

Videregående Algoritmik

David Pisinger, DIKU

Reeksamen, April 2005

Bisection problemet

Givet en uvægtet graf $G = (V, E)$ samt et heltal k . En *bisection* af grafen G er en opdeling af knuderne i V i to *lige store* mængder S og T . MAX-BISECTION afgørlighedsproblemet er givet ved

$$\text{MAX-BISECTION}(V, E, k) = \left\{ \langle V, E, k \rangle : \begin{array}{l} \text{der findes en bisection af } G = (V, E) \\ \text{hvor } k \text{ eller flere kanter krydser snittet.} \end{array} \right\}$$

Tilsvarende er MIN-BISECTION problemet givet ved

$$\text{MIN-BISECTION}(V', E', k') = \left\{ \langle V', E', k' \rangle : \begin{array}{l} \text{der findes en bisection af } G = (V, E) \\ \text{hvor } k' \text{ eller færre kanter krydser snittet.} \end{array} \right\}$$

En instans af MAX-BISECTION kan omskrives til en instans af MIN-BISECTION. Lad i det følgende \bar{E} betegne komplementærmængden af E defineret som $(i, j) \in \bar{E} \Leftrightarrow (i, j) \notin E$.

Q 11: Hvilken transformation af MAX-BISECTION til MIN-BISECTION er korrekt

- | | |
|---|--|
| 11A) $V' := V, E' := E$ og $k' := 2k$. | 11D) $V' := V, E' := \bar{E}$ og $k' = 2k - V $. |
| 11B) $V' := V, E' := E$ og $k' := V ^2 - 2k$. | 11E) $V' := V, E' := \bar{E}$ og $k' := (V /2)^2 - k$. |
| 11C) $V' := V, E' := E$ og $k' := V - k$. | 11F) $V' := V, E' := \bar{E}$ og $k' := 2k$ |

■

Q 12: Hvilket af følgende udsagn gælder med sikkerhed

- 12A) $\text{MAX-BISECTION} \leq_p \text{MIN-BISECTION}$ og $\text{MIN-BISECTION} \not\leq_p \text{MAX-BISECTION}$
 12B) $\text{MAX-BISECTION} \not\leq_p \text{MIN-BISECTION}$ og $\text{MIN-BISECTION} \leq_p \text{MAX-BISECTION}$
 12C) $\text{MAX-BISECTION} \leq_p \text{MIN-BISECTION}$ og $\text{MIN-BISECTION} \leq_p \text{MAX-BISECTION}$
 12D) $\text{MAX-BISECTION} \not\leq_p \text{MIN-BISECTION}$ og $\text{MIN-BISECTION} \not\leq_p \text{MAX-BISECTION}$
 12E) $\text{MAX-BISECTION} \in \mathcal{P}$
 12F) $\text{MIN-BISECTION} \in \mathcal{P}$

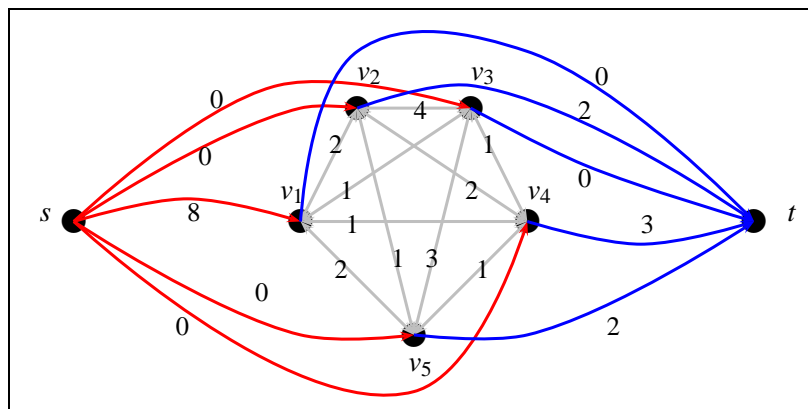
Her betyder $P \not\leq_p Q$ at der helt sikkert ikke findes en polynomiel reduktion af P til Q . ■

Bisection som optimeringsproblem

$\text{MIN-BISECTION}(V', E', k')$ kan formuleres som et minimeringsproblem BISECTION-OPT givet på formen:

$$\begin{array}{ll} \text{minimize} & \sum_{i=1}^n \sum_{j=1}^n e_{ij} x_i (1 - x_j) \\ \text{subject to} & \sum_{j=1}^n x_j = n/2 \\ & x_j \in \{0, 1\}, \quad j = 1, \dots, n. \end{array} \quad (1)$$

hvor $n = |V'|$. Konstanterne $e_{ij} = 1$ hvis kanten $(i, j) \in E'$, mens $e_{ij} = 0$ hvis kanten $(i, j) \notin E'$. Beslutningsvariablene kan fortolkes ved sammenhængen $x_j = 1 \Leftrightarrow j \in S$, og $x_j = 0 \Leftrightarrow j \in T$.



Q 15: Hvad er den tilhørende instans (d_{ij}) af QP?

15A)

$i \setminus j$	1	2	3	4	5
1	2	2	1	1	2
2	2	-11	4	2	1
3	1	4	-9	1	3
4	1	2	1	-8	1
5	2	1	3	1	-9

15D)

$i \setminus j$	1	2	3	4	5
1	-14	2	1	1	2
2	2	-7	4	2	1
3	1	4	-9	1	3
4	1	2	1	-2	1
5	2	1	3	1	-5

15B)

$i \setminus j$	1	2	3	4	5
1	0	2	1	1	2
2	2	0	4	2	1
3	1	4	0	1	3
4	1	2	1	0	1
5	2	1	3	1	0

15E)

$i \setminus j$	1	2	3	4	5
1	-8	2	1	1	2
2	2	2	4	2	1
3	1	4	0	1	3
4	1	2	1	3	1
5	2	1	3	1	2

15C)

$i \setminus j$	1	2	3	4	5
1	8	2	1	1	2
2	2	-2	4	2	1
3	1	4	0	1	3
4	1	2	1	-3	1
5	2	1	3	1	-2

15F)

$i \setminus j$	1	2	3	4	5
1	8	2	1	1	2
2	2	2	4	2	1
3	1	4	0	1	3
4	1	2	1	3	1
5	2	1	3	1	2

■

Q 16: Find et minimalt snit (S, T) i netværket \mathcal{N} . Hvad er kapaciteten af dette snit?

- 16A) $c(S, T) = 4$
- 16B) $c(S, T) = 5$
- 16C) $c(S, T) = 6$

- 16D) $c(S, T) = 7$
- 16E) $c(S, T) = 8$
- 16F) $c(S, T) = 9$

■

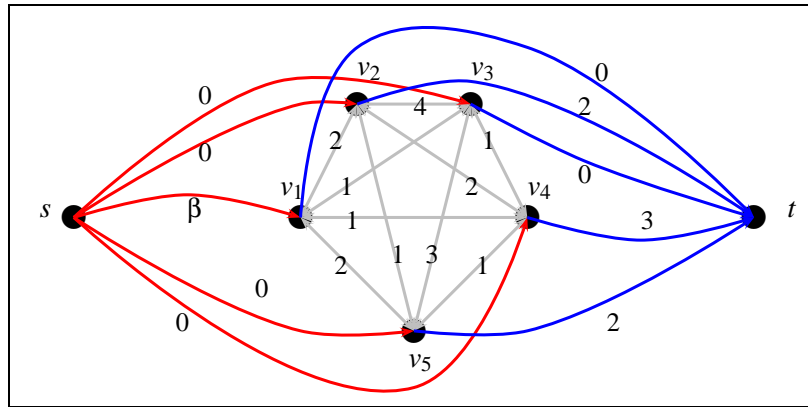
Q 17: Hvad er den optimale løsningsværdi z af den tilhørende QP-instans?

- 17A) $z = 1$
- 17B) $z = 2$
- 17C) $z = 3$

- 17D) $z = 4$
- 17E) $z = 5$
- 17F) $z = 6$

■

Q 18: Kapaciteten af kanten $(s, 1)$ i netværket \mathcal{N} sættes nu til værdien $c_{s1} = \beta$, således at vi får følgende netværk:



For hvilke værdier af β vil den optimale løsning $(x_1, x_2, x_3, x_4, x_5)$ til den tilhørende QP instans være den samme som i spørgsmål Q17?

- | | |
|---------------------|---------------------|
| 18A) $\beta \leq 0$ | 18D) $\beta \geq 0$ |
| 18B) $\beta \leq 3$ | 18E) $\beta \geq 3$ |
| 18C) $\beta \leq 6$ | 18F) $\beta \geq 6$ |

■

Approximationsalgoritmer

Q 19: Givet en uvægtet graf $G = (V, E)$, spørger MAX-CUT optimeringsproblemet om at finde en opdeling af V i S og $T = V \setminus S$ som maksimerer antallet af kanter som krydser snittet. Afgørlighedsproblemet vides at være \mathcal{NP} -fuldstændigt.

APPROX-MAX-CUT(V, E)

$S \leftarrow \emptyset$

$T \leftarrow V$

while $\exists v \in V$ så flytning af v , enten fra S til T eller fra T til S , øger snittets værdi **do** flyt v

return (S, T)

Bevis at APPROX-MAX-CUT er en polynomieltids 2-approximationsalgoritme ved at svare på følgende spørgsmål. Det antages at algoritmen har fået grafen $G = (V, E)$ som inddata og at den returnerer snittet (S, T) .

- Argumenter at APPROX-MAX-CUT kører i polynomieltid.
- For et vilkårligt $v \in V$, lad E_v^c være mængden af kanter incidente med v som indgår i snittet (S, T) , og lad E_v^n være mængden af kanter incidente som *ikke* indgår i snittet. Hvorledes forholder E_v^c sig til E_v^n ?
- Angiv en nedre grænse for antal kanter i snittet (S, T) udtrykt ved $|E|$.
- Fuldfør beviset for at APPROX-MAX-CUT er en polynomieltids 2-approximationsalgoritme for MAX-CUT optimeringsproblemet.

■

Talteori og kryptografi

Q 20:

- a) Brug EXTENDED-EUCLID til at finde $d = \gcd(a, b) = ax + by$ for $a = 29$ og $b = 48$. Vis alle mellemregninger f.eks. ved brug af en tabel.
- b) Alice og Bob bruger RSA kryptosystemet når de kommunikerer med hinanden. Alices offentlige nøgle er $(e, n) = (29, 65)$. Bob bruger denne nøgle til at sende hende en kodet besked $C(M) = 4$. Faktoriser $n = 65$ og brug dette til at finde den originale besked M .

■

Vejledende svar

S 11 Den rigtige transformation er at sætte: $V' := V$, $E' := \bar{E}$ og $k' := (|V|/2)^2 - k$. Med denne transformation vil vi vise at $\text{MAX-BISECTION}(V, E, k) = 1$ hvis og kun hvis $\text{MIN-BISECTION}(V', E', k') = 1$.

Antag for en graf $G = (V, E)$ at $\text{MAX-BISECTION}(V, E, k) = 1$, dvs. der findes et snit (S, T) hvor mindst k kanter krydser snittet. Da $|S| = |T| = |V|/2$ vil der i en komplet graf være $(|V|/2)^2$ kanter over snittet. Hvis vi benytter samme snit (S, T) gælder for komplementærgrafen at der højst er $(|V|/2)^2 - k$ kanter over snittet.

Den modsatte implikation vises tilsvarende. Så det rigtige svar er 11E). ■

S 12 Fra forrige svar ses let at $\text{MAX-BISECTION} \leq_p \text{MIN-BISECTION}$ samt at $\text{MIN-BISECTION} \leq_p \text{MAX-BISECTION}$. Det rigtige svar er 12C). ■

S 13 Der er tale om en relaxering for alle $\lambda \in \mathbb{R}$. For at indse dette ses at objektfunktion og løsningsmængde for det originale problem er

$$f(x) = \sum_{i=1}^n \sum_{j=1}^n e_{ij} x_i (1 - x_j) \quad S = \left\{ (x_1, \dots, x_n) \in \{0, 1\}^n \mid \sum_{j=1}^n x_j = n/2 \right\}$$

Det Lagrange relaxerede problem har objektfunktion og løsningsmængde

$$g(x) = \sum_{i=1}^n \sum_{j=1}^n e_{ij} x_i (1 - x_j) + \lambda \left(\sum_{j=1}^n x_j - n/2 \right) \quad T = \left\{ (x_1, \dots, x_n) \in \{0, 1\}^n \right\}$$

Det ses let at $g(x) = f(x)$ når $x \in S$ idet det sidste led i $g(x)$ bliver nul for alle værdier af $\lambda \in \mathbb{R}$. Samtidig gælder der oplagt at $S \subseteq T$. Så 13F) er korrekt. ■

S 14 Ved Lagrange relaxering med $\lambda = 0$ fås problemet

$$\begin{aligned} \text{minimize} \quad & \sum_{i=1}^n \sum_{j=1}^n -e_{ij} x_i x_j + \sum_{j=1}^n x_j \\ & x_j \in \{0, 1\}, \quad j = 1, \dots, n. \end{aligned} \quad (3)$$

Der kan omskrives til et maksimeringsproblem

$$\begin{aligned} \text{maximize} \quad & \sum_{i=1}^n \sum_{j=1}^n e_{ij} x_i x_j - \sum_{j=1}^n x_j \\ & x_j \in \{0, 1\}, \quad j = 1, \dots, n. \end{aligned} \quad (4)$$

Dette er et kvadratisk 0-1 optimeringsproblem QP givet ved matricen

$i \setminus j$	1	2	3	4	5
1	-1	1	0	1	1
2	1	-1	1	1	0
3	0	1	-1	1	1
4	1	1	1	-1	0
5	1	0	1	0	-1

Den optimale løsning til dette problem er at vælge alle $x_j = 1$.

Dette kunne vi også have indset ved at betragte det originale problem (2), som oplagt antager sit minimum hvis alle knuder er i samme mængde, dvs. f.eks. $x_j = 1$ for alle j .

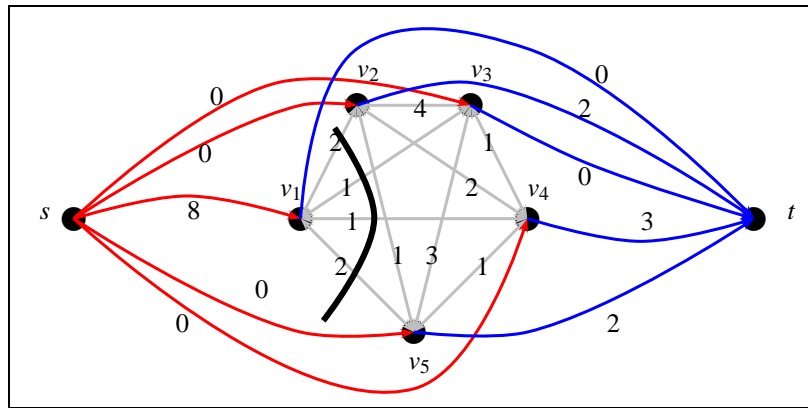
Så det rigtige svar er 14.A). ■

S 15 Den rigtige instans er

$i \setminus j$	1	2	3	4	5
1	2	2	1	1	2
2	2	-11	4	2	1
3	1	4	-9	1	3
4	1	2	1	-8	1
5	2	1	3	1	-9
	8	-2	0	-3	-2

hvor summen af hver søjle er angivet i nederste række. Det rigtige svar er 15.A). ■

S 16 Det minimale snit er markeret på fi guren:



Kapaciteten af snittet er $c(S, T) = 6$. Så det rigtige svar er 16.C). ■

S 17 Fra max-flow-min-cut sætningen vides at den maksimale strømning i netværk \mathcal{N} har værdien $|f^*| = c(S, T) = 6$.

Fra projektopgave 3 vides at den optimale løsning til QP har løsningsværdi $z^* = \sum_{i \in V} c_{si} - |f^*| = (8 + 0 + 0 + 0 + 0) - 6 = 2$. Det rigtige svar er 17B). ■

S 18 Fra fi guren i svar S16 ses at det minimale snit er $S = \{s, 1\}$ og $T = \{t, 2, 3, 4, 5\}$. Fra projektopgave 3 erindres at den optimale løsning til QP problemet findes som $x_j = 1$ hvis og kun hvis $j \in S$. Så længe $\beta \geq c(S, T)$ er snittet uændret. Så det rigtige svar er 18.F). ■

S 19 De enkelte spørgsmål besvares som:

- I hver iteration øges objektfunktionen (snittets værdi) med mindst 1. Objektfunktionen kan ikke blive større end $|E|$, så vi udfører højst $O(E)$ iterationer som hver tager højst $O(V^2)$ tid. Dermed er det vist at APPROX-MAX-CUT kører i $O(V^2E)$ tid.
- For et vilkårligt $v \in V$ må der gælde at $|E_v^c| \geq |E_v^n|$ når algoritmen terminerer idet vi ellers ville have flyttet knuden til den modsatte mængde.
- Ved at summere resultatet fra forrige delspørgsmål for alle knuder v , må der gælde at antal kanter E^c over snittet er større end antal øvrige kanter E^n . Da $|E^c| + |E^n| = |E|$ må der gælde at $|E^c| \geq |E|/2$.
- En optimal løsning C^* er opadtil begrænset af $|E|$. Approximationsalgoritmen finder en løsning C^A som mindst er $|E|/2$. Dermed har vi $C^*/C_A \leq 2 = \rho$.

Dermed er det vist at APPROX-MAX-CUT er en polynomieltids 2-approximationsalgoritme for MAX-CUT. ■

S 20

a) Vi finder $d = \gcd(a, b) = ax + by$ som $1 = 29 \cdot 5 + 48 \cdot (-3)$.

a	b	$\lfloor a/b \rfloor$	d	x	y
29	48	0	1	5	-3
48	29	1	1	-3	-5
29	19	1	1	2	-3
19	10	1	1	-1	2
10	9	1	1	1	-1
9	1	9	1	0	1
1	0	-	1	1	0

Dermed ser vi også at den multiplikativt inverse af 29 i gruppen \mathbb{Z}_{48}^* er 5.

b) Alice har offentlig nøgle $(e, n) = (29, 65)$.

Da $n = 5 \cdot 13$ finder vi $\phi(n) = (5 - 1)(13 - 1) = 48$.

Den multiplikativt inverse af e modulo $\phi(n)$ er $d = 5$, som vist i opgave a).

Den inverse transformation er $M = C(M)^d \bmod n = 4^5 \bmod n = 1024 \bmod 65 = 49$

■