1 P, NP and NPC

Definition P

P = Sprog der kan bestemmes i polymiel tid at en TM

Dette betyder at en TM der bestemmer et sprog vil på et givet input x bestemme om x er i sproget eller ej i $p(|x|)$ tid hvor p er et polynomie.

Definition NP

NP indeholder de sprog hvor der eksisterer $L' \in P$ og et polynomie p så:

$$\forall x: x \in L \Leftrightarrow \exists y \in \{0,1\}^* : |y| \leq p(|x|) \wedge \langle x, y \rangle \in L'$$

P=NP? Propersition 2

Hvis P=NP så er der en algoritme der tager som input et formelt udsagn t af ZFC og hvis der eksisterer et bevis af længde n outputter dette i polymiel tid.

Bevis:

- Vi kan effektivt tjekke om et bevis er korrekt.

Definer $MATH = \{\langle t, 0^{(n)}, S \rangle : \exists$ ZFC bevis af længde n starter med S$\}$

$MATH \in NP$ da alle strenge af længde $n-|S|$ blot kan forsøges.

Hvis P=NP er $MATH \in P$.

Vi kan da give MATH input $\langle t, 0^{(1)}, \lambda \rangle$, $\langle t, 0^{(2)}, \lambda \rangle$ indtil 1 input accepteres. Derefter findes beviset ved binær søgning: $\langle t, 0^{(n)}, 0 \rangle$ $\langle t, 0^{(n)}, 01 \rangle$ osv.

Dette tager blot polymiel tid.

Detination reduction

$L_1 \leq L_2$ hvis der eksisterer et polymielt tids beregneligt map r så:

$\forall x : x \in L_1 \Leftrightarrow r(x) \in L_2$

Propersition 3

Hvis $L_1 \leq L_2$ og $L_2 \leq L_3$ da er $L_1 \leq L_3$

Bevis:

Vi har r_1 og r_2 så:

$\forall x : x \in L_1 \Leftrightarrow r_1(x) \in L_2$ og

$\forall y : y \in L_2 \Leftrightarrow r_2(y) \in L_3$

Dette giver os

$\forall x : x \in L_1 \Leftrightarrow r_2 \circ r_1(x) \in L_3$ og $r_2 \circ r_1$ er et polymielt beregneligt map □

Detination NP-hard

NP-hard:

$\forall L_1 \in NP : L_1 \leq L_2$ L_2 er da NP-hard

Propersition 5

Lad $L \in$ NP-hard. Hvis $P \neq NP$ så er $L \notin P$.

Bevis:

Da $L \in$ NP-hard gælder: $\forall L_1 \in NP : L_1 \leq L$ og hvis $L \in P$ da vil alle sprog i NP kunne udføres polymielt, så $P = NP$.

Defination NPC

Et sprog er NPC hvis sproget er NP-hard og tilhører NP.

Propersition 6

Lad $L \in NPC$. Så $P=NP \Leftrightarrow L \in P$.

Bevis:

$\Rightarrow$ Hvis $P=NP$, så da $L \in NP$ så $L \in P$ også

$\Leftarrow$ Hvis $L \in P$, og da $L \in NP$-hard da er $NP=P$