# Lecture 23

Note Title

Today: Average-Case Complexity

- Motivation
- Algorithmic Efforts
- Definitions
- Complexity Results

---

## Motivation

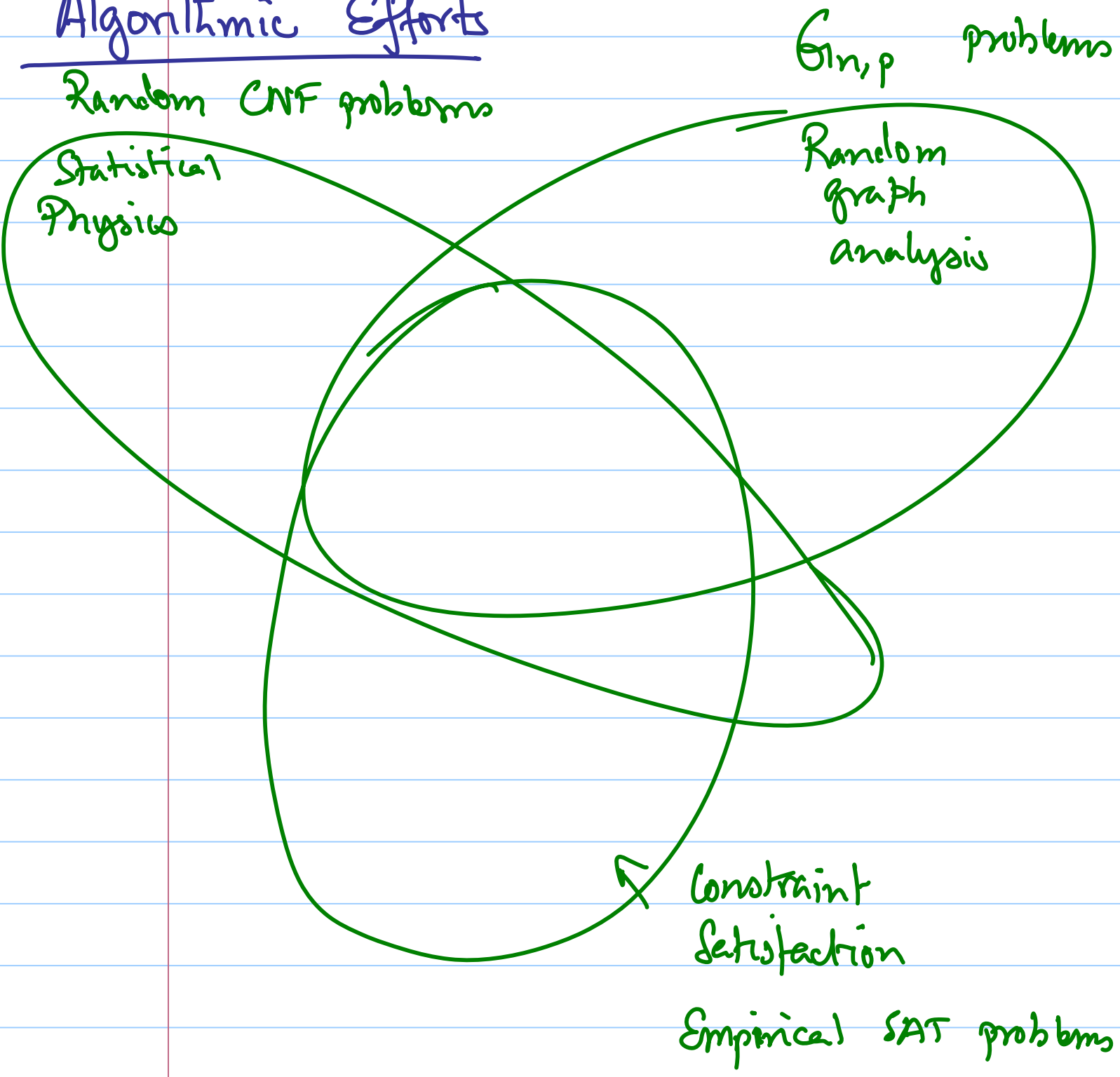
- Empirical Complexity:
  Naturally occuring instances don't appear to be as hard as worst-case instances.
  Why? How to study them?

- Cryptography: Here we can not count on worst-case hardness; Need to be

able to generate hard problems (with known solution).

---

## Algorithmic Efforts



# Typical Theorems

① $G_{n,p}$ world: With h.p. can find large clique ($\Omega(\log n)$) in $n$-vertex graph; can prove no longer clique exists w.h.p. [but not on specific instance]

② Random CNF: Pick $m$ clauses ind. from $8\cdot\binom{n}{3}$ possibilities; Find sat. assgmt. if $m \le \alpha \cdot n$. Prove no assgmt exist if $m > \alpha n$ w.h.p.

③ Constraint SAT / SAT solvers: find SAT solution or resolution proof of unsat.

Emphasis in ①, ② often to ensure $\mathbb{E}[\text{runtime}] \le \text{poly}(n)$. Is this the right measure?

# Definitions

(1) How should we model problems?

∃ two components - $\Pi$ relation on $\{0,1\}^* \times \{0,1\}^*$

- $D = \{D_n\}_n$, $D_n$ distribution on $\{0,1\}^n$.

(2) What is Easy?

Basic defn: $\mathbb{E}_{D_n}[\text{Time to solve } \Pi \text{ on } x] = \text{poly}(n)$

Why? Not robust under polytime reductions

Good defn. 1: [Impagliazzo] $\exists q$ (poly) s.t. $\forall p$

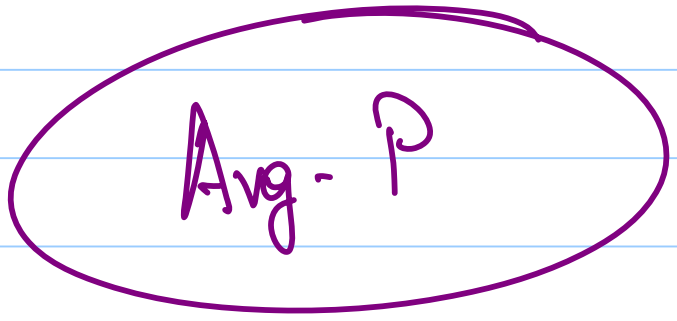
s.t. $\Pr\left[T_\pi(x) \geq q(n)\right] \leq \frac{1}{p(n)}$

Good defn. 2 [Levin] $\exists c$ s.t.

$$\mathop{E}_{x}\left[ T_\pi(x)^{1/c} \right] \leq a(n)$$

Vaguely: Defns. seem equivalent.

(but don't trust me on this!)



## (3) What is Hard-on-average? (& interesting)

**(3.1)** $\forall \Pi \in NP - P$, $\exists D = D_\Pi$ s.t. $(\Pi, D) \notin Avg\text{-}P$

Proof: $D_n$ = supported on instances where $M_n$ incorrect on $\{0,1\}^n$

To be interesting $D$ should be restricted

Defn ↑ : Poly time computable

$\forall x$, $\sum_{y<x} D(y)$ computable in poly time

↑ standard ordering on $\{0,1\}^*$

## Defn 2: Polytime samplable

$\exists$ polytime algorithm $S$ s.t.

$S(n, R)$ produces $x$ with probability $D_n(x)$ when $R$ uniform

## Nice aspect:

Suppose $\Pi_1 \leq \Pi_2$ &

& $(\Pi_1, D_1)$ - hard

then $\leq$ includes distribution $D_2$ on $\Pi_2$ s.t.

$(\Pi_2, D_2)$ hard.

$D_1$ samplable $\Rightarrow$ $D_2$ samplable !

## Complexity Class : $DNP = \{(\Pi, D)\}$

NP problem — Samplable distribution.

## Reductions : $R : (\Pi_1, D_1) \longrightarrow (\Pi_2, D_2)$

if algorithm running in Avg-P for $(\Pi_2, D_2)$ solves $(\Pi_1, D_1)$ in Avg-P.

⭐ Even Identity is non-trivial reduction

$D_2$ $\epsilon$-dominates $D_1$ if $\exists$ poly $p$

s.t. $$\Pr_{x \leftarrow D_1}\left[ D_2(x) < \frac{D_1(x)}{p(|x|)} \right] \leq \epsilon$$

Identity reduces : $(\Pi_1, D_1) \to (\Pi_1, D_2)$

if $\epsilon = n^{-\omega(1)}$

---

## Main Results

### DNP-Completeness

[Levin]: Basic DNP-completeness for "artificial problems"

⋮

[Impagliazzo & Levin] DNP-completeness of "artificial problem" on uniform distribution. (stronger result)

# Worst-Case → Average-Case reductions

- Notion

- Hardness Results (Mostly Lattice Problems)

  [Ajtai],

  [Regev]

  [Micciancio]

  [Peikert]

- "Impossibility Results"

  [Fortnow Feigenbaum]

  [Bogdanov Trevisan]

- "Weakness of Impossibility Results" [Guttfreund Shaltiel Ta-Shma]

# References


[Impagliazzo]: Many Worlds

[Goldreich]: Conceptual Underpinnings

[Bogdanov - Trevisan]:

? Lattice ?