

Videregående Algoritmik

David Pisinger, DIKU

Eksamen, januar 2006

Schedulering

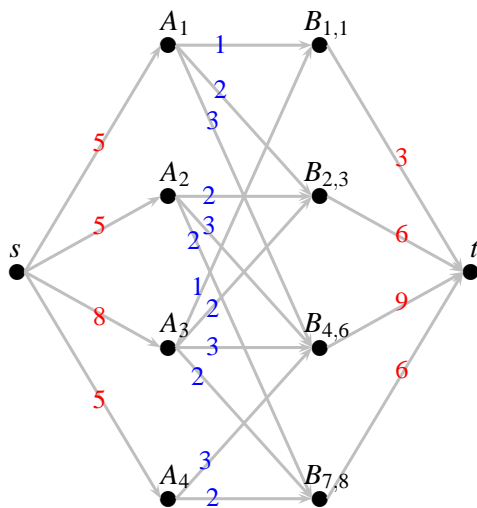
Vi betragter et scheduleringsproblem SCHED med M identiske (*uniforme*) maskiner der arbejder parallelt og en mængde J af job som skal udføres på maskinerne. Hvert job $j \in J$ har en behandlingstid (*process time*) p_j , en starttid (*release time*) r_j og en sluttid (*due date*) d_j . En maskine kan 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 Projekt opgave-2 (2005): Lad $T = \{t_1, \dots, t_m\}$ være mængden af starttider og sluttider sorteret i voksende rækkefølge. Vi konstruerer en orienteret graf $G = (V, E)$. For hvert job $i \in J = \{1, \dots, n\}$ 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 $B_{t_i, t_{i+1}}$. 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
	$M = 3$			

11D)

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

11B)

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

11E)

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

11C)

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

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) $J' = \{1, 2, 3, 4\}$

12D) $J' = \{1, 2, 3\}$

12B) $J' = \{2, 3, 4\}$

12E) $J' = \{1, 3, 4\}$

12C) $J' = \{1, 2\}$

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) $z' = 0$

13D) $z' = 1$

13B) $z' = z - 1$

13E) $z' = z + 1$

13C) $z' = z$

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) $z' = 0$

14D) $z' = 1$

14B) $z' = z - 1$

14E) $z' = z + 1$

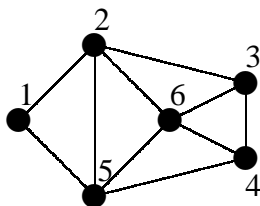
14C) $z' = z$

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 MIN-VERTEX-COVER(G) søger den mindste knudeoverdækning af størrelse $z = |U|$.



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

- | | |
|--------------|--------------|
| 15A) $z = 1$ | 15D) $z = 4$ |
| 15B) $z = 2$ | 15E) $z = 5$ |
| 15C) $z = 3$ | 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) $\mathcal{L} = k$ | 16D) $\mathcal{L} = k + 1$ |
| 16B) $\mathcal{L} = m$ | 16E) $\mathcal{L} = 2m$ |
| 16C) $\mathcal{L} = t$ | 16F) $\mathcal{L} = t/2$ |

■

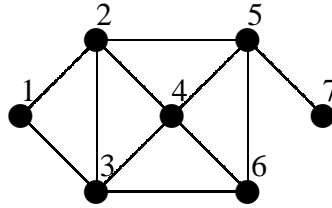
Problemtransformation

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

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

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

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



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

- | | |
|----------------|----------------|
| 17A) $ U = 0$ | 17D) $ U = 3$ |
| 17B) $ U = 1$ | 17E) $ U = 4$ |
| 17C) $ U = 2$ | 17F) $ U = 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) $G := G', h := V - k$ | 18E) $G := \overline{G'}, h := V - k$ |
| 18C) $G := G', h := 2k$ | 18F) $G := \overline{G'}, h := 2k$ |

hvor \overline{G} angiver komplementærgraphen til G . ■

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. Bevis at det er en 2-approximationsalgoritme. *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

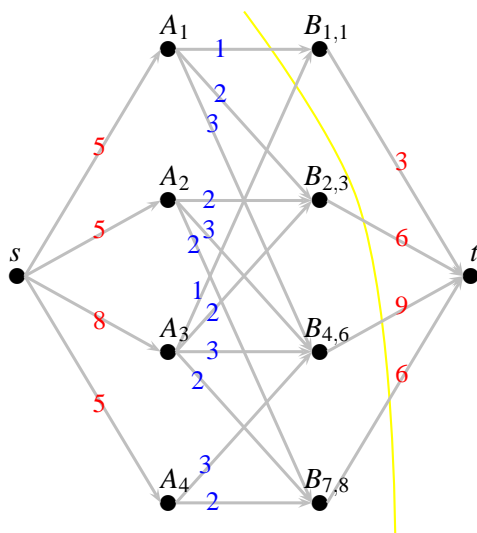
$$\begin{aligned} e \cdot d &\equiv 1 \pmod{8} \\ e \cdot d &\equiv 1 \pmod{9} \end{aligned}$$

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.

■

Vejledende svar



S 11 Den rigtige instans af SCHED er givet ved følgende tabel (med tilhørende løsning til scheduleringsproblemet)

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

job	maskine	start	slut
1	1	1	5
2	3	2	3
2	1	6	6
3	2	1	8
4	3	4	8

(tiden mellem job 1 og 2 kan deles på flere måder). Det rigtige svar er 11.B). ■

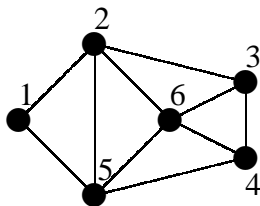
S 12 Det minimale snit er indtegnet ovenfor. Kapaciteten af det minimale snit er $c(S, T) = 23$ og dermed er den maximale strømning $z = 23$. Da $\sum_{j=1}^4 p_j = 23$ gælder der at alle job kunne scheduleres. Dermed er det rigtige svar $J' = \{1, 2, 3, 4\}$, dvs. 12.A). ■

S 13 Idet vi ved at det minimale snit S, T i grafen G er entydigt, må der gælde at der i residualgrafen findes en vej fra s til alle knuder $v \in S$, og at der i residualgrafen findes en vej fra t til alle knuder $v \in T$. Følgelig hvis kanten (s, A_j) ligger på det minimale snit, findes der en vej i residualgrafen fra A_j til t . Da alle kantvægte er heltallige, betyder det at vi har en værdiforøgende vej (augmenting path) med kapacitet mindst 1 fra A_j til t .

Hvis vi øger produktionstiden p_j af job j med 1 enhed, vil kapaciteten af kanten (s, A_j) blive øget med 1 enhed, og følgelig har vi en værdiforøgende vej fra s til t med kapacitet 1. Dette betyder at løsningsværdien bliver øget med 1 enhed, og dermed er $z' = z + 1$. Rigtige svar er 13.E). ■

S 14 Da det minimale snit S, T er entydigt, bemærker vi de samme observationer som i forrige opgave. Da kanten $(B_{a,b}, t)$ ikke ligger på det minimale snit, må $B_{a,b}$ ligge i mængden T . Hvis vi øger kapaciteten af kanten $(B_{a,b}, t)$ vil det derfor ikke påvirke kapaciteten af det minimale snit, og følgelig gælder ifølge max-fbw-min-cut sætningen at løsningen er uændret, så $z' = z$. Rigtige svar er 14.C). ■

S 15 Grafen G er

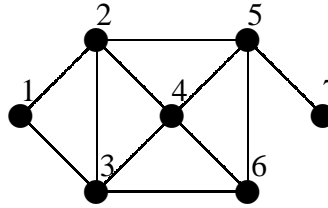


En mindste knudeoverdækning er f.eks. knuderne $\{2, 3, 4, 5\}$.

Det er ikke muligt at finde en mindre knudeoverdækning, da det kræver mindst tre knuder at dække delgrafen 2,3,4,5,6, og disse kan enten være $\{2, 4, 6\}$ eller $\{3, 5, 6\}$. I ingen af dækningerne får man dækket begge kanter til knude 1. Så det rigtige svar er $z = 4$, dvs. 15.D). ■

S 16 Hvis E' er en parring i grafen $G = (V, E)$ så kræver det mindst $|E'|$ knuder at dække kanterne i E' . Så enhver parring E' er en nedre grænseværdi for knudeoverdækningsproblemet, og dermed er den største parring også en nedre grænseværdi $\mathcal{L} = m = |E'|$. Rigtige svar 16.B). ■

S 17 Grafen $G = (V, E)$ er



En største uafhængig mængde er $U = \{1, 4, 7\}$. Det ses let at det er en uafhængig mængde, idet ingen kanter i E rører ved mere end een knude fra U .

Så det rigtige svar er $|U| = 3$, dvs. 17.D). ■

S 18 Lad $G = (V, E)$ være input til klike problemet og lad $S \subseteq V$ være en max klike i G . I vores transformation benytter vi komplementgrafen \overline{G} som input til indepenent set problemet. Vi argumenterer nu at S er et max independent set i G . Siden S per definition er en klike i G betyder det at for alle $u, v \in S$; $(u, v) \in E$. Per definition af \overline{G} , gælder for alle $u, v \in S$, $(u, v) \notin E$ og følgelig er S et independent set i \overline{G} . Rigtige svar 18.D).

Vi kan også vise at der ikke findes et større independent set i \overline{G} . Antag at der fandtes. Lad S' være et sådant independent set i \overline{G} hvor $|S'| \geq |S|$. Men, hvis S' er et independent set i \overline{G} så medfører dette at for alle $u, v \in S'$, $(u, v) \notin E$. Så følger det at for alle $u, v \in S'$, $(u, v) \in E$ og følgelig er S' en klike i G hvilket strider mod at S var en max klike. ■

S 19 Antag at vi fik en 2-approximationsalgoritme A for independent set problemet. Vi har netop vist reduktionen $\text{CLIQUE} \leq_p \text{INDEPENDENT-SET}$ og bruger denne til at konstruere en approximationsalgoritme for klike problemet ved brug af algoritme A . **KLIKE-APPROX** benytter reduktionen til at transformere input G for klike til input \overline{G} for independent set. Vi anvender nu approximationsalgoritmen A for independent set på \overline{G} . Lad $S \subseteq V$ være det independent set som returneres af A . Vi return S som output for **KLIKE-APPROX**.

Vi viser nu at **KLIKE-APPROX** er en 2-approximationsalgoritme. Lad S^* være en max klike i G og lad $C^* = |S^*|$. Fra beviset ovenfor ved vi at S^* udgør et independent set i \overline{G} . Så, siden A er en 2-approximation følger det umiddelbart at $|S| \geq C^*/2$. Siden S returneres følger det at $C^*/S \leq 2$ som krævet for at vise at **KLIKE-APPROX** er en 2-approximationsalgoritme.

Bemærk: vi kender *ikke* en 2-approximationsalgoritme for independent set (eller klike). ■

S 20 Alices offentlige nøgle er $(e, n) = (29, 91)$. Det er nemt at faktorisere $n = 91 = 7 \cdot 13 = p \cdot q$. Dermed ved vi at $\phi = (p-1)(q-1) = 6 \cdot 12 = 72$.

- a) Da $\phi = 72 = 8 \cdot 9$ er et sammensat tal kan vi i stedet for at regne modulo ϕ regne modulo 8 og 9 (ifølge den kinesiske restklasse sætning).

$$\begin{aligned} e \cdot d &\equiv 1 \pmod{8} \\ e \cdot d &\equiv 1 \pmod{9} \end{aligned} \quad \Leftrightarrow \quad e \cdot d \equiv 1 \pmod{72}$$

Løsningen til de to ligninger er $d = 5$ da $e \cdot d = 29 \cdot 5 = 145 \equiv 1 \pmod{8}$ og $e \cdot d = 29 \cdot 5 = 145 \equiv 1 \pmod{9}$. ($144 = 18 \cdot 8 = 16 \cdot 9$).

- b) Den hemmelige nøgle er netop blevet bestemt til $d = 5$. Dermed er $C^d = 32^5 = (2^5)^5 = 2^{25} = 33554432$ og følgelig $M = C^d \pmod{n} = 33554432 \pmod{91} = 2$.

For de snedige findes der en endnu nemmere løsning til opgaven: Idet $91 = 7 \cdot 13$ giver den kinesiske restsætning at den multiplikative gruppe modulo 91 er det direkte produkt af to grupper af orden $6 = 7 - 1$ og $12 = 13 - 1$. Dermed har alle elementer i den multiplikative gruppe modulo 91 en orden der dividerer 12. Det betyder at $e = 29$ er det samme som $e = 5$, idet $5 \equiv 29 \pmod{12}$. Det er nu klart at message er $M = 2$, idet $2^5 = 32$.

■