The $P \neq NP$ Hypothesis

We assume that $P \neq NP$.

Set A is NP-hard if for every $B \in NP$, there exists a polynomial-time computable function f such that:

polynomial time reduction

$$\forall x : x \in B \text{ iff } f(x) \in A.$$

<u>Theorem</u>: Assuming $P \neq NP$, if A is NP-hard then $A \notin P$.

proof: Suppose $A \in P$.

Consider any $B \in NP$. There exists a poly-time reduction f such that $x \in B$ iff $f(x) \in A$

A poly-time algorithm for B:

Input x. Compute $f(x)$. Run poly-time algorithm for A on $f(x)$.

Let $|x| = n$. Then $|f(x)| \leq p(n)$.

Running poly-time algo for A on $f(x)$ takes time $\leq q(p(n))$. $\boxtimes$

Theorem: SAT is NP-hard.

proof: Let M be a non-deterministic poly-time TM. $M = (Q, \Sigma, q_0, \delta, F_{accept})$

runs for $\leq p(n)$ steps on inputs of size n.

Consider input x with $|x| = n$.

$State(q,t)$: $q \in Q$ & $0 \leq t \leq p(n)$

→ TM is in state q at time t

$Head(j,t)$: $1 \leq j \leq p(n)$, $0 \leq t \leq p(n)$

→ Head of M at time t points to j^{th} cell.

$Tape(s,j,t)$: $1 \leq j \leq p(n)$, $0 \leq t \leq p(n)$, $s \in \Sigma$

→ Value of j^{th} cell at time t is symbol s

At $t = 0$

$\text{State}(q_0, 0) \wedge \text{Head}(1, 0) \wedge$

$\text{Tape}(x[1], 1, 0) \wedge \text{Tape}(x[2], 2, 0) \wedge \dots$

$\wedge \text{Tape}(x[n], n, 0) \wedge \text{Tape}(\cancel{B}, n+1, 0) \wedge$

$\dots \wedge \text{Tape}(\cancel{B}, p(n), 0) \wedge$

$\neg \text{State}(q, 0)$ [for all $q \neq q_0$] $\wedge$

$\neg \text{Head}(j, 0)$ [for all $j > 1$] $\wedge$

$\neg \text{Tape}$ [removing all non-desirable contents]