PSEUDORANDOMNESS
(a short survey)

by

Oded GOLDREICH

REFERENCES:

- [BM] BLUM, MICALI. SIAM J. COMPUT., Vol. 13, 1984.
  [GGM] GOLDREICH, GOLDWASSER, MICALI. JACM, Vol. 33, 198
- [GL] GOLDREICH, LEVIN. 21st STOC, 1989.
- •• [GM] GOLDWASSER, MICALI. JCSS, Vol. 28, 1984.
- [Y] YAO. 23rd FOCS, 1982.

MOTIVATION

PSEUDORANDOMNESS – A BEHAVIORISTIC APPROACH:

A DISTRIBUTION IS PSEUDORANDOM IF IT "LOOK RANDOM" TO ALL "EFFICIENT TESTS".

⇒ PSEUDORANDOM DISTRIBUTIONS ARE "COMPUTATIONALLY EQUIVALENT" TO UNIFORM DISTRIBUTIONS.

⇒ PSEUDORANDOM SEQUENCES CAN REPLACE "TRUELY RANDOM" SEQUENCES IN ALL "EFFICIENT APPLICATIONS". E.G., IN

- PROBABILISTIC ALGORITHMS
- PROBABILISTIC CONSTRUCTIONS
- CRYPTOGRAPHY

KEY NOTION: COMPUTATIONAL INDISTINGUISHABILITY [GM, Y]

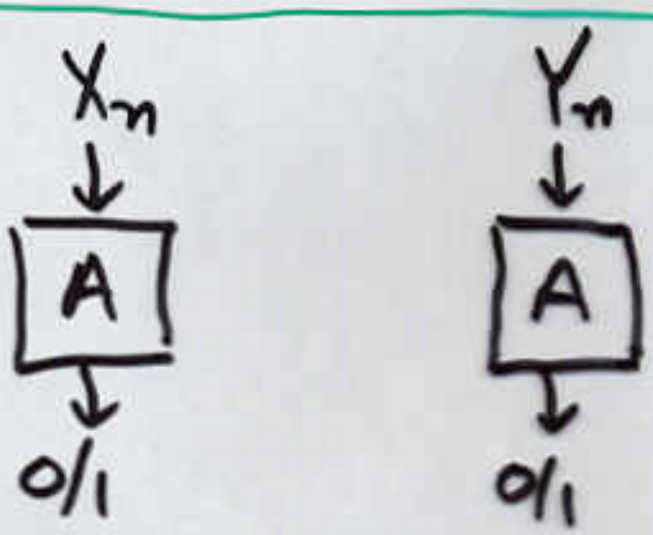
LET X_n & Y_n BE RANDOM VARIABLES RANGING OVER $\{0,1\}^n$.

$\{X_n\}_n$ & $\{Y_n\}_n$ ARE **POLYNOMIALLY INDISTINGUISHABLE**

IF $\forall^{(\text{PROB.})}$ POLY-TIME ALGORITHM A $\forall c>0$

$\forall$ SUFFICIENTLY LARGE n

$$\left|\text{PROB}(A(X_n)=1) - \text{PROB}(A(Y_n)=1)\right| < \frac{1}{n^c}$$



PSEUDORANDOMNESS & EXAMPLES

- U_n DENOTES UNIFORM DIST. OVER $\{0,1\}^n$

DEF: $\{X_n\}_n$ IS PSEUDORANDOM IF IT IS POLYNOMIALLY INDISTINGUISHABLE OF $\{U_n\}$

EXAMPLE 1: X_n UNIFORM OVER $\left\{\alpha \in \{0,1\}^n : \begin{array}{l}\#\ 0\text{'s IN} \\ \alpha \text{ IS } \lfloor n/2 \rfloor\end{array}\right\}$

$\{X_n\}$ IS NOT PSEUDORANDOM AS THE TEST A OUTPUTTING 1 IFF $\#_0(\alpha) = \lfloor n/2 \rfloor$ HAS

$$\text{PROB}(A(X_n)=1) = 1$$

$$\text{PROB}(A(U_n)=1) \approx 1/\sqrt{n}$$

EXAMPLE 2: X_n UNIFORM OVER $\{0,1\}^n - \{ww\}$

X_n AND U_n ARE STATISTICALLY CLOSE

$$\sum_{\alpha} \left| \text{PROB}(X_n=\alpha) - \text{PROB}(U_n=\alpha) \right|$$

$$= \sum_{ww} \left| 0 - \frac{1}{2^n} \right| + \sum_{\substack{\alpha = wu \\ w \neq u}} \left| \frac{1}{2^n - 2^{n/2}} - \frac{1}{2^n} \right| < \frac{2}{2^{n/2}}$$

On the non-triviality of PseudoRANDOMNESS
(or, of comput. indisting.)

THM: ∃ Pseudorandom distributions that are statistically far from uniform.

This unconditional result uses a non-explicit construction.

THM: "effective" non-triviality of Comp. Ind
⟺ ∃ one-way functions
⟺ pseudorandom generators.

Proof "outline"

∃ OWF ⇒ ∃ PRG

*⇒ "effective non-triviality"

*) This is the only easy/trivial part.

PSEUDORANDOM GENERATORS - DEF. [BM, Y]

A PR GENERATOR IS AN EFFICIENT ALGORITHM EXPANDING "RANDOM" STRINGS INTO LONGER PSEUDORANDOM SEQUENCES.

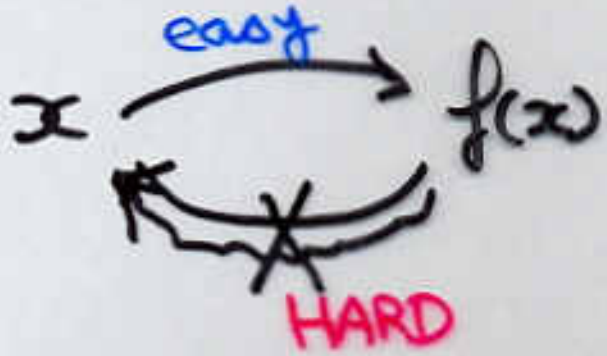
DEF: LET $G:\{0,1\}^n \to \{0,1\}^{\ell(n)}$ BE A DETERMINSTIC POLY-TIME ALGORITHM, WHERE $\ell(n) > n$.

G IS A PSEUDORANDOM GENERATOR (PRG) IF $\{G(U_n)\}_n$ AND $\{U_{\ell(n)}\}_n$ ARE POLYNOMIALLY-INDISTINGUISHABLE.

- ℓ IS THE EXPANSION FACTOR OF G.

On the existence of PRG

One-way function



E.G: $(p, q) \longrightarrow p \cdot q$
$|p| = |q|$

Thm: If $\exists$ one-way functions
then $\exists$ pseudorandom generators.

Proof for special case (f is 1-1 and $|f(x)| = |x|$):

Lemma 1: $\exists$ one-way f (of special case)
$\Rightarrow \exists$ PRG with expansion $Q_1(n) = n+1$.

Lemma 2: $\exists$ PRG with expansion $Q_1(n) = n+1$
$\Rightarrow \forall$ poly. Q $\exists$ PRG with expansion Q.

PROOF OUTLINE FOR LEMMA 1 [GL]

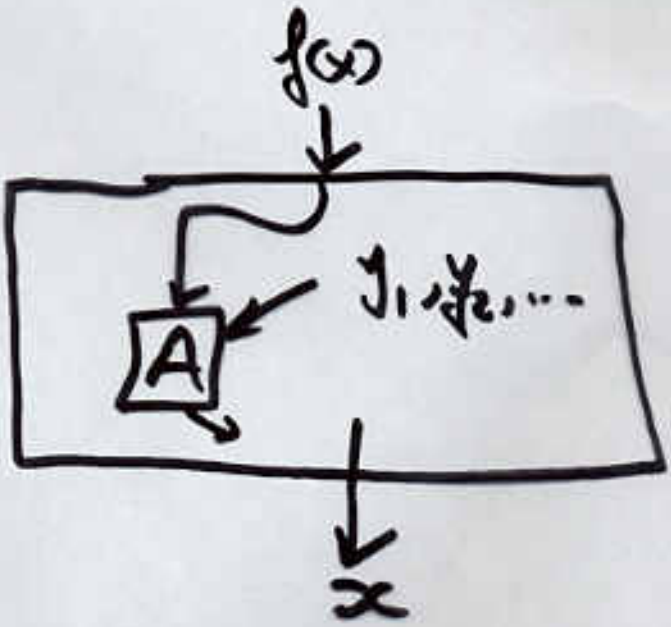
LET f BE ONE-WAY AS GUARANTEED.

- THEN $\forall$ POLY-TIME A $\forall c>0$ AND SUFF. LARGE n

$$\text{PROB}\left(A(f(x),y) = \left(\sum_{i=1}^{n} x_i y_i \bmod 2\right)\right) < \frac{1}{2} + \frac{1}{n^c}$$

$f'(x,y) = f(x),y$ $\quad$ $b(x,y)$ = INNER PRODUCT MOD 2

OTHERWISE



- IT FOLLOWS THAT

$$G(x,y) \triangleq f(x) \circ y \circ b(x,y)$$

IS A PSEUDORANDOM GENERATOR (WITH EXP. D_n).

CONTRADICTION ARGUEMENT FOR

$$\text{PROB}\left(A(f(x),y) = b(x,y)\right) > \frac{3}{4} + \varepsilon$$

unrealistic!

A MENTAL EXPERIMENT (FIXED x)

$x = 101$

ALL y's	$b(x,y)$		$A(f(x),y)$
000	0	=	0
001	1	=	1
010	0	=	0
011	1	≠	0
100	1	=	1
101	0	=	0
110	1	=	1
111	0	=	0

GUESSING THE i-th BIT OF x, DENOTED x_i

- CHOSE y AT RANDOM
- LET $y^{(i)}$ BE y WITH i-th BIT FLIPPED.

$$x_i = b(x,y) \oplus b(x,y^{(i)})$$

WITH PROB $\geq \frac{1}{2} + 2\varepsilon$

$$= A(f(x),y) \oplus A(f(x),y^{(i)})$$

∎

CONTRADICTION ARGUEMENT FOR

$$\text{PROB}(A(f(x), y) = b(x, y)) > \frac{1}{2} + \varepsilon$$

- L_k LIST OF CANDIDATES FOR k-PREFIX OF x

- FOR "MANY" $y'' \in \{0,1\}^{n-k}$

$$\text{PROB}(A(f(x), y'y'') = b(x, y'y''))$$

IS AWAY FROM $1/2$

AND SO IS

$$\text{PROB}(A(f(x), y'y'') = b(x', y'))$$

(WHERE x' IS K-PREFIX OF x)

- $\forall\, y''$ VERY FEW $z' \in \{0,1\}^k$ HAVE

$$\text{PROB}(A(f(x), y'y'') = b(z', y'))$$ AWAY FROM $\frac{1}{2}$.

- $L_{k+1} \leftarrow \{z'\sigma : z' \in L_k, \sigma \in \{0,1\} \text{ s.t. } \ldots(z'\sigma)\}$

LEMMA 2 - PROOF SKETCH

LET G_1 BE A PRG WITH EXPANSION $Q_1(n) = n+1$

AND Q BE A POLYNOMIAL.

$$G_Q(r) = \sigma_1 \sigma_2 \cdots \sigma_{Q(|r|)}$$

WHERE $r_0 = r$

$$r_1 \sigma_1 = G_1(r_0)$$
$$\vdots$$
$$r_i \sigma_i = G_1(r_{i-1})$$

- G_Q IS A PRG WITH EXPANSION Q

INTUITION: ASSUME

(1) X_n IS PSEUDORANDOM

(2) G_1 IS PR GENERATOR

THEN $G_1(X_n)$ IS PSEUDORANDOM.

$$X_n \overset{(2)}{\approx} U_n$$
$$\Downarrow$$
$$G_1(X_n) \equiv G(U_n) \overset{(2)}{\approx} U_{n+1}$$