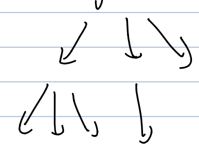
Back to Cook-Levin Thm:

Some non-determinstic situation:

step 1 : given



step 2

none

step 3

⋮

Want to take a non-det Tm, M, and input w,

set $n = |w| =$ length w, assume all possible computation path halt within n^{5} steps. Want to give a

n^{20}

Boolean formula $f = f(x_1, x_2, \ldots, x_{Cn^{10}})$,

n^{40}

C = some constant, depending on M s.t.

f is satisfiable $\Longleftrightarrow$ M accept w.

Eventually: want f, or some variant of it, to be in 3CNF form.

(don't do this) and (don't do that) ...

Me $\to$ children:

$$\underbrace{(\neg x_2) \text{ and } (\neg x_5) \text{ and } \ldots \text{ and } (\neg x_{14})}_{1\ \text{CNF}}$$

3 CNF ( ) and ( ) and ... and ( )

x_1 OR x_2 OR $\neg x_{17}$

x_5 OR $\neg x_6$ OR x_3

...

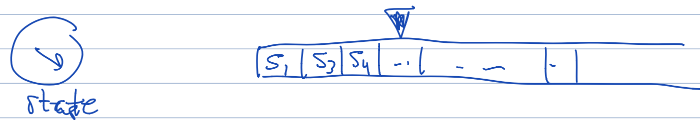
Start:

step 1 input

$\omega = w_1 \dots w_n$

step 2

⋮



step i

$$X_{ijr} = \begin{cases} \text{True} & \text{if step } i\text{, cell } j\text{, the symbol } r \text{ appears} \\ \text{False} & \text{otherwise} \end{cases}$$

$$Y_{ij} = \begin{cases} T & \text{if at step } i\text{, tape head is at cell } j \\ F & \text{otherwise} \end{cases}$$

$$Z_{iq} = \begin{cases} T & \text{if at step } i \text{ we are in state } q \\ F & \text{otherwise} \end{cases}$$

What is a valid accepting computation of M on input ω?

(valid on step 1) AND (step 1 → step 2 valid) AND (step 2 → step 3 valid)

AND -- AND ... AND (step n^5-1 → step n^5 valid)

AND $\underbrace{(\text{end in state } q_{acc})}_{Z_{n^5, q_{acc}} \text{ is true}}$

$Z_{n^5, q_{acc}}$ is true $\Longleftrightarrow$ $\overbrace{(Z_{n^5,q_{acc}} \text{ OR } Z_{n^5,q_{acc}} \text{ OR } Z_{n^5,q_{acc}})}^{\text{part of a 3CNF}}$

Rem: We want, Z_{iq} ~~for~~ for $q \in Q$, we want exactly one to be true. Similarly, for each i, j we want X_{ijr} to have one T, the rest F.

Say $u_1, \ldots, u_{20}$ are Boolean variables.

(Exactly one of $u_1, \ldots, u_{20}$ is True)

$\iff$ $(\neg u_1 \text{ OR } \neg u_2)$ AND $(\neg u_1 \text{ OR } \neg u_3)$ AND ....

AND $(u_1 \text{ OR } u_2 \text{ OR } u_3 \text{ OR} \ldots \text{OR } u_{20})$

$\underset{1 \le i < j \le 20}{\text{AND}}$ $(\neg u_i \text{ OR } \neg u_j \text{ OR } \neg u_j)$ $\leftarrow$ At most one u_i is T

AND $\underbrace{(u_1 \text{ OR } u_2 \text{ OR } \ldots \text{ OR } u_{20})}_{\text{this can be as a 3CNF}}$ $\longleftrightarrow$

$\boxed{(u_1 \text{ OR } u_2 \text{ OR } u_3 \text{ OR } u_4) \text{ will be true} \iff (u_1 \text{ OR } u_2 \text{ OR } \underline{w}) \text{ AND } (\underline{\neg w} \text{ OR } u_3 \text{ OR } u_4)}$

is satisfiable

Say $u_1 \leftarrow T$

$u_2, u_3, u_4 \leftarrow F$

$$(\underset{T}{u_1} \text{ OR } \underset{F}{u_2} \text{ OR } \underset{F}{w}) \text{ AND } (\underset{T}{\neg w} \text{ OR } \underset{F}{u_3} \text{ OR } \underset{F}{u_4})$$

Say $u_1, u_2, u_3, u_4 \leftarrow F$

$$\rightarrow (F \text{ OR } F \text{ OR } w) \text{ and } (\neg w \text{ OR } F \text{ OR } F)$$

can't be satisfied

We're headed to NP-completeness:

<u>Def</u>: We say that a language L is NP-complete if

(1) $L \in NP$, and

(2) If L' is any language NP, then $L' \leq_p L$

We are taking L' that is recognized by a poly time non-det Turing machine, M,

M, time bound (e.g. n^5), input w $\longrightarrow$ $\boxed{}$ $\longrightarrow$ Boolean formula in 3CNF

$$\downarrow$$

$$f(x_1, \ldots, \underbrace{x_{20x^{10}}}_{\text{poly \# of vars}})$$

$$= f_{M, w, \text{time bound}}$$

M accepts w $\iff$ $f = f_{M, w, \text{time bound}}$ is satisfiable