \{0,1\}$:

  Small AC^0 circuits cannot generate (Y, b(Y))

- Proof: b := first bit of AC^0 extractor

  Suppose C generates (Y, b(Y))

  Apply restriction.

  Fix uniformly additional < log n bits that determine b(Y)

  (path in small-depth decision tree)

  b(Y) fixed but Y has lots of entropy. Contradiction.

Simple extractor for NC^0

- Previous theorems use Rao's affine extractor
  (In some settings can use others, e.g. [Bourgain])

- Somewhat complicated

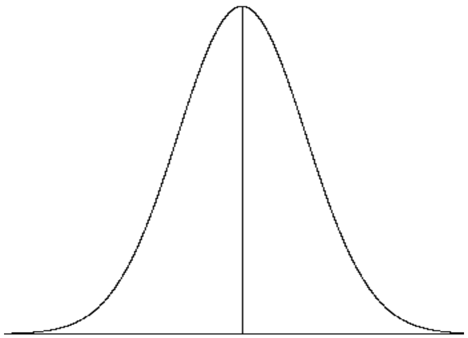
- Want: simple extractors
  ($\Rightarrow$ sampling lower bound for simple functions)

- Theorem Hamming weight extracts $\omega(1)$ bits with error $o(1)$
  from NC^0 sources of entropy $n - \sqrt{n}$

Tool for extractor proof

- Central limit theorem:

  $x_1, x_2, \ldots, x_n$ independent $\Rightarrow \sum x_i \approx$ normal



- Bounded-independence central limit theorem [Diakonikolas Gopalan Jaiswal Servedio V.]

  $x_1, x_2, \ldots, x_n$ k-wise independent $\Rightarrow \sum x_i \approx$ normal

$$\forall\, t \quad \left| \Pr[\textstyle\sum x_i < t] - \Pr[\text{normal} < t] \right| < 1/\sqrt{k}$$

Simple extractor for NC^0

- Theorem Hamming weight extracts $\omega(1)$ bits with error $o(1)$ from NC^0 sources of entropy $n - \sqrt{n}$

- Proof:

  $n-\sqrt{n}$ output bits are almost 100-wise independ. [Shaltiel V]

  $NC^0 \Rightarrow$ exactly 100-wise independent

  Bounded-independence central limit theorem [Diakonikolas Gopalan Jaiswal Servedio V.] Qed

Summary

- First extractors for circuit sources: NC^0 , local, AC^0

  Techniques:

  local = convex comb. of bit-block, use Rao's affine extractor

  for AC^0 also bound entropy loss in restrictions

- Extractor $\Leftrightarrow$ Circuit lower bound for sampling

  (1 bit from k=n-1) [V 2010]

- Corollary: Explicit $b : \{0,1\}^n \to \{0,1\}$:

  Small AC^0 circuits cannot generate (Y, b(Y))

Open problems

- Min-entropy k 2-local source $f : \{0,1\}^* \rightarrow \{0,1\}^n$
- Current extractor applies when $k > n^{2/3}$
- Given better affine extractor, when $k > n^{1/2}$
- Challenge: extract from $k < n^{1/2}$

Open problems

- Note $\exists$ 2-local $f : \{0,1\}^{2n} \to \{0,1\}^{n}$

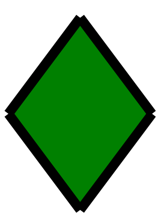
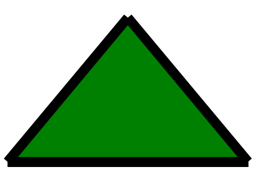
  Distance($f(X)$, $W_{n/4}$ = uniform w/ weight $n/4$) = $1 - \Theta(1)/\sqrt{n}$

- Challenge: Distance $1 - 2^{-\Omega(n)}$ input length = $H(1/4)n+o(n)$

- Recall: AC^0 can generate (Y, majority(Y)), error $2^{-|Y|}$

  Challenge: error 0?

  - Related [Lovett V.] Any bijection

    $\{0,1\}^{n}$ =  $\to$  $= \{x \in \{0,1\}^{n+1} : \sum x_i \geq n/2 \}$

    has large expected hamming distortion? (n even)

- $\sum\prod\surd\cap\notin\cup\supset\supseteq\not\subset\subset\subseteq\in\Downarrow\Rightarrow\Uparrow\Leftarrow\Leftrightarrow\vee\wedge\geq\leq\forall\exists\Omega\alpha\beta\varepsilon\gamma\delta\rightarrow$
- $\neq\approx$TAΘω
- $\in$ $\notin$
-
-
- $\sum\prod\surd\cap\notin\cup\supset\supseteq\not\subset\subset\subseteq\in\Downarrow\Rightarrow\Uparrow\Leftarrow\Leftrightarrow\vee\wedge\geq\leq\forall\exists\Omega\alpha\beta\varepsilon\gamma\delta\rightarrow$
- $\neq\approx$TAΘ
-
- Recall: edit style changes ALL settings.
- Click on “line” for just the one you highlight