# Hardness versus Randomness

NOEL ARTECHE
(Lund University)

Meta-Complexity Project — ILLC, Amsterdam
(January 2024)

# Randomness

A language $L \subseteq \{0,1\}^*$ is in ...

P **BPP** if $\exists$ poly-time TM $M(x,r)$ s.t.

$$x \in L \Rightarrow \Pr_r[M(x,r)=1] \geq 2/3$$

$$x \notin L \Rightarrow \Pr_r[M(x,r)=1] < 1/3$$

NP **MA** if $\exists$ poly-time TM $V$ and a polynomial $p$

$$x \in L \Rightarrow \exists w \in \{0,1\}^{p(|x|)} : \Pr_r[V(x,w,r)=1] \geq 2/3$$

$$x \notin L \Rightarrow \forall w \in \{0,1\}^{p(|x|)} : \Pr_r[V(x,w,r)=1] < 1/3$$

P vs. NP        BPP vs. MA

But wait... NP is also $\{L \subseteq \{0,1\}^* \mid L \leq_p SAT\}$.

↳ $\exists$ reductions $R$ : $x \in L \iff R(x) \in SAT$.

So an alternative "randomized NP" is

$$AM := \{L \subseteq \{0,1\}^* \mid L \leq_r SAT\}$$

Randomized reduction $R$
$$\begin{cases} x \in L \implies \Pr_r[R(x,r) \in SAT] \geq 2/3 \\ x \notin L \implies \Pr_r[R(x,r) \in SAT] < 1/3 \end{cases}$$

$$P \subseteq ZPP \subseteq RP \subseteq BPP \subseteq MA \subseteq AM$$
$$RP \subseteq NP \subseteq MA$$

Derandomization is about making all these classes COLLAPSE!

# Non-uniformity buys you randomness

**Theorem.** (Adleman, 1977)

BPP $\subseteq$ P/poly.

**Proof.** Suppose $M(x, r)$ is a randomized machine. Do error-reduction. Suppose $r \in \{0,1\}^m$.


$\{0,1\}^m$

($2^m$ strings)

In fact, $\bigcup_{x_i \in \{0,1\}^n} \text{Bad}_i \subsetneq \{0,1\}^m$ so some $r$ is "good" for all $x$.

# The HARDNESS versus RANDOMNESS PARADIGM

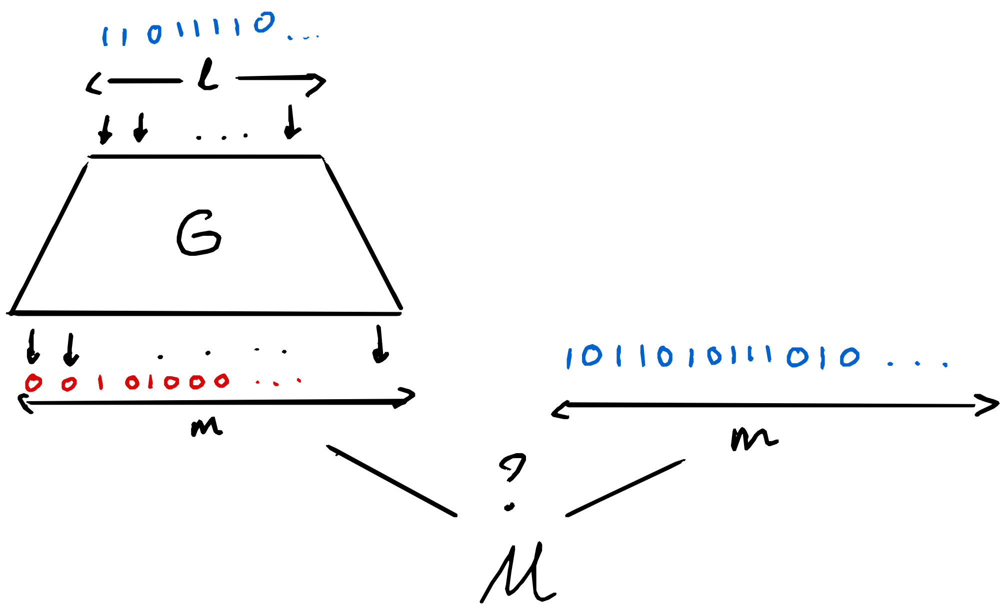
(literally their title!)

- Nisan & Wigderson '88
- Impagliazzo & Wigderson '97

↪ "CIRCUIT LOWER BOUNDS imply DERANDOMIZATION"

# How can one derandomize?

Use FAKE randomness! a.k.a PSEUDORANDOMNESS



**Def.** (Complexity-theoretic PRG)

A function $G : \{0,1\}^{\ell} \to \{0,1\}^{m}$ is an $\varepsilon$-PSEUDORANDOM GENERATOR of STRETCH $S(\ell)$ AGAINST $\mathcal{C}$ if

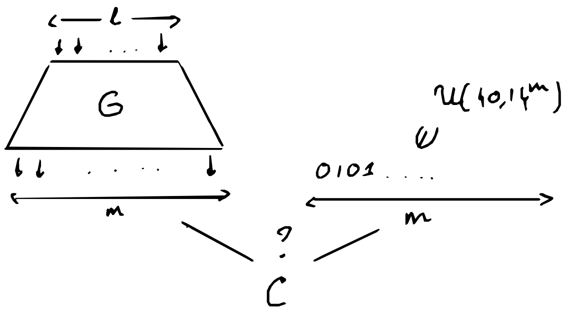
Circuit class

(i) $G$ runs in time $2^{O(\ell)}$;

(ii) $m = S(\ell)$;

(iii) for every circuit $C$ in $\mathcal{C}$,

$$\left| \Pr_{r \sim \{0,1\}^{\ell}}[C(G(r))=1] - \Pr_{u \in \{0,1\}^{m}}[C(u)=1] \right| < \varepsilon .$$




For us,

- $\varepsilon = 1/10$;
- stretch $S(\ell) = 2^{O(\ell)}$
- $\mathcal{C} = \mathbf{SIZE}(n^3)$.

**Note!** It suffices to derandomize

$\mathrm{BPTIME}(n)$, even assuming we use EXCTLY $n$ random bits.

↳ PADDING!

If $L \in \mathrm{BPTIME}(n^c)$, let

$$L' := \{ x \cdot 1^{|x|^c} \mid x \in L \}.$$

Then, $L' \in \mathrm{BPTIME}(n)$.

So $\mathrm{BPTIME}(n) \subseteq P$ suffices!

<u>Idea</u>: Use a PRG with exponential stretch!

$$G : \{0,1\}^{O(\log n)} \longrightarrow \{0,1\}^{O(n)}$$ pseudorandom against $SIZE(n^3)$.

Simulate $\overset{\text{time } O(n)}{M}(x, r)$ as follows:

1. Enumerate all SEEDS: $s \in \{0,1\}^{O(\log n)}$
   ↳ $2^{O(\log n)} = n^{O(1)}$
2. Run $M(x, G(s))$. Record the output.
   ↳ Time $n^{O(1)}$
3. If the majority accepted, accept.

We run in polynomial-time!

But did we fool $M$?

Suppose NOT. i.e. there are infinitely many inputs $x \in \{0,1\}^k$ s.t.

$$\Pr_r[M(x,r)=1] \not\approx^{\pm\varepsilon} \Pr_s[M(x,G(s))=1]$$

Consider the circuit $\boxed{C = M_x(r)}$; $|C| = O(n^2)$.

But this circuit is a DISTINGUISHER!

↳ So $G$ is NOT pseudorandom against SIZE$(n^3)$!

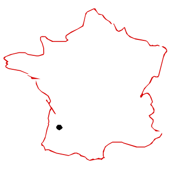
CONTRADICTION!

Actually, only need to fool SIZE$(n^2)$ or even lower!

# Cryptographic vs. Complexity-Theoretic PRGs

(HILL'99)
[Håstad-Impagliazzo-Levin-Luby '99]

If OWFs exist, then there are CRYPTOGRAPHIC PRGS.



| | Running time $T$ | Stretch $S(\ell)$ | Adversaries $C$ |
|---|---|---|---|
| CRYPTO PRG | $\ell^c$ | $\ell+1$ | BPP |
| CT PRG | $2^\ell$ | $2^\ell$ | $SIZE(n^3)$ |

Yes! Under believable assumptions
(i.e. circuit lower bounds)

**Nisan & Wigderson '88**

Suppose there exists a function $f \in E$ which is HARD ON AVERAGE for subexponential-size circuits. Then, "good" CT-PRGs exist.

- $E = TIME(2^{O(n)})$ vs. $EXP = TIME(2^{n^{O(1)}})$
- "subexponential": $2^{o(n)}$ i.e. $SUBEXP/poly = \bigcap_{\varepsilon > 0} SIZE(2^{\varepsilon n})$
- "on average": $\forall C : \Pr_{x \in \{0,1\}^n}[C(x) = f(x)] < \frac{1}{2} + \frac{1}{|C|}$

**Nisan - Wigderson '88**

If there $f \in E$ that it is AVERAGE-CASE HARD for subexponential-size circuits, then $P = BPP$

WORST-CASE TO AVERAGE-CASE REDUCTION!

**Impagliazzo - Wigderson '97**

If thre is $f \in E$ such that it is WORT-CASE HARD for subexp-size circuits, then $P = BPP$

# So suppose I have a hard $f$ ...

# HOW DO I BUILD A PRG?

**TOY EXAMPLE**: Stretch $\ell + 1$

Ingredients I have:
* $\ell$ truly random bits
* time $2^{O(\ell)}$
* hard function $f \in E$,
  $f : \{0,1\}^\ell \to \{0,1\}$

Well... $G(s) := (s, f(s))$

one bit!

☑ Stretch $\ell+1$ □ Pseudorandom against
☑ Time $2^{O(\ell)}$ ? $\mathrm{SIZE}(n^3)$

*Proof.* Use YAO'S NEXT-BIT PREDICTOR THEOREM
(a.k.a. "unpredictability $\Rightarrow$ pseudorandomness")

Let $G : \{0,1\}^{\ell} \to \{0,1\}^{m}$. Suppose there is $S > O(n)$ and $\varepsilon > 0$ such that for all circuit of size $2 \cdot S$, for every $i \in [m]$

$$\Pr_{s \in \{0,1\}^{\ell}}\left[ C(G_1(s), G_2(s), \ldots, G_{i-1}(s)) = G_i(s) \right] \leq \frac{1}{2} + \frac{\varepsilon}{m}.$$

Then, $G$ is $\varepsilon$-pseudorandom against size $S$.

If $G(s) = s \cdot f(s)$ is NOT pseudorandom, there is $C$ and $i \in [m]$ s.t. $C$ predicts the $i$-th bit. But $i$ can only be $m$, since $s \in \{0,1\}^{\ell}$ is actually random.

For $\ell+2$ bits...

$$G(s) := s_1 \cdots s_\ell \cdot f(s_1 \cdots s_{\ell/2}) \cdot f(s_{\ell/2+1} \cdots s_\ell)$$

In general, $\ell+k$ bits by splitting $s$ in $\ell/k$ sections...

But limit is $k=\ell$ i.e $\ell+\ell = 2\ell$

$$G(s) := s_1 \cdots s_\ell \cdot f(s_1) \cdot \cdots \cdot f(s_\ell)$$

If we want $k \cdot \ell$ for $k > 2$,

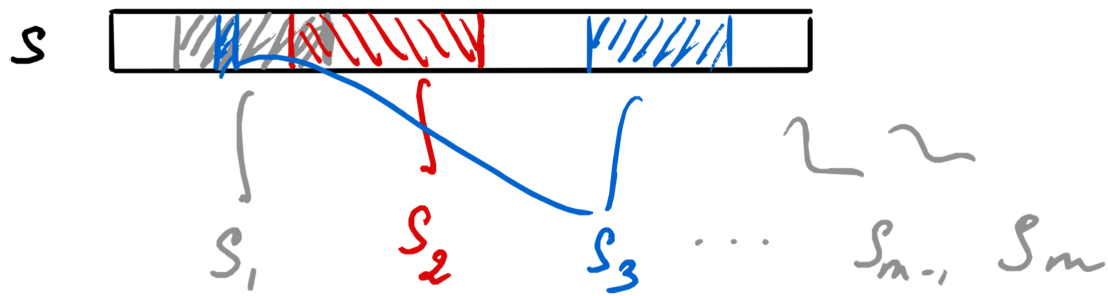
NEW IDEAS NEEDED...

let alone $2^\ell$...

In general, for

$$G : \{0,1\}^{\ell} \to \{0,1\}^{m}$$

split $s \in \{0,1\}^{\ell}$ into $m$ (overlapping) sections




and output

$$G(s) := f(s_1) \cdot \ldots \cdot f(s_m)$$

But the partition must be careful…

## Idea: COMBINATORIAL DESIGNS

A collection $\mathcal{A} = \{S_1, \dots, S_m\}$, $S_i \subseteq \{1, \dots, \ell\}$ is an $(\ell, k, t)$-DESIGN if

i) $|S_i| = t \quad \forall i \in [m]$

ii) $|S_i \cap S_j| \leq k \quad \forall i,j \in [m],\ i \neq j$

We view $\mathcal{A}$ as a 0/1 $m \times \ell$ matrix:

$$A = \begin{array}{c} S_1 \\ S_2 \\ \vdots \\ \\ S_m \\ \\ \end{array} \begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots \\ 1 & 1 & 0 & \cdots & \vdots \\ 0 & 1 & 1 & \cdots & \vdots \\ & \vdots & & a_{i,j} & \\ 1 & 1 & 0 & \cdots & \end{pmatrix} \begin{array}{c} \\ \end{array}$$
$$\quad\quad\quad\quad 1 \;\; 2 \;\; 3 \;\; \cdots \;\; \ell$$

$a_{i,j} = 1$

$\Updownarrow$

$j \in S_i$

# The Nisan-Wigderson generator

Suppose $f : \{0,1\}^n \to \{0,1\}$ is the HARD ON AVERAGE FUNCTION.

Suppose $A = \{S_1, \dots, S_m\}$ is an $(\ell, \log n, n)$ design.

universe $[\ell]$

intersection $|S_i \cap S_j|$

$|S_i|$

Then, $NW^f_A : \{0,1\}^{\ell} \longrightarrow \{0,1\}^m$

$$s \longmapsto f(s\restriction_{S_1}) \cdots f(s\restriction_{S_m})$$

is pseudorandom against $SIZE(n^3)$.

Stretch?
To get $m = n^{O(1)}$, choose $\ell = O(\log n)$; then it run in time $n^{O(1)} \cdot 2^{O(n)} = 2^{O(n)}$

**Proof.** Sophisticated version of the $l+1$ generator argument, using Yao's thm.

There's something left...

Do $(l, \log n, n)$-DESIGNS even exist ???

**Lemma.** Let $l \in \mathbb{N}$. There exists a family $\{A_n\}_{n \in \mathbb{N}}$ of $(l, \log n, n)$-designs. Furthermore, there's a poly-time TM $M$ s.t. $M(1^n) = A_n$.

# Recap

[IW'97]

$\boxed{\exists f \in E \text{ subexponentially hard for circuits in WC}}$ $\Longrightarrow$ $\exists f \in E$ subexponentially hard for circuits on AVG

$\Downarrow$ [NW'88]

The $NW^f$ generator has exponential stretch and is pseudorandom against $SIZE(n^3)$

(Yao) $\Longleftarrow$

$BPTIME(n) \subseteq P$

$\Uparrow$

(padding)

$P = BPP$

$\boxed{\exists f \in E \text{ subexponentially hard for circuits on AVG.}}$

$$P \subseteq ZPP \subseteq RP \subseteq BPP \subseteq MA \subseteq AM$$

$$RP \subseteq NP \subseteq MA$$

???

?

$MA \overset{?}{=} NP$

**MA** if $\exists$ poly-time TM $V$ and a polynomial $p$

$$x \in L \Rightarrow \exists w \in \{0,1\}^{p(|x|)} : \Pr_r[V(x,w,r)=1] \geq 2/3$$

$$x \notin L \Rightarrow \forall w \in \{0,1\}^{p(|x|)} : \Pr_r[V(x,w,r)=1] < 1/3$$

$$AM = \{ L \subseteq \{0,1\}^* : L \leq_r SAT \}$$

↳ randomized reductions!

Randomized reduction $R$

$\forall x \in \{0,1\}^*$ $\quad x \in L \implies R(x) \in SAT$ (w.h.p.)

$\quad x \notin L \implies R(x) \notin SAT$ (w.h.p.)

$$NP \stackrel{?}{=} AM$$

$\exists f \in E$ subexponentially hard for circuits on AVG.

$\exists f \in E$ subexponentially hard for circuits on AVG., even in the presence of SAT oracle gates

# Recap

Believable, but HARD ... NATURAL PROOFS

[IW'97]

$\boxed{\exists f \in E \text{ subexponentially hard for circuits in WC.}}$ $\Longrightarrow$ $\exists f \in E$ subexponentially hard for circuits on AVG

$\Uparrow$ (kind of)

$\Downarrow$ [NW'88]

P = BPP

(padding) $\Uparrow$

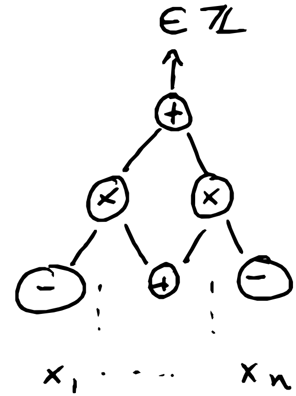
The $NW^f$ generator has exponential stretch and is pseudorandom against $SIZE(n^3)$

$BPTIME(n) \subseteq P$ $\Longleftarrow$ (Yao)

Can we find an alternative route?

Kabanets & Impagliazzo '03 ... No

# POLYNOMIAL IDENTITY TESTING (PIT)




Input : Arithmetic circuit $C$ over $\mathbb{Z}$.

Goal : Is $C \equiv 0$ ?

**Fact.**

$\text{PIT} \in \mathbf{coRP} \subseteq \mathbf{BPP}$.

If $\mathbf{BPP} = \mathbf{P}$, then of course $\text{PIT} \in \mathbf{P}$ . . .
and the converse is almost true!

↳ "PIT is 'derandomization-complete'"

**Theorem** (Kabanets - Impagliazzo '03)
Suppose $\text{PIT} \in \mathbf{P}$. Then, either
$\mathbf{NEXP} \not\subseteq \mathbf{P}/\text{poly}$ or $\text{Perm} \notin \mathbf{AlgP}/\text{poly}$.

# So... randomness is useless?

**RANGE AVOIDANCE** (a.k.a. AVOID)

- Input: circuit $C : \{0,1\}^n \to \{0,1\}^{n+1}$
- Task: output $y \in \{0,1\}^{n+1}$ s.t. $y \notin \mathrm{rng}(C)$

$\forall x \in \{0,1\}^n : C(x) \neq y$

**Prop.** RANGE AVOIDANCE $\in$ FBPP.

**Proof.** Choose $y \in_R \{0,1\}^{n+1}$. $\Pr_{y \in_R \{0,1\}^{n+1}} [\forall x : C(x) \neq y] \geq 1/2$. $\square$

So... $FP = FBPP$ and RANGE AVOIDANCE $\in FP$?

"The Hardest Explicit Construction"

**Theorem.** (Korten, 2021)

If RANGE AVOIDANCE $\in$ **FP** (or even $\mathbf{FP}^{\mathbf{NP}}$), then there exists $f \in \mathbf{E}$ without subexponential-size circuits.

Proof idea. Consider the circuit $T : \{0,1\}^{n^c} \to \{0,1\}^{2^n}$ mapping a circuit of size $n^c$ to its truth table.

Clearly, some truth-tables don't have $n^c$-circuits.

An algorithm for RANGE AVOIDANCE would give us a "hard truth table".

In fact, under CRYPTOGRAPHIC ASSUMPTIONS,
RANGE AVOIDANCE $\notin$ FP unless NP = coNP.

(Li-Ilango-Williams '21)

Meta-Complexity paper

Actually...

Theorem. (Aaronson-Buhrman-Kretschmer '23)
Unconditionally, FBPP $\neq$ FP.

So randomness IS useful...
sometimes.

# Derandomization in PH

Recall we don't know if $BPP \overset{?}{\subseteq} NP$.

<u>Theorem</u>. (Sipser - Gács - Lautemann)

$BPP \subseteq \Sigma_2 P \cap \Pi_2 P$.

Proof. $BPP \subseteq \Sigma_2 P$.

$\hookrightarrow \underset{\underset{BPP}{\shortparallel}}{coBPP} \subseteq co\Sigma_2 P = \Pi_2 P$

So, 1) Guess hard truth table $f$. ($\exists$)

2) Check NO small circuit computes it ($\forall$).

3) Use $NW^f$.

QED.

# Recap

- HARDNESS can be traded for RANDOMNESS: following the NISAN-WIGDERSON paradigm of COMPLEXITY-THEORETIC PRGs,

  $\exists$ HARD function (a.k.a. circuit lower bounds) $\Longrightarrow$
  - $P = BPP$
  - $NP = MA = AM$

- Unfortunately, circuit lower bounds are needed for DERANDOMIZATION.

- In meta-complexity, reductions are often RANDOMIZED... in the hope of DERANDOMIZING later.