On Randomness Extraction in AC^0

June 2015

Emanuele Viola

NEU

Joint work with Oded Goldreich and Avi Wigderson

Extracting randomness from sources

- Min-entropy [Nisan Zuckerman '96, …, Guruswami Umans Vadhan, Dvir Wigderson, ...]
- Bit-fixing [Chor Friedman Goldreich Hastad Rudich Smolensky '85, Cohen Wigderson, Kamp Zuckerman, …]
- Independent blocks [Chor Goldreich 88, Barak Bourgain Impagliazzo Kindler Rao Raz Shaltiel Sudakov Wigderson Li ...]
- Many more types
- [This work] Which of these extractors is in AC^0 ?

Motivation

- Still far from understanding power of AC^0

  - Better switching lemma for non-random restriction?

  - AC^0 vs. communication complexity under uniform?

- [Goldreich Wigderson '14] Error reduction in AC^0 for "derandomizing algorithms that err extremely rarely"

  Recently obtained without AC^0 extractors

- pseudorandom generator constructions

Outline

- Seeded extractors
- Deterministic extractors

Previous results on seeded AC^0 extractors

- Ext : $\{0,1\}^n \times \{0,1\}^r \to \{0,1\}^m$ min-entropy k source

- Negative: $m \leq 1.01r$ unless $k/n \geq 1/\text{polylog } n$ [V]

- Positive: $m = r + 1$, $r = n$ [Impagliazzo Naor, V]
  Generate (x, y, InnerProduct(x,y))

  [Nisan Zuckerman, Vadhan] "Sample-then-extract"
  t samples have min-entropy $t \cdot k/n$

Our results on seeded extractors

- $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^m$ min-entropy k source

- Extracting 1 bit ($m = r+1$):

  Can $\Leftrightarrow$ $r \geq (n/k) / \log^{O(1)} n + 10 \log n$

- Extracting more bits:

  - If $k/n \leq 1/\log^{\omega(1)} n$: Can $\Leftrightarrow$ $m/r \leq 1 + \log^{O(1)}(n)\, k/n$

    "extraction rate ≤ 1 + entropy rate"

    Strong extraction impossible

  - If $k/n \geq 1/\log^{O(1)} n$: Can with $m = 1.01r$, $r = O(\log n)$

    Strong

    Open problem: $m = \Omega(k)$?

Our AC^0 extractor construction

- Sampling gives shorter source [Vadhan]
  ➔ can extract with smaller complexity/seed

- In general we need new explicit sampler

- To extract 1 bit from entropy k, sample n/k bits

  - If $n/k \leq \log^{O(1)} n$, apply best-known extractor
  - If $n/k \geq \log^{\omega(1)} n$, apply "inner product" extractor, seed n/k

- To extract t bits repeat with t independent seeds

Outline

- Seeded extractors
- Deterministic extractors

Extractors for bit-fixing sources

- Bit-fixing source = restriction
  Entropy = number of unfixed variables

- Switching Lemma: [Furst Saxe Sipser, Ajtai, Yao, Hastad]
  Any depth-d circuit becomes constant
  on random restriction leaving $n/\log^{d-1} n$ variables

- [This work]
  Some depth-d circuits are far from constant
  on any restriction leaving $n/\log^{\Omega(d)} n$ variables

"Pick restriction after circuit? No better than random"

Our extractor for bit-fixing sources

- [Ajtai Linial]: $\exists$ depth-3 circuit : $\{0,1\}^n \to \{0,1\}$ that extracts if k = n - n/polylog(n) bits uniform, other n - k function of those k

- Want k = n/polylog(n). Idea: combine [AL] with sparse linear map: $\{0,1\}^{n \text{ polylog}(n)} \to \{0,1\}^n$: any n x n submatrix has rank ≥ n – n/polylog(n)

- Could not prove existence of linear map. Instead:
  - Get map over large field [Blomer Karp Welzl]
  - Combine that with codes, non-linear "condenser"

Extractors for independent sources

#	Best k/n for P-time	Best k/n for AC^0 [This work]
2	0.499 [Bourgain]	1-1/polylog(n) not explicit
3	$n^{-0.49}$ [Li]	1-1/polylog(n) not explicit
4	$n^{-0.49}$ [Li]	0.99
O(1)	polylog(n)/n [Li]	0.01

- Open: Only AC^0 lower bound $k/n \geq 1/\text{polylog}(n)$

Conclusion

- Randomness extraction in AC^0
- Min-entropy source:
  complete picture for $m=r+1$, or for $k/n \leq 1/\log^{\omega(1)} n$
- Bit-fixing source:
  "Pick restriction after circuit? No better than random"
- Independent sources

… and much more on samplers, zero-fixing sources, generalizations of inner-product extractor, converting min-entropy sources into block, etc.