Impagliazzo's Five Worlds

P vs NP and Cryptography

$\mathbb{P} \neq \mathbb{NP} \Longleftarrow$ Existence of 1-way functions (Secure encryption with keys polynomially smaller than messages)

$\Uparrow$

$\mathbb{NP} \neq \text{co-}\mathbb{NP} \Longleftarrow$ Public Key Cryptography
Needs "highly structured 1-way functions" (FACTORING, DISCRETE LOG)

---

(1) Algorithmica: $\mathbb{P} = \mathbb{NP}$

No cryptography. But amazing algorithms.

Non-determinism can be efficiently simulated.

2) Heuristica: $\mathbb{P} \neq \mathbb{NP}$ but $\mathbb{NP}$ is "easy on average".

~~A 1-way implies that~~ If $\mathbb{NP}$ problems can be solved (efficiently) on "random" inputs, then 1-way functions do not exist.

[Levin] Theory of average-case complexity

Maybe $\mathbb{P} \neq \mathbb{NP}$ (for $L \in \mathbb{NP}$, hard inputs exist).

~~Combina~~ Maybe coming up with hard inputs is itself hard!

Let A be an (det.) algorithm that solves/decides an $\mathbb{NP}$ language L.

$\forall \mathcal{D}$

$$\boxed{\mathop{\mathbb{E}}_{\substack{x \sim \mathcal{D} \\ x \in \{0,1\}^n}} [\text{running time of } A \text{ on } x] \leqslant n^c}$$

$\mathcal{D}$ ← distribution of inputs

Furthermore $\mathcal{D}$ is "poly-time" samplable: samples for $\mathcal{D}$ can be generated in polynomial time.

Then $L \in \text{dist}\,\mathbb{P}$

Maybe $\text{dist}\,\mathbb{NP} \subseteq \text{dist}\,\mathbb{P}$.

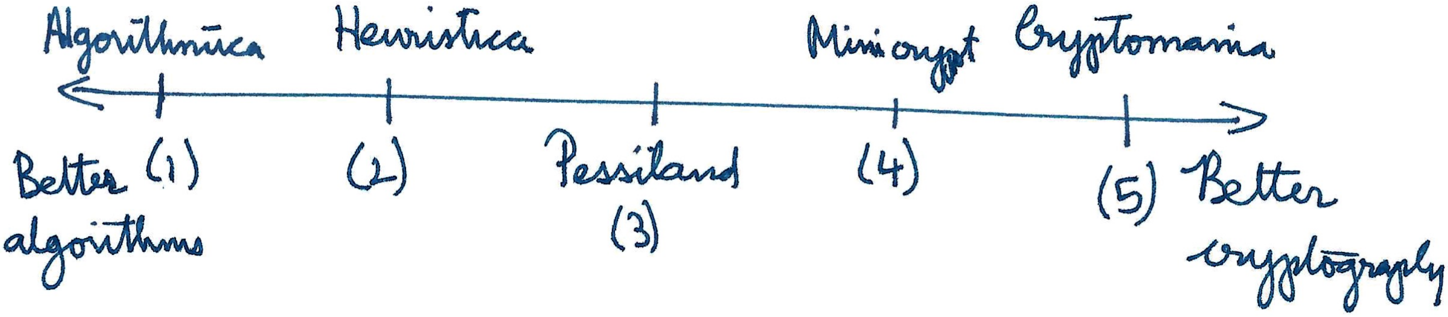
If 1-way fn. exist, $\text{dist}\,\mathbb{NP} \not\subseteq \text{dist}\,\mathbb{P}$.

(2) <u>Heuristica</u>: $\mathbb{P} \neq \mathbb{NP}$ but $\text{dist}\,\mathbb{NP} = \text{dist}\,\mathbb{P}$

1-way fns. do not exist. No cryptography.

But we can "practically" solve any $\mathbb{NP}$ problem.

(Random SAT: choose 3CNF randomly. One can generate seemingly hard instances for any solver.)



5) Cryptomania: FACTORING is hard (not solvable in polynomial time). (we think $\mathbb{NP} \neq \text{co-}\mathbb{NP}$)

We think we live in this world.

Public key crypto, PRGs, etc.

But algorithms are "weak" against $\mathbb{NP}$ problems.

4) Minicrypt: FACTORING is easy (maybe $\mathbb{NP} \cap \text{co-}\mathbb{NP} = \mathbb{P}$)

No Public-Key Crypto, as far as we know

But one-way fns. exist.

PRGs, secure encryption with poly. smaller keys

3) Pessiland: $\text{dist}\,\mathbb{P} \neq \text{dist}\,\mathbb{NP}$ & one-way fns. do not exist.

No algorithmic benefits, no crypto

Can we rule out Pessiland?

Quantum computing

[Shor 94] A (suitable) quantum computer can factor integers in polynomial time.

BQP ← poly time quantum algorithms

BPP = BQP (Church-Turing thesis extended)

FACTORING & BPP

Quantum computers can be physically built.

Shor's algorithm requires a specific kind on quantum computer (NOT adiabatic, which is what most startups are building).

Levin & Goldreich: Shor's algorithm requires measurement of "superposition" (and other physical quantities) at a precision far far beyond our (current) capacities.

FACTORING : best algorithm $2^{[(\log N)^{1/3} \ldots]}$ ← Subexponential!

(N = size $\boxed{\log_2 N} = n$)

$2^{n^{1/3}}$ ↔ $2^{\alpha n}$ ← constant

SAT : The best algorithm are $2^{\alpha n}$

Graph Isomorphism : [Babai 16] Algorithm runtime $n^{\text{poly}(\log n)}$.

What is the optimal running time for SAT?

It is $\geq 2^{\alpha n}$ (α constant) : ETH (Exponential Time Hypothesis)

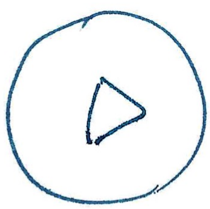
For k-SAT, runtime as $k \to \infty$ $\geq \underline{2^n}$ (upto poly factors) SETH (Strong ETH)

Finer-grained Complexity

<u>Complexity within P</u> : Depends on RAM model vs TMs.

RAM model, and linear time reductions.

If there are subquadratic time algorithms for many problem stuck at quadratic time (edit distance, subgraph counting . .), then SETH is false.

$G =$ 

<u>Counting triangles / finding triangle</u>

The complexity of this problem (we think $\geq m^{4/3}$) can be related to other problems via reductions

m = # edges

Why is progress of $\mathbb{P}$ vs $\mathbb{NP}$ stalled?

For every technique proposed, in a few years, someone proves impossibility for that technique.

$$\mathbb{P} \neq \mathbb{EXP} \leftarrow \text{diagonalization}$$

[Baker-Gill-Solovay 70s] No! Diagonalization proofs ~~do~~ ~~not~~ "relativize" but $\mathbb{P}$ vs $\mathbb{NP}$ does not relativize...

$\exists$ lang. B s.t. $\mathbb{P}^B = \mathbb{NP}^B$ $\qquad$ $\exists$ lang. B s.t. $\mathbb{P}^B \neq \mathbb{NP}^B$

Diagonalization proofs enumerate code, which is independent of oracle.

[Razborov-Rudich 94] "Natural proofs" cannot separate $\mathbb{P}$ vs $\mathbb{NP}$. ($\mathbb{NP} \not\subseteq \mathbb{P}/\text{poly}$), assuming 1-way fns. exist.

[Mulmuley-Sohoni 2000-2010s] Geometric Complexity Theory (GCT).

A new approach for $\mathbb{P}$ vs $\mathbb{NP}$ using algebraic geometry.

Recently, barriers for GCT have been found.

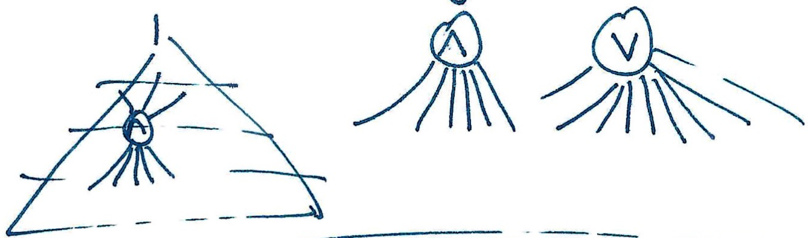
A success story:

[Williams 2014] NEXP does not have constant depth circuits (with mod gates).

[Håstad 99] Prove circuit lower bound.

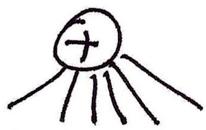
Simplest kind of circuit. Constant depth, but unbounded fanin

AC_0



Parity $\notin AC_0$ $\quad x_1 \cdots x_n \quad \boxed{x_1 \oplus x_2 \cdots \oplus x_n}$

Suppose we have mod_2 gates



[Razborov-Smolensky] mod_3 cannot be computed

mod_q cannot be computed using constant depth circuits of mod_p gates ($p \neq q$, primes)

Suppose we have mod_6 gates. Constant depth circuit. ACC_0

$NP \notin ACC_0$ (Huge open problem)

[Williams] $NEXP \notin ACC_0$