Complexiteit

Uitwerkingen Opgaven

opgave 59a
SAT: gegeven een logische formule ϕ in CNF. Bestaat er een waardering van de in ϕ voorkomende logische variabelen die ϕ waarmaakt?
Om te bewijzen dat SAT $\in \mathcal{NP}$ is het voldoende om een polynomiaal begrensd niet-deterministisch algoritme A te geven voor SAT. De invoer voor A is een logische formule ϕ. Merk op dat n, het aantal verschillende in ϕ voorkomende logische variabelen $x_1, x_2, \ldots, x_n$, in een polynomiaal aantal stappen kan worden bepaald. Immers (bijvoorbeeld): loop van links naar rechts door ϕ heen en voor elke logische variabele die je zo tegenkomt kijk je of er rechts van je in ϕ nog een exemplaar van staat. Zo ja dan tel je hem niet mee, zo nee, dan wel tellen. Zo tel je precies het meest rechter voorkomen van elke variabele in de formule, en daarmee krijg je precies het aantal verschillende logische variabelen in $O(|\phi|^2)$ stappen. Aangezien dit dus polynomiaal kan, heeft dit geen invloed op de polynomialiteit van Fase 2, en kunnen we ook wel (zonder beperking der algemeenheid) aannemen dat we weten dat er n verschillende logische variabelen in ϕ staan. Voor het gemak veronderstellen we dus dat n bekend is.
Intuïtief: een certificaat (waarmee je eenvoudig kunt laten zien dat een ja-instantie inderdaad een ja-instantie is) zal hier een waardering zijn die de invoerformule ϕ waarmaakt. Immers, precies het bestaan van zo'n waardering maakt ϕ tot een ja-instantie.

1. Fase 1 (gokfase)
   Er wordt een string s gegenereerd, hierna te interpreteren als een rij booleans (waardering van de gebruikte logische variabelen).
   // Hopelijk stelt dit een waarmakende waardering voor

2. Fase 2 (verificatiefase)
   Er wordt gecontroleerd of s een waarmakende waardering voorstelt (interpreteer de i-de boolean als de waarheidswaarde voor de i-de logische variabele):
   (1) controleer dat er precies n logische waarden staan: s aflopen en tellen (en meteen checken dat elke s_i een boolean T of F voorstelt): $O(|s|)$
   (2) controleer dat de waardering voorgesteld door s een waarmakende waardering is voor ϕ. Hiertoe ϕ aflopen, clausule voor clausule. Voor elke clausule kijken of een der voorkomende literals volgens s true is. Daarvoor de waardering van elke literal ophalen uit s. Dat kan samen zeker in $O(|\phi| \cdot |s|)$ stappen.
   Als beide controles positief zijn retourneert het verificatie-algoritme True, anders wordt False geretourneerd of gaat het programma in een oneindige loop of blijft hangen, of ...

3. Fase 3 (uitvoerfase)
   Als fase 2 True oplevert wordt "ja" uitgevoerd, anders geen uitvoer.

Er geldt: als ϕ een ja-instantie is dan bestaat er een waardering die ϕ waarmaakt, dus dan bestaat er een string s (het certificaat) die een waarmakende waardering voorstelt, hetgeen in Fase 2 nu juist gecontroleerd wordt. Ergo, dan *is er een* executie van A die "ja" als uitvoer geeft (namelijk die correspondeert met een waarmakende waardering).

Voor nee-instanties bestaat er geen waarmakende waardering en is er dus geen "goede" (= door Fase 2 goedgekeurde) string. Derhalve levert geen enkele executie van A daarop een uitvoer.

Hieruit volgt: het antwoord van A voor invoer x (dat is hier dus ϕ) is "ja" $\iff$ x is een ja-instantie voor SAT (en het antwoord van A voor x is "nee" $\iff$ x is een nee-instantie). Het algoritme A geeft derhalve voor elke invoer x het juiste antwoord.

En verder: A is polynomiaal begrensd.
Namelijk: als x $(= \phi)$ een ja-instantie is, en s een goede string, dan bestaat s uit n waarheidswaarden, dus $|s| \in O(|x|)$, en de verificatiefase is dan $O(|x|^2)$, polynomiaal in $|x|$. Dus voor elke invoer x waarvoor het antwoord van A "ja" is, is er een executie die dat in $O(|x|)$ (Fase 1) + $O(|x|^2)$ (Fase 2) $\subseteq O(|x|^2)$ stappen doet.

opgave 65
HC2 is het probleem te bepalen of een ongerichte graaf een Hamiltoncircuit heeft. We bewijzen HC2 $\leq_{\mathrm{P}}$ TSP. Voorgestelde reductie: $\mathcal{G} \xrightarrow{\mathtt{T}} \langle \mathcal{G}', c, 0 \rangle$ met $\mathcal{G}'$ en c zoals in de opgave. Te bewijzen:

(1) T is polynomiaal begrensd, ofwel de constructie van $T(\mathcal{G})$ uit $\mathcal{G}$ kan in een polynomiaal aantal stappen.

(2) $\mathcal{G}$ is ja-instantie van HC2 $\iff$ $T(\mathcal{G})$ is ja-instantie van TSP, ofwel:

$\mathcal{G}$ heeft een Hamiltonkring $\iff$ $\mathcal{G}'$ heeft een Hamiltonkring met totaalgewicht ≤ 0

(1) De $|V|$ knopen van $\mathcal{G}$ kopiëren en alle mogelijke takken aanbrengen (dat zijn er $O(|V|^2)$, dus $O(|V|^2)$ werk). Dan voor elke tak (i, j) het bijbehorende gewicht bepalen: in $\mathcal{G}$ kijken of er een tak tussen i en j zit (dat is bijvoorbeeld $O(|E|)$ bij gebruik van de adjacency-list). Gewichten bepalen is zo dus $O(|V|^2 \cdot |E|) \subseteq O(|\mathcal{G}|^3)$. Totale hoeveelheid werk is dan $O(|\mathcal{G}|^3)$, dus polynomiaal.
(2) Te bewijzen: $\mathcal{G}$ heeft een Hamiltonkring $\iff$ $\mathcal{G}'$ heeft een Hamiltonkring met totaalgewicht ≤ 0.
"$\Longrightarrow$": Stel $\mathcal{G}$ heeft een Hamiltonkring H. Elke tak uit H zit per definitie in E, dus (is zeker een tak in $\mathcal{G}'$ omdat $\mathcal{G}'$ volledig is en) heeft gewicht 0 in $\mathcal{G}'$. Derhalve is H een Hamiltonkring in $\mathcal{G}'$ ($\mathcal{G}'$ is volledig) met totaalgewicht 0.
"$\Longleftarrow$": Stel $\mathcal{G}'$ heeft een Hamiltonkring H' met totaalgewicht ≤ 0. Omdat de gewichten op de takken van $\mathcal{G}'$ altijd 0 of 1 zijn, kan H' alleen maar takken bevatten met gewicht $= 0$, met andere woorden alle takken uit H' zitten ook in E. Derhalve is H' ook een Hamiltonkring in $\mathcal{G}$.