COL 352 Lecture 38 April 27

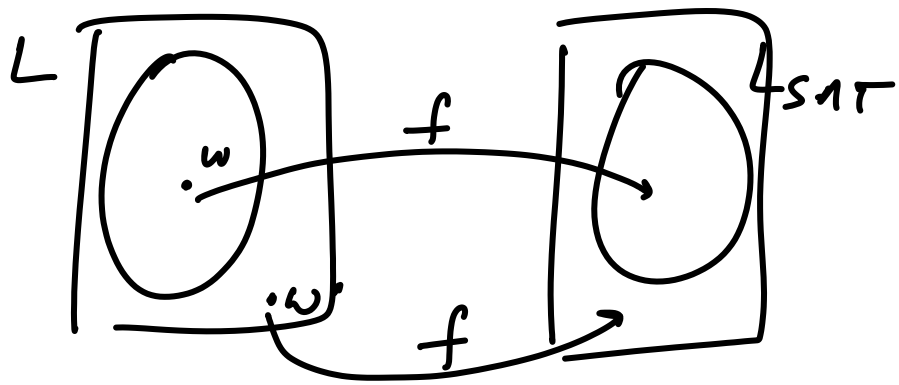
Cook-Levin Theorem: The satisfiability problem of boolean expression is NP-complete

Part 1: $L_{SAT} \in NP$: easy

Part 2: for any $L \in NP$ $L \leq_{poly} L_{SAT}$

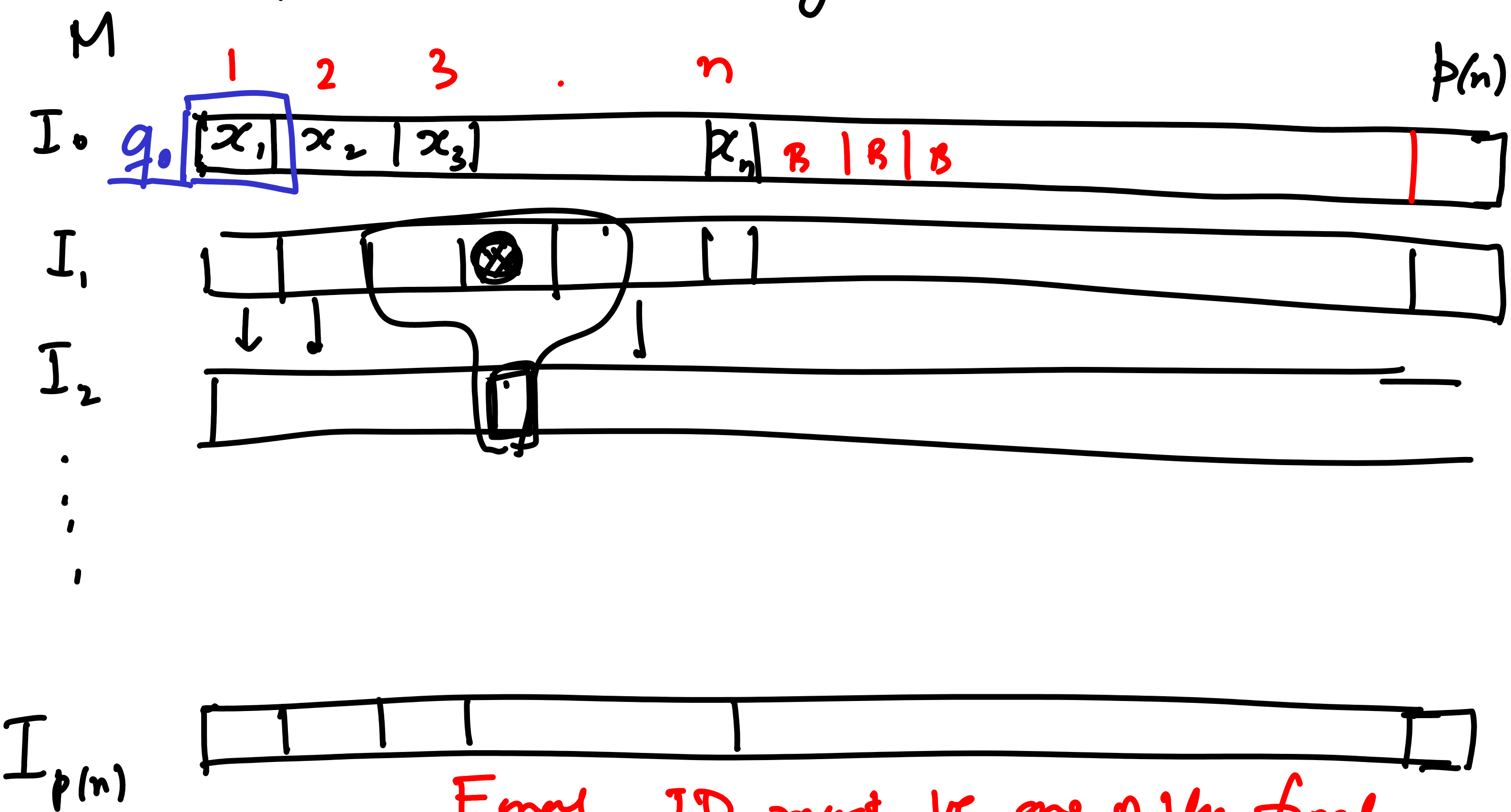
$\Rightarrow \exists$ a Nondet M s.t. $L(M) = L$

Given any w, we have to construct a turing computable polynomial-time function f s.t. $f(w) \in L_{SAT}$ iff $w \in L$



Note: $f(w)$ is a boolean expression (not too long)

NDTM M takes atmost $p(n)$ steps for any input of length n where p is some polynomial.



Final ID must be one of the final accepting states

δ_M is a transition function that may have multiple successors (non-det)

$w \in L$ iff

(1) I_0 contain w as initial input

and

(2) $I_{p(n)}$ contains a final state

and

(3) $\forall j \le p(n)$ I_{j+1} follows from I_j using a legal transition function of M.

$$\boxed{\text{The goal is to represent the above conditions as a boolean formula } F_M(w) \text{ which is satisfiable iff } w \in L}$$

redn function f

moreover f is computable in poly-time

$\Rightarrow$ $|F_M(w)|$ is of polynomial length

Idea: To guess each of the $p(n) \times p(n)$ symbols and verify conditions 1, 2, 3.

guess $\rightarrow$ $\{1, 2, \ldots K\}$

To convert from a K-valued variable to a boolean variable, we can introduce K variables for each variable

$X_{1,1} \quad X_{1,2} \quad X_{1,K} \quad X_{2,1}\, X_{2,2} \cdot X_{2,K}$

$$\underbrace{X_1}_{1 \;\; 2, \,\cdots\, K} \quad \underbrace{X_2}_{1 \;\; 2, \,\cdots\, K} \quad X_3 \quad \cdot \quad X_{p(n)\times p(n)}$$

$X_{i,j}$ are boolean variables s.t.

$$X_{i,j} = \begin{cases} \text{true} & \text{if } X_i = j \in \{1, \ldots K\} \\ \text{false} & \text{otherwise} \end{cases}$$

Addition condition (beyond 1, 2, 3)

(4) Exactly one $X_{i,j}$ must be true for each $i \leq p(n) \times p(n)$

$$(X_{i,1} \vee X_{i,2} \vee \cdot \; X_{i,K}) \bigwedge_{j \neq j'} (\underbrace{X_{i,j} \Rightarrow \overline{X}_{i,j'}}_{(\overline{X}_{ij} \vee \overline{X}_{ij'})})$$

Total boolean variables : $p(n) \times p(n) \times K$