Pseudorandom bits for polynomials

Emanuele Viola & Andrej Bogdanov

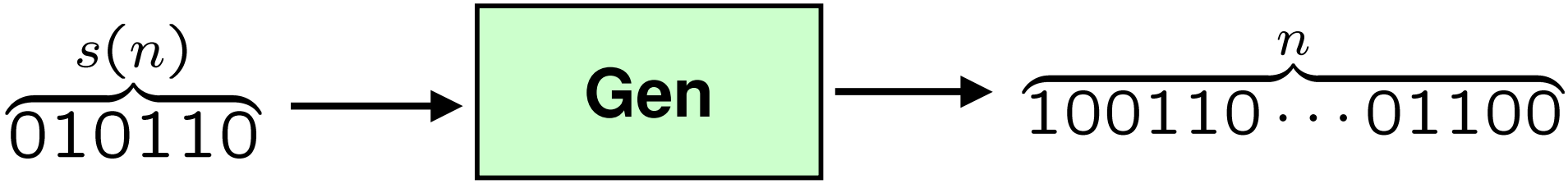
Columbia University
work done while at IAS

ITCS, Tsinghua University
work done while at DIMACS

October 2007

Pseudorandom generator

[Blum Micali; Yao; Nisan Wigderson]



- Efficient
- Short seed s(n) << n
- Output ``looks random''

Want to fool polynomials

- "Looks random":

  fools degree-d n-variate polynomials over field {0,1}

  E.g., $p = x_1 + x_5 + x_7$ degree d = 1

  $p = x_1 \cdot x_2 + x_3$ degree d = 2

  Want: $\forall$ p of degree d

  $$\left| \Pr_{X \in \{0,1\}^n}[p(X) = 0] - \Pr_{S \in \{0,1\}^s}[p(Gen(S)) = 0] \right| \leq \varepsilon$$

- Fundamental model: coding theory, lower bounds, etc.

Previous results

- Th.[Naor & Naor '90]: Fools linear, seed = $O(\log n/\varepsilon)$
  - Applications: derandomization, PCP, expanders, learning…
- Th.[Luby Velickovic Wigderson '93]:
  Fools constant degree, seed = $\exp(\sqrt{\log n}/\varepsilon)$
  - [V] gives modular proof of more general result
- Th.[Bogdanov '05]: Any degree, but over large fields
- Over small fields such as {0,1}:

  no progress since 1993, even for degree d=2

Our results

- New approach based on “Gowers norm”

- Theorem[This work]:
  Unconditionally:
  Fool degree d=2 with seed = $2 \cdot \log(n) + \log(1/\varepsilon)$
  Fool degree d=3 with seed = $3 \cdot \log(n) + f(\varepsilon)$

- Theorem[This work]:
  Under “d vs. d-1 Gowers inverse conjecture”:
  Fool any degree d with seed = $d \cdot \log(n) + f(d,\varepsilon)$

- Results apply to any prime field.
  Focus on {0,1} for simplicity

[Green & Tao] + Our results

- Breaking news[Green & Tao; very recently]:
  The “d vs. d-1 Gowers inverse conjecture” is true

- Corollary [Green & Tao] + [This work]:
  Fool any degree d with seed = $d \cdot \log(n) + f(d,\varepsilon)$

Our generator

- Generator that fools degree d:

  Let $L \in \{0,1\}^n$ fool linear polynomials [NN]

  bit-wise XOR d independent copies of L:

  Generator := $L^1 + \ldots + L^d$

- Seed length $d \cdot \log(n) + f(d,\varepsilon)$ optimal for fixed d, ε

  $\Rightarrow$ XORing d-1 copies is not enough.

Other recent development

- After this work
  Th.[Lovett]: The XOR of 2^d generators for degree 1 fools degree d, without using Gowers norm.

- Recall our generator:
  XOR d copies, seed length $d \cdot \log(n) + f(d,\varepsilon)$
  Better seed for fixed degree d, error ε
  worse dependency on ε

Outline

- Overview
- Our results
- Gowers norm
- Proof

Gowers norm

[Gowers '98; Alon Kaufman Krivelevich Litsyn Ron '03]

- Measure closeness to degree-d polynomials: check if random d-th derivative is biased

- Derivative in direction $y \in \{0,1\}^n$: $D_y\, p(x) := p(x+y) - p(x)$
  - E.g. $D_{y_1\, y_2\, y_3}(x_1\, x_2 + x_3) = y_1 x_2 + x_1 y_2 + y_1 y_2 + y_3$

- Norm $N_d(p) := E_{Y^1 \ldots Y^d \in \{0,1\}^n} \mathrm{Bias}_X[D_{Y^1 \ldots Y^d}\, p(X)] \in [0,1]$

  (Bias [Z] := | Pr[Z = 0] - Pr[Z = 1] |)

  $N_d(p) = 1 \Leftrightarrow$ p has degree d

- From combinatorics [Gowers; Green Tao], to PCP [Samorodnitsky Trevisan], lower bounds [V. Wigderson], …

Proof idea

- Recall: want to fool degree-d polynomial p
- Case analysis based on
  closeness of p to degree **d-1** polynomials,
  measured by Gowers norm $N_{d-1}(p)$
- Case $N_{d-1}(p)$ small $\Rightarrow$ directly fool p
- Case $N_{d-1}(p)$ large $\Rightarrow$ reduce to fooling degree-(d-1),
  induction.

Case $N_{d-1}(p)$ small

- Recall: $L^1, \ldots, L^d$ fool linear polynomials
  Goal: Bias $[p(X)] \approx$ Bias $[p(L^1 + \ldots + L^d)] \approx 0$

- Lemma[Gowers]: Bias $[p(X)] \leq N_{d-1}(p) \approx 0$

- Lemma[This work]: Bias $[p(L^1 + \ldots + L^d)] \leq N_{d-1}(p) \approx 0$

- Proof: Bias $[\, p(L^1 + \ldots + L^d) \,]$

  $\leq E_{L^1 \ldots L^{d-1}}$ Bias$_X [\, D_{L^1 \ldots L^{d-1}} p(X) \,]$

  $\approx E_{Y^1 \ldots Y^{d-1}}$ Bias$_X [\, \underbrace{D_{Y^1 \ldots Y^{d-1}} p(X)}_{\text{(linear in each } Y^i\text{)}} \,] = N_{d-1}(p)$

Q.E.D.

Case $N_{d-1}(p)$ large

- $N_{d-1}(p)$ large

Gowers inverse theorem
[Green & Tao; Samorodnitsky]

- p barely close to degree d-1 polynomial (51 %)

Self-correction
[This work]

- p very close to (function of) degree d-1 polynomials (99 %)

Apply induction

Conclusion

- New approach to fooling degree-d polynomials
  - Fool degree d = 2,3 with seed O(log n)
  - Using recent results [Green & Tao]
    fool any degree d with seed O(log n)
- Proof: case analysis based on Gowers norm
  Recurrent theme in combinatorics
- Open problem: Power of our generator?