<u>Def</u>: Let φ be a boolean formula, φ is in <u>conjunctive normal form</u> (<u>cnf</u>) if

$$\varphi = C_1 \wedge \cdots \wedge C_k \quad \text{(some } k\text{)}$$

where each C_i (a <u>clause</u>) is of the form

$$C_i = \ell_1 \vee \cdots \vee \ell_r \quad \text{(some } r\text{)}$$

where each ℓ_j (called a <u>literal</u>) is a boolean var or the negation of a bool. var.

<u>Ex</u>:

$$\varphi = (x_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_2)$$

[$\bar{x}$ means x negated]

satisfiable?

<u>Fact</u>: If φ is a cnf fmla, a satisfying assignment to φ is one that makes at least one literal true in every clause.

<u>Def</u>: CNF-SAT is the decision problem:

<u>Instance</u>: A cnf formula φ.

<u>Question</u>: Is φ satisfiable?

<u>Theorem</u>: CNF-SAT is NP-complete.

<u>Proof</u>: (1) CNF-SAT $\in$ NP:

If φ is sat, an <u>easily</u> (in time $Poly(|\langle\varphi\rangle|)$) verifiable proof of such is a satisfying assignment. ✓

CNF-SAT is NP-hard:

($\forall B \in NP$, $B \le_m$ CNF-SAT).

Fix a language $B \in NP$.

We define a function

$$x \longmapsto \varphi_x \quad (x \in \Sigma^*)$$

such that is ptime computable and $\forall x \in \Sigma^*$, φ_x is a cnf fmla, and $x \in B \iff \varphi_x$ is satisfiable

Let V be a TM such $\forall x, y \in \Sigma^*$,

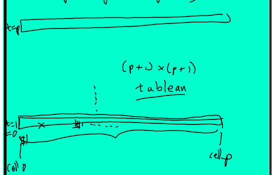
$V(x\#y)$ runs in time $p(|x|)$ [p is a polynomial]

& $x \in B \iff \exists y,\ V(x\#y)$ accepts

[assume wlog $\# \notin \Sigma$]

Fix an input $x = x_1 \cdots x_n$ ($|x| = n$) we construct φ_x:

Let $p := p(n) = p(|x|)$



WLOG assume that

- V starts with $x# ... on its tape
- $ appears in no other cell but stays in cell 0.
- If V is scaning $, it never tries to move left.
- When/if V enters its accepting state, it doesn't halt, but stays in the accept state. [but acceptance still means entering this state within p steps.)

Construction of φ_x

[in time $Poly(|x|) = Poly(n)$.]

$\forall i,\ 0 \le i \le p,\ \forall t,\ 0 \le t \le p$

$h_{i,t}$ — "V's head is scanning cell i at time t"

$\forall a \in \Gamma,\ \forall i,\ 0 \le i \le p$
$\forall t,\ 0 \le t \le p,$

$c_{i,a,t}$ ~ "Cell i contains a at time t"

all the vars of φ_x

Clauses of φ_x:

"Sanity clauses"

$\forall q, r \in Q$ with $q \ne r$ and $\forall t,\ 0 \le t \le p$, add the clause,

$$\overline{S_{q,t}} \vee \overline{S_{r,t}}$$

"V is in only one state at time t"

$\forall 0 \le t \le p,\ \forall 0 \le i < j \le p$

clause $\overline{h_{i,t}} \vee \overline{h_{j,t}}$

"the head can't be in 2 places at once"

$\forall a, b \in \Gamma$ with $a \ne b$,
$\forall 0 \le t \le p,\ \forall 0 \le i \le p,$

$$\overline{c_{i,a,t}} \vee \overline{c_{i,b,t}}$$

"a tape cell can hold ≤ 1 symbol at a time"

Initial conditions: add these clauses:

$S_{q_0,0}$ — "V is in state q_0 at $t=0$"

$h_{0,0}$ — "V scans cell 0 at time $t=0$"

{recall: $x = x_1 \cdots x_n$

$\forall 1 \le i \le n$ clauses

$c_{i,x_i,0}$ — "x is in cells 1—n initially"

$c_{0,\$,0}$

$c_{n+1,\#,0}$

$\forall i,\ n+2 \le i \le p$ add the clause

$$\bigvee_{a \in \Gamma} c_{i,a,0}$$

"each cell $i \ge n+2$ has some symbol in it."

Final conditions: add clause

$S_{q_{acc},p}$ — "V is in state q_{acc} at the end"

Clauses for transitions

Digression: p, q boolean.

$p \to q$ "if p then q"

$\equiv \bar{p} \vee q$

$\forall 0 \le t \le p-1,\ \forall i,\ 0 \le i \le p,$
$\forall a \in \Gamma,$

$$c_{i,a,t} \wedge \overline{h_{i,t}} \to c_{i,a,t+1}$$

"unscanned cells don't change contents in a time step"

$$c_{i,a,t} \wedge h_{i,t} \to c_{i,a,t+1}$$
$$\equiv \overline{(c_{i,a,t} \wedge \overline{h_{i,t}})} \vee c_{i,a,t+1}$$

$$\equiv \overline{c_{i,a,t}} \vee h_{i,t} \vee c_{i,a,t+1}$$

$\forall q \in Q,\ \forall a \in \Gamma$ such that

$\delta(q,a) = (r, b, R)$ $\left[\begin{matrix} r \in Q \\ b \in \Gamma \end{matrix}\right]$

$\forall t,\ 0 \le t \le p-1,\ \forall 0 \le i \le p-1$ add

$$S_{q,t} \wedge h_{i,t} \wedge c_{i,a,t} \to S_{r,t+1}$$
$$\text{"} \to h_{i+1,t+1}$$
$$\text{"} \to c_{i,b,t+1}$$

Similarly, for $\delta(q,a) = (r,b,L)$,
$\forall 1 \le i \le p,\ \forall 0 \le t \le p-1$, add

$$S_{q,t} \wedge h_{i,t} \wedge c_{i,a,t} \to S_{r,t+1}$$
$$\text{"} \to h_{i-1,t+1}$$
$$\to c_{i,b,t+1}$$

End of φ_x's description