Classes of Problems

- Polynomial Time Verification
- The Classes P and NP
- The Classes coNP and EXP
- NP-Hard and NP-Complete Problems
- Proving NP-Hardness
- A first NP-Complete Problem

Imdad ullah Khan

The Classes P and NP of Problems

The Class P: Decision problems that can be **solved** in polynomial time

The Class NP: Decision problems that can be **verified** in polynomial time

$$\mathrm{P} \subseteq \mathrm{NP}$$

The Class $\textsc{coNP}$ of Problems

The Class $\textsc{coNP}$: Decision problems whose **No instances can be verified** in polynomial time

Their **No** instances are **Yes** instances of their complement problems

They are the complements of problems in NP

▷ Think of an NP problem as a set of **Yes** instances

Examples: $\overline{\textsc{SAT}}(f)$, $\overline{\textsc{Hamiltonian}}(G)$

Note that (the class) coNP is not the complement of the class NP

Question: Is $\mathrm{NP} = \textsc{coNP}$**?**

Irrespective of the answer to P vs NP**?** can we certify in polynomial time that G has no Hamiltonian cycle

NP vs coNP

The Class coNP: Decision problems whose **No** instances can be **verified** in polynomial time

The following result is not very difficult to see

$$\mathrm{P} \subset \mathrm{coNP}$$

Thus,

$$\mathrm{P} \subset \mathrm{NP} \cap \mathrm{coNP}$$

We also know that

If $\mathrm{P} = \mathrm{NP}$, then $\mathrm{NP} = \mathrm{coNP}$

This easily follows (read notes) but the converse is not known to be true

PRIME and FACTORING

It is widely believed that $\mathrm{P} \subsetneq \mathrm{NP} \cap \mathrm{coNP}$

FACTOR(n, k) is in $\mathrm{NP} \cap \mathrm{coNP}$

- FACTOR$(n, k) \in \mathrm{NP}$: A factor $p \leq k$ of n would certify that and can be verified with one division
- FACTOR$(n, k) \in \mathrm{coNP}$: Prime factorization of n can be a certificate that can be verified by checking if "factors" indeed are primes (PRIME$(t) \in \mathrm{P}$)

Is FACTOR$(n, k) \in \mathrm{P}$?

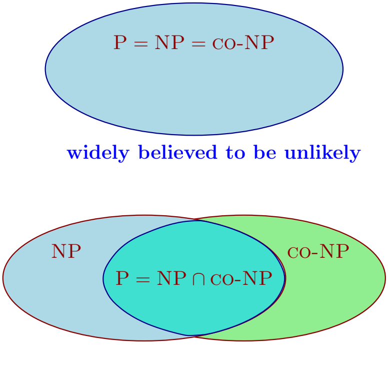
Majority believe it to be not in P, this belief is the basis of RSA cryptosystem

Thus, by this belief $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$

NP = coNP?

The Class coNP: Decision problems whose **No** instances can be **verified** in polynomial time

Following are possibilities of relationships between these complexity classes



The Class EXP of Problems

The Class EXP: Decision problems that can be **solved** in exponential time

There exists an algorithm that correctly outputs **Yes/No** on any instance and runtime is bounded by an exponential function in size of input

$\text{NP} \subseteq \text{EXP}$ and $\text{coNP} \subseteq \text{EXP}$

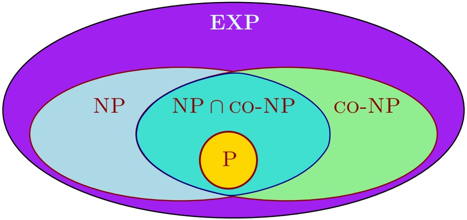
Given that the problem is in NP (coNP) ▷ there exists a verifier

Run the polynomial time verification algorithm on all possible certificates

▷ there are at most exponentially many certificates

If on any (all) of the possible certificates we get a **Yes** (**No**) answer from the verifier we get a decision

This gives us the following containment (believed by many to be so)



more likely hierarchy of the discussed complexity classes