Dertiende college complexiteit

21 april 2008

NP-volledigheid IV

$P \leq_P Q$ betekent dat er een polynomiale reductie T van P naar Q bestaat:

1. T beeldt elke invoer x van P af op een invoer $T(x)$ van Q.

2. De constructie van $T(x)$ uit x is polynomiaal ($O(|x|^k)$).

3. Voor elke x uit I (= invoerverzameling van P) geldt: x is een ja-instantie voor $P \iff T(x)$ is een ja-instantie voor Q.

Stelling
Als $P \leq_P Q$ en $Q \in \mathcal{P}$, dan $P \in \mathcal{P}$.

Definitie
Een probleem Q is NP-hard als elk probleem P in $\mathcal{NP}$ polynomiaal reduceerbaar is tot Q, dat wil dus zeggen dat $P \leq_P Q$ voor alle $P \in \mathcal{NP}$.

Definitie
Een probleem Q is NP-volledig als

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

2. Q is NP-hard

Notatie
De klasse van NP-volledige problemen geven we aan met $\mathcal{NPC}$ (NP-complete).

Stelling
Als een of ander NP-volledig probleem in $\mathcal{P}$ zit, dan is $\mathcal{P} = \mathcal{NP}$.

Dit betekent dus: als één enkel NP-volledig probleem P polynomiaal begrensd is, dan zijn alle problemen uit $\mathcal{NP}$ polynomiaal begrensd.
Omgekeerd: als een willekeurig probleem in $\mathcal{NP}$ niet polynomiaal begrensd is, dan zijn *alle* NP-volledige problemen niet polynomiaal begrensd.

Lemma

$\leq_P$ is transitief, dat wil zeggen: als $P_1 \leq_P P_2$ en $P_2 \leq_P P_3$ dan is $P_1 \leq_P P_3$.

Stelling

Stel P is een probleem waarvoor geldt dat $Q \leq_P P$ voor een of andere $Q \in \mathcal{NPC}$. Dan is P NP-hard.
Als bovendien $P \in \mathcal{NP}$, dan geldt dat $P \in \mathcal{NPC}$.

Dus door een bekend NP-volledig probleem te reduceren tot P reduceren we impliciet alle problemen uit $\mathcal{NP}$ tot P. Dit geeft ons derhalve een methode om aan te tonen dat een probleem P NP-volledig is.

1. Bewijs dat $P \in \mathcal{NP}$
2. Kies een bekend NP-volledig probleem Q
3. Toon aan dat $Q \leq_P P$

Stap 3 valt uiteen in:

3a. Geef een functie T van I (de invoerverzameling van Q) naar I' (de invoerverzameling van P) die elke $x \in I$ afbeeldt op een element van I'

3b. Laat zien dat $T(x)$ uit x geconstrueerd kan worden in polynomiaal begrensde tijd ($O(|x|^k)$ voor zekere $k \geq 0$)

3c. Toon aan dat T voldoet aan: $x \in I$ is een ja-instantie voor Q $\iff$ $T(x) \in I'$ is een ja-instantie voor P

In 1971 bewees Stephen Cook op een directe manier (dus door een reductie te geven van alle problemen uit $\mathcal{NP}$ naar SAT) dat SAT NP-volledig is.

Stelling
Gegeven een willekeurig probleem $P \in \mathcal{NP}$. Dan is P reduceerbaar tot SAT: $P \leq_P$ SAT.

Sindsdien is met behulp van de reductiemethode van zeer veel bekende problemen aangetoond dat ze NP-volledig zijn. Bijvoorbeeld voor enige voorbeeldproblemen:

$$\text{SAT} \leq_P \text{3SAT} \leq_P \text{Kliek} \leq_P \text{VC}$$
$$\text{3SAT} \leq_P \text{HC} \leq_P \text{TSP}$$
$$\text{SAT} \leq_P \text{3Kleur} \leq_P \text{4Kleur}$$

Schets van het bewijs

1. Omdat $P \in \mathcal{NP}$, is er een niet-deterministisch algoritme A (een niet-deterministische Türingmachine) voor P. Verder is A polynomiaal begrensd ($O(|x|^k)$).
2. Dit algoritme zal voor elke invoer x van P gemodelleerd worden als een logische formule $\phi = T(x)$ in CNF: deze ϕ beschrijft a.h.w. de berekening van A, werkend op x.
3. De formule ϕ is weliswaar lang, maar kan in hooguit $O(|x|^l)$ stappen geconstrueerd worden.
4. Een ja-executie vergt voor ja-instanties x hooguit $N = c \cdot |x|^k$ stappen (want A is polynomiaal begrensd).
5. Een waarmakende waardering voor ϕ correspondeert precies met een executie van A die een "ja" produceert (voor zekere string s dus).

Boolese variabelen in ϕ:

${Q_i}^q$: op tijdstip i is de machine in toestand $q \in Q$, $0 \leq i \leq N$

H_{ij}: op tijdstip i scant de machine cel j, $0 \leq i, j \leq N$

${S_{ij}}^a$: op tijdstip i bevat cel j symbool $a \in \Sigma$, $0 \leq i, j \leq N$

De formule ϕ is een conjunctie van:

- ${Q_0}^{\texttt{start}} \wedge \cdots \wedge H_{00} \wedge {S_{01}}^{x_1} \wedge {S_{02}}^{x_2} \wedge {S_{03}}^{x_3} \cdots$

  de machine start in toestand `start`;

  x bevindt zich op de posities 1 t/m $|x|$; ...

- $Q_N^{q_Y} \wedge H_{N0} \wedge \cdots$

  op tijdstip N stopt de berekening in de ja-toestand

- $\wedge_{0 \leq i \leq N}(\vee_{q \in Q}\ {Q_i}^q) \wedge \wedge_{0 \leq i \leq N}(\wedge_{p,q \in Q, p \neq q}(\neg {Q_i}^p \vee \neg {Q_i}^q))$

  te allen tijde is de machine in precies één toestand

- $\wedge_{0 \leq i,j \leq N}(\vee_{a \in \Sigma}\ {S_{ij}}^a) \wedge \wedge_{0 \leq i,j \leq N}(\wedge_{a,b \in \Sigma, a \neq b}(\neg {S_{ij}}^a \vee \neg {S_{ij}}^b))$

  te allen tijde bevat elke cel precies één symbool

- $\wedge_{0 \leq i \leq N}(\vee_{0 \leq j \leq N}\ H_{ij}) \wedge \wedge_{0 \leq i \leq N}(\wedge_{0 \leq j < k \leq N}(\neg H_{ij} \vee \neg H_{ik}))$

  te allen tijde scant de machine precies één cel

- $Q_i^{\,p} \wedge H_{ij} \wedge S_{ij}^{\,a} \longrightarrow$
  $\vee_{((p,a),(q,b,d))\in\delta}\ (Q_{i+1}^{\,q} \wedge H_{i+1,j+d} \wedge S_{i+1,j}^{\,b})$

  elke stap van de machine verloopt volgens de transitiefunctie δ

- $S_{ij}^{\,a} \wedge \neg H_{ij} \longrightarrow S_{i+1,j}^{\,a}$

  elke cel die op tijdstip i niet gescand wordt bevat op tijdstip $i+1$ hetzelfde symbool

Een waarmakende waardering correspondeert aldus precies met een echte executie van de niet-deterministische Türingmachine die eindigt in "ja" na een polynomiaal (nl. N) aantal stappen.

HC1: **gegeven** een *gerichte* graaf $\mathcal{G}= (V, E)$.
Vraag: heeft $\mathcal{G}$ een Hamiltonkring?

HC2: **gegeven** een *ongerichte* graaf $\mathcal{G} = (V, E)$.
Vraag: heeft $\mathcal{G}$ een Hamiltonkring?

Bewering: HC1 $\leq_P$ HC2

Opmerking: er geldt ook: HC2 $\leq_P$ HC1. Bedenk zelf een eenvoudige reductie.

Transformatie T die een gerichte graaf $\mathcal{G} = (V, E)$ op een ongerichte graaf $T(\mathcal{G}) = \mathcal{G}' = (V', E')$ afbeeldt:

- $V' = \{v_1, v_2, v_3 : v \in V\}$: elke knoop $v \in V$ wordt afgebeeld op een drietal knopen v_1, v_2, v_3.
- $E' = \{(v_1, v_2), (v_2, v_3) : v \in V\} \cup \{(v_3, w_1) : (v, w) \in E\}$: binnen elk drietal knopen corresponderend met v loopt een tak tussen v_1 en v_2 en tussen v_2 en v_3, en voor elke tak van v naar w in $\mathcal{G}$ komt een tak in $\mathcal{G}'$ tussen v_3 en w_1.

Dan geldt:

1. T kan in polynomiaal begrensde tijd berekend worden (constructie van $T(\mathcal{G})$ uit $\mathcal{G}$ is $O(|\mathcal{G}|)$)
2. $\mathcal{G}$ is een ja-instantie voor HC1 $\iff$ $T(\mathcal{G})$ is een ja-instantie voor HC2, ofwel: $\mathcal{G}$ heeft een gerichte Hamiltonkring $\iff$ $\mathcal{G}'$ heeft een ongerichte Hamiltonkring

3SAT

Gegeven een logische formule ϕ in 3-CNF. Bestaat er een waardering die ϕ True maakt?

Definitie

Een logische formule ϕ staat in 3-CNF als ϕ een conjunctie is van clausules, waarbij elke clausule een disjunctie is van drie verschillende literals.

Kliek

Gegeven een ongerichte graaf $\mathcal{G} = (V, E)$ en een geheel getal k $(0 \leq k \leq |V|)$. Is er in $\mathcal{G}$ een kliek ter grootte k?

Definitie

Een kliek in een ongerichte graaf $\mathcal{G} = (V, E)$ is een deelverzameling $V' \subseteq V$ zodanig dat voor elk tweetal knopen $u, v \in V'$ $(u \neq v)$ geldt dat $(u, v) \in E$. (M.a.w.: tussen elk tweetal knopen uit V' zit een tak.)

Er geldt: 3SAT $\leq_P$ Kliek. Om dit aan te tonen moeten we een logische formule in 3-CNF afbeelden op een ongerichte graaf.

Zij ϕ een logische expressie (formule) in 3-CNF, met zeg m clausules: $\phi = C_1 \wedge C_2 \wedge \ldots \wedge C_m$. Hierin is $C_r = l_1^r \vee l_2^r \vee l_3^r$ $(r = 1, \ldots, m)$ en l_1^r, l_2^r en l_3^r steeds verschillend bij vaste r.

Construeer nu een ongerichte graaf $\mathcal{G}_\phi = (V, E)$ als volgt.

Voor elke clausule C_r uit ϕ doen we 3 knopen v_1^r, v_2^r en v_3^r in V (deze corresponderen dus met l_1^r, l_2^r en l_3^r). $\mathcal{G}_\phi$ heeft derhalve $3m$ knopen.

Er komt een tak tussen twee knopen v_i^r en v_j^s als:

- v_i^r en v_j^s in verschillende drietallen zitten (dus $r \neq s$)
- de bijbehorende l_i^r en l_j^s zó zijn dat $l_i^r \neq \neg l_j^s$, met andere woorden: l_i^r en l_j^s zijn niet elkaars negatie

Definieer nu de transformatie T als: $T(\phi) =< \mathcal{G}_\phi, m >$.
Dan geldt:

- T kan in polynomiaal begrensde tijd berekend worden.
- Er is een waardering die ϕ waarmaakt $\Longleftrightarrow$ $\mathcal{G}_\phi$ heeft een kliek ter grootte m.

Voorbeeld

Laat $\phi = C_1 \wedge C_2 \wedge C_3$, met $C_1 = x_1 \vee \neg x_2 \vee \neg x_3$, $C_2 = \neg x_1 \vee x_2 \vee x_3$ en $C_3 = x_1 \vee x_2 \vee x_3$. Hier is dus $m = 3$.

Dan $v_1^1 \leftrightarrow x_1, v_2^1 \leftrightarrow \neg x_2, v_3^1 \leftrightarrow \neg x_3$; alle uit clausule C_1, etcetera

- een waardering w die ϕ waarmaakt is bijvoorbeeld: $w(x_1) = w(x_2) =$ False en $w(x_3) =$ True. Een bijbehorende kliek in $\mathcal{G}_\phi$ ter grootte 3 is dan $\{v_2^1, v_3^2, v_3^3\}$(*).

- een kliek ter grootte 3 in $\mathcal{G}_\phi$ is bijvoorbeeld $\{v_1^1, v_2^2, v_2^3\}$. Een bijbehorende waardering is $w(x_1) = w(x_2) = w(x_3) =$ True. Deze maakt ϕ waar.

(*) De bovenindex geeft aan met welke clausule een knoop correspondeert.

SAT

Gegeven een logische formule ϕ in CNF. Bestaat er een waardering van de in ϕ voorkomende logische variabelen die ϕ True maakt?

Definitie

Een logische formule ϕ staat in Conjunctive Normal Form als ϕ een conjunctie is van clausules, waarin een clausule een disjunctie is van literals.

3SAT

Gegeven een logische formule ϕ in 3-CNF. Bestaat er een waardering die ϕ True maakt?

Definitie

Een logische formule ϕ staat in 3-CNF als ϕ een conjunctie is van clausules, waarbij elke clausule een disjunctie is van drie verschillende literals.

Er geldt: SAT $\leq_P$ 3SAT. Om dit aan te tonen moeten we een logische formule ϕ in CNF afbeelden op een logische formule ϕ' in 3-CNF. We gaan er voor het gemak van uit dat de $l_1, l_2, \ldots, l_k$ per clausule al verschillend zijn (kan in $O(|\phi|^2)$ worden bewerkstelligd). Op clausuleniveau werkt de transformatie T als volgt:

$$l_1 \longrightarrow (l_1 \vee \widetilde{l_2} \vee \widetilde{l_3}) \wedge (l_1 \vee \widetilde{l_2} \vee \neg\widetilde{l_3}) \wedge (l_1 \vee \neg\widetilde{l_2} \vee \widetilde{l_3}) \wedge (l_1 \vee \neg\widetilde{l_2} \vee \neg\widetilde{l_3})$$
$$l_1 \vee l_2 \longrightarrow (l_1 \vee l_2 \vee \widetilde{l_3}) \wedge (l_1 \vee l_2 \vee \neg\widetilde{l_3})$$
$$l_1 \vee l_2 \vee l_3 \longrightarrow l_1 \vee l_2 \vee l_3$$
$$l_1 \vee l_2 \vee l_3 \vee l_4 \longrightarrow (l_1 \vee l_2 \vee \widetilde{l_5}) \wedge (l_3 \vee l_4 \vee \neg\widetilde{l_5})$$
$$l_1 \vee l_2 \vee l_3 \vee l_4 \vee l_5 \longrightarrow (l_1 \vee l_2 \vee \widetilde{l_6}) \wedge (l_3 \vee \neg\widetilde{l_6} \vee \widetilde{l_7}) \wedge (l_4 \vee l_5 \vee \neg\widetilde{l_7})$$

En in het algemeen voor $k \geq 4$:

$$l_1 \vee l_2 \vee \ldots \vee l_{k-1} \vee l_k \longrightarrow (l_1 \vee l_2 \vee \widetilde{l_{k+1}}) \wedge (l_3 \vee \neg\widetilde{l_{k+1}} \vee \widetilde{l_{k+2}}) \wedge (l_4 \vee \neg\widetilde{l_{k+2}} \vee \widetilde{l_{k+3}}) \wedge \ldots \wedge (l_{k-2} \vee \neg\widetilde{l_{2k-4}} \vee \widetilde{l_{2k-3}}) \wedge (l_{k-1} \vee l_k \vee \neg\widetilde{l_{2k-3}})$$

Hierin zijn $\widetilde{l_{k+1}}, \widetilde{l_{k+2}}, \ldots, \widetilde{l_{2k-3}}$ steeds nieuwe, frisse, logische variabelen.
Een clausule met k (verschillende) literals wordt zo getransformeerd in een conjunctie van $k-2$ clausules met elk 3 verschillende literals.
Het beeld van een conjunctie van clausules definiëren we als een conjunctie van de beelden van de samenstellende clausules:

$$\phi = C_1 \wedge C_2 \wedge \ldots \wedge C_m \longrightarrow T(C_1) \wedge T(C_2) \wedge \ldots \wedge T(C_m) = T(\phi)$$

Voor deze transformatie T geldt:

- De constructie van $T(\phi)$ uit ϕ kan met een polynomiaal begrensd ($= O(|\phi|^k)$) algoritme.

- ϕ is een ja-instantie van SAT $\Longleftrightarrow$ $T(\phi)$ is een ja-instantie van 3SAT.

- Ofwel: er is een waardering die ϕ waarmaakt $\Longleftrightarrow$ er is een waardering die $T(\phi)$ waarmaakt.

- Conclusie uit de vorige punten: SAT $\leq_P$ 3SAT.

- maandag 21 april: 13.45-15.30 laatste werkcollege
- dinsdag 22 april: 11.15-13.00 laatste college: oud tentamen
- dinsdag 6 mei: 11.15-13.00 KI, dus geen wCom
- tentamen: donderdag 5 juni 2008, 14.00-17.00
- vragenuur: ?????