

Tentamen Algoritmiek

4 november 2008, 15.00 – 17.00, Vechtse banen Hal 1.

1. DFS en Cross edges.

- (a) Wat verstaan we bij DFS onder een *cross edge*?
- (b) Waarom komen cross edges niet voor als een DFS wordt gedaan in een ongerichte graaf?
- (c) Is de bewering *Elke uitgaande kant van de startknoop bij DFS wordt een tree-edge* WAAR of ONWAAR? (Motiveer!)

2. Maximum Spannende Boom.

Gegeven een gewogen graaf $G = (V, E, w)$. De gewichten $w(e)$ zijn allemaal positief; je mag aannemen dat G samenhangend is.

Beschrijf een algoritme dat een *maximale opspannende boom* berekent. Motiveer waarom je algoritme correct is. Wat is de complexiteit?

3. Langste Simpel Pad.

Gegeven een gewogen graaf $G = (V, E, w)$. De gewichten $w(e)$ zijn allemaal positief; je mag aannemen dat G samenhangend is.

We kijken naar het bepalen van een *langste simpel pad*.

- (a) Een informaticus beweert dat deze aanpassing van het Floyd-Warshall algoritme, na k ronden, de lengte van het langste simpele k -pad heeft berekend:

```
forall u,v { if uv in E ( d[u,v] = w(u,v) )
              else { d[u,v] = infty } }
for k = 1 to n
  forall u,v
    if ( d[u,k] + d[k,v] > d[u,v] )
      { d[u,v] = d[u,k] + d[k,v] }
```

Is dit juist? Motiveer!

- (b) Bestaat er een snel algoritme voor een langste simpel pad? (Hint: reductie van Hamiltonian Cycle.)

4. Randomiserende algoritmen.

Gegeven is dat array A van lengte n slechts twee verschillende waarden bevat, elk $n/2$ keer. Geef een randomiserend algoritme dat die twee waarden bepaalt. Wat is de slaagkans, de terminatiekans en de verwachte complexiteit? Is het een Monte Carlo, Las Vegas of Sherwood algoritme?

5. Cryptografie.

Een geheim getal x wordt versleuteld tot $y = x.z$ door vermenigvuldiging met een onbekend getal z .

- (a) Laat zien dat een aanvaller die y onderschept, zonder kennis van z of x , de boodschap kan vervangen door y' , zo dat bij decryptie de boodschap $x' = 2x$ ontstaat.
- (b) Is het mogelijk om, zonder dat je z kent, een boodschap y' te produceren die na decryptie de uitkomst $x' = x + 1$ geeft?