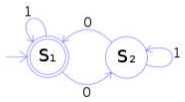
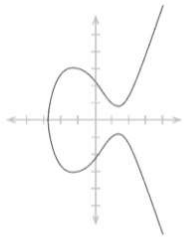
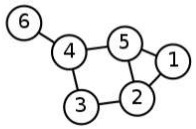
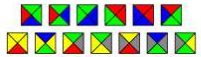
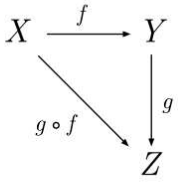
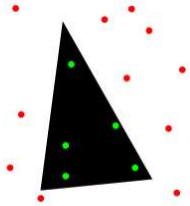
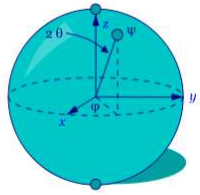
CS 598 TH1

(Recent) Advances in Theory CS

Instructor: Ruta Mehta
TA: None

Theory CS (TCS)

How to compute? And fast?

$P \to Q$					**P = NP ?**
Mathematical logic	Automata theory	Number theory	Graph theory	Computability theory	Computational complexity theory
GNITIRW-TERCES	$\Gamma \vdash x : \mathrm{Int}$				
Cryptography	Type theory	Category theory	Computational geometry	Combinatorial optimization	Quantum computing theory

Too vast to even touch every topic.

Our goal:

Together learn about some interesting new results within TCS and attempt to solve open problems.

Fuzzy!

- **Pre-req:** CS 473. Advanced theory courses like approximation/randomized algorithms would help further.
- **Course Format: Seminar course**
  - I/you/guest lectures on an interesting topic, and discuss open problems around it.
  - An open problem session.
  - Repeat.
- **Project:**
  - Pick an open problem and try to solve it by yourself. You have the entire semester to try.

- **What is expected from you**
  - Active participation in the class
  - Present a paper of your choice, and discuss open problems around it.
  - Work on an open problem, and present findings at the end of the semester.
- **Grading:** (all good as far as you are sincere and put in hard work)
  - Class participation (5%)
  - Paper presentation (50%)
  - Project + presentation (45%)

Administrativia

- Webpage: https://courses.engr.illinois.edu/cs598th1/sp2023
- Slack: CS598 TH1 – Advances in TCS (registered students should have received an invite to join)
  - Others, please sign up through the link on the webpage.
- Issue about the classroom!

Check webpage/slack at least twice a week for the updates.

Tentative Topics

- TFNP classes and (open) problems therein
  - Query, communication, crypto complexity
- Discrete optimization through continuous opt.
- Fast algorithms to solve LP
- Beyond worst-case
- Expander decomposition and apps. to graph algo.
- Massively Parallel Algorithms
- Discrepancy theory and Quantum connection?
- ML: differential privacy, fairness, learning augmented algorithms, GANs for counter examples
- …..

Topic 1:
Total Function NP (TFNP) zoo

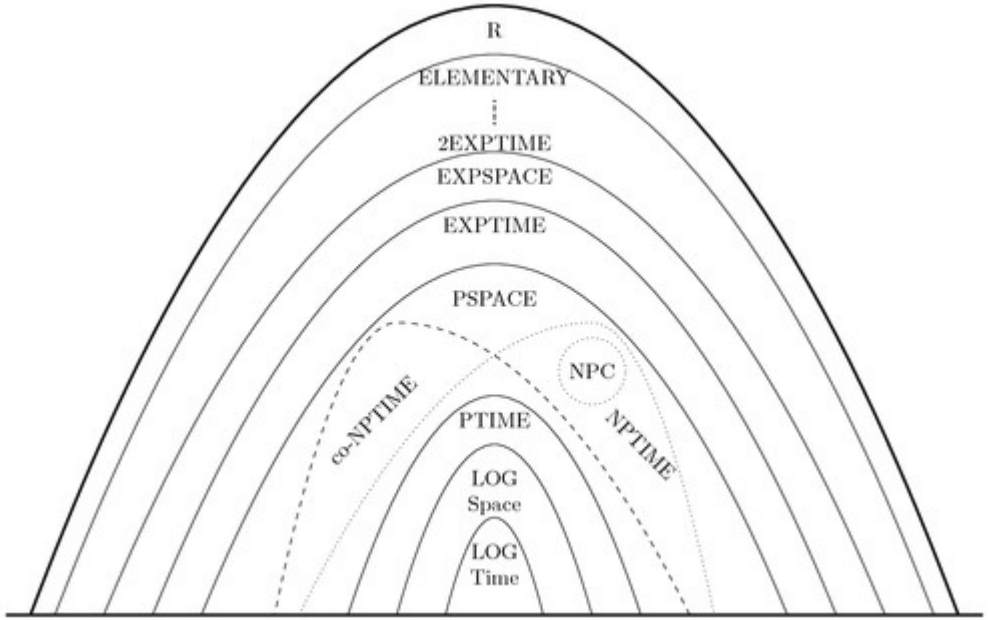
- What is TFNP? And why?
- Classes within TFNP: Intuition, formal description, complete problems w/ interesting existence theorems.
- Relation between the classes.

Computable? (Decidable?)

Halting problem: Given a program and its input, can one/computer decide if the program will halt?

NO! Un-decidable!!!

Decidable:



NP

∃ a soln?

YES answers are poly-time verifiable.

3-SAT ϕ on n variables

$x_i = a_i \in \{T, F\}$

$\phi(x_1, \ldots, x_n)$ is True.

co-NP

NO is easy

3-SAT ϕ is ϕ tautology ?

NP

co-NP

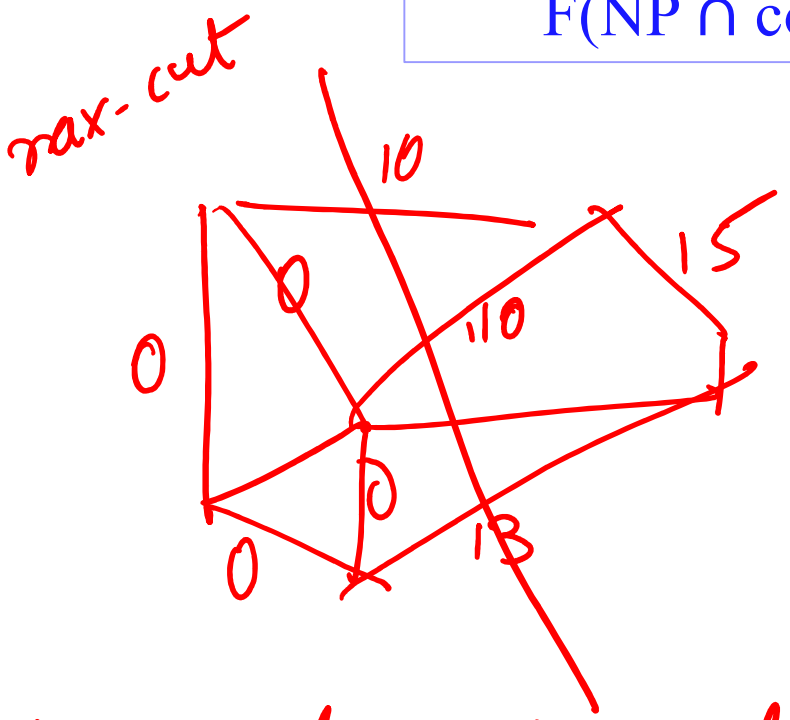
Total Function NP

F(NP ∩ co-NP)

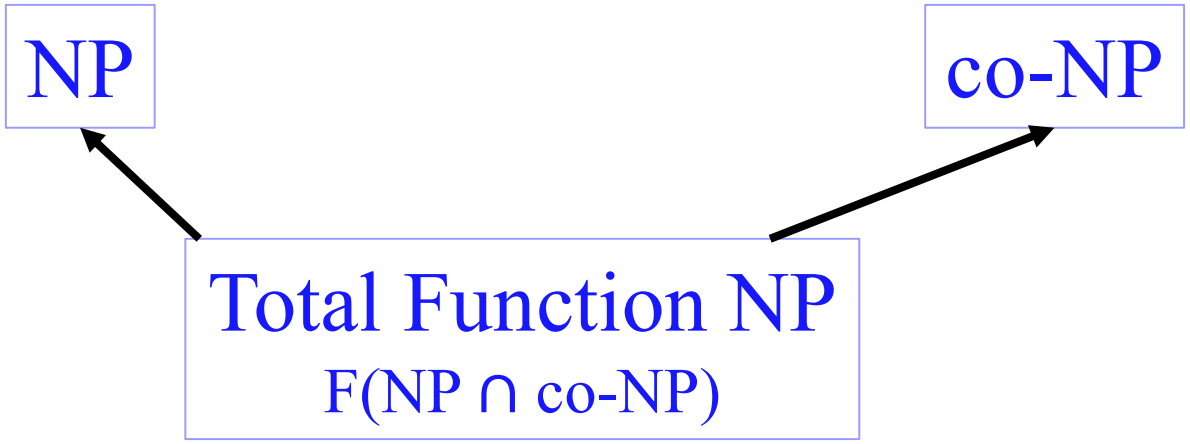
Total: Solution always exist. Aka YES instances only.

Function: Goal is to find a solution. Aka Search problems.

NP: Solution is poly-time verifiable



local-max-cut: Find a cut that can't be improved by flipping a vertex.



Integer factorization: Given +ve integers. n, k s.t. $n > k$, check if $\exists$ a prime factor of n less than k.

TFNP

PLS
(Polynomial local search)

Formal: $N, V, \to$

$\{0,1\}^n \to N \to \{0,1\}^n$

$\{0,1\}^n \to P \to \mathbb{R}_+$

$v \to V$ iff $V = N(v)$ & $P(V) > P(v)$

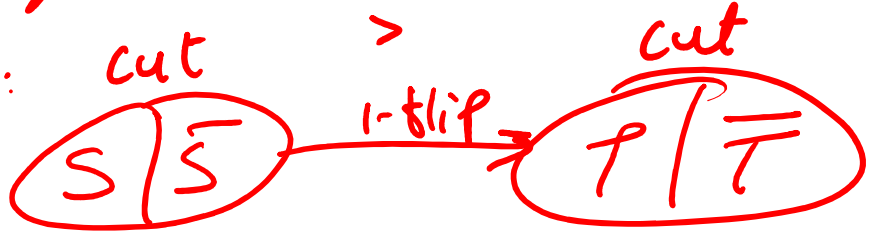
size = size(N, P)

Intuition: Every DAG has a SINK.

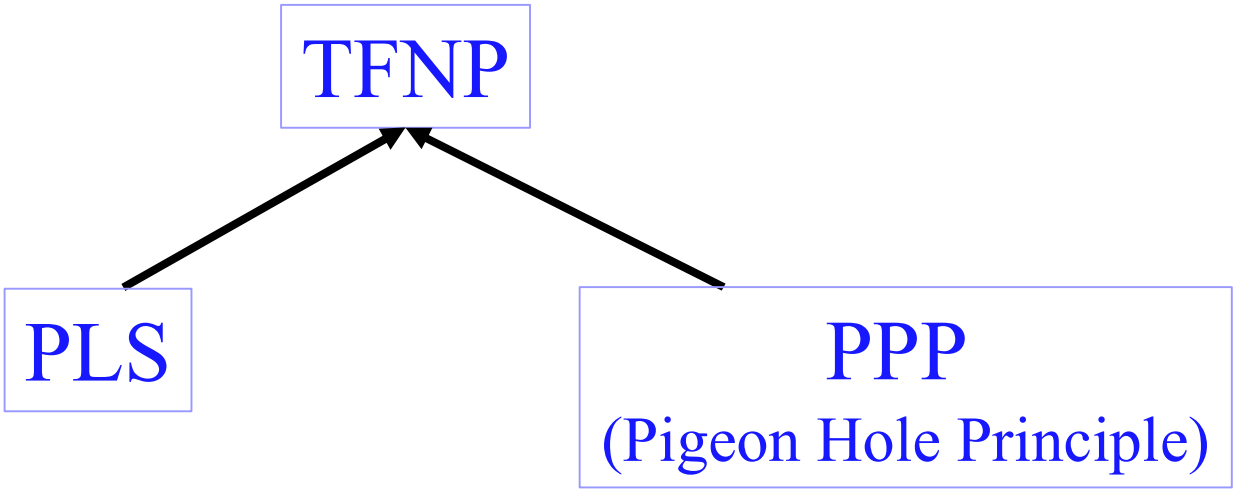
Problems by simple local search algorithm

- local-max-cut G
- weighted-max-SAT / flip of a variable
- :

Vertices: all possible partitions of the vertices of G.



PLS
(Polynomial Local Search)



Intuition: $f: [n] \to [n]$ then

either $\exists x \in [n]$ s.t. $f(x) = 0$

or $\exists x, y$ s.t. $f(x) = f(y)$

Formal: $\{0,1\}^n \to \boxed{C} \to \{0,1\}^n$

either find x s.t. $C(x) = 0^n$

or x, y s.t. $C(x) = C(y)$

PPP

PPP - complete
- short Int. Sol^n

- Equal-sum:

Given n integers +ve, $a_1, \ldots, a_n$,

$\sum_{i=1}^{n} a_i < 2^n - 1$, find $S \neq T \subseteq \{1, \ldots n$

s.t. $\sum_{i \in S} a_i = \sum_{i \in T} a_i$

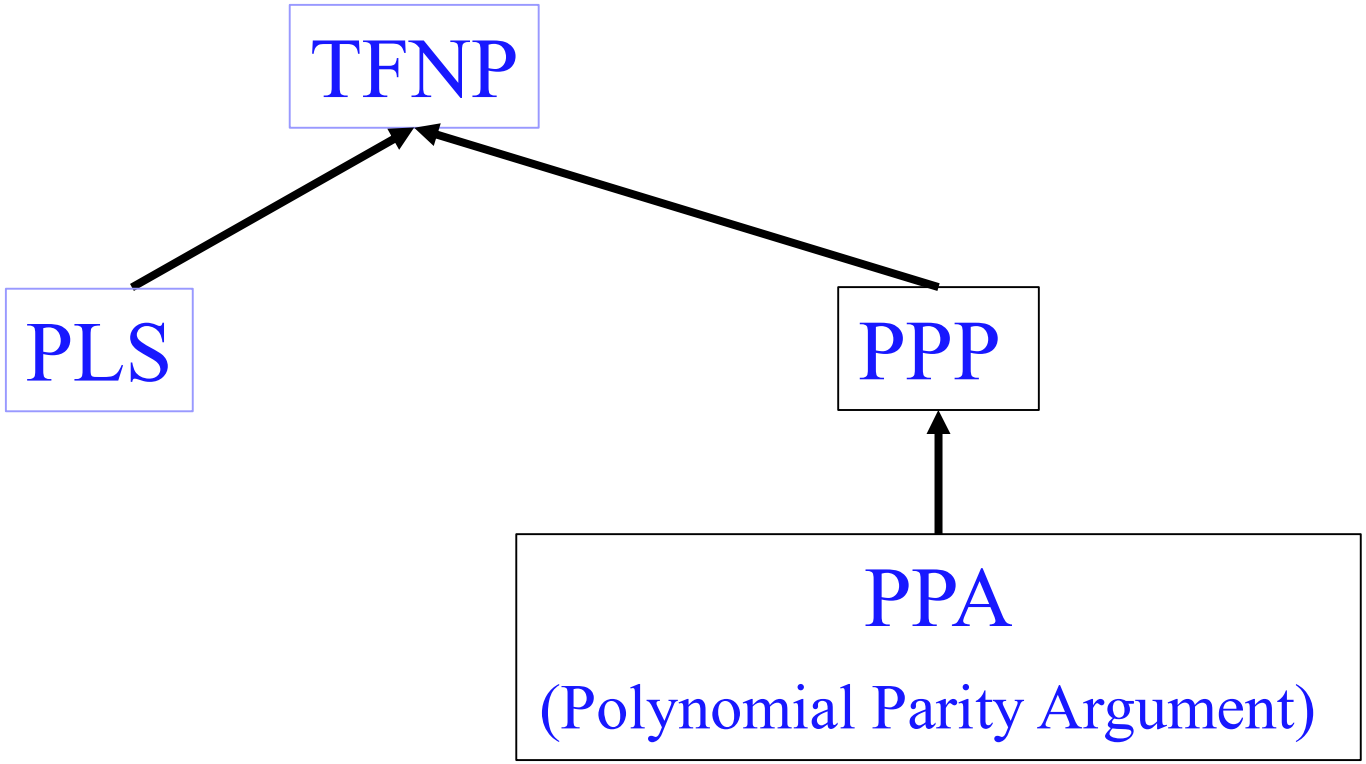
- Minkowski: Given matrix $A_{n \times n}$ s.t.

$|\det(A)| < 1$, Find the int. linear combination

of A's rows s.t. its l_∞ norm < 1.

- Dirichlet: Given n rational no. $a_1, \ldots a_n$ & int N, Find integers $q, p_1, \ldots, p_n$ s.t. $\forall i, \left|a_i - \frac{p_i}{q}\right| < \frac{1}{qN}$

$1 \leq q \leq N^n$


TFNP
PLS
PPP
PPA
(Polynomial Parity Argument)