Extractors for circuit sources

Emanuele Viola

Northeastern University

October 2011

Randomness extractors

- Want: turn weak randomness (correlation, bias, ...)
  into close to uniform

- **Extractor** for sources (distributions) S on $\{0,1\}^n$

  Deterministic, efficient map : $\{0,1\}^n \to \{0,1\}^m$

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

- Starting with [Von Neumann '51] major line of research

Sources

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

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

- One-way, space-bounded algorithm [Blum '86, Vazirani, Koenig Maurer, Kamp Rao Vadhan Zuckerman]

- Affine set [BKSSW, Bourgain, Rao, Ben-Sasson Kopparty, Shaltiel]

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

Outline of talk

- Extractors and the complexity of distributions
- Local sources
- Bounded-depth circuit (AC^0) sources
  - Sampling lower bound

Trevisan Vadhan; 2000

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

- Extractor $\Rightarrow$ Lower bound for C
  (even 1 bit
  from k=n-1)

- Extractor $\Leftarrow$ $\text{Time}(2^{O(n)}) \not\subseteq \exists\forall\exists\forall\exists$–circuit size $2^{o(n)}$

This work

- Extractor $\Leftrightarrow$ Sampling lower bound
  (1 bit from k=n-1)

$f : \{0,1\}^n \to \{0,1\}$ (balanced) $\Leftrightarrow$ small circuits cannot sample $f^{-1}(0)$ (uniformly, given random bits)

- Sampling lower bounds advocated in [V], more in [Lovett V]

([V]$\Rightarrow$ extract 1 bit, err. < 1, from entropy k = n-1 NC^0 source)

Outline of talk

- Extractors and the complexity of distributions

- Local sources

- Bounded-depth circuit (AC^0) sources
    - Sampling lower bound

Extractors for local functions

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

---

- 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. $T = k^c$ from $k = n^{1-c}$, $d = n^c$
- Note: always need $k > d$
- $d = O(1) \Rightarrow NC^0$ source. Independently [De Watson]

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:

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

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

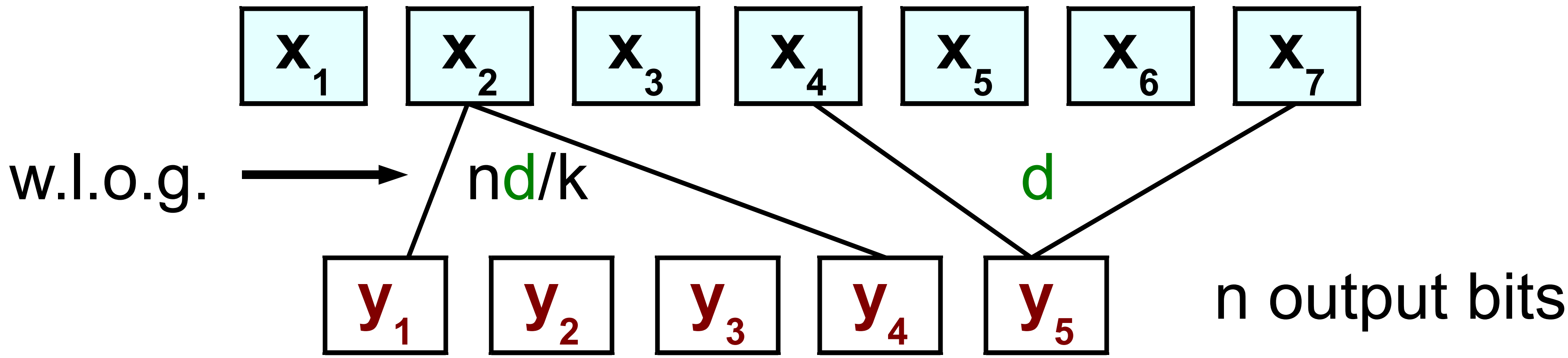
  $0 <$ occurrences of $X_i <$ block-size $= dn/k$

- Special case of low-weight affine sources

  Use [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 $k\, k^2/n^2 d^3$ blocks

♦

Outline of talk

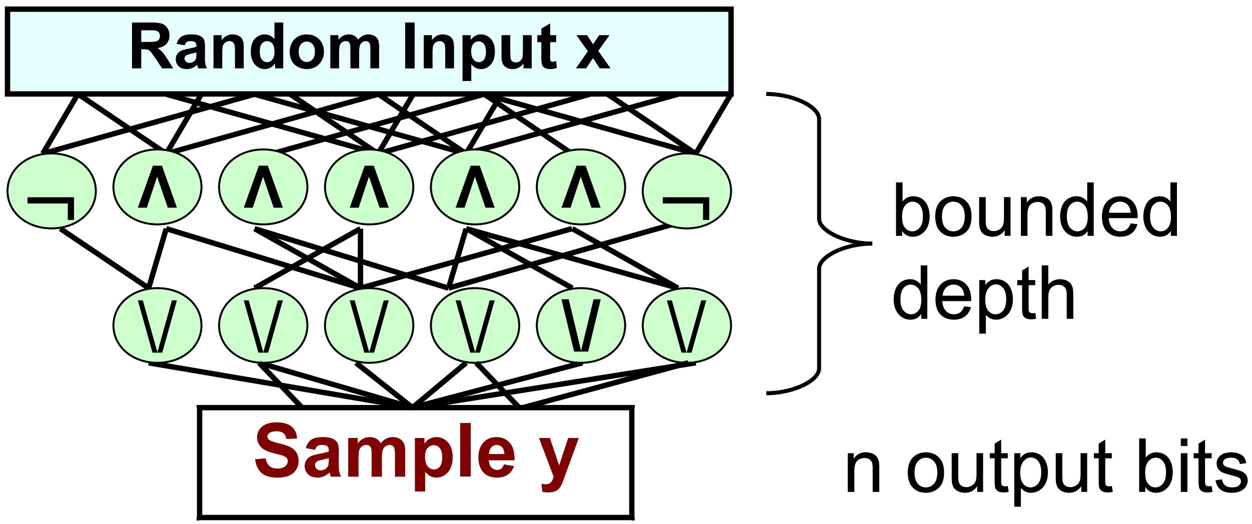
- Extractors and the complexity of distributions

- Local sources

- Bounded-depth circuit (AC^0) sources

    - Sampling lower bound

Bounded-depth circuits (AC^0)



\/ = or
/\ = and
¬ = not

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

  Extract k 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

  R random restriction, Pr[*] = p

  W.h.p., $f|_R(X)$ min-entropy pk

- Proof builds on [Lovett V]

Outline of talk

- Extractors and the complexity of distributions

- Local sources

- Bounded-depth circuit (AC^0) sources
  - Sampling lower bound

Bounded-depth circuits (AC^0)

- Corollary to AC^0 extractor

  Explicit boolean f : AC^0 cannot sample (Y, f(Y))

  f := 1-bit affine extractor for min-entropy $k = n^{0.99}$

- Note: For $k > 1/2$, Inner Product 1-bit affine extractor, and AC^0 can sample (Y, InnerProduct(Y)) [Impagliazzo Naor]

- Explains why affine extractors for $k < 1/2$ more complicated

Summary

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

  local → convex comb. bit-block, use affine extractor

  for AC^0 also bound entropy loss in restrictions

- Extractor ⇔ Circuit lower bound for sampling

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

- Corollary Explicit boolean f : AC^0 cannot sample (Y, f(Y))

- MANY NEW PROBLEMS AND DIRECTIONS!