Videregående Algoritmik

David Pisinger, DIKU

Eksamen, januar 2006

Schedulering

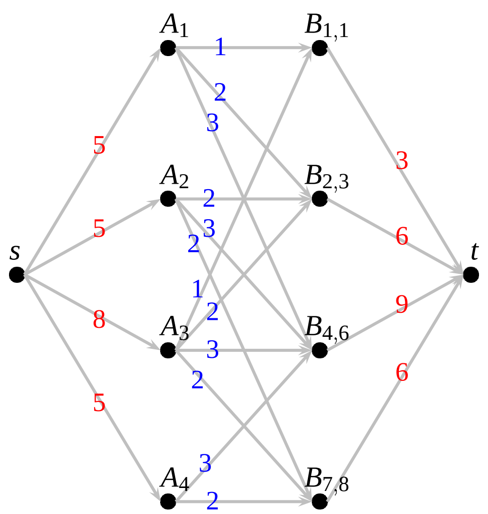
Vi betragter et scheduleringsproblem SCHED med M identiske (*uniforme*) maskiner der arbejder parallelt og en mængde J af job som skal udføres på maskinerne. Hvert job $j \in J$ har en behandlingstid (*process time*) p_j, en starttid (*release time*) r_j og en sluttid (*due date*) d_j. En maskine kan højst arbejde på et job ad gangen, og hvert job kan højst behandles på en maskine ad gangen. Job må godt afbrydes og fortsætte på samme eller anden maskine. Alle tider er *heltal*.

Scheduleringsproblemet kan transformeres til et maximum-flow problem ved brug af metoden beskrevet i Projektopgave-2 (2005): Lad $T = \{t_1, \ldots, t_m\}$ være mængden af starttider og sluttider sorteret i voksende rækkefølge. Vi konstruerer en orienteret graf $G = (V, E)$. For hvert job i $J = \{1, \ldots, n\}$ opretter vi en knude A_j. For hvert tidsinterval (t_i, t_{i+1}) svarende til to på hinanden følgende tider i T opretter vi en knude $B_{t_i, t_{i+1}-1}$. Endelig har vi knuderne $\{s, t\}$.

For alle A_j knuder oprettes en kant (s, A_j) med kapacitet p_j. For alle knuder $B_{a,b}$ oprettes en kant $(B_{a,b}, t)$ med kapacitet $M(b-a+1)$. Endelig oprettes en kant mellem hver A_j knude og $B_{a,b}$ knude med kapacitet $(b-a+1)$ såfremt $r_j \leq a$ og $b < d_j$.

SCHED er afgørlighedsproblemet som besvarer om de J jobs kan udføres på M maskiner. Det tilhørende optimeringsproblem MAX-SCHED søger at få mest mulig produktionstid scheduleret, dvs. at finde den størst mulige strøm i det tilhørende maximum-flow problem.

Q 11: Betragt følgende instans af maximum-flow problemet som er fremkommet ved den ovenstående transformation:



Hvad er den tilhørende instans af SCHED?

11A)

j	1	2	3	4
p_j	5	8	5	5
r_j	1	2	4	4
d_j	7	9	9	9
	$M=3$			

11B)

j	1	2	3	4
p_j	5	5	8	5
r_j	1	2	1	4
d_j	7	9	9	9
	$M=3$			

11C)

j	1	2	3	4
p_j	5	8	8	5
r_j	1	2	1	4
d_j	9	9	9	9
	$M=3$			

11D)

j	1	2	3	4
p_j	5	8	5	5
r_j	1	2	4	4
d_j	7	9	9	9
	$M=2$			

11E)

j	1	2	3	4
p_j	5	5	8	5
r_j	1	2	1	4
d_j	7	9	9	9
	$M=2$			

11F)

j	1	2	3	4
p_j	5	8	8	5
r_j	1	2	1	4
d_j	9	9	9	9
	$M=2$			

■

Q 12: Et minimalt snit for ovenstående graf er givet ved $S = \{s, A_1, A_2, A_3, A_4, B_{2,3}, B_{4,6}, B_{7,8}\}$ og $T = \{B_{1,1}, t\}$. Vi betragter nu MAX-SCHED varianten af problemet. Hvad er den største mængde af job J' som det var muligt at schedulere helt?

- 12A) $J' = \{1,2,3,4\}$
- 12B) $J' = \{2,3,4\}$
- 12C) $J' = \{1,2\}$
- 12D) $J' = \{1,2,3\}$
- 12E) $J' = \{1,3,4\}$
- 12F) $J' = \{3,4\}$

■

I det følgende betragter vi en vilkårlig instans af MAX-SCHED. Endvidere antager vi at der findes et *entydigt* snit S, T i den tilhørende maximum flow formulering.

Q 13: Antag at kanten (s, A_j) for et givet job j ligger på det minimale snit, og at den nuværende løsningsværdi for MAX-SCHED er z. Hvis produktionstiden p_j øges med 1 tidsenhed for job j, hvad er løsningsværdien z' for den nye instans af MAX-SCHED?

- 13A) $z' = 0$
- 13B) $z' = z - 1$
- 13C) $z' = z$
- 13D) $z' = 1$
- 13E) $z' = z + 1$
- 13F) $z' = 2z$

■

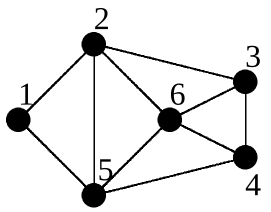
Q 14: Antag at kanten $(B_{a,b}, t)$ *ikke* ligger på det minimale snit, og at den nuværende løsningsværdi for MAX-SCHED er z. Hvis man udvider produktionskapaciteten med en ekstra maskine i tidsrummet (a, b), hvad er løsningsværdien z' for den nye instans af MAX-SCHED?

- 14A) $z' = 0$
- 14B) $z' = z - 1$
- 14C) $z' = z$
- 14D) $z' = 1$
- 14E) $z' = z + 1$
- 14F) $z' = 2z$

■

Knudeoverdækning

En knudeoverdækning af en graf $G = (V, E)$ er en delmængde $U \subseteq V$ så der for alle kanter $(u, v) \in E$ gælder at $u \in U$ eller $v \in U$. Optimeringsproblemet $\text{MIN-VERTEX-COVER}(G)$ søger den mindste knudeoverdækning af størrelse $z = |U|$.



Q 15: Løs $\text{MIN-VERTEX-COVER}(G)$ for ovenstående graf G. Hvad er den optimale løsningsværdi?

15A) $z = 1$
15B) $z = 2$
15C) $z = 3$
15D) $z = 4$
15E) $z = 5$
15F) $z = 6$

■

Betragt nu en vilkårlig graf $G = (V, E)$.
Lad k være størrelsen (dvs. antal knuder) af den største klike i G.
Lad m være størrelsen (dvs. antal kanter) af den største parring (*matching*) i G.
Lad t være længden (målt i antal kanter) af det mindste udspændende træ i G.

Q 16: Hvilken af følgende værdier er en lovlig nedre grænseværdi $\mathcal{L}$ for MIN-VERTEX-COVER?

16A) $\mathcal{L} = k$
16B) $\mathcal{L} = m$
16C) $\mathcal{L} = t$
16D) $\mathcal{L} = k + 1$
16E) $\mathcal{L} = 2m$
16F) $\mathcal{L} = t/2$

■

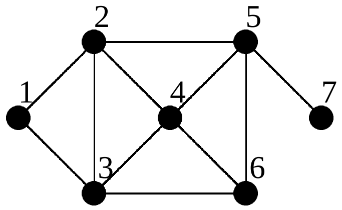
Problemtransformation

En uafhængig mængde (*independent set*) i en graf $G = (V, E)$ er en delmængde $U \subseteq V$ af knuder som opfylder at enhver kant i E er incident med højst en knude i U. Independent set problemet søger at finde den største mængde U som er en uafhængig mængde i G. Det tilhørende afgørlighedsproblem er givet ved

$$\text{INDEPENDENT-SET}(G, h) = \\ \{\ < G, h > \quad : \quad \text{der findes en uafhængig mængde } U \text{ af størrelse } h \text{ i grafen } G\ \}$$

En klike (*clique*) i en graf $G' = (V', E')$ er en delmængde $U \subseteq V'$ af knuder som opfylder at alle par af knuder i U er forbundet med en kant i E'. Klike problemet søger at finde den største mængde U som er en klike i G'. Det tilhørende afgørlighedsproblem er givet ved

$$\text{CLIQUE}(G', k) = \\ \{\ < G', k > \quad : \quad \text{der findes en klike } U \text{ af størrelse } k \text{ i grafen } G'\ \}$$



Q 17: Betragt ovenstående graf $G = (V, E)$. Hvad er størrelsen af en største uafhængige mængde i G?

17A)	$\lvert U\rvert = 0$	17D)	$\lvert U\rvert = 3$
17B)	$\lvert U\rvert = 1$	17E)	$\lvert U\rvert = 4$
17C)	$\lvert U\rvert = 2$	17F)	$\lvert U\rvert = 5$

■

Q 18: Hvilken af følgende transformationer $\text{CLIQUE}(G', k) \leq_{pol} \text{INDEPENDENT-SET}(G, h)$ er korrekt

18A)	$G := G'$, $h := k$	18D)	$G := \overline{G'}$, $h := k$
18B)	$G := G'$, $h := \lvert V\rvert - k$	18E)	$G := \overline{G'}$, $h := \lvert V\rvert - k$
18C)	$G := G'$, $h := 2k$	18F)	$G := \overline{G'}$, $h := 2k$

■

Approximationsalgoritmer

Antag at du blev givet en approximationsalgoritme A for INDEPENDENT-SET problemet med *approximations-ratio* $\rho = 2$.

Q 19: **(tekst spørgsmål)**
Beskriv hvorledes du kan bruge A til at finde en 2-approximationsalgoritme for CLIQUE problemet. *Hint:* brug reduktionen fra forrige opgave. ■

Talteori og kryptografi

Q 20: **(tekst spørgsmål)**
Alice bruger RSA kryptosystemet til at sende en besked til Bob. Alices offentlige nøgle er $(e, n) = (29, 91)$. Bob bruger denne nøgle til at sende hende en kodet besked $C(M) = 32$.

a) En ekspert i kryptering (der kan faktorisere n) opsnapper Bob's besked. For at bryde beskeden, hævder han at det er tilstrækkeligt at finde et d så

$$e \cdot d \equiv 1 \pmod 8$$
$$e \cdot d \equiv 1 \pmod 9$$

Forklar hvorfor eksperten har ret.

b) Find Alices hemmelige nøgle d og den besked M som Bob sendte til Alice. Giv tilstrækkeligt med detaljer til at man kan følge beregningerne.

■