Tentamen Gevorderde Algoritmen en Datastructuren

donderdag 10 april 2014, 9 - 12 uur

Je hoeft slechts 4 van de 5 opgaven te maken: de opgave met het minste aantal punten telt niet mee. Elke opgave levert maximaal 25 punten op. Het tentamencijfer T is (p/10), waarbij p de som van de vier hoogste aantallen punten per opgave is.

Met de zinsnede 'geef een algoritme' in een opgave wordt bedoeld:

> **beschrijf een algoritme in pseudocode, licht de werking ervan toe, beargumenteer de correctheid en de tijdscomplexiteit.**

1. We gebruiken een hash-tabel $T[0..m-1]$ voor het opslaan van key-object paren (k, o). De hashfunctie h beeldt elke mogelijke keywaarde af op een getal in $[0..m-1]$. Geef algoritmen voor het opzoeken, toevoegen en verwijderen van een key-object paar in de hash-tabel.
   Aanwijzing: gebruik *open addressing* met *linear probing* om te voorkomen dat 2 of meer key-object-paren op dezelfde positie in de hash-tabel worden geplaatst. Je mag aannemen dat het aantal key-object-paren in de hash-tabel altijd kleiner is dan m.

2. Gegeven zijn n positieve gehele getallen $c_0, \cdots, c_{n-1}$ en een positief geheel getal K. Gevraagd: is er een deelverzameling S van $\{0, \cdots, n-1\}$ met de eigenschap

   $$\sum_{i \in S} c_i = K \ ?$$

   (a) Beargumenteer dat een naïeve aanpak van dit probleem leidt tot een algoritme met exponentiële tijdscomplexiteit. (Je hoeft het algoritme niet in pseudocode te beschrijven.)

   (b) Geef een algoritme voor dit probleem dat gebruik maakt van dynamisch programmeren.

3. Gegeven is een ongerichte gewogen graaf G die samenhangend en enkelvoudig is. De gewichten van de kanten zijn positieve gehele getallen.

   (a) Wat is een opspannende boom (*spanning tree*) van G? En een *minimale* opspannende boom?

   (b) Geef een algoritme dat een minimale opspannende boom van G vindt, met tijdscomplexiteit $O(m \log n)$ (n het aantal knopen, m het aantal kanten). Je mag gebruik maken van een priority queue.

4. Het cryptografisch systeem RSA werkt als volgt.

   Kies twee priemgetallen p en q en bepaal $n = pq$.
   Kies e relatief priem met $\phi(n) = (p-1)(q-1)$.
   Bepaal d, de multiplicatieve inverse van e modulo $\phi(n)$. Met andere woorden: d voldoet aan $d \cdot e \bmod \phi(n) = 1$.
   Definieer de openbare sleutel $S_o = (n, e)$ en private sleutel $S_p = d$.

   (a) Geef aan hoe een bericht, weergegeven door een getal $B < n$, mbv. S_o versleuteld kan worden tot het gecodeerde bericht C. Geef vervolgens aan (en beargumenteer) hoe B verkregen kan worden uit C mbv. S_p.

   (b) Op welke argumenten berust de betrouwbaarheid van RSA?

   (c) Voor het gebruik van RSA is het berekenen van de multiplicatieve inverse nodig. Geef een efficiënt algoritme hiervoor.

5. Deze opgave gaat over complexiteitsklassen.

   (a) Geef definities van de complexiteitsklassen P (polynomiaal) en NP (non-deterministisch polynomiaal).

   (b) Wanneer is een probleem NP-volledig (NP-*complete*)?

   (c) Formuleer een NP-volledig probleem en laat zien dat het in de klasse NP zit (je hoeft dus niet de NP-*volledigheid* te bewijzen).