

MIN-QP problemet

Det kvadratiske 0-1 optimeringsproblem QP er givet ved

$$\begin{aligned} & \text{maximize} && \sum_{i \in N} \sum_{j \in N} d_{ij} x_i x_j \\ & \text{subject to} && x_j \in \{0, 1\}, \quad j \in N \end{aligned}$$

defineret på mængden $N = \{1, \dots, n\}$, og med $d_{ij} \in \mathbb{R}$ for $i, j \in N$.

Det kvadratiske 0-1 optimeringsproblem i *minimeringsversion*, MIN-QP, er givet ved

$$\begin{aligned} & \text{minimize} && \sum_{i \in N} \sum_{j \in N} d_{ij} x_i x_j \\ & \text{subject to} && x_j \in \{0, 1\}, \quad j \in N \end{aligned}$$

Det tilhørende afgørlighedsproblem, MIN-QP-DECISION (d, k) er givet ved

$$\text{MIN-QP-DECISION}(d, k) = \left\{ \langle d, k \rangle : \begin{array}{l} \text{der findes } (x_1, \dots, x_n) \in \{0, 1\}^n \text{ så} \\ \sum_{i \in N} \sum_{j \in N} d_{ij} x_i x_j \leq k \end{array} \right\}$$

Q 11: Hvilket af følgende udsagn er med sikkerhed rigtigt

- 11A) MIN-QP-DECISION $\in \mathcal{P}$
- 11B) MIN-QP-DECISION $\in \mathcal{NP}$ og QP-DECISION \leq_{pol} MIN-QP-DECISION
- 11C) MIN-QP-DECISION $\in \mathcal{NP}$ men QP-DECISION $\not\leq_{pol}$ MIN-QP-DECISION
- 11D) MIN-QP-DECISION $\notin \mathcal{P}$ og MIN-QP-DECISION $\notin \mathcal{NP}$

■

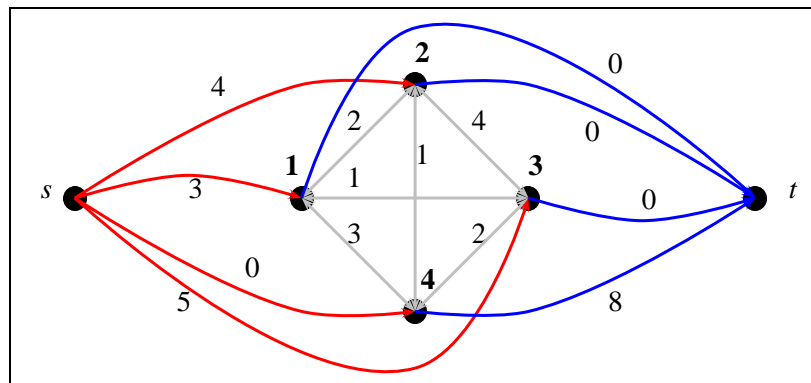
En instans af QP overholder følgende kriterier fra Projekt opgave 3:

- $d_{ij} \in \mathbb{R}_0^+$ for alle $i, j \in N, i \neq j$
- $d_{ii} \in \mathbb{R}$ for alle $i \in N$

Endvidere er matricen (d_{ij}) symmetrisk. For at løse instansen transformeres den til en instans af MAXIMUM-FLOW ved at sætte $V = N \cup \{s, t\}$ og $E = \{s\} \times N \cup N \times N \cup N \times \{t\}$. Kapaciteten af kanterne sættes til:

$$\begin{aligned} c_{si} &= \max\{0, \sum_{j \in N} d_{ij}\}, & i \in N \\ c_{ij} &= d_{ij}, & i, j \in N, i \neq j \\ c_{ii} &= 0, & i \in N \\ c_{it} &= \max\{0, -\sum_{j \in N} d_{ij}\} & i \in N \end{aligned}$$

Herved fremkommer følgende netværk, som vi betegner \mathcal{N} :



Q 12: Hvad er den tilhørende instans af QP?

12A)

i^j	1	2	3	4
1	-3	2	1	3
2	2	-3	4	1
3	1	4	-2	2
4	3	1	2	-14

12D)

i^j	1	2	3	4
1	-9	2	1	3
2	2	-11	4	1
3	1	4	-12	2
4	3	1	2	2

12B)

i^j	1	2	3	4
1	3	2	1	3
2	2	4	4	1
3	1	4	5	2
4	3	1	2	-8

12E)

i^j	1	2	3	4
1	-3	2	1	3
2	2	-4	4	1
3	1	4	-5	2
4	3	1	2	8

12C)

i^j	1	2	3	4
1	0	2	1	3
2	2	0	4	1
3	1	4	0	2
4	3	1	2	0

12F)

i^j	1	2	3	4
1	10	2	1	3
2	2	10	4	1
3	1	4	10	2
4	3	1	2	10

■

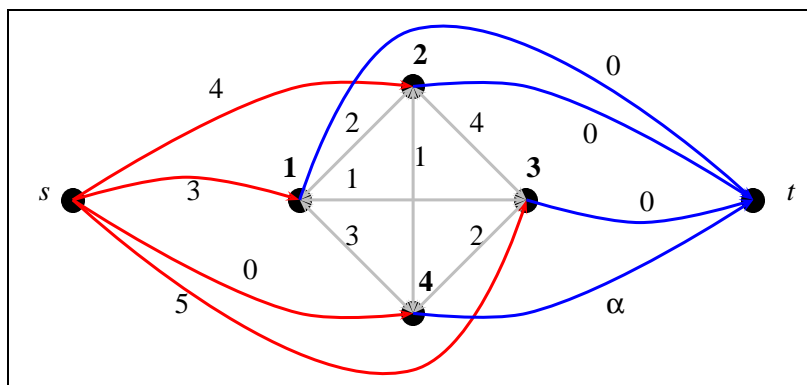
Q 13: Et minimalt snit (S, T) i netværket \mathcal{N} har kapaciteten $c(S, T) = 6$. Hvad er den optimale løsningsværdi z af den tilhørende QP-instans?

- 13A) $z = 4$
 13B) $z = 5$
 13C) $z = 6$

- 13D) $z = 7$
 13E) $z = 8$
 13F) $z = 9$

■

Q 14: Kapaciteten af kanten $(4, t)$ i netværket \mathcal{N} sættes nu til værdien $c_{4t} = \alpha$, således at vi får følgende netværk:



For hvilke værdier af α vil den optimale løsning (x_1, x_2, x_3, x_4) til den tilhørende QP instans være den samme som i spørgsmål Q13?

- 14A) $\alpha \leq 0$
 14B) $\alpha \leq 3$
 14C) $\alpha \leq 6$

- 14D) $\alpha \geq 0$
 14E) $\alpha \geq 3$
 14F) $\alpha \geq 6$

■

Dense-subgraph-pblemet

Dense-subgraph-problemet DSP er givet som følgende optimeringsproblem

$$\begin{aligned}
 & \text{maximize} && \sum_{j=1}^n \sum_{i=1}^n a_{ij} x_i x_j \\
 & \text{subject to} && \sum_{j=1}^n x_j = p \\
 & && x_j \in \{0, 1\}, \quad j = 1, \dots, n.
 \end{aligned} \tag{1}$$

hvor $a_{ij} \in \mathbb{R}$.

Man kan transformere enhver instans givet ved matrixen (a_{ij}) til en ækvivalent instans givet ved matrixen (a'_{ij}) således at alle koefficienter a'_{ij} bliver ikke-negative. Lad den optimale løsningsværdi til den originale instans være z mens den optimale løsningsværdi til den transformerede instans er z' .

Q 15: Hvilken transformation er rigtig

- 15A) Ved at sætte $a'_{ij} = -a_{ij}$ fås en instans med $z' = -z$.
- 15B) Ved at sætte $a'_{ij} = a_{ij} - M$ hvor $M = \min a_{ij}$ fås en instans med $z' = z + Mp^2$.
- 15C) Ved at sætte $a'_{ij} = a_{ij} - M$ hvor $M = \min a_{ij}$ fås en instans med $z' = z - Mp^2$.
- 15D) Ved at sætte $a'_{ij} = a_{ij} - M$ hvor $M = \max a_{ij}$ fås en instans med $z' = z + Mn^2$.
- 15E) Ved at sætte $a'_{ij} = a_{ij} - M$ hvor $M = \max a_{ij}$ fås en instans med $z' = z - Mn^2$.
- 15F) Ved at sætte $a'_{ij} = |a_{ij}|$ fås en instans med $z' = |z|$.

■

Det tilhørende afgørlighedsproblem til DSP er

$$\text{DSP-DECISION}(a, p, k) = \left\{ \begin{array}{l} \langle a, p, k \rangle : \text{der findes } (x_1, \dots, x_n) \in \{0, 1\}^n \text{ så} \\ \sum_{i \in N} \sum_{j \in N} a_{ij} x_i x_j \geq k \\ \sum_{j=1}^n x_j = p \end{array} \right\}$$

Vi ønsker at vise at DSP-DECISION er \mathcal{NP} -fuldstændigt ved reduktion fra CLIQUE problemet, der er defineret som

$$\text{CLIQUE}(V, E, h) = \left\{ \langle V, E, h \rangle : \text{der findes en klike af størrelse } h \text{ i grafen } G = (V, E) \right\}$$

Q 16: Hvilken reduktion $\text{CLIQUE} \leq_{\text{pol}} \text{DSP-DECISION}$ er korrekt

Talteori og kryptografi

Q 19:

- a) Brug EXTENDED-EUCLID til at finde $d = \gcd(a, b) = ax + by$ for $a = 7$ og $b = 20$. Giv tilstrækkeligt med detaljer til at man kan følge løsningsmetoden.
- b) Alice har offentlig nøgle $(e, n) = (7, 33)$. Bob bruger Alice's offentlige nøgle til at sende hende en kodet besked $C(M)$. Alice's nabo, H.Ackermann, opsnapper den kodede besked. Da han kender Alice's offentlige nøgle, prøver han at faktorisere $n = 33 = 3 \cdot 11$, og er dermed i stand til at afkode beskeden. Hvilken besked M sendte Bob til Alice?

■

Approximationsalgoritmer

En approximationsalgoritme til løsning af et problem siges at have *absolut* performance garanti γ , hvis der for enhver instans I af problemet gælder at

$$|z^A(I) - z^*(I)| \leq \gamma$$

hvor $z^*(I)$ er den optimale løsningsværdi til instansen I , og $z^A(I)$ er den værdi som approximationsalgoritmen returnerer.

Q 20: Vis at der ikke findes en approximationsalgoritme med absolut performance garanti for DSP problemet, med mindre $\mathcal{NP} = \mathcal{P}$. *Hint:* Hvis en sådan algoritme fandtes, hvad ville det betyde for CLIQUE problemet? ■

Vejledende svar

S 11 Det ses let at MIN-QP-DECISION $\in \mathcal{NP}$ da vi kan vælge certifikatet til løsningsvektoren x , og en verifikationsalgoritme som udregner objektfunktionen og sammenholder den med k .

Reduktionen QP-DECISION \leq_{pol} MIN-QP-DECISION vises ved at skifte fortegn på alle værdier af d_{ij} .

Af ovenstående to observation ses at QP-DECISION er \mathcal{NP} -fuldstændig. Dermed er det ikke videre sandsynligt at MIN-QP-DECISION $\in \mathcal{P}$.

Så det rigtige svar er 11B). ■

S 12 Ved transformation baglæns findes (d_{ij}) matricen til

$i \setminus j$	1	2	3	4	$\sum_{j \in N} d_{ij}$
1	-3	2	1	3	3
2	2	-3	4	1	4
3	1	4	-2	2	5
4	3	1	2	-14	-8

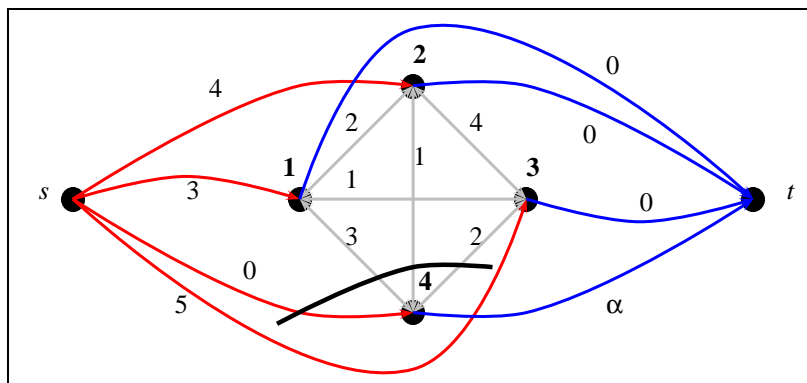
hvor den sidste søjle angiver summen $\sum_{j \in N} d_{ij}$ i hver række. Det rigtige svar er 12A). ■

S 13 Fra max-flow-min-cut sætningen vides at den maksimale strømning i netværk \mathcal{N} har værdien $|f^*| = c(S, T)$.

Fra projektopgave 3 vides at den optimale løsning til QP har løsningsværdi $z^* = \sum_{i \in V} c_{si} - |f^*| = (3 + 4 + 5 + 0) - 6 = 6$.

Det rigtige svar er 13C). ■

S 14 Netværket ser således ud



hvor det minimale snit er markeret som $S = \{s, 1, 2, 3\}$ og $T = \{t, 4\}$. 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 $\alpha \geq c(S, T)$ er snittet uændret, og dermed er løsningen (x_1, x_2, x_3, x_4) uændret. Hvis $\alpha < c(S, T)$ bliver snittet $S = \{s, 1, 2, 3, 4\}$ og $T = \{t\}$, og dermed er løsningen (x_1, x_2, x_3, x_4) ændret.

Så det rigtige svar er 14F). ■

S 15 Den rigtige transformation er at sætte $a'_{ij} = a_{ij} - M$ hvor $M = \min a_{ij}$. Hermed fås en instans hvor $a'_{ij} = a_{ij} - \min_{i,j} a_{ij} \geq 0$. Da præcis p værdier af $x_j = 1$ vil ialt p^2 produkter $x_i x_j = 1$, så vi har øget objektfunktionen med $z' = z - Mp^2$.

Så 15C) er rigtig. ■

S 16 Afbildningen $f : \text{CLIQUE}(V, E, h) \mapsto \text{DSP-DECISION}(a, p, k)$ givet ved

$$N := V, p := h, k := p(p-1), a_{ij} := \begin{cases} 1 & \text{hvis } (i, j) \in E \\ 0 & \text{ellers} \end{cases}$$

er korrekt. Det rigtige svar er 16A). ■

S 17 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

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

Det Lagrange relaxerede problem har objektfunktion og løsningsmængde

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

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 17E) er korrekt. ■

S 18 Ved Lagrange relaxering med $\lambda = 5$ fås problemet

$$\begin{aligned} \text{maximize} \quad & \sum_{j=1}^n \sum_{i=1}^n d_{ij} x_i x_j + \lambda p \\ & x_j \in \{0, 1\}, \quad j = 1, \dots, n. \end{aligned}$$

hvor d_{ij} er givet ved matricen

$i \setminus j$	1	2	3	4
1	-3	2	1	3
2	2	-3	4	1
3	1	4	-2	2
4	3	1	2	-16

Problemet genkendes som særtilfælde af den instans af QP der blev løst i opgave 14. Da $c_{4t} = -\sum_{j \in N} d_{4j} = 10 = \alpha \geq 6$ er løsningen som tidligere $x_1 = x_2 = x_3 = 1$ med løsningsværdi 6. Hertil skal vi i (2) huske at lægge konstant-leddet $\lambda p = 5 \cdot 2 = 10$, hvorved den samlede løsning bliver 16.

Dermed er 18D) rigtig. ■

S 19

a) Vi finder $d = \gcd(a, b) = ax + by$ som $1 = 7 \cdot 3 + 20 \cdot (-1)$.

a	b	$\lfloor a/b \rfloor$	d	x	y
7	20	0	1	3	-1
20	7	2	1	-1	3
7	6	1	1	1	-1
6	1	6	1	0	1
1	0	-	1	1	0

Dermed ser vi også at den multiplikativt inverse af 7 i gruppen \mathbb{Z}_{20}^* er 3.

b) Alice har offentlig nøgle $(e, n) = (7, 33)$.

Da $n = 3 \cdot 11$ finder vi $\phi(n) = (3-1)(11-1) = 20$.

Den multiplikativt inverse af e modulo $\phi(n)$ er $d = 3$, som vist i opgave a).

Den inverse transformation er $M = C(M)^d \bmod n = C(M)^3 \bmod 33$.

■

S 20 Antag at der fandtes en approximationsalgoritme for DSP problemet som havde absolut performance garanti γ , dvs. for enhver instans gælder

$$|z^A(I) - z^*(I)| \leq \gamma$$

For en instans af CLIQUE givet ved grafen $G = (V, E)$ samt klike-størrelsen h konstruerer vi en instans af DSP ved at sætte

$$N := V, \quad p := h, \quad a_{ij} = \begin{cases} \gamma + 1 & \text{hvis } (i, j) \in E \\ 0 & \text{ellers} \end{cases}$$

Hvis der findes en klike i grafen G af størrelse h , vil der være en optimal løsning til DSP med værdi $z^* = h(h-1)(\gamma+1)$. Approximationsalgoritmen vil returnere en løsning z^A hvor

$$|z^A - h(h-1)(\gamma+1)| \leq \gamma$$

Da alle kantvægte er delelige med $\gamma+1$ vil z^A være delelig med $\gamma+1$ og dermed må z^A præcis svare til z^* . Dermed kan vi løse CLIQUE til optimalitet.

Da approximationsalgoritmer ifølge Cormen bogen kører i polynomiel tid, kan vi løse CLIQUE i polynomiel tid. Dermed er NP=P. ■