

Föreläsning 24 i ADK

Cooks sats

Viggo Kann

KTH

SAT – satisfierbarhetsproblemet

Definition av SAT:

- **Indata:** Boolesk formel ϕ med booleska variabler.
Formeln får innehålla operatorerna $\wedge, \vee, \neg, \Rightarrow, \equiv$, till exempel $((x_1 \Rightarrow x_2) \vee (x_1 \vee \overline{x_3} \vee \overline{x_4})) \wedge (x_1 \equiv (x_2 \vee x_3))$
- **Fråga:** Finns det någon variabeltilldelning som satisfierar ϕ , dvs gör formeln sann?

SAT ligger i NP eftersom det går att verifiera en lösning (en variabeltilldelning) i polynomisk tid.

Verifieringsalgoritm: Givet formeln och en variabeltilldelning, evaluera formeln med den givna variabeltilldelningen och svara **ja** om formeln är sann och **nej** annars.

NP-fullständiga problem

- Ett beslutsproblem Q är NP-fullständigt om

- 1 $Q \in \mathcal{NP}$

- 2 $Q' \leq_p Q$ för alla $Q' \in \mathcal{NP}$

Där $\leq_p$ är en Karpreduktion som går i polynomisk tid

- Ett problem som uppfyller villkor 2 är NP-svårt
- Ännu inte bevisad tes:
 - NP-svåra problem kan inte lösas i polynomisk tid, dvs. $\mathcal{P} \neq \mathcal{NP}$

Cooks sats (1971)

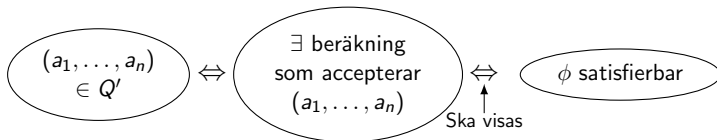
SAT, satisfierbarhetsproblemet, är NP-fullständigt

Följdsats

$\text{SAT} \leq_p Q \Rightarrow Q$ är NP-svårt

Bevis av Cooks sats

- 1 Visa att $\text{SAT} \in \mathcal{NP}$ (enkelt, se första bilden)
 - 2 Visa att $Q' \in \mathcal{NP} \Rightarrow Q' \leq_p \text{SAT}$
- $Q' \in \mathcal{NP} \Rightarrow$ Det finns en ickedeterministisk turingmaskin M som accepterar Q' i tid $k \cdot n^c$ där n är indatas längd
 - Vi kan anta att M har ett (halvoändligt) band och alfabet $\{0,1,\#\}$
 - Givet indata $(a_1, \dots, a_n)$. Då gäller att $(a_1, \dots, a_n) \in Q' \Leftrightarrow \exists$ beräkning i tid $k \cdot n^c : M(a_1, \dots, a_n)$ accepterar
 - Låt oss försöka beskriva M -s beräkning med hjälp av en boolesk formel ϕ så att $(a_1, \dots, a_n) \in Q' \Leftrightarrow \phi$ är satisfierbar, alltså:



Inbäddning av turingmaskin som SAT-problem

- Numrera M -s tidssteg från 1 till $k \cdot n^c$
- Vid varje tidpunkt t beskrivs beräkningen av
 - aktuellt tillstånd q
 - bandets aktuella innehåll
 - huvudets position på bandet
- Obs: vad som finns bortom position $k \cdot n^c$ på bandet är inte intressant
- Inför booleska variabler:
 - x_{qt} $q \in Q$, $1 \leq t \leq k \cdot n^c$
 - y_{ijt} $i \in \{0,1,\#\}$, $1 \leq j \leq k \cdot n^c$, $1 \leq t \leq k \cdot n^c$
 - z_{jt} $1 \leq j \leq k \cdot n^c$, $1 \leq t \leq k \cdot n^c$
- Vi vill att
 - $x_{qt} = 1$ omm M är i tillstånd q vid tid t
 - $y_{ijt} = 1$ omm tecknet i står i ruta j på bandet vid tid t
 - $z_{jt} = 1$ omm huvudet står i ruta j vid tid t

Bevis av Cooks sats

" $\exists$ beräkning i tid $k \cdot n^c$ så att $M(a_1, \dots, a_n)$ accepterar" $\Leftrightarrow$

$\Leftrightarrow \begin{cases} \textcircled{1} & \text{Beräkningen börjar med } a_1, \dots, a_n \\ \textcircled{2} & x, y, z \text{ beskriver en giltig (ickedeterministisk) beräkning} \\ \textcircled{3} & \text{beräkningen accepterar} \end{cases}$

$$\textcircled{1} \begin{cases} x_{q,1} = 1 & \text{om } q = q_0 \\ x_{q,1} = 0 & \text{annars} \\ y_{i,j,1} = 1 & \text{om } (i = a_j \text{ och } 1 \leq j \leq n) \text{ eller } (i = \# \text{ och } j > n) \\ y_{i,j,1} = 0 & \text{annars} \\ z_{1,1} = 1 \\ z_{j,1} = 0 & \text{för } j > 1 \end{cases}$$

$$\textcircled{3} \quad x_{q_a,1} = 1 \vee x_{q_a,2} = 1 \vee \dots \vee x_{q_a,k \cdot n^c} = 1$$

Där q_a är det accepterande tillståndet

Bevis av Cooks sats

- ②
- För varje $2 \leq t \leq k \cdot n^c$ konstruera formel som beskriver tillåtna samband mellan $x_{q,(t-1)}, y_{i,j,(t-1)}, z_{j,(t-1)}$ och $x_{q,t}, y_{i,j,t}, z_{j,t}$
 - Ex: övergången



(om # står i rutan, skriv 0 och flytta huvudet ett steg åt höger) beskrivs som

$$x_{q',(t-1)} = 1 \wedge y_{\#,j,(t-1)} = 1 \wedge z_{j,(t-1)} = 1 \Rightarrow$$

$$\Rightarrow [x_{q'',t} = 1 \wedge \bigwedge_{q \neq q''} x_{q,t} = 0 \wedge$$

$$\wedge y_{0,j,t} = 1 \wedge y_{1,j,t} = 0 \wedge y_{\#,j,t} = 0 \wedge$$

$$\wedge \bigwedge_{\substack{i \in \{0,1,\#\} \\ j' \neq j}} y_{i,j',t} = y_{i,j',(t-1)} \wedge$$

$$\wedge z_{j+1,t} = 1 \wedge \bigwedge_{j' \neq j+1} z_{j',t} = 0]$$

för $1 \leq j \leq k \cdot n^c$