

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

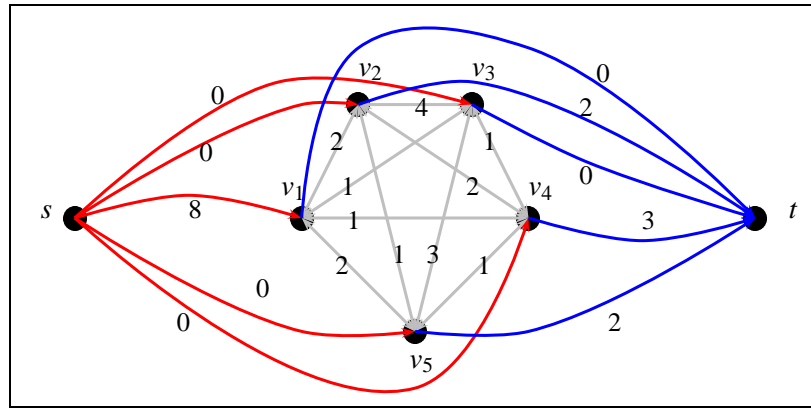
Her betyder $P \not\leq_p Q$ at der helt sikkert ikke findes en polynomiell reduktion af P til Q . ■

Bisection som optimeringsproblem

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)

$i \ j$	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)

$i \ j$	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)

$i \ j$	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)

$i \ j$	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)

$i \ j$	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)

$i \ j$	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) $c(S, T) = 4$

16D) $c(S, T) = 7$

16B) $c(S, T) = 5$

16E) $c(S, T) = 8$

16C) $c(S, T) = 6$

16F) $c(S, T) = 9$

■

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

17A) $z = 1$

17D) $z = 4$

17B) $z = 2$

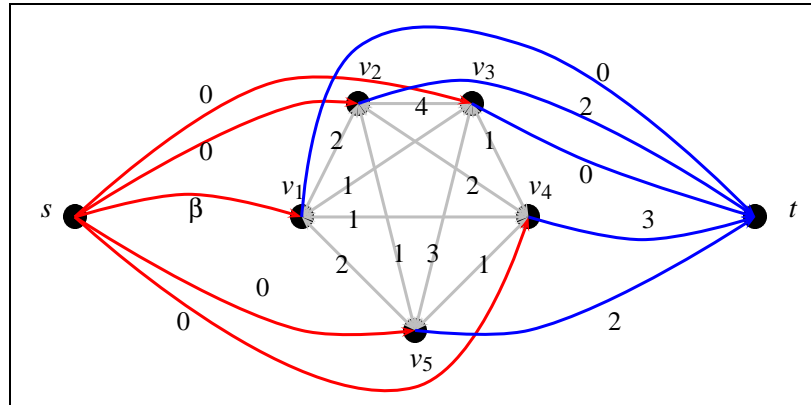
17E) $z = 5$

17C) $z = 3$

17F) $z = 6$

■

Q 18: Kapaciteten af kanten $(s,1)$ i netværket \mathcal{N} sættes nu til værdien $c_{s,1} = \beta$, 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 .

■