$\mathcal{NP}$-completezza di SAT

Sappiamo che SAT $\in \mathcal{NP}$ (si genera non deterministicamente un assegnamento e lo si verifica in tempo polinomiale), e che CIRCUIT SAT $\leq$ SAT, quindi è sufficiente verificare che CIRCUIT SAT è $\mathcal{NP}$-completo.

Per farlo, adattiamo la riduzione usata per la $\mathcal{P}$-completezza di CIRCUIT SAT al caso non deterministico. Non funziona immediatamente perché non c'è un'unica tabella di computazione.

Quindi, dato un problema $I \in \mathcal{NP}$ deciso in tempo polinomiale dalla macchina non deterministica N,

- costruiamo N' in cui le scelte non deterministiche sono sempre tra due alternative. Possiamo sempre farlo:
  - aggiungendo una scelta che è duplicato della prima dove ce n'è una sola;
  - scegliendo tra la prima scelta e le altre $s-1$ se ce ne sono $s > 2$ (aggiungiamo $s-2$ nuovi stati).

  Una computazione di N' è quindi una sequenza di bit $b_0 \dots b_{n^k-1}$;
- costruiamo la tabella di computazione di una specifica esecuzione, indicando in una colonna aggiuntiva le scelte effettuate. Le celle sono determinate dalle funzioni $F_1, \dots, F_m$:

$$\begin{aligned} s_{i,j,l} = F_l(&\overbrace{s_{i-1,n^k+1}}^{b_{i-1}} \\ &s_{i-1,j-1,1}, \dots, s_{i-1,j-1,m}, \\ &s_{i-1,j,1}, \dots, s_{i-1,j,m}, \\ &s_{i-1,j+1,1}, \dots, s_{i-1,j+1,m}), \end{aligned}$$

  che sono calcolate da un circuito $\overline{C}$ con $3m+1$ ingressi e m uscite;
- la riduzione f costruisce un circuito C componendo copie di $\overline{C}$ in modo analogo a quella per CIRCUIT VALUE, ma inserendo porte variabili nelle posizioni corrispondenti all'ultima colonna. Esiste un assegnamento delle variabili del circuito $f(x)$ che lo soddisfa se e solo se esiste una computazione di N' che termina in uno stato di accettazione.

Altri problemi $\mathcal{NP}$-completi (a cui si riduce SAT): HAM, CRICCA, TSP.