

Čaulu programmas un kvantu vaicājošie algoritmi

Students: Agnis Āriņš aa07048

Darba vadītājs: profesors Andris Ambainis

Rīga, 2013. gada 16. oktobris

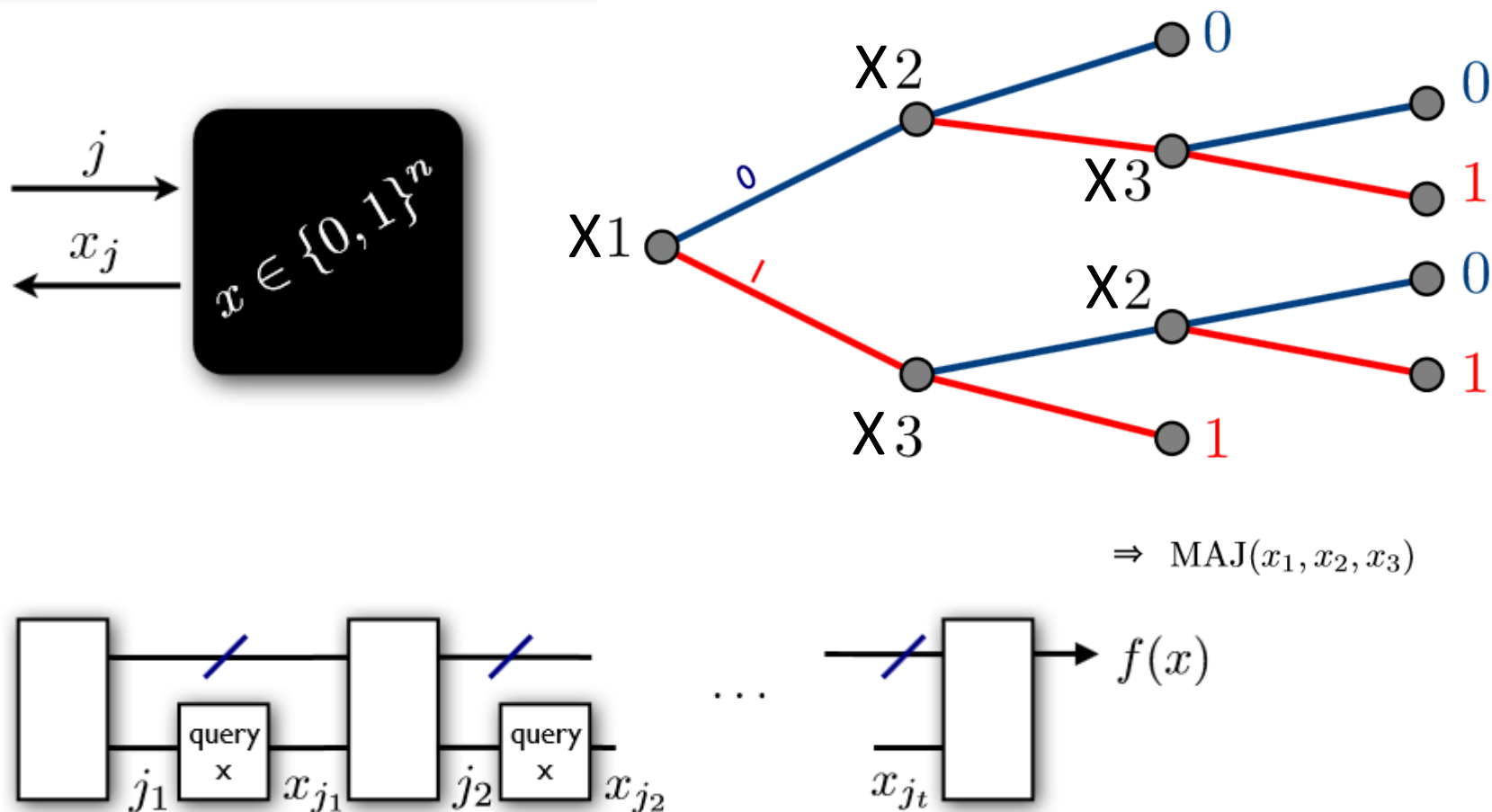


LATVIJAS
UNIVERSITĀTE

Tēmas būtība un aktualitāte

- ❑ Viens no kvantu skaitļošanas teorijas galvenajiem uzdevumiem ir identificēt problēmas, kuras kvantu dators spētu risināt ātrāk par klasisko datoru
- ❑ Čaulu programmas ir līdzvērtīgas kvantu vaicājošiem algoritmiem (efektīva saikne starp abiem modeļiem pierādīta 2010.g)
- ❑ Čaulu programmu pielietojamība ir maz pētīta

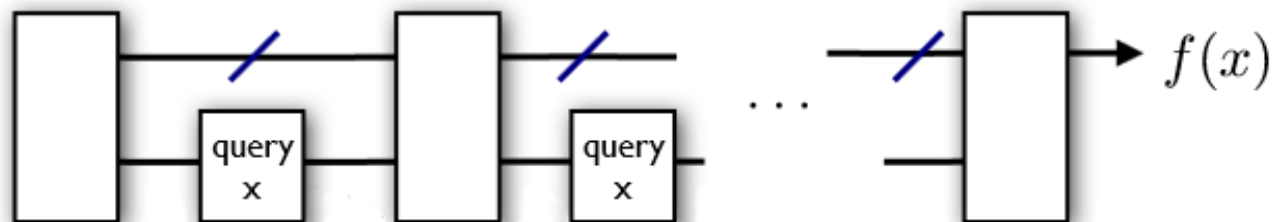
Vaicājošie algoritmi



Kvantu vaicājošie algoritmi



$$|x\rangle_I |\psi_x^t\rangle_A = U_t O U_{t-1} \dots U_1 O U_0 |x\rangle_I |1, 0\rangle_Q |0\rangle_W$$



Vaicājumu sarežģītība

- Vaicājumu sarežģītība $\leq$ Laika sarežģītība
- $\widetilde{\deg}(f) \leq Q(f) \leq R(f) \leq D(f) \leq \underbrace{\widetilde{\deg}(f)^6}_{\text{Visur definētām funkcijām}}$

Funkciju aproksimējošā
polinoma pakāpe

Visur definētām funkcijām

- Pastāv hipotēze, ka $D(f) = O(Q(f)^2)$
- Čaulu programām $wsiz(P_f) = O(Q(f))$

Vektoru telpa

- ❑ Vektoru telpa pār lauku F ir kopa V ar divām binārām operācijām (reizināšana/saskaitīšana)
- ❑ Kopas V elementus sauc par vektoriem
- ❑ Piemēram, $V = R^3$ (trīsdimensiju telpa), kur $F = R$.
- ❑ Vektoru telpai jāizpildās 8 sekojošām īpašībām (aksiomām):

Vektoru telpa

Aksioma

Nozīme

Asociativitāte saskaitīšanai

$$\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$$

Komutativitāte saskaitīšanai

$$\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$$

Identitātes elements saskaitīšanai

Eksistē $\mathbf{0} \in V$, saukts par nules vektoru, ka izpildās $\mathbf{v} + \mathbf{0} = \mathbf{v}$ katram $\mathbf{v} \in V$.

Pretējais elements saskaitīšanai

Katram $\mathbf{v} \in V$, eksistē elements $-\mathbf{v} \in V$, ka izpildās $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$

Vektoru telpa

Aksioma

Nozīme

Distributivitāte reizināšanai ar skalāru lielumu attiecībā pret vektoru saskaitīšanu

$$a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$$

Distributivitāte reizināšanai ar skalāru lielumu attiecībā pret lauka elementu saskaitīšanu

$$(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$$

Skalārās un lauka reizināšanas saderība

$$a(b\mathbf{v}) = (ab)\mathbf{v}$$

Identitātes elements skalārai reizināšanai

$1\mathbf{v} = \mathbf{v}$, kur 1 apzīmē multiplikatīvo identitātes elementu iekš lauka F .

Vektoru telpas bāze

- ❑ Lineārā čaula ir vektoru telpa, ko definē kā $Span(S) = \{\sum_{i=1}^k \lambda_i v_i \mid k \in N, v_i \in S, \lambda_i \in F\}$, kur S ir vektoru kopa, kas veido šo čaulu.
- ❑ Par vektoru telpas V bāzi B sauc lineāri neatkarīgu kopas V apakškopu B , kur izpildās $Span(B) = V$.
- ❑ $B = \{b_1, b_2, \dots, b_N\}$
- ❑ $v = a_1 b_1 + a_2 b_2 + \dots + a_N b_N$, kur $a_i \in F$

Vektoru koordinātas

- ❑ Sanumurējot bāzes B vektorus ar skaitļiem no 1 līdz N iegūstam sakārtotu bāzi
- ❑ $v = a_1 b_1 + a_2 b_2 + \dots + a_N b_N$
- ❑ $[v]_B = (a_1, a_2, \dots, a_N)$ - rindas vektors
- ❑ $[v]_B = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_N \end{pmatrix}$ - kolonas vektors

Vektoru apzīmējumi

▣ Kolonas vektors $|v\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_N \end{pmatrix}$

▣ Rindas vektors $\langle u| = (c_1, c_2, \dots, c_N)$

▣ Skalārais reizinājums:

$$\langle u|v\rangle = a_1c_1 + a_2c_2 + \dots + a_Nc_N$$

▣ Vektora norma: $\|v\| = \sqrt{a_1^2 + a_2^2 + \dots + a_N^2}$

Čaulu programmas

- ❑ Čaulu programmu piegājiens ir radies kā rezultāts darbam pie kvantu algoritmiem formulu izpildei, kur ir dota Būla formula $F(x_1, \dots, x_N)$, kas sastāv no loģiskajiem vārtiem (AND, OR, NOT).
- ❑ Formula iepriekš ir zināma, bet mainīgo $x_1, \dots, x_N$ vērtības nav zināmas.
- ❑ Uzdevums ir noteikt $F(x_1, \dots, x_N)$ vērtību ar minimālu vaicājumu skaitu.

Čaulu programmas

Čaulu programma P uz n ieejas bitiem:

Vektoru telpa: V

Mērķa vektors: $|t\rangle$

Apakštelpas: $V_{1,0}, V_{1,1}, \dots, V_{n,0}, V_{n,1}, V_{free}$

P «rēķina» $f_P : \{0,1\}^n \rightarrow \{0,1\}$

$$f_P(x) = 1 \iff |t\rangle \in \text{Span} \left(V_{free} \cup \bigcup_j V_{j,x_j} \right)$$

Čaulu programmas

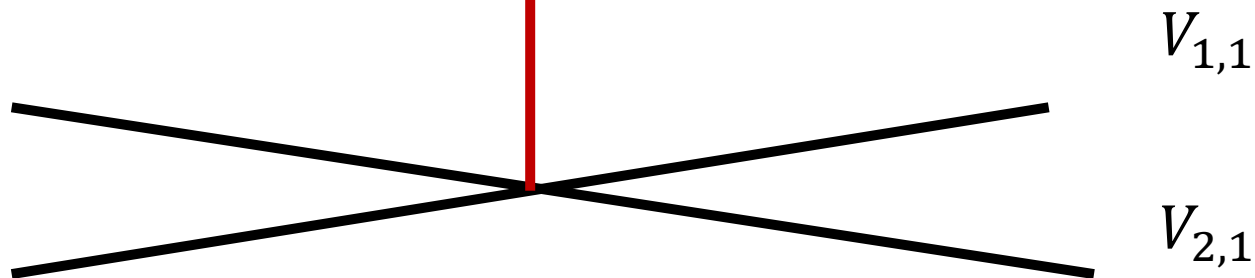
Piemērs: $V = R^2$

$$V_{1,0} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$$

$$V_{2,0} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$$

$|t\rangle$

$$\Rightarrow f_P = AND_2$$



Čaulu programma „XOR”

- Dots: $f(x_1, x_2) = x_1 \oplus x_2$
- Par mērķa vektoru izraugāties divdimensiju vektoru $|t\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
 - ja $x_1 = 1$, tad varam izmantot vektoru $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$;
 - ja $x_1 = 0$, tad varam izmantot vektoru $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$;
 - ja $x_2 = 1$, tad varam izmantot vektoru $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$;
 - ja $x_2 = 0$, tad varam izmantot vektoru $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Čaulu programma „XOR”

- ❑ Dots: $f(x_1, x_2) = x_1 \oplus x_2$
- ❑ Telpas bāzes vektori: $\{|0\rangle, |1\rangle\}$
- ❑ Par mērķa vektoru izraugāties divdimensiju vektoru $|t\rangle = |0\rangle + |1\rangle$
 - ❑ ja $x_1 = 1$, tad varam izmantot vektoru $|0\rangle$
 - ❑ ja $x_1 = 0$, tad varam izmantot vektoru $|1\rangle$
 - ❑ ja $x_2 = 1$, tad varam izmantot vektoru $|0\rangle$
 - ❑ ja $x_2 = 0$, tad varam izmantot vektoru $|1\rangle$

Pozitīvā sarežģītība

- A – pieejamo vektoru kolonu matrica
- Ja $f_P(x) = 1$:
$$wsize_1(P, x) = \min_{|w\rangle: A|w\rangle=|t\rangle} ||w\rangle||^2$$
- $|w\rangle$ - pozitīvā liecība
- $wsize_1(P, x)$ – koeficientu kvadrātu summa pie vektoriem, kuri tiek izmantoti lai izteiktu mērķa vektoru
- $wsize_1(P) = \max_{x \in \{0,1\}^n} wsize_1(P, x)$

Negatīvā sarežģītība

- $V(x) = V_{free} \cup \bigcup_{j \in [1..n]} V_{j, x_j}$
- Ja $f_P(x) = 0$: tāds $|w'\rangle$, ka $\langle w'|t\rangle = 1$ un $\forall |y\rangle \in V(x) \ (|w'\rangle \perp |y\rangle)$
- $|w'\rangle$ - negatīvā liecība
- $wsiz_0(P, x) = \min_{|w'\rangle} \sum_{|y\rangle \in V(\neg x)} \langle w'|y\rangle^2$
- $wsiz_0(P) = \max_{x \in \{0,1\}^n} wsiz_0(P, x)$

Čaulu programmu sarežģītība

- ❑ $wsiz(P) = \sqrt{wsiz_1(P) * wsiz_0(P)}$
- ❑ $wsiz(P_f) = O(Q(f))$ - sarežģītība ir līdzvērtīga kvantu vaicājošo algoritmu sarežģītībai konkrētai Būla funkcijai

Pētījumu virzieni

- ❑ Turpināt meklēt jaunus kvantu algoritmus izmantojot jau esošo čaulu programmu skaitļošanas modeli
- ❑ Jaunu ietvaru izstrāde, kas balstās uz čaulu programmām
- ❑ Sīkāk apgūt semidefinitās programmēšanas metodi

Pētījumu virzieni

- ❑ Pētīt iespējas vispārināt čaulu programmas, lai ar tām varētu risināt arī daļēji definētas Būla funkcijas, saglabājot sasaisti ar kvantu vaicājošiem algoritmiem
- ❑ Pētīt iespējas automatizēt efektīvu algoritmu meklēšanu izmantojot datoru

PALDIES PAR UZMANĪBU!



Grafa divdaļības pārbaude

- ❑ Grafs ir divdaļīgs, ja visas grafa virsotnes var nokrāsot divās krāsās tā, lai nekādas divas vienas krāsas virsotnes nebūtu savienotas ar šķautni
- ❑ Grafs ir divdaļīgs tad un tikai tad, ja grafā nav nepāra garuma cikls
- ❑ Risinājuma ideja – katrai virsotnei pārbaudīt, vai eksistē nepāra garuma ceļš, kas sākas un beidzas šajā virsotnē

Grafa divdaļības pārbaude

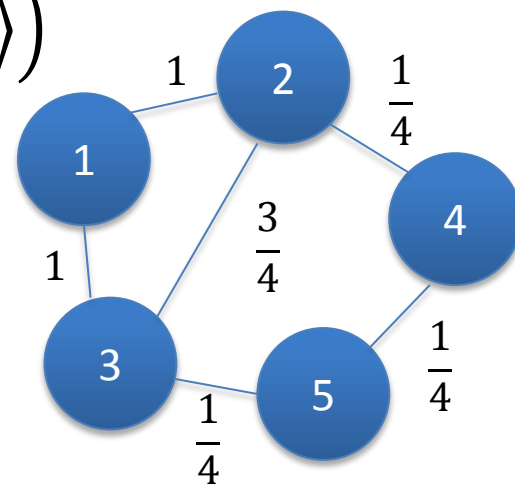
- ❑ $k \in [1..N]$ - virsotnes indekss
- ❑ mērķa vektors ir $|t\rangle = |0\rangle$;
- ❑ katram k : brīvais vektors ir $|0\rangle + |k_{k0}\rangle + |k_{k1}\rangle$;
- ❑ katram k : ja grafā ir šķautne $u - v$ (respektīvi $x_{uv} = 1$, kur $u, v \in [1..N]$), tad var izmantot vektorus:
 $|u_{k0}\rangle + |v_{k1}\rangle$ un $|u_{k1}\rangle + |v_{k0}\rangle$.

Grafa divdaļības pārbaude

$$\begin{aligned}
 |t\rangle = & \left(|0\rangle + |1_{1,0}\rangle + |1_{1,1}\rangle \right) - \left(|1_{1,0}\rangle + |2_{1,1}\rangle \right) \\
 & + \frac{3}{4} \left(|2_{1,1}\rangle + |3_{1,0}\rangle \right) \\
 & + \frac{1}{4} \left(\left(|2_{1,1}\rangle + |4_{1,0}\rangle \right) - \left(|4_{1,0}\rangle + |5_{1,1}\rangle \right) \right. \\
 & \left. + \left(|5_{1,1}\rangle + |3_{1,0}\rangle \right) \right) - \left(|3_{1,0}\rangle + |1_{1,1}\rangle \right)
 \end{aligned}$$

$$wsize_1(x)$$

$$\begin{aligned}
 &= 1^2 + (-1)^2 + \left(\frac{3}{4}\right)^2 + \left(\frac{1}{4}\right)^2 + \left(-\frac{1}{4}\right)^2 \\
 &+ \frac{1}{4} + (-1)^2 = 3 + \frac{12}{16}
 \end{aligned}$$



Grafa sakarības pārbaude

- ❑ Grafu sauc par sakarīgu, ja tajā jebkuras divas virsotnes savā starpā ir savienotas – grafā eksistē ceļš, kas sastāv no grafa šķautnēm un šīs virsotnes savieno
- ❑ Risinājuma ideja – atrast grafā ceļus no virsotnes ar indeksu 1 uz visām pārējām virsotnēm

Grafa sakarības pārbaude

- ❑ $k \in [2..N]$ - virsotnes indekss
- ❑ mērķa vektors ir $|t\rangle = |0\rangle$;
- ❑ brīvais vektors ir
 $|0\rangle + (|0_2\rangle + |0_3\rangle + \dots + |0_N\rangle)$
- ❑ katram k : brīvais vektors ir $|0_k\rangle + |1_k\rangle - |k_k\rangle$
- ❑ katram k : ja grafā ir šķautne $u - v$ (respektīvi $x_{uv} = 1$), tad var izmantot vektoru:
 $|u_k\rangle - |v_k\rangle$

Eilera cikls grafā

- ❑ Par Eilera ciklu sauc noslēgtu ceļu grafā, kurš izmantot visas grafa šķautnes tieši vienu reizi. Sakarīgā grafā eksistē Eilera cikls tad un tikai tad, ja katrai grafa virsotnei ir pāra pakāpe
- ❑ Risinājuma ideja - pārbaudīt virsotņu pakāpes un mēģināt atrast virsotni, kurai ir nepāra pakāpe – ja šādi virsotne eksistēs, tad Eilera cikls grafā neeksistēs

Eilera cikls grafā

- ❑ mērķa vektors ir $|t\rangle = |0\rangle$
- ❑ katrai virsotnei $k \in [1..N]$ izveidojam vektorus:
 - ❑ brīvo vektoru $|0\rangle + |k_{0,0}\rangle - |k_{n,1}\rangle$
 - ❑ katram $i \in [1..N]$:
 - ❑ ja grafā ir šķautne $k - i$ ($x_{k,i} = 1$), tad var izmantot vektorus:
 $-|k_{i-1,0}\rangle + |k_{i,1}\rangle$ un $-|k_{i-1,1}\rangle + |k_{i,0}\rangle$
 - ❑ ja grafā nav šķautne $k - i$ ($x_{k,i} = 0$), tad var izmantot vektorus:
 $-|k_{i-1,0}\rangle + |k_{i,0}\rangle$ un $-|k_{i-1,1}\rangle + |k_{i,1}\rangle$

Grafa šķautnes tiltiņa pārbaude

- ❑ Grafa šķautni sauc par tiltiņu, ja šo šķautni no grafa izmetot grafā palielinās saistīto komponentu skaits
- ❑ Grafa šķautne ir tiltiņš tad un tikai tad, ja tā iekš grafa neietilpst nevienā ciklā
- ❑ Risinājuma ideja – izvēlas šķautni $A - B$ un pārbauda, vai grafā eksistē ceļš no A uz B , kurš neizmanto šķautni $A - B$

Grafa šķautnes tiltiņa pārbaude

- ❑ mērķa vektors ir $|t\rangle = |0\rangle$
- ❑ ja ir šķautne $A - B$ (respektīvi $x_{AB} = 1$), tad var izmantot vektoru:

$$|0\rangle + |A\rangle - |B\rangle$$

- ❑ Ja grafā ir šķautne $u - v$ (respektīvi $x_{uv} = 1$) un tā nesakrīt ar šķautni $A - B$, tad var izmantot vektoru:

$$|u\rangle - |v\rangle$$

Algoritmu sarežģītība

- ❑ Grafa divdaļības pārbaude - $\theta(N\sqrt{N})$
- ❑ Grafa sakarības pārbaude - $\theta(N\sqrt{N})$
- ❑ Eilera cikls grafā - $\theta(N\sqrt{N})$
- ❑ Grafa šķautnes tiltiņa pārbaude - $O(N\sqrt{N})$

PALDIES PAR UZMANĪBU!

