

Tweede deelloets Algoritmiiek

18 april 2012, 8.30 – 10.30, Educ- γ .

Motiveer je antwoorden *kort!* Zet je mobiel uit. Stel geen vragen over deze toets; als je een vraag niet duidelijk vindt, schrijf dan op hoe je de vraag interpreteert en beantwoord de vraag zoals je hem begrijpt.

1. **De In-graad:** Een gerichte graaf G (met n knopen en m kanten) is gegeven in de vorm van een adjacency list: lijst $L[u]$ bevat v als $uv \in E$. Hoe kun je, voor een gegeven knoop w , de *in-graad* van w (het aantal kanten met eindpunt w) bepalen? Hoeveel tijd kost dit?
2. **Discovery en Finishing times:** Laat d_u en f_u de *discovery* en *finishing* time van knoop u zijn in een DFS van een graaf. Kan het, voor burenen u en v , voorkomen dat $d_u < d_v < f_u < f_v$? Kan het voor willekeurige knopen voorkomen?
3. **MST en kant-toevoeging:** Gegeven een gewogen graaf $G = (V, E)$ en een minimum spanning tree T van G . Aan G wordt een kant toegevoegd: dwz., we vormen $E' = E \cup \{h\}$, waar h twee knopen van G verbindt. Beschrijf een algoritme dat vanuit T een nieuwe boom T' berekent, die een MST van $G' = (V, E')$ is. (Je hoeft geen correctheids-argument te geven; het kan in $O(n)$ tijd.)
4. **Augmenterende paden:** De Ford-Fulkerson methode voor Flow laat steeds de flow toenemen over een pad van s naar t . Als je zo'n pad zoekt, kan je dan het best (a) Breadth-First search, (b) Depth-First search, (c) een "breedst" pad (van maximale restcapaciteit), gebruiken? *Zeg ook waarom.*
5. **Routeplanning:** Een routeplanner berekent kortste paden in een wegennetwerk. Wat is het voordeel van het gebruik van een Fibonacci-heap in Dijkstra's algoritme voor een routeplanner?
6. **Negatieve Cykel:** Deze vraag gaat over berekening van kortste paden, gebruik makend van relaxaties. Bewijs dat, als er ooit een relaxatie plaatsvindt waarbij de afstandsschatting d van de startknoop s verandert, dan bevat de graaf een negatieve cykel.
7. **Elgamal encryptie:** Bij Elgamal encryptie heeft elke gebruiker een *private key* a en een *public key* b . De encryptie van boodschap x is het paar $(u, v) = (g^k, x \cdot b^k)$.
 - (a) Wat is de relatie tussen de public en de private key?
 - (b) Hoe wordt de boodschap ontsleuteld?
8. **NP-Volledige Problemen:** Noem zes NP-volledige problemen.
9. **NP-Volledige Uitdaging:** Je baas vraagt je om een snel algoritme voor een optimaliseringsprobleem R , maar je collega zegt dat R NP-volledig is. Wat kun je doen om het probleem aan te pakken? (Geef minstens vier suggesties.)
10. **Handelsreiziger benadering:** De afstandsmatrix in een instantie van TSP (Handelsreiziger) kan de eigenschappen **Symmetrie** en/of **Driehoeksongelijkheid** hebben.
 - (a) Wat betekenen deze eigenschappen (formule!)?
 - (b) Welke approximatie-ratio is mogelijk (met een polynomiaal algoritme) wanneer beide eigenschappen *niet* gelden?
 - (c) Welke approximatie-ratio is mogelijk (met een polynomiaal algoritme) wanneer beide eigenschappen *wel* gelden?