Pseudorandomness

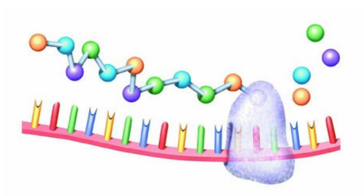
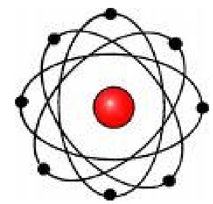
Emanuele Viola

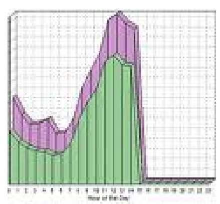
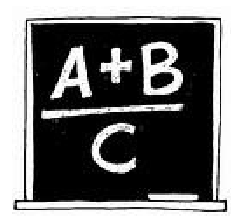
Columbia University

April 2008

Computation

- The universe is computational
- Computation of increasing importance to many fields

biology  physics 

economics  mathematics 

- Goal: understand computation

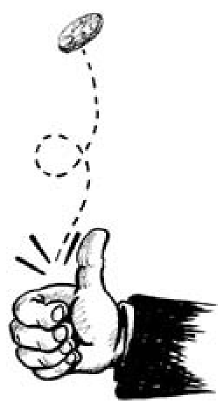
Milestones

- Uncomputability
  [Gödel, Turing, Church; 1930's]

- NP-completeness
  [Cook, Levin, Karp; 1970's]

  $P \neq NP$?

- Randomness
  [...; today]



  $P = RP$?

Pseudorandomness

- Key to understanding randomness
- Goal of Pseudorandomness:

  Construct objects that "look random" using little or no randomness

- Example:
  Random 10-digit number is prime with probab. 1/10

  Challenge: Deterministic construction?

Motivation for Pseudorandomness (1)

- Algorithm design, Monte Carlo method

- Breakthrough [Reingold 2004]
  Connectivity in logarithmic space (SL = L)

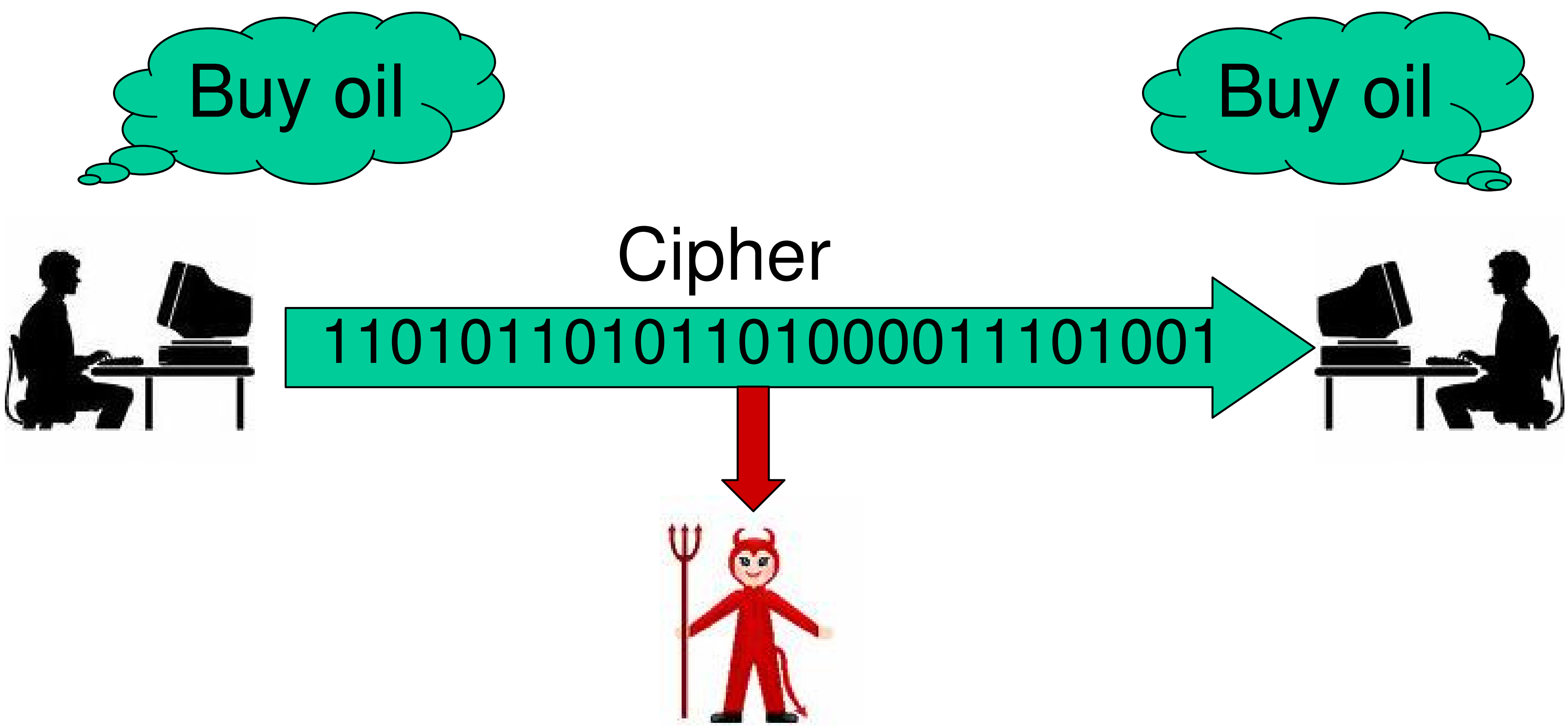
- Breakthrough [Agrawal Kayal Saxena 2002]
  Primality in polynomial time (PRIMES $\in$ P)

- Originated from pseudorandomness

Motivation for Pseudorandomness (2)

[Shannon 1949; Goldwasser Micali 1984]

- Cryptography



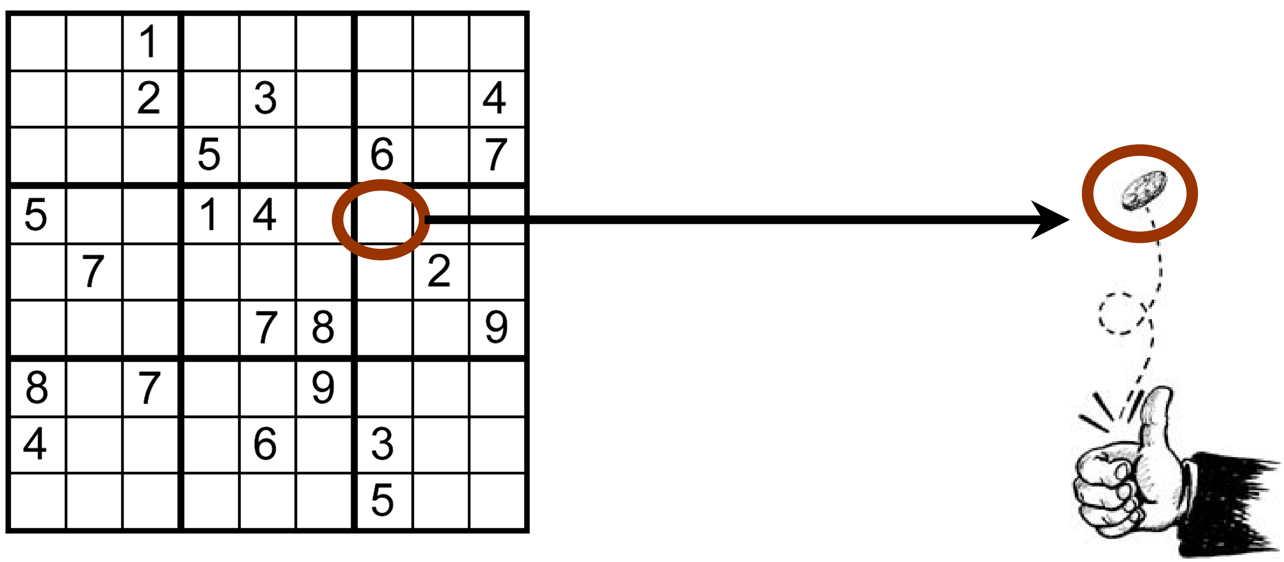
- Security ≡ cipher looks random to eavesdropper

Motivation for Pseudorandomness (3)

- Surprise: " P ≠ NP ⇔ P = RP " (1980's-present)
  Hard problems exist ⇔ randomness does not help

  [Babai Fortnow Kabanets Impagliazzo Nisan Wigderson…]

- Idea: Hard problem ⇒ source of randomness



Outline

- Overview

  Motivation

- Pseudorandom generators

  Examples

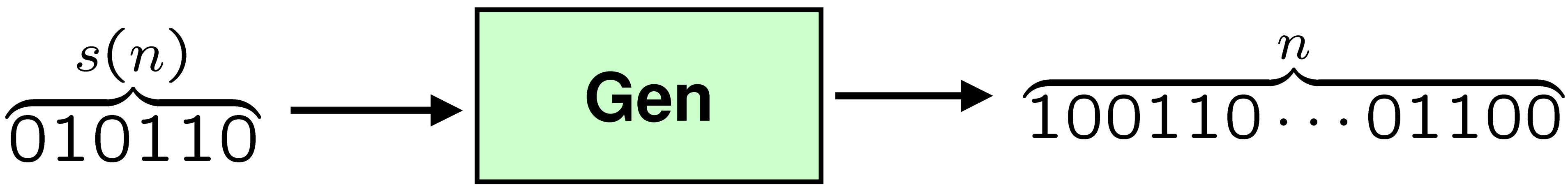
  Circuits

  Polynomials

- Future directions

Pseudorandom generator

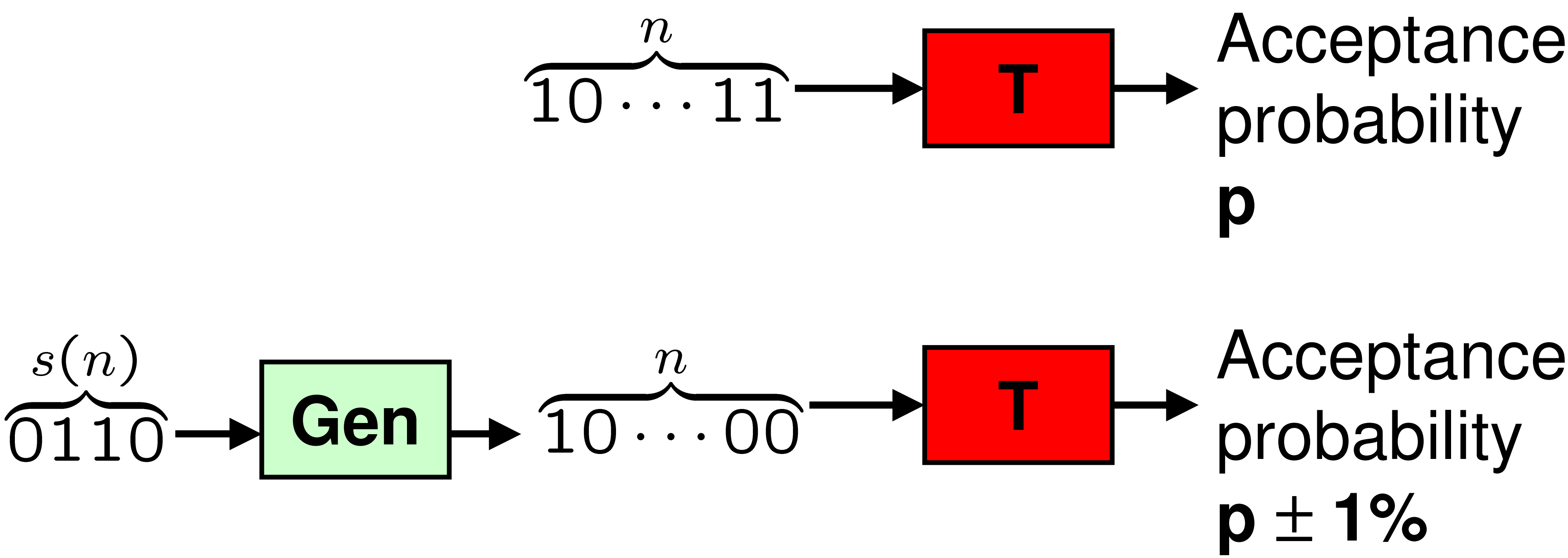
[Blum Micali; Yao; Nisan Wigderson]



- Efficient, deterministic
- Short seed s(n) << n
- Output “looks random”

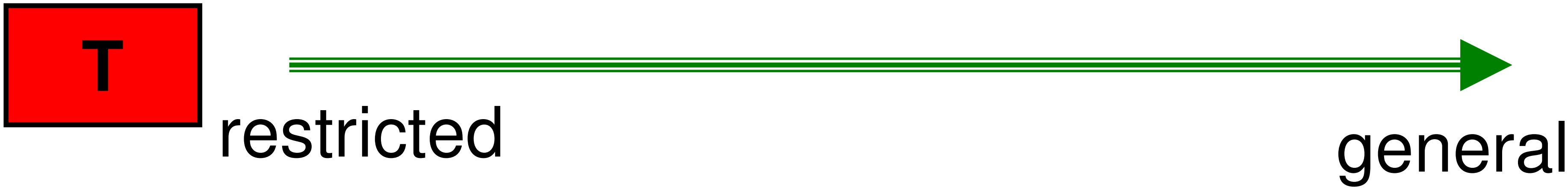
Definition of “looks random”

- “Looks random” to test T: $\{0,1\}^n \to \{0,1\}$



- Example: T = “Does pattern 1010 occur?”

Classes of tests

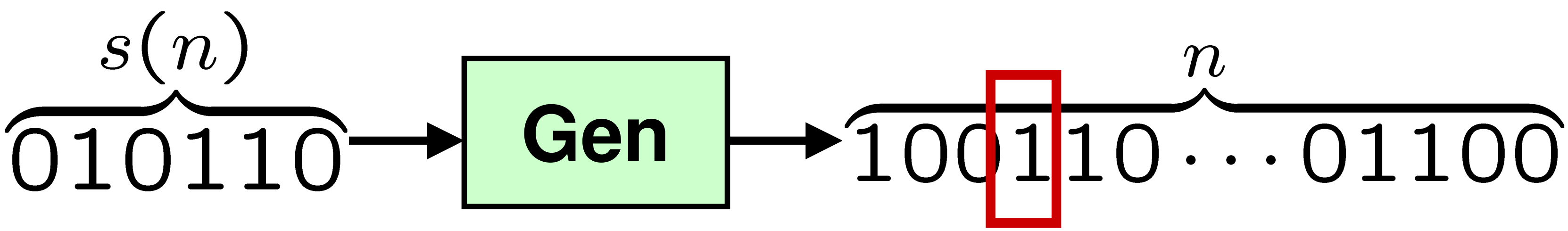


- General: P = RP, cryptography, etc.. Conditional
  T = any algorithm

- Restricted: Also many applications. Unconditional
  T = Space bounded [Nisan, Reingold Trevisan Vadhan,…]
  Rectangles [Armoni Saks Wigderson Zhou, Lu]
  look at k bits [Chor Goldreich, Alon Babai Itai,…]
  Circuits [Nisan, Luby Velickovic Wigderson, V.]
  Polynomials [Naor Naor, Bogdanov V., V.]

Toy example

- Test: Just look at 1 bit (but you don't know which)

- Want: 

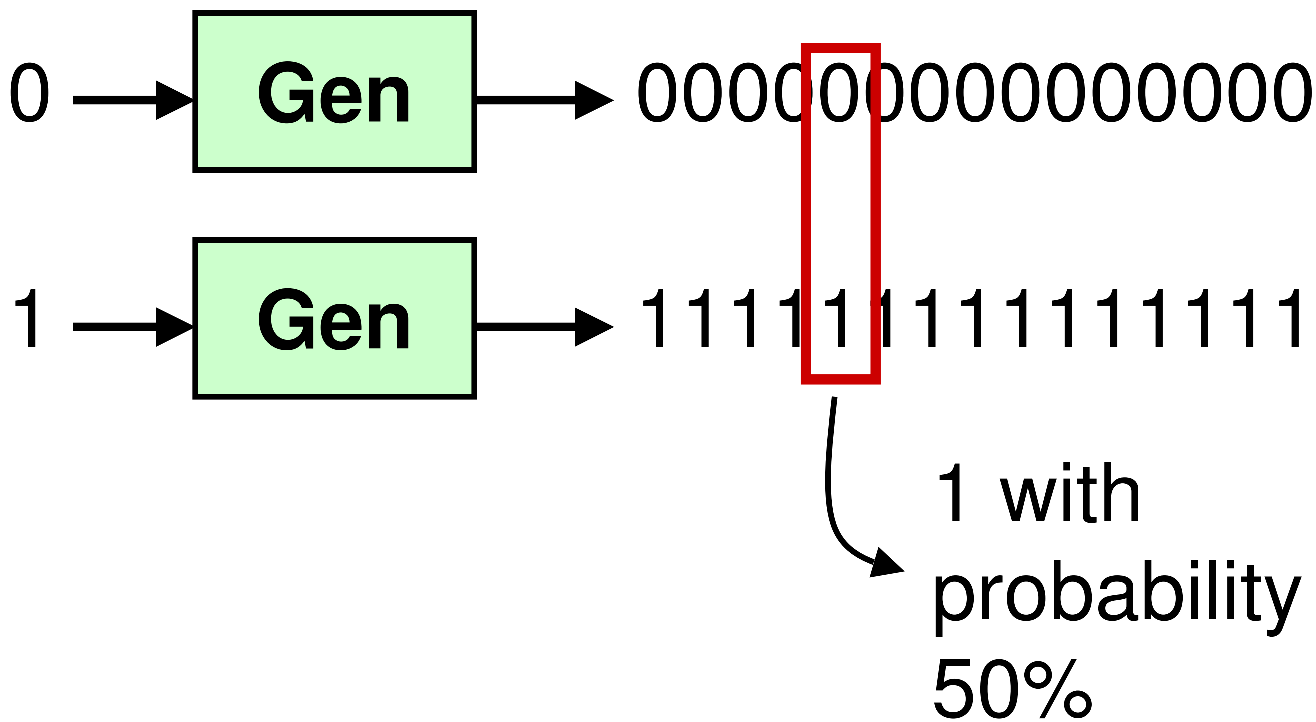
  each output bit is random

  1 with probability 50%

- Question: Minimal seed length s?

Solution to toy example

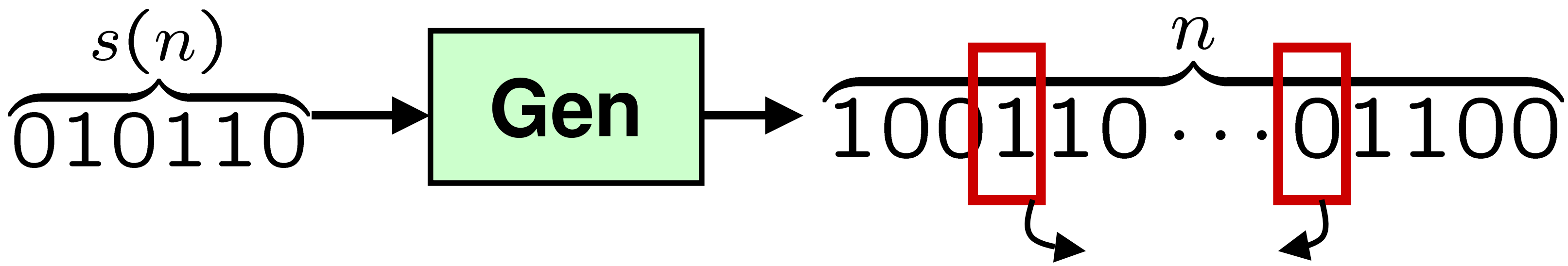
- Solution: Seed length s = 1 !



Pairwise independence

- Test: Just look at 2 bits

- Want:



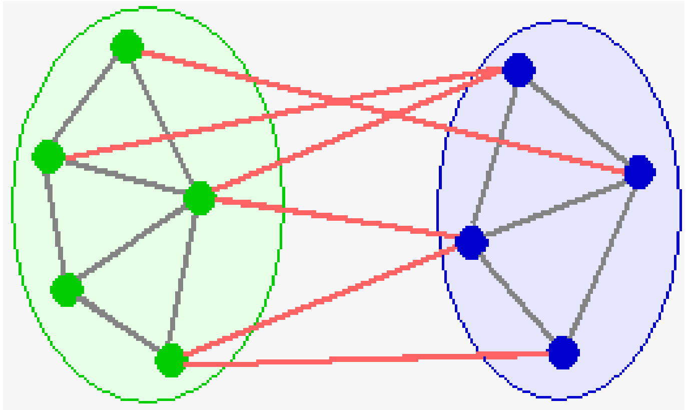
every two output bits are random: 00, 01, 10, 11 with prob. 25%

- Theorem[Carter Wegman '79,…] s = log n

- Idea: y-th output bit: $\text{Gen}(x)_y := \sum_i x_i \cdot y_i \in \{0,1\}$
  $|x|=|y|=\log n$

Application to MAXCUT

[Chor Goldreich, Alon Babai Itai]



- Want: Cut in graph that maximizes edges crossing
- Random cut: C(v) = 0, 1 with prob. 1/2
  E[# edges crossing] = $\sum_{(u,v)}$ Prob[C(u) $\neq$ C(v)] = |E|/2
- Pairwise independent cut suffices!
  $\Rightarrow$ deterministic algorithm (try $2^{\log n} = n$ cuts)
- "The amazing power of pairwise independence"

Outline

- Overview

  Motivation

- Pseudorandom generators

  Examples

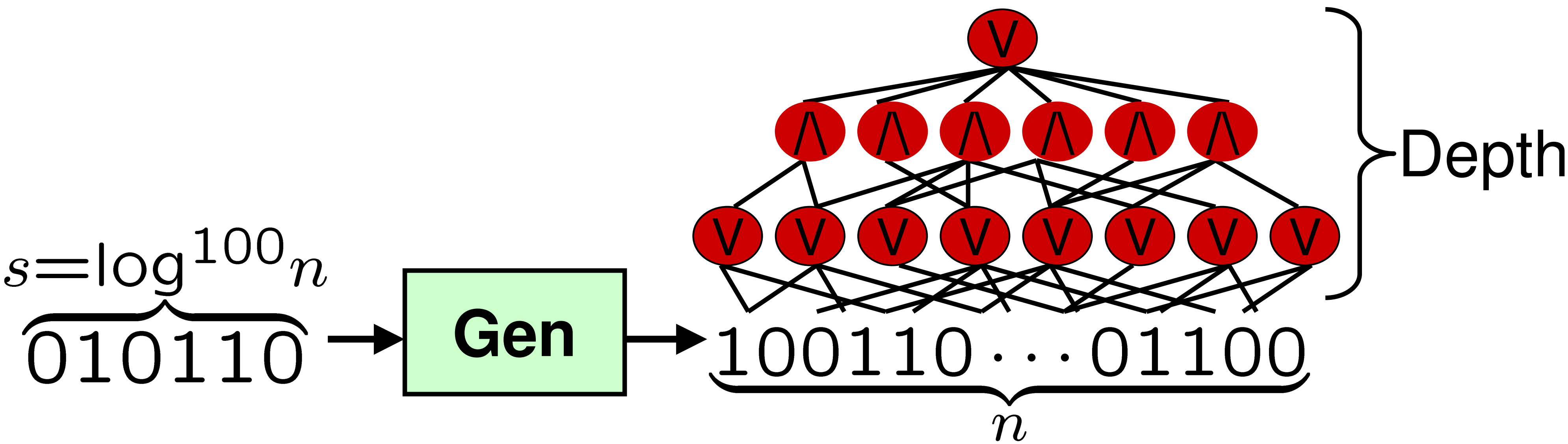
  Circuits

  Polynomials

- Future directions

Previous results for circuits

- Theorem [Nisan '91]: Generator for constant-depth circuits with AND (/\), OR (V) gates



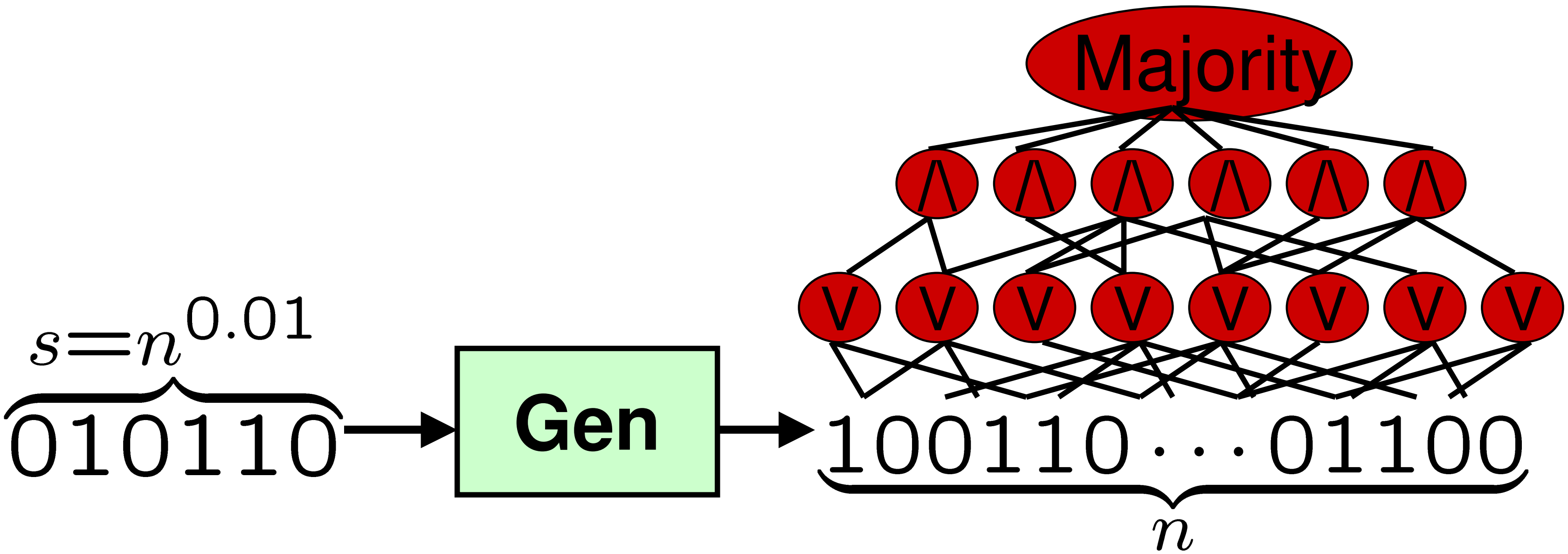
- Application to average-case "P vs NP" problem

[Healy Vadhan V.; SIAM J. Comp. STOC special issue]

Our Results

[V.; SIAM J. Comp., SIAM student paper prize 2006]

- **Theorem:** Generator for constant-depth circuits with few Majority gates



- Richest circuit class for which pseudorandom generator is known

Outline

- Overview

  Motivation

- Pseudorandom generators

  Examples

  Circuits

  Polynomials

- Future directions

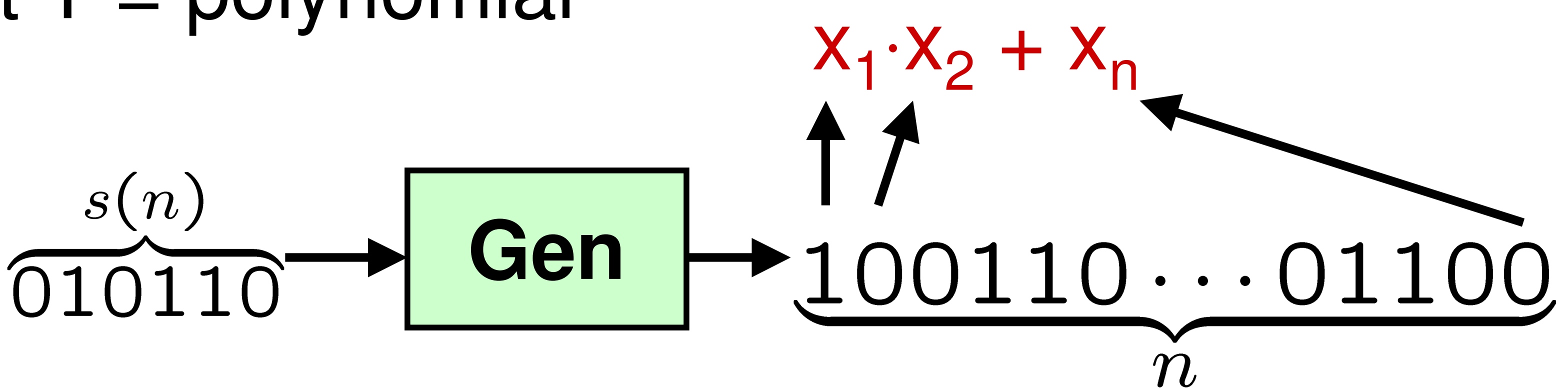
Polynomials

- Polynomials: degree d, n variables over $F_2 = \{0,1\}$

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

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

- Test T = polynomial



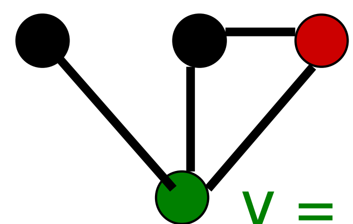
- We focus on the degree of polynomial

Previous results

- Theorem[Naor Naor '90]: Generator for linear polynomials, seed length $s(n) = O(\log n)$

- Myriad applications: matrix multiplication, PCP's

  Expander graphs:
  (sparse yet highly connected)



$x \in \{0,1\}^n$

$y = x +$ generator

- For degree $d \geq 2$, no progress for 15 years

Our results
[Bogdanov V.; FOCS ’07 special issue]

- For degree d:
  Let L $\in$ $\{0,1\}^n$ look random to linear polynomials [NN]
  bit-wise XOR d independent copies of L:

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

- Theorem:
  (I) Unconditionally: Looks random to degree d=2,3
  (II) Under “Gowers inverse conjecture”: Any degree

Recent developments after [BV]

- Th.[Lovett]: The sum of 2^d generators for degree 1 looks random to degree d, unconditionally.
  - [BV] sums d copies

- Progress on "Gowers inverse conjecture":

- Theorem[Green Tao]:
  True when |Field| > degree d
  - Proof uses techniques from [BV]

- Theorem [Green Tao], [Lovett Meshulam Samorodnitsky]:
  False when Field = {0,1}, degree = 4

Our latest result
[V. CCC ‘08]

- Theorem:
  The sum of d generators for degree 1
  looks random to polynomials of degree d.
  For every d and over any field.

  (Despite the Gowers inverse conjecture being false)

- Improves on both [Bogdanov V.] and [Lovett]

- Also simpler proof

Proof idea

- Induction: Assume for degree d,
  prove for degree-(d+1) p

  Inductive step: Case-analysis based on

  Bias(p) := $|\ \mathrm{Prob}_{\text{uniform } X}[p(X)=1] - \mathrm{Prob}_X[p(X)=0]\ |$

- Bias(p) small $\Rightarrow$ Pseudorandom bias small
  use expander graph given by extra generator

- Bias(p) large $\Rightarrow$
  (1) self-correct: p close to degree-d polynomial
  This result used in [Green Tao]
  (2) apply induction

What we have seen

- Pseudorandomness:
  Construct objects that “look random”
  using little or no randomness

- Applications to algorithms, cryptography, P vs NP

- Pseudorandom generators
  Constant-depth circuits [N,LVW, V]
  Recent developments for polynomials [BV,L,GT,LMS]
  Sum of d generators for degree 1 $\Rightarrow$ degree d [V]

Outline

- Overview

  Motivation

- Pseudorandom generators

  Examples

  Circuits

  Polynomials

- Future directions

Future directions (1)

- Pseudorandomness

  Open: Generator for polynomials of degree log n?

- Communication complexity

  Recent progress on long-standing problems

  [V. Wigderson, Sherstov, Lee Shraibman, David Pitassi V.]

- Computer science and economics

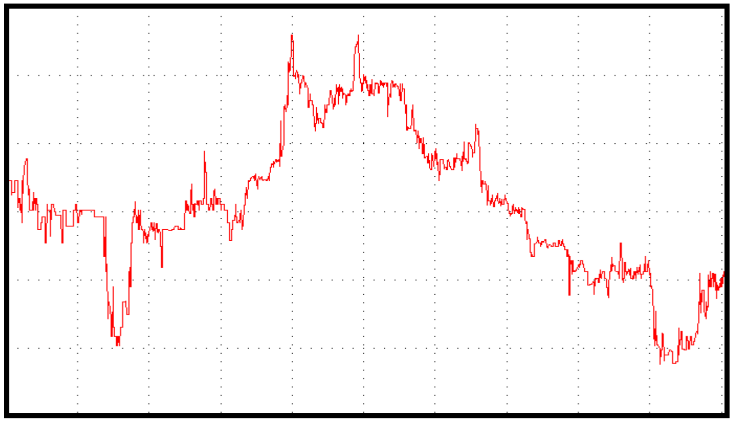
  Complexity of Nash Equilibria

  [Daskalakis Goldberg Papadimitriou, …]

  Mechanism design

Future directions (2)

- Finance



- Are markets random?

  Efficient market hypothesis

  [Bachelier 1900, Fama 1960,…]

- Raises algorithmic questions

  E.g. Zero-intelligence traders [Gode Sunder; 1993]

- Work in progress with Andrew Lo