CPSC 421/501 Nov 24, 2025

- Last time:
  - Boolean functions in $x_1, \ldots, x_n$

    $\{T,F\}^n \to \{T,F\}$ or $\{0,1\}^n \to \{0,1\}$

    $T=1$, $F=0$

  - Number functions $2^{(2^n)}$

  - Boolean formulas in $x_1, \ldots, x_n$ in $\vee, \wedge,$ $\neg, (,)$

    Most require formula size $\approx 2^n/n$

  - Stated:

    Subbotovskaya (1961):

    $f(x_1, \ldots, x_n) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$

    requires formula size $\geq n^{1.5}$ in $\vee, \wedge, \neg$

Conjunctive $\wedge$ AND

Defined 3CNF

$$C_1 \wedge C_2 \wedge C_3 \dots \wedge C_m$$

C_i : ___ $\vee$ ___ $\vee$ ___

3 literals $\quad x_1, \neg x_1, x_2, \neg x_2, \dots, x_n, \neg x_n$

Why all this interest?

Theorem (Cook-Levin): $3SAT \in P$

$\Rightarrow P = NP$.

Same holds with 3SAT replaced with SAT, 3COLOUR, CLIQUE, PARTITION, SUBSET-SUM, ...

$$3SAT = \left\{ \langle f \rangle \;\middle|\; \begin{array}{l} f \text{ is in } 3CNF \text{ form,} \\ \text{and } f \in SAT \end{array} \right\}$$

$f = f(x_1, \ldots, x_n)$

say

$$\underline{(x_1 \vee x_2 \vee x_3) \wedge (x_{12} \vee \neg x_2 \vee x_4)} \wedge \ldots$$

$f \in SAT \iff$

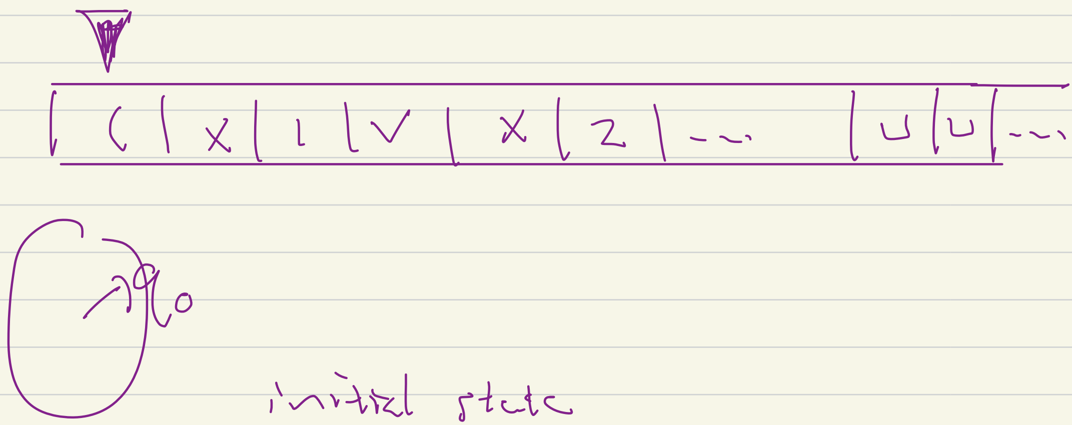
$$\exists\, x_1, \ldots, x_n \in \{T, F\} \text{ s.t. } f(\vec{x})$$

$$= f(x_1, \ldots, x_n) = T$$

$$\Sigma_{\text{Bool form}} = \{0, \ldots, 9, x, \wedge, \vee, \neg, (,), \#\}$$

$(x1 \vee x2 \vee x_3) \wedge$

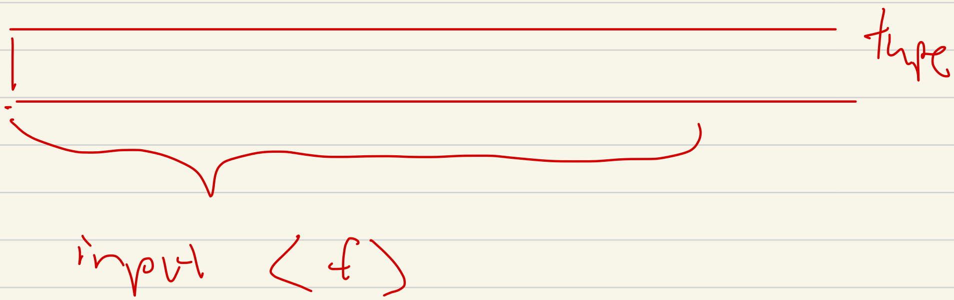
$(x12$ ...

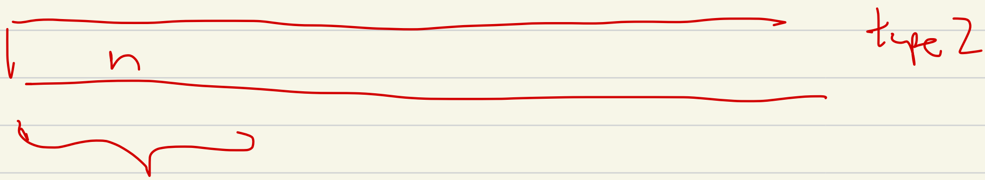


Claim: $\exists$ non-deterministic poly time algorithm to decide 3SAT

<u>Algorithm:</u> (Turing machines)

<u>Phase 1</u>: Find out how many variables in input = $\langle f \rangle$.





write down n = # of Boolean variables

<u>Phase 2</u>: Check $\langle f \rangle$ is really a true 3CNF formula

Phase 3:

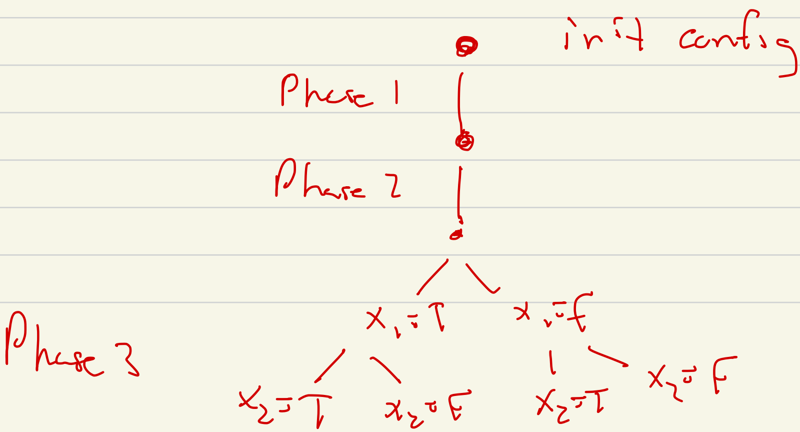
Deterministic $\quad \delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$

multitape $\quad \delta : Q \times \Gamma^k \to Q \times \Gamma^k \times \{L, R, S\}^k$

non-deterministic

$$\delta : Q \times \Gamma^k \to \text{Power}\left(\qquad \right)$$

Use this to "non-deterministically guess" values $x_1, x_2, \ldots, x_n$



etc ;

$x_n := T$ $x_n := F$ --- $x_n := T$ $x_n := F$

tape 3

T	F	T	F	F	T	⊔	⊔	---

$x_1 := T$ $x_2 := F$ $x_3 := F$ $x_6 := F$

$(n = 6)$

"non-deterministic guess"

for values $x_1, \ldots, x_n$

CPSC 320 "verifiers" of some sort

of magically appearing black box thing

Phase 4: "Verify" or "check" if non-deterministic guess is a satisfying assignment

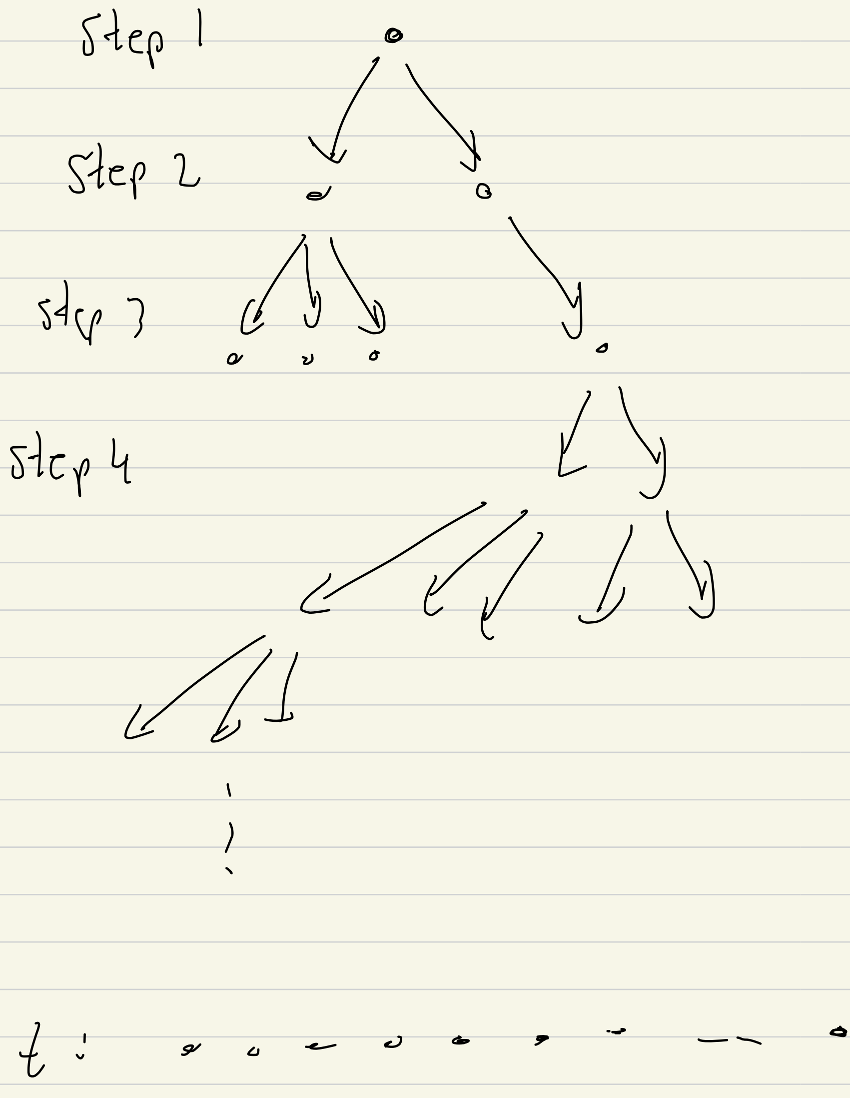
Claim 1: All this can be done in a <u>polynomial</u> in length(<f>) amount of steps/time.

Then

Claim 2: There exist an accepting configuration path iff

$$\langle f \rangle = \left\{ \begin{array}{c} \text{the description} \\ \text{of a 3SAT} \\ \text{formula} \end{array} \right\}$$

Computation:



does ≥ 1 possible configuration end in q_{acc}

Claim:

$$3SAT = \left\{ \langle f \rangle \;\middle|\; \begin{array}{l} f \text{ is a Boolean} \\ \text{in } 3SAT \end{array} \right\}$$

is therefore in NP;

$$3COLOUR = \left\{ \langle G \rangle \;\middle|\; \begin{array}{l} G \text{ is a 3-colourable} \\ \text{graph} \end{array} \right\}$$

PARTITION = ...

Now: If $L \subset \Sigma^* = \{1, \ldots, n_\Sigma\}^*$,

and $L \in NP$, specifically L is decidable

in time $\leq C n^k$ (C, k constants) by

a non-det T.m. $M = (Q, \Sigma, \Gamma, \delta, q_0, q_{acc}, q_{rej})$

then we can write down a Boolean

formula, $f = f(M, i)$,

given an $i \in \Sigma^n$ input

to M:

(1) $f = f(M, i)$ is a 3CNF formula

(2) M accepts i iff

$$f(M, i) \in 3SAT$$

(i.e. $f(M, i)$ is satisfiable)

(3) $$|\langle f(M,i) \rangle| \leq C'_M |i|^{k'_M}$$

C'_M, k'_M constants depend on M