Dimostriamo adesso il Teorema di Cook-Levin.

TEO SAT è NP-completo.

DIM. Già abbiamo mostrato che $SAT \in NP$. (Dato $x = \langle \phi \rangle$, il certificato y è l'assegnamento che la soddisfa.)

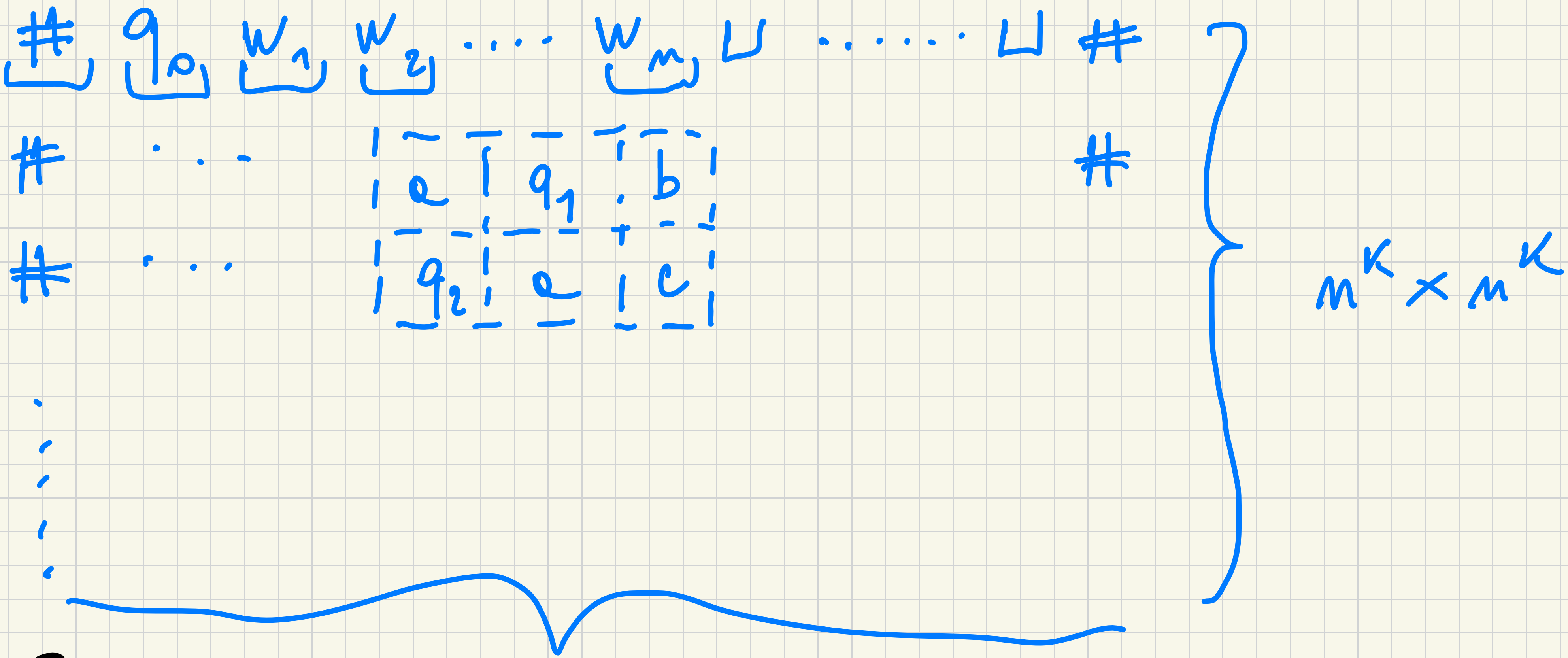
Resta da mostrare che SAT è NP-DIFFICILE.

Ovvero per ogni $A \in NP$, abbiamo $A \leq_m^p SAT$.

Sia N la NTM di tempo polinomiale che decide A, ovvero $L(N) = A$.

suppongo tempo $n^k (-3)$.

Associamo alla TM N una tabella di computazione su un dato input $w = w_1 \dots w_n$.



Per una NTM N avremo diverse tabelle, una per ogni ramo di computazione di N.
Le righe corrispondono alle diverse configurazioni

delle NTM durante la computazione.
Una tabella è ACCETTANTE se contiene lo stato q_{acc}; o meglio una tabella che contiene una configurazione valida e accettante.
N accetta un input x sse esiste una tabella di computazione valida e accettante.
La riduzione: Data N produrrà una formula ϕ che di fatto simula l'esecuzione di N su w.
Quali sono le variabili?

$$i, j \in [n^k]$$

$$x_{i,j,s} \qquad s \in S = Q \cup \Gamma \cup \{\#\}.$$

Poniamo $x_{i,j,s} = 1$ sse $cell[i,j] = s$
dove $cell[i,j]$ indica la cella in pos. (i,j).
Ora progetto la ϕ in modo che un assegnamento che la soddisfa corrisponde ad una tabella valida e accettante per N su input w.

$$\phi = \phi_{cell} \wedge \phi_{start} \wedge \phi_{move} \wedge \phi_{acc}$$

Ad es.: ϕ_{start} corrisponde al fatto che la prima riga deve contenere $\# q_0 w_1 \dots w_n \sqcup \dots \sqcup \#$.

$\underline{\phi_{start}}$: $x_{1,1,\#} \wedge x_{1,2,q_0} \wedge x_{1,3,w_1} \wedge \dots$

$\dots x_{1,n+2,w_n} \wedge x_{1,n+3,\sqcup} \wedge$

$\dots x_{1,n^k-1,\sqcup} \wedge x_{1,n^k,\#}$

$$\underline{\phi_{acc}} : \bigvee_{i,j \in [n^k]} x_{i,j,q_{acc}}$$

Ovvero, almeno una riga contiene q_{acc}.

$\underline{\phi_{cell}}$: Intuitivamente ci dice che se la cell$[i,j]$ contiene s (ovvero $x_{i,j,s}=1$) allora cell$[i,j]$ non può contenere $t \neq s$ (ovvero $x_{i,j,t\neq s}=0$).

$$\Phi_{cell} = \bigwedge_{i,j \in [n^k]} \left(\left(\bigvee_{s \in S} x_{i,j,s} \right) \wedge \left(\bigwedge_{\substack{s,t \in S \\ s \neq t}} \left(\overline{x_{i,j,s}} \vee \overline{x_{i,j,t}} \right) \right) \right)$$

Il termine $\bigvee_{s \in S} x_{i,j,s}$ assicura che almeno una variabile associata alla cell[i,j] assume valore 1.

Il termine $\bigwedge_{\substack{s,t \in S \\ s \neq t}} \overline{x_{i,j,s}} \vee \overline{x_{i,j,t}}$ invece assicura che per ogni coppia di variabili non più di una assume valore 1.

<u>Φ_{move}:</u> Mi assicuro che la riga successiva segue quella precedente in accordo ad una delle possibili transizioni garantite dalla δ della NTM N.

Questo si ottiene assicurandosi che ogni finestra di celle 2×3 sia lecita (ovvero non violi le transizioni ammesse dalla δ).

FINESTRE NON LECITE:

a	b	b
a	b	c

$\cdots\cdots\ q\ a \cdots$ ✗

$q_2\ a\ b$

$q_2\ a\ q_3$ ✗

Finestra LECITA : . . . .

a	q_1	b
q_2	a	c

. . . . ✓

$$\delta(q_1, b) = \{(q_2, c, L), (q_1, b, R)\}$$

a	b	c
a	b	c

. . . . . q

$$\Phi_{move} : \bigwedge_{(i,j)\in[n^k]} (\text{la finestra } (i,j) \text{ è LECITA})$$

"la finestra (i,j) è LECITA" : $\left(\begin{array}{c|c|c} e_1 & e_2 & e_3 \\ \hline e_4 & e_5 & e_6 \end{array}\right)$

$$\bigvee_{\substack{e_1 \dots e_6 \\ \text{finestre} \\ \text{lecite}}} x_{i,j-1,e_1} \wedge x_{i,j,e_2} \wedge x_{i,j+1,e_3} \wedge x_{i+1,j-1,e_4} \wedge x_{i+1,j,e_5} \wedge x_{i+1,j+1,e_6}$$

Complessità di tempo: # variabili $x_{i,j,s}$ è il # celle (n^{2k}) per tutti i possibili simboli in $S = \Gamma \cup \{\#\} \cup Q$. Ma $|S|$ è indipendente da n $\Rightarrow$ # variabili è poly(n).

Le dimensioni pure sono polinomiali di

ciascuna sotto formula ϕ_{start}, ϕ_{move}, ϕ_{acc}
e ϕ_{cell}

Usando le riduzioni, possiamo mostrare che molti dei problemi che abbiamo incontrato sono NP-completi.

TEO SAT $\leq_m^P$ CIRCUIT-SAT.

Banale: perché una formula è un circuito.
Ma allora CIRCUIT-SAT è NP-completo perché sta in NP ed inoltre:

$$\forall A \in NP : A \leq_m^P SAT \leq_m^P \text{CIRCUIT-SAT}$$

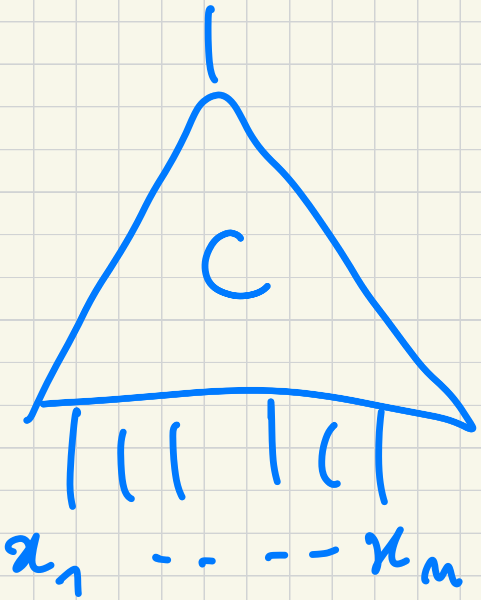
ovvero : $A \leq_m^p$ CIRCUIT-SAT.

COR CIRCUIT-SAT è NP-completo.

Altro esempio : 3SAT.

TEO. CIRCUIT-SAT $\leq_m^p$ 3SAT.

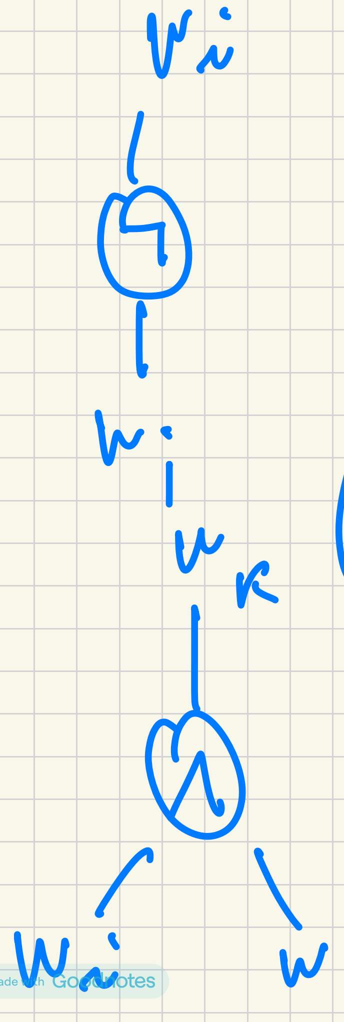
Dim. Dato C, circuito, devo costruire ϕ_C



$\Longleftrightarrow$ ϕ_C (3-CNF)

t.c. $C(x) = 1$ sse $\phi_C(w) = 1$

Le variabili w corrispondono ai cavi del circuito. Devo codificare i valori dei cavi in modo consistente al circuito. Lo faccio gate per gate (e poi considero l'$\wedge$).



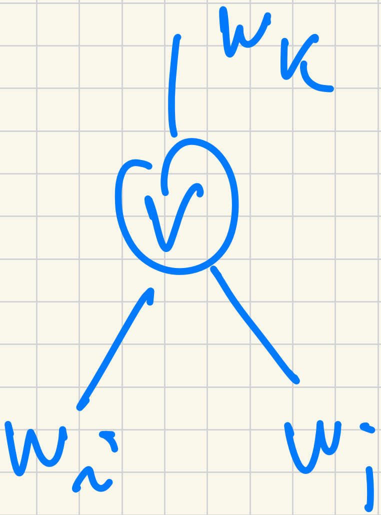
$$\text{"} w_j \Longleftrightarrow \overline{w_i} \text{"} \equiv (w_i \vee w_j) \wedge (\overline{w_i} \vee \overline{w_j})$$

$$((\overline{w_i} \wedge \overline{w_j}) \rightarrow \overline{w_k}) \wedge ((\overline{w_i} \wedge w_j) \rightarrow \overline{w_k}) \wedge$$

$$((w_i \wedge \overline{w_j}) \rightarrow \overline{w_k}) \wedge ((w_i \wedge w_j) \rightarrow w_k)$$

$$(w_i \vee w_j \vee \overline{w_k}) \wedge (w_i \vee \overline{w_j} \vee \overline{w_k}) \wedge$$

$$(\overline{w_i} \vee w_j \vee \overline{w_k}) \wedge (\overline{w_i} \vee \overline{w_j} \vee w_k)$$



$$(w_i \vee w_j \vee \overline{w_k}) \wedge (w_i \vee \overline{w_j} \vee w_k) \wedge (\overline{w_i} \vee w_j \vee w_k) \wedge (\overline{w_i} \vee \overline{w_j} \vee w_k)$$

$\blacksquare$

$\Rightarrow$ <u>Cor</u> 3SAT è NP-completo.

$3COL \le 4COL \le SAT \le CIRCUIT\text{-}SAT \le 3SAT \le 3COL$

(Per ora non lo facciamo.)

$3SAT \le CLIQUE$

Tutti NP-completi.