Hardness vs. Randomness within Alternating Time

Emanuele Viola
Harvard University

July 2003

OVERVIEW

- Pseudorandom Generators (PRGs)

- Hardness vs. Randomness:

  PRG constructions from complexity assumptions

- The problem we study:

  Complexity of PRG constructions

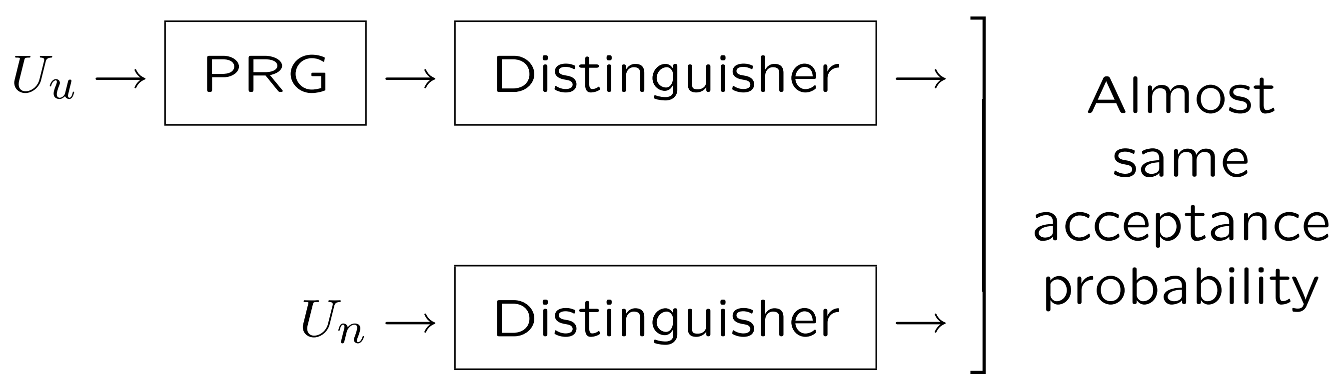
- Our Results:

  New tight upper and lower bounds on the complexity of PRG constructions

PSEUDORANDOM GENERATORS (PRGs)

$$\underbrace{01\ldots00}_{u} \longrightarrow \boxed{\text{PRG}} \longrightarrow \underbrace{01010010\ldots010011010}_{n}$$

$PRG(U_u), U_n$ computationally indistinguishable



TWO DIFFERENT KINDS OF PRGs

- Blum-Micali-Yao type [BM82,Y82]

  Based on one-way functions [HILL90]

- Nisan-Wigderson type [NW88] (our focus)

  Based on functions hard for circuits

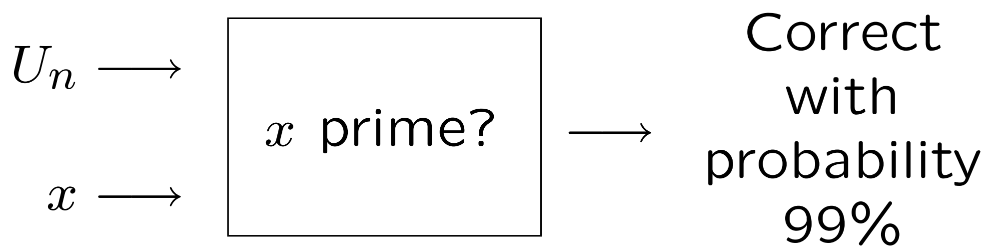
  [BFNW,NW,I,IW,ACR,STV,ISW,SU,U,A,...]

  Computational indistinguishability

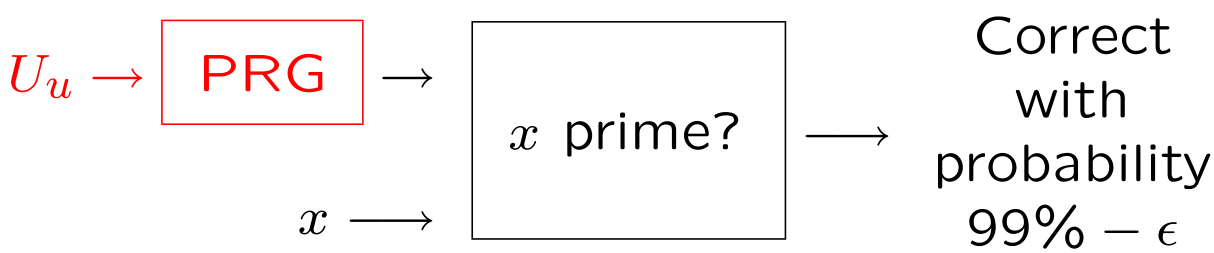
  $\forall$ circuit C of size n:

  $$\left| \Pr[C(\mathrm{PRG}(U_u)) = 1] - \Pr[C(U_n) = 1] \right| \leq \epsilon$$

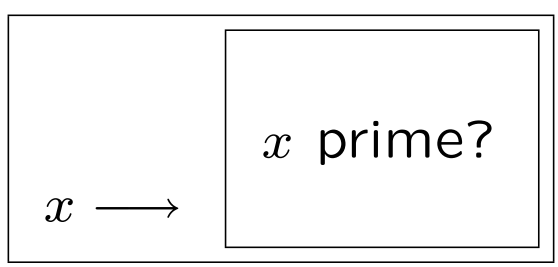
DERANDOMIZATION



Save Randomness



Proof: If not, circuit



distinguishes PRG(U_u) from U_n ∎

"High-end" Derandomization

$u = O(\log n) \Rightarrow BP \cdot P = P$

HARDNESS vs. RANDOMNESS

PRGs based on Hard Functions

$$f \text{ hard for small circuits} \\ \Downarrow \\ \text{PRG}^f$$

- Worst-case hard
  $\forall \text{ small } C : C \neq f$

- Mildly average-case hard
  $\forall \text{ small } C : \Pr[C(U_l) \neq f(U_l)] \geq \frac{1}{\text{poly}(l)}$

- $\vdots$

- Strongly average-case hard
  $\forall \text{ small } C : \Pr[C(U_l) \neq f(U_l)] \approx \frac{1}{2}$

Want PRGs from worst-case hardness:
Weakest and Clearest assumption

HARDNESS vs. RANDOMNESS cont.

f worst-case hard

$\Downarrow$

Hardness Amplification

$\Downarrow$

f' strongly hard on average

$\Downarrow$

Nisan-Wigderson PRG

$\Downarrow$

$PRG^{f'}$

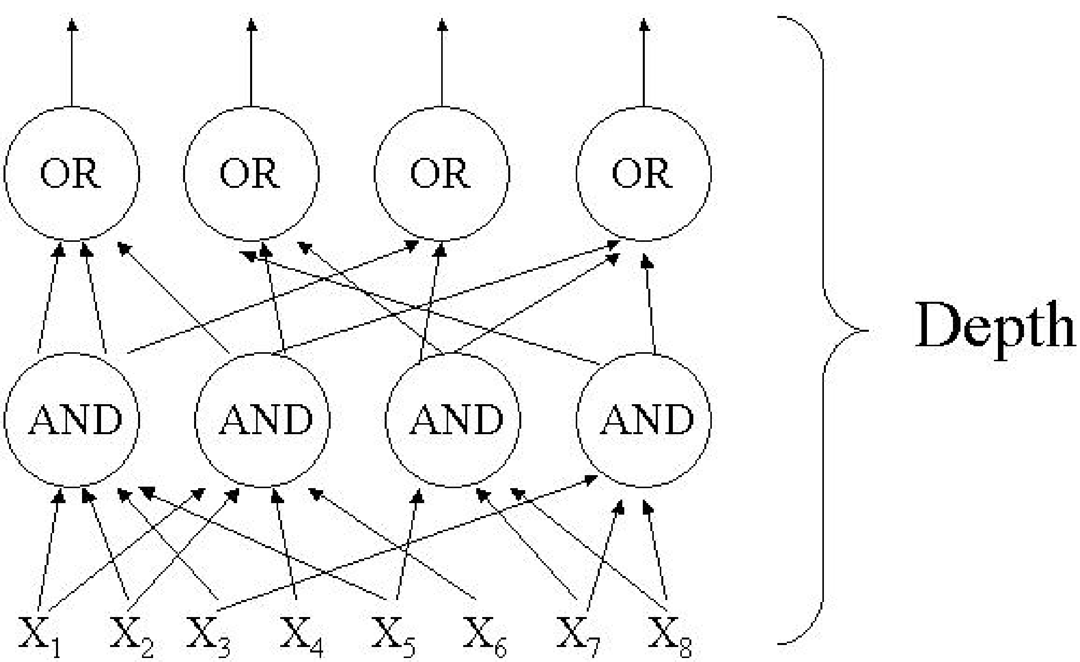
THE PROBLEM WE STUDY

What is the complexity of building a PRG from a hard function?

Our main question

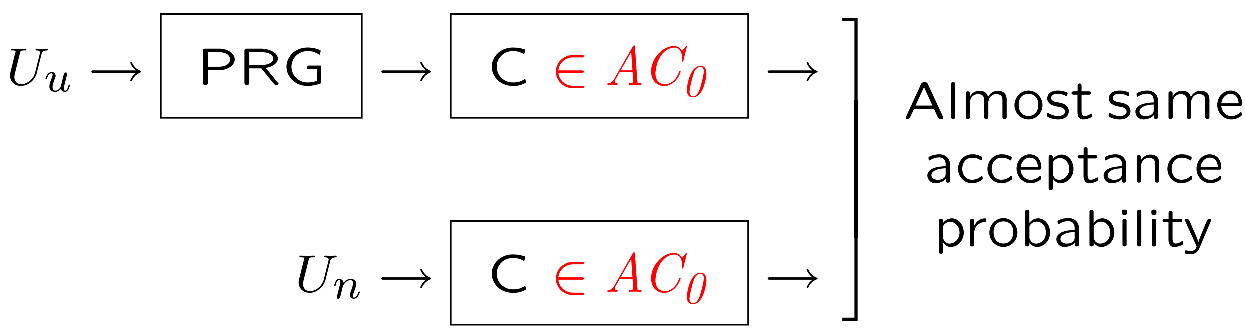
Starting from a hard function can you build a PRG in AC_0?

AC_0 = constant depth circuits

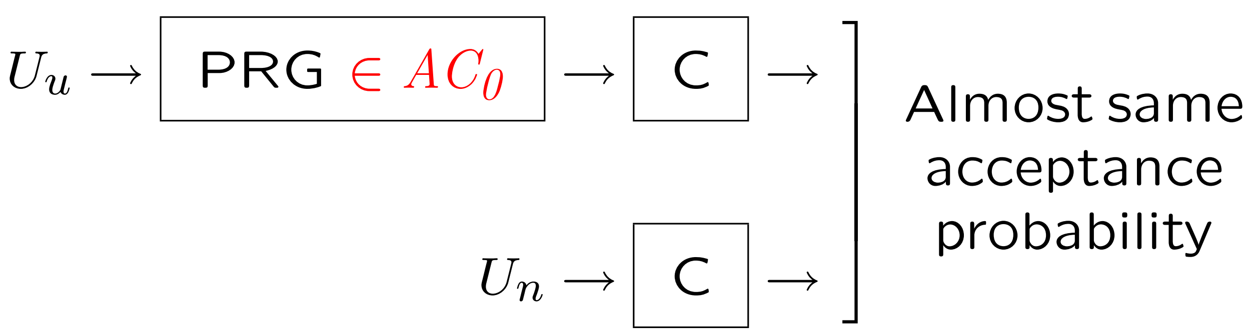


TWO SEPARATE ISSUES

- PRG against AC_0 [AW,N,K,A,...] (in paper, not in talk)



- PRG in AC_0 [IN,NR,CM,...] (in talk)



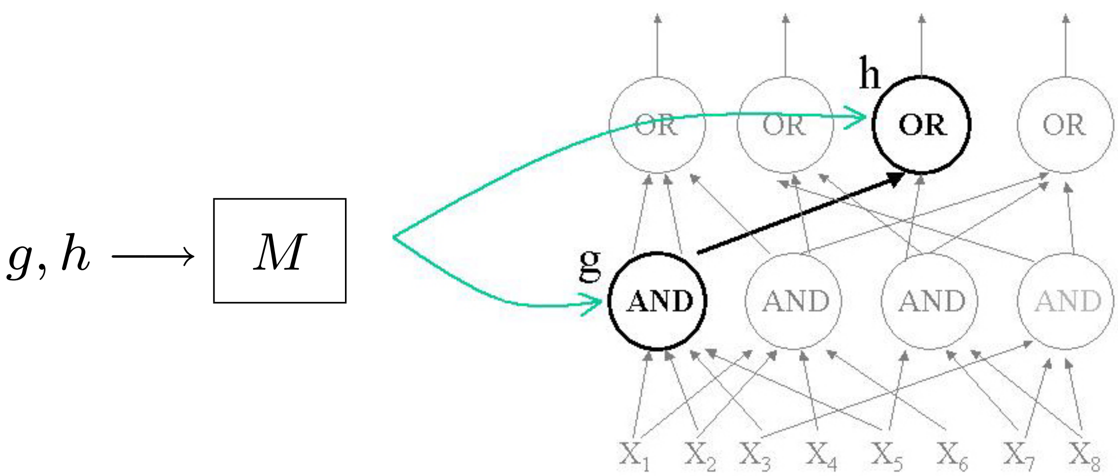
UNIFORMITY

Uniformity of C := complexity of describing C

Problem: Slack uniformity $\Rightarrow$ slack question

Solution: *DLOGTIME*-uniformity

Given indices to two gates can decide type and connection in linear time in index size



Right uniformity for AC_0 [BIS]

Our results hold under *DLOGTIME*-uniformity

MOTIVATIONS

Why build PRG in AC_0?

- Understand Hardness vs. Randomness
- Very efficient PRG
  - AC_0 = Constant parallel time
- Derandomization of probabilistic AC_0 ($BP \cdot AC_0$)
  - Previous results [AW,N,K,A] do not hold under $DLOGTIME$-uniformity

OUR MAIN RESULTS

- Upper bounds

Mildly average-case hard f

$\Downarrow$

PRG in AC_0

- Lower Bounds for black-box constructions from worst-case hard functions
  - No PRG construction in AC_0
  - No hardness amplification in AC_0

- Our bounds match

MEANING OF OUR RESULTS

Consider the construction

$$f \text{ worst-case hard}$$
$$\Downarrow$$
$$\boxed{??}$$
$$\Downarrow$$
$$PRG^f$$

Our results help understand its complexity

$$f \text{ worst-case hard}$$
$$\Downarrow$$
$$\boxed{\text{High complexity: } \notin AC_0}$$
$$\Downarrow$$
$$f' \text{ mildly average-case hard}$$
$$\Downarrow$$
$$\boxed{\text{Low complexity: } \in AC_0}$$
$$\Downarrow$$
$$PRG^{f'}$$

LOWER BOUND FOR HARDNESS AMPLIFICATION

- Define black-box worst-case hardness amplification
- Define list-decodable codes
- Black-box worst-case hardness amplification yields list-decodable codes
- Prove lower bound for list-decodable codes

BLACK-BOX HARDNESS AMPLIFICATION

f worst-case hard $\longrightarrow$ [Amp] $\longrightarrow$ Amp^f average-case hard

Most constructions black-box: Only use information theoretic properties

Formally, Amp is δ-black-box worst-case hardness amplification if for every f, A :

$$\Pr[A(U_l) \neq Amp^f(U_l)] \leq \delta,$$

$\exists$ small C such that $C^A = f$.

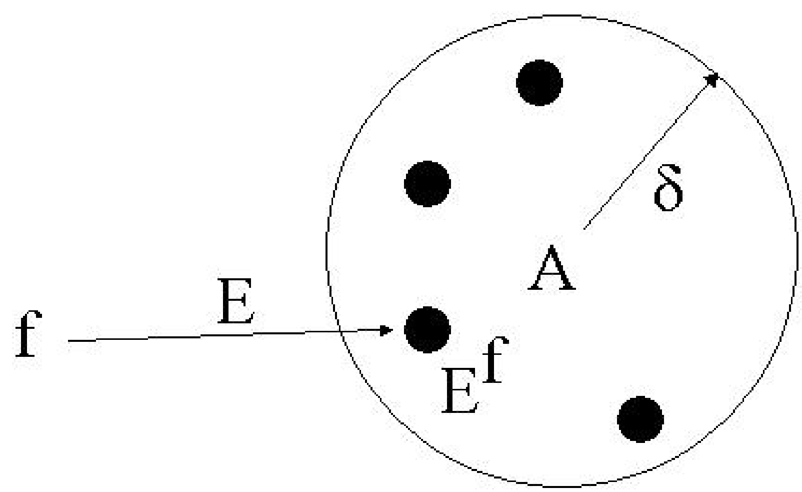
Note:

f worst-case hard $\Rightarrow$ Amp^f average-case hard

LIST-DECODABLE CODES

E is δ-list-decodable if $\forall A$ there are few f:

$$\Pr[A(U_l) \neq E^f(U_l)] \leq \delta$$



DEFINITIONS

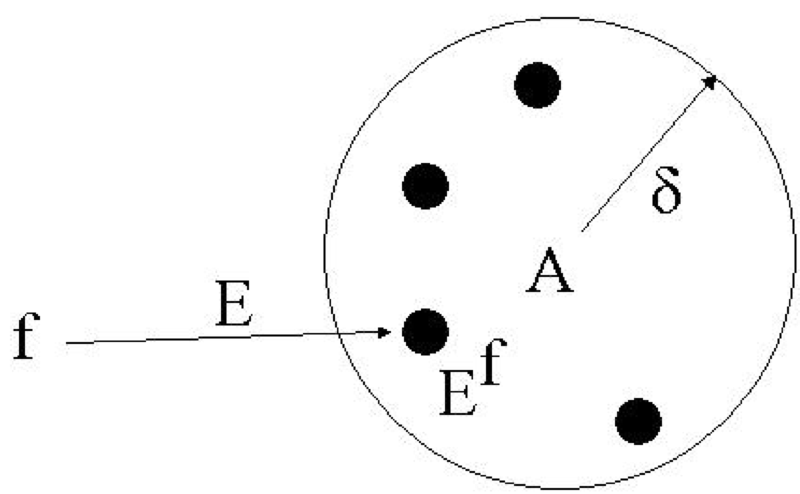
- Amp is δ-black-box worst-case hardness amplification if for every f, A:

$$\Pr[A(U_l) \neq Amp^f(U_l)] \leq \delta,$$

$\exists$ small C such that $C^A = f$.

- E is δ-list-decodable if $\forall A$ there are few f:

$$\Pr[A(U_l) \neq E^f(U_l)] \leq \delta$$



HARDNESS AMPLIFICATION $\Rightarrow$ CODE

Truth-table of f = message

Truth-table of Amp^f = codeword

Theorem (Following STV,TV).

$$Amp \ \ \delta\text{-black-box hardness amplification}$$
$$\Downarrow$$
$$Amp \ \ \delta\text{-list-decodable}$$

Proof:

- For every f : $\Pr[A(U_l) \neq Amp^f(U_l)] \leq \delta$ there is a small circuit $C : f = C^A$

- Only few small circuits $\Rightarrow$ only few f

■

LOWER BOUND FOR LIST-DECODABLE CODES

Main tool Noise Sensitivity

Noise sensitivity of h is $\Pr[h(X) \neq h(X+\eta)]$ where X is random input, η random noise

- Codes have high noise sensitivity

  We show it

- Constant depth circuits have low noise sensitivity

  Theorem (LMN,B,O). C circuit of depth d and size s, η noise with parameter p:

$$\Pr_{X,\eta}[C(X) \neq C(X+\eta)] \leq p \log^d s$$

LOWER BOUND FOR LIST-DECODABLE CODES

Theorem. Let $E : \{0,1\}^n \to \{0,1\}^{\bar{n}}$ be $(\delta, 2^m)$-list-decodable and computable by a circuit of depth d and size s, then $\log^d s \geq n\delta/m$

Proof: η noise with parameter $(m+1)/n$

Consider $\Pr_{i,X,\eta}[E_i(X) \neq E_i(X+\eta)]$

$\forall$ fixed x, a : $\Pr_\eta[x+\eta = a] \leq \frac{1}{2^{m+1}}$

By list-decodability:

$$\Pr_{X,\eta}\left[\Pr_i[E_i(X) \neq E_i(X+\eta)] \leq \delta\right] \leq \frac{2^m}{2^{m+1}} = \frac{1}{2}$$

So: $\Pr_{i,X,\eta}[E_i(X) \neq E_i(X+\eta)] \geq \frac{\delta}{2}$

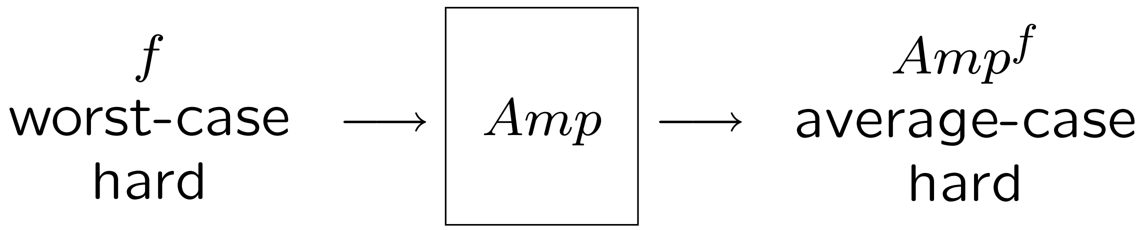
By low sensitivity:

$$\Pr_{i,X,\eta}[E_i(X) \neq E_i(X+\eta)] \leq \frac{m \log^d s}{n}$$ ■

HARDNESS AMPLIFICATION: CONCLUSION

Theorem. There is no black-box worst-case hardness amplification computable in AC_0.

We show more: There is no black-box Amp:



- $f : \{0,1\}^l \rightarrow \{0,1\}$

- Amp in time $2^{o(l)}$ with $O(1)$ alternations

Corollary. No black-box worst-case hardness amplification within polynomial-time hierarchy

We give matching upper bound

LOWER BOUND FOR PRG CONSTRUCTIONS

- Black-box PRG constructions yield extractors [T]

- Lower bound for extractors

  – Extractors have high noise sensitivity

    We show it

  – Constant depth circuits have low noise sensitivity

    [LMN,B,O]

CONCLUSION

- PRGs useful tool: Derandomization

- PRGs are built from hard functions

- We study the complexity of PRG constructions, and we show

$$f \text{ worst-case hard}$$

$$\|$$

$$\boxed{\text{High complexity: } \notin AC_0}$$

$$\Downarrow$$

$$f' \text{ mildly average-case hard}$$

$$\|$$

$$\boxed{\text{Low complexity: } \in AC_0}$$

$$\Downarrow$$

$$PRG^{f'}$$

ACKNOWLEDGEMENT

Many thanks to Salil Vadhan for encouragement, illuminating discussions, and suggesting the problem.