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 $\text{AC}^0$?
Motivation

● Still far from understanding power of $\text{AC}^0$
  - Better switching lemma for non-random restriction?
  - $\text{AC}^0$ vs. communication complexity under uniform?

● [Goldreich Wigderson '14] Error reduction in $\text{AC}^0$ for “derandomizing algorithms that err extremely rarely”

  Recently obtained without $\text{AC}^0$ extractors

● Pseudorandom generator constructions
Outline

- Seeded extractors
- Deterministic extractors
Previous results on seeded $\text{AC}^0$ extractors

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

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

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

\[\text{[Nisan Zuckerman, Vadhan]}\] “Sample-then-extract” $t$ samples have min-entropy $t \cdot k/n$
Our results on seeded extractors

- Ext : \( \{0,1\}^n \times \{0,1\}^r \rightarrow \{0,1\}^m \) min-entropy k source

- Extracting 1 bit (\( m = r+1 \)):
  Can \( \iff \) \( r \geq (n/k) / \log^{O(1)} n + 10 \log n \)

- Extracting more bits:
  - If \( k/n \leq 1/\log^{\omega(1)} n \): Can \( \iff \) \( m/r \leq 1 + \log^{O(1)}(n) \) \( k/n \)
    “extraction rate \leq 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 \( \frac{n}{\log^{d-1} n} \) variables

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

"Pick restriction after circuit? No better than random"
Our extractor for bit-fixing sources

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

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

- Could not prove existence of linear map. Instead:
  - Get map over large field [Blomer Karp Welzl]
  - Combine that with codes, non-linear “condenser”
<table>
<thead>
<tr>
<th>#</th>
<th>Best k/n for P-time</th>
<th>Best k/n for AC⁰ [This work]</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0.499 [Bourgain]</td>
<td>1-1/polylog(n) not explicit</td>
</tr>
<tr>
<td>3</td>
<td>n⁻⁰.⁴⁹ [Li]</td>
<td>1-1/polylog(n) not explicit</td>
</tr>
<tr>
<td>4</td>
<td>n⁻⁰.⁴⁹ [Li]</td>
<td>0.99</td>
</tr>
<tr>
<td>O(1)</td>
<td>polylog(n)/n [Li]</td>
<td>0.01</td>
</tr>
</tbody>
</table>

- Open: Only AC⁰ lower bound $k/n \geq 1/polylog(n)$
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.