SAT is NP-complete

Let $L \in \text{NP}$ be decided by a 1-tape non-deterministic TM $M = (Q, \Gamma, \Sigma, q_s, q_a, q_r, \Delta)$ in time n^k for some integer k. For any input x, we will produce a Boolean formula ϕ_x so that $x \in L$ if an only if ϕ_x is satisfiable. ϕ_x will be the conjunction of several smaller formulae.

The formula ϕ_x will have the following variables.

- State variables: For $1 \le i \le n^k$ and $q \in Q$, $S_{i,q}$. These variables will be true if at time i, M is in state q. There will be $|Q|n^k$ of them.
- Head variables: For $1 \le i, j \le n^k$ $H_{i,j}$. These variables will be true if at time i, the head is in cell j. There will be n^{2k} of them.
- Tape variables: For $1 \le i, j \le n^k$ and $\sigma \in \Gamma$ $T_{i,j,\sigma}$. These variables will be true if at time i cell j contains the symbol σ. There will be $|\Gamma|n^{2k}$ of them.

We can use these variables to express the computation of M on x as follows. The final formula ϕ_x will be conjuction of formulae $\mathcal{I}, \mathcal{S}, \mathcal{H}, \mathcal{T}, \mathcal{M}_1, \mathcal{M}_2$ and $\mathcal{A}$; i.e., $\phi_x = \mathcal{I} \wedge \mathcal{S} \wedge \mathcal{H} \wedge \mathcal{T} \wedge \mathcal{M}_1 \wedge \mathcal{M}_2 \wedge \mathcal{A}$. Each of these sub formulae are described below. For the ease of description, we will use the operators $\wedge$ (AND), $\vee$ (OR), $\neg$ (NOT), and $\Rightarrow$ (Implication). We can easily see that by using the equivalence $P \Rightarrow Q \equiv \neg P \vee Q$, we can modify the formulae to get a Boolean formula (almost the same size) with operators $\wedge$, $\vee$, and $\neg$.

$$\mathcal{S} \; : \; \bigwedge_i \bigwedge_q \left(S_{i,q} \Rightarrow \neg(\bigvee_{q' \neq q} S_{i,q'}) \right)$$

$\mathcal{S}$ asserts that at time i if M is in state q then it cannot be in any other state.

$$\mathcal{H} \; : \; \bigwedge_i \bigwedge_j \left(H_{i,j} \Rightarrow \neg(\bigvee_{j' \neq j} H_{i,j'}) \right)$$

$\mathcal{H}$ asserts that if at time i if the head is on the cell j then it cannot be on any other cell.

$$\mathcal{T} \; : \; \bigwedge_i \bigwedge_j \bigwedge_\sigma \left(T_{i,j,\sigma} \Rightarrow \neg(\bigvee_{\rho \neq \sigma} T_{i,j,\rho}) \right)$$

$\mathcal{T}$asserts that if at time i cell j contains σ, then it cannot contain any other symbol.

$$\mathcal{I} \; : \; S_{1,s} \wedge H_{1,0} \wedge T_{1,0,\triangleright} \bigwedge_{1 \le j \le n} T_{1,j,x_j} \bigwedge_{n+1 \le j \le n^k} T_{1,j,\sqcup}$$

$\mathcal{I}$ asserts that at time 1 M is in the initial configuration.

$$\mathcal{M}_1 \; : \; \bigwedge_i \bigwedge_j \bigwedge_{j' \neq j} \bigwedge_\sigma (H_{i,j} \wedge T_{i,j',\sigma} \Rightarrow T_{i+1,j',\sigma})$$

$$\mathcal{M}_2 \; : \; \bigwedge_i \bigwedge_j \bigwedge_q \bigwedge_\sigma \left(S_{i,q} \wedge H_{i,j} \wedge T_{i,j,\sigma} \Rightarrow \bigvee_\Omega (S_{i+1,p} \wedge H_{i+1,j'} \wedge T_{i+1,j,\rho}) \right)$$

$\mathcal{M}_1$ and $\mathcal{M}_1$ are the part of the formula which implements one move of the machine M. $\mathcal{M}_1$ asserts that if at time i, the head is not on cell j' then at time $i+1$ the contents of that cell does not change. Here $\Omega = \{(q,\sigma),(p,\rho,D) | (q,\sigma),(p,\rho,D) \in \Delta\}$ is a finite set of choices for M, and $j' = j$ if $D = -$, $j' = j+1$ if $D = \rightarrow$, and $j' = j-1$ if $D = \leftarrow$

$$\mathcal{A} \quad : \quad \bigvee_i S_{i,q_y}$$

Finally, $\mathcal{A}$ asserts for at some time step i, M should move to state q_y.

Note that, by using the equivalence $P \Rightarrow Q \equiv \neg P \vee Q$, each of the formulae other than $\mathcal{M}_2$ can be expressed in CNF. For M_2, the formula within parenthesis is of constant size and hence can be easily rewritten in CNF form with only a constant blow-up in the size. Hence the entire formula ϕ_x can be expressed as a CNF. This shows that CNF-SAT is NP-complete.