Non-deterministic Turing Machine (NTM)

NTM accepts a Language L

- $\forall w \in L$, $AF(0 \vee 1)$ every branch running on w terminates.
- $\forall w \in L$, $EF(1)$ at least one branch accepts.

  $\forall w \notin L$, $AF(0)$ all branches reject.

$$NTime(f(n)) \sim \max_{\forall w, \forall branch} = O(f(n))$$

Similarly, NSPACE

$$NP = \bigcup_{k \in \mathbb{N}^+} NTime(n^k)$$

$$\boxed{\begin{array}{l} NPSPACE \\ = PSPACE \end{array}} \begin{array}{l} = \bigcup_{k \in \mathbb{N}^+} NSPACE(n^k) \\ = \bigcup_{k \in \mathbb{N}^+} DSPACE(n^k) \end{array}$$

CLIQUE

$\triangleq \{ (G, k) \mid \forall k \in \mathbb{N}^+, \forall G \in \{\text{undirected graph}\}$ where G has a clique of size $\geq k \}$

total subgraph

Given graph $G(V, E)$ where $|G| = n$, $k \in \mathbb{N}^+$.

Def $s :: V \to \{0, 1\}$, a binary classifier on vertices representing a size-k partition of G.

where $\sum_{v \in V} s(v) = k$.

Goal if $\exists s$, $filter(s, G)$ is a k-clique.

time complexity

$\#$ of partitions of size $k = \binom{n}{k}$

when $k = \frac{n}{2}$, $\binom{n}{\frac{n}{2}} \approx \frac{2^n}{\sqrt{n}}$ $\Rightarrow$ CLIQUE $\in$ ExpTime

for NTM, CLIQUE $\in$ NP

3-SAT $\triangleq \{ \phi \mid \phi \text{ is satisfiable} \}$

Def n Boolean variables $X = \{ x_1, \ldots, x_n \}$

$$\phi(X) = (x_1 \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee x_4) \wedge \cdots$$

Given X, ϕ

Goal if $\exists X \in \{0,1\}^n$, $\phi(X) = 1$

time complexity

$\#$ of assignments $= 2^n \Rightarrow$ 3-SAT $\in$ ExpTime

for NTM, 3-SAT $\in$ NP

Theorem

$$L \in NP \overset{\text{iff}}{\Longleftrightarrow} L \text{ has a polynomial time "verifier"}$$

Def a polynomial time verifier is a deterministic TM, $V(x,c)$

- $x \in L$, input string
- $c \in \mathbb{L}$, certificate / proof
- Let $n = |x|$
- a polynomial function, P

$V \in \widehat{TM}$ computable, (higher-order function $:: L \to \mathbb{L} \to \{0,1\}$ $\simeq$ $:: (L, \mathbb{L}) \to \{0,1\}$

such that

① the time complexity of V is $O(P(n))$.

$\sim \exists n_0, a \in \mathbb{N}^+.$

$\forall x, c.$ if $n = |x| \geq n_0$,

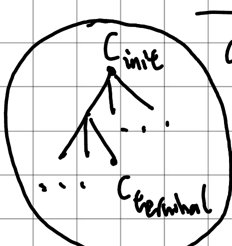
then $V(x,c)$ terminates in $(a\,P(n))$ steps.

② $\forall x \in L,\ \exists\ c \in \mathbb{L} \wedge |c| \leq P(n),\ V(x,c) = 1$

$\forall x \notin L,\ \forall c \in \mathbb{L},\ V(x,c) = 0$

idea

- $\Leftarrow$ **Given** verifier, construct a NTM with T.C. $O(P(n))$



configuration space

a path from root to leaf $\simeq$ a unique certificate, c.

given $x \in L$
$\begin{cases} \text{(P-time) non-deterministically construct certificate} \\ \text{(P-time) verification} \end{cases} \Rightarrow$ P-time

- $\Rightarrow$ <u>Given</u> a NTM, D, with T.C. $O(p(n))$, $L(D)$

construct deterministic TM verifier, $V(x, c) :: L \to \mathbb{L} \to \{0, 1\}$

GNP

<u>Given</u> $x \in L$, $c \in \mathbb{L}$.

- decode certificate c uniquely into a path in the configuration space of D.
- deterministically traverse the configuration space of D following the path

length of path at most: $O(p(n))$

hit a leaf node $\Rightarrow$ accept

otherwise $\Rightarrow$ reject

	NTM	TM
configuration space	branching	sequential

- deterministic traversal : degenerate to deterministic TM
- non-deterministic traversal :

sample the distribution of all choices at each step

$\sim$ simultaneously traversing all branches