The Complexity Class NP

1   Certificates

Every yes-instance of an NP problem has a short and easily checkable certificate, for example a satisfying assignment for satisfiability

2   Verifiers

Definition: Acceptor

An acceptor machine V which halts on all inputs is called a verifier for a language $\mathcal{L}$ if

$$\mathcal{L} = \{w | V \text{ accepts } "w; c" \text{ for some string c}\}$$

- The string c is called a certificate (or witness) for w

- A verifier is said to be polynomial-time if it is a polynomial-time TM, and there is a polynomial $p(x)$ such that, for any $w \in \mathcal{L}$, there is a certificate c with $|c| \leqslant p(|w|)$

3   The class NP

Definition: NP

The class of languages that have polynomial-time verifiers is called NP

Problem: Composite Number

Instance - A positive integer k
Question - Are there integers $u, v > 1$ such that $u \cdot v = k$

Problem: Subset Sum

Instance - A collection of positive integers $S = \{a_1, ..., a_k\}$ and a target integer t
Question - Is there a subset $T \subseteq S$ such that $\sum_{i \in T} = t$

4   Problems (probably) not in NP

Problem: No Hamiltonian Cycle

Instance - A graph G
Question - Is it true that G has no Hamiltonian cycle?

Problem: Checkers

Instance - An integer n and a position in checkers on $n \times n$ board
Question - Is it a winning position for white?

5 Nondeterministic Machines

We can get an alternative definition of the class NP by considering non-deterministic machines.

Recall that if NT is a non-deterministic Turing Machine, then NT(x) denotes the tree of configurations which can be entered with input x, and NT accepts x if there is some accepting path in NT(x).

Definition: Time Complexity

The time complexity of a non-deterministic Turing Machine NT is the function $NTime_{NT}$ such that $NTime_{NT}(x)$ is the number of steps in the shortest accepting path $NT(x)$ is there is one, otherwise it is the number of steps in the shortest rejecting path

---

6 Non-Deterministic time complexity