# RANDOMNESS and COMPUTATION

Oded GOLDREICH

WEIZMANN INST., ISRAEL

http://www.wisdom.weizmann.AC.IL/~oded

+ foc.html FOUNDATIONS OF CRYPTO.
+ cc.html COMPLEXITY THEORY
+ rnc.html ~ this talk

WWW.WISDOM.WEIZMANN.AC.IL/

~ oded

# Outline

- PSEUDORANDOMNESS
- PROBABILISTIC PROOF SYSTEMS
- CRYPTOGRAPHY
- SUBLINEAR-TIME ALG.

## CLARIFICATION

"RANDOM STRING" (of specified length)

≡ string distributed uniformly among all possible

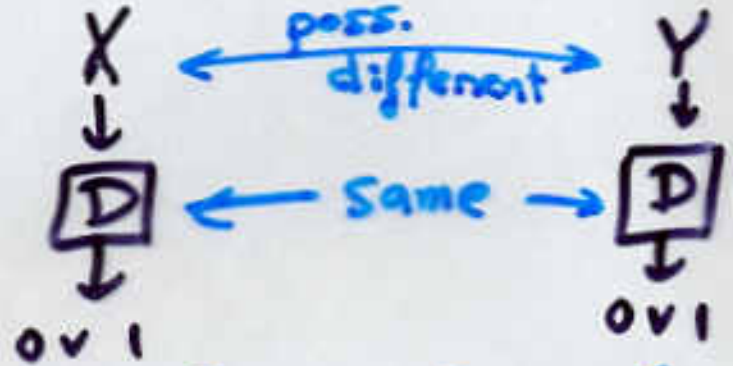
≈ sequence of unbiased coin tosses.

# PSEUDORANDOMNESS – THE CONCEPT

## IDEAL vs INDISTINGUISHABLE FROM IDEAL

(philo: indist. is enough, certainly in practice)

→ COMPUTATIONAL INDISTINGUISHABILITY




$Prob[D(X)=1] \approx Prob[D(Y)=1]$ means that D does not distinguish.

C.I. ≙ no efficient alg. distinguishes.

→ PSEUDORANDOM sequences

≙ C.I. from random.

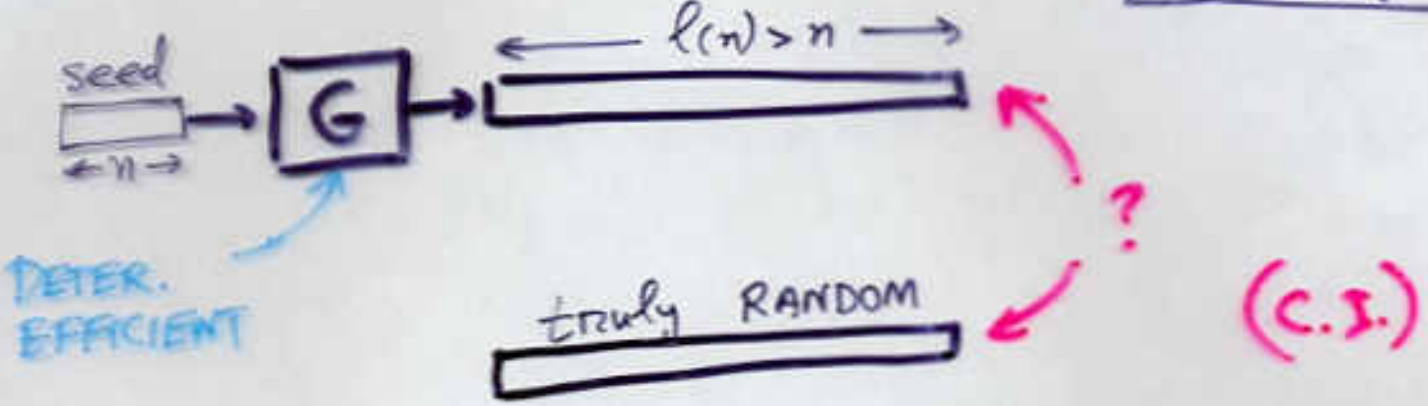
(potentially, can be generated from shorter random sequences.)

→ Other applications in Cryptography

→ defining security

# PSEUDORANDOM GENERATORS

$\ell(n) = \text{poly}(n)$




THM: IF FACTORING IS HARD (on the average)
THEN ∃ PSEUDORANDOM GENERATORS.

general paradigm

COMPUTATIONAL DIFFICULTY ⇄ PSEUDORANDOMNESS

Applications to private-key CRYPTOGRAPHY

PRG → PRF → ENC.
PRF → MAC

# P vs NP QUESTION/Conjecture

$P \cong$ class of questions that are easy to solve.

$\sim$ assertions that are easy to check

$NP \cong$ class of assertions having proofs that are easy to verify.

---

Ex: $\{n^2 : n \in \mathbb{N}\} \in P$

$\{n : n \text{ is not a prime}\} \in NP$

---

$S \in NP$ if $\exists$ poly $p$ & polytime alg. $V$ s.t. (V: verification)

Completeness: $x \in S \Rightarrow \exists y \in \{0,1\}^{p(|x|)}$ $V(x,y) = 1$ ($y$ is accepted as a proof)

SOUNDNESS: $x \notin S \Rightarrow \forall y \quad V(x,y) \neq 1$

---

$P \neq NP \sim$ "proofs are useful" (in some cases)

# PROBABILISTIC PROOF systems

PREL.: NP as a proof system

verification procedure

$S \in NP$ iff $\exists$ poly. $p$ & poly-time alg. $V$

$x \in S \Leftrightarrow \exists y \in \{0,1\}^{p(|x|)}$ $V(x,y)=1$.

($y$: certificate/witness)

Now,
allow the VERIFICATION PROC. to toss coins
& rule by statistical evidence (i.e., error prob.)
+ interaction, but still maintain total
poly-time (w.r.t. input length)

→ $IP \stackrel{def}{=}$ INTERACTIVE PROOFS
(e.g., two colon spots protocol)

THM: $coNP \subseteq IP = PSPACE$

[Recall: common conjecture is $NP \neq coNP$]

Proving $\exists$ of easily recognizable objects $= NP$

proving $\nexists$ of easily rec. obj.
can be done via an **IP**.

# PPS #2 : ZERO-KNOWLEDGE

Usually, PROOFS REVEAL KNOWLEDGE.

IN contrast, (interactive)
ZERO-KNOWLEDGE proofs reveal nothing beyond the validity of the assertion.

E.g., the "two colors graphs protocol":

THM: If FACTORING IS HARD (on the average)
then NP has zero-knowledge proofs.

⇒ proving ∃ of easily recog. obj.
without yielding any addl info.

Applications to CRYPTOGRAPHY:
"forcing proper behavior"
(i.e. behavior according to one's secrets)

without revealing these secrets!

# PPS#3: Prob. Checkable Proofs

NP has ("redundant") proof systems
[of the NP type]
that allow for probabilistic verification
that trades-off efficiency & error-probability.

In these proof systems, the probabilistic
verifier reads only a constant number
of bits in the proof, and yet

- completeness: correct assertions
  (w. adequate proofs)
  are accepted w.p. 1.

- soundness: wrong assertions
  (w. any wrong proof)
  are rejected w.p. $> 1/2$.

# RANDOMNESS and COMPUTATION

## EXERCISES

① Prove the existence of PSEUDORANDOM Sequences (w.o. eff. generat.) that are "far from RANDOM". [vs alg. or circuits]

② Prove that "IP w.o. RANDOMNESS" collapses to NP. Same for zero error probability (even just on $x \notin S$).

③ Prove that "non-interactive" (i.e. "NP type") zero-knowledge proofs exist only for BPP. Note that BPP has ("trivial") zero-knowledge proofs.

VARIOUS EXPOSITIONS ARE AVAILABLE FROM

www.wisdom.weizmann.ac.il/~oded

E.G.,

COMPLEXITY THEORY – cc.html

FOUNDATIONS of CRYPTO – foc.html

RANDOMNESS & COMPUT. – r+c.html