LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

PRECĪZIE KVANTU ALGORITMI, IZMANTOJOT 1-KVANTU-VAICĀJUMA IZSAUKUMUS

MAĢISTRA DARBS

Autors: **Zigmārs Rupenheits**
Stud. apl. ZR11002
Darba vadītājs: prof. Dr.dat. Juris Smotrovs

RĪGA 2018

Anotācija

Precīzi kvantu vaicājumu algoritmi ir algoritmi, kuri, izmantojot kvantu vaicājumus, ar pilnīgu precizitāti (ar varbūtību $P = 1$) izdod pareizo atbildi. Precīzo kvantu vaicājumu sarežģītību sauc par minimālo kvantu vaicājumu skaitu, kas ir nepieciešams pareizas atbildes izdošanai visām ieejas vērtībām. Līdz šim ir izdevies pierādīt, ka Būla funkciju precīzo kvantu vaicājumu sarežģītība ir mazāka par klasisko vaicājumu sarežģītību gandrīz visām Būla funkcijām. Vai uzlabojums ir ievērojams, ir zināms tikai dažiem gadījumiem. Līdz šim arī nav pētīts, kādām vispārīgām īpašībām būtu jāizpildās kvantu vaicājumam, lai tas sniegtu precīzu informāciju par aprēķināmo funkciju, un tādējādi varētu uzkonstruēt precīzo kvantu vaicājumu algoritmu.
Darbā tiks pētītas precīzo kvantu vaicājumu algoritmu konstrukcijas, izmantojot 1-kvantu-vaicājumu izsaukumus, un īpašības, kādas nepieciešamas vaicājumam, lai tas sniegtu precīzu informāciju par aprēķināmo funkciju.

Atslēgas vārdi: precīzie kvantu algoritmi, Būla funkciju vaicājuma sarežģītība

Abstract

Exact quantum query algorithms using single-quantum-query subroutines

Exact quantum algorithms are algorithms which by using quantum queries compute value correctly with certainty (probability $P = 1$). Quantum query complexity is minimal number of queries required for correct value to be returned over all inputs. It is proven, that for almost all Boolean functions quantum query complexity is less than (classical) decision tree complexity, but only for few of them it is known of what order lower is quantum query complexity. To this day, there is no study of general properties of quantum query that have to be satisfied, for it to derive some exact information about the computable function.
In the thesis exact quantum query algorithms using single-quantum-query subroutines will be studied, as well as properties of a quantum query to get some exact information about the computable function.

Keywords: exact quantum algorithms, Boolean function query complexity

Autoreferāts

Darbā ir analizēti zināmi unikāli precīzie kvantu algoritmi, kuru īpašības ir atšķirīgas no citiem literatūrā atrodamiem algoritmiem, un uzsākts pētīt iespējas vispārināt šajos algoritmos esošos paņēmienus. Darbā ir noformulēts jauns skaitļošanas modelis, kas ir saistīts ar precīzo kvantu vaicājumu modeli. Veikti skaitliski aprēķini, lai palīdzētu saprast jaunā modeļa iespējas un ierobežojumus. Izteiktas hipotēzes un virzieni, kādos turpināt analīzi un pētījumu.

Saturs

Ievads un motivācija **2**

1 Ieskats nepieciešamajās priekšzināšanas **3**
1.1 Būla funkcijas . . . 3
1.2 Lineārā algebra . . . 3
1.3 Kvantu skaitļošana . . . 4
1.3.1 Vaicājumu sarežģītības modeļi . . . 5

2 Esošie rezultāti **7**
2.1 Precīzā kvantu vaicājumu sarežģītība Būla funkcijām EXACT un THRESHOLD . . . 7
2.1.1 EXACT_k^n . . . 7
2.1.2 $\mathrm{THRESHOLD}_k^n$ . . . 8
2.2 EXACT un THRESHOLD kvantu algoritmu kopīgās īpašības un paņēmieni . . . 8

3 Viena kvantu vaicājuma izsaukumu lēmumkoks **11**

4 Lineāru polinomu komplektu mērījumu modelis **14**
4.1 Modeļa definīcija un salīdzinājums . . . 14
4.2 LPKL atsevišķa polinoma analīze . . . 15
4.2.1 Veselo skaitļu koeficientu lineāri polinomi . . . 16
4.2.2 Skaitliskie aprēķini . . . 16

5 Rezultāti un secinājumi **19**

Izmantotā literatūra un avoti **20**

Ievads un motivācija

Vēsturiski viens no pirmajiem rezultātiem, pēc kura aizsākās aktīva kvantu skaitļošanas pētniecība, ir [1]. Šajā darbā Doičs (Deutsch) pirmais izklāstīja universālu kvantu skaitļošanas mašīnas modeli un arī parādīja interesantu kvantu algoritma piemēru XOR aprēķināšanai tikai ar vienu kvantu vaicājumu (bet ar nelielu kļūdas varbūtību) [1, p. 112].

Pēc dažiem gadiem sadarbībā ar vēl vienu zinātnieku Doičs izveido pirmo kvantu algoritmu daļēji definētas Būla funkcijas aprēķinam, kuras vaicājuma sarežģītība ir ar eksponenciālu uzlabojumu klasiskajai vaicājuma sarežģītībai [2].

Nedaudz vēlāk [1] 2-bitu XOR aprēķina paņēmienu uzlabo [3] un parāda *precīzu* XOR aprēķina algoritmu ar vienu kvantu vaicājumu. Kā arī parādīja, ka precīzā kvantu vaicājumu sarežģītība paritātei ir $Q_E(\text{PARITY}_n) = \frac{n}{2}$.

Montanaro 2011. gadā [4] veica skaitliskos aprēķinus, lai noskaidrotu kvantu vaicājumu sarežģītību Būla funkcijām pie neliela ievades vārda izmēra (līdz 4 bitiem visām Būla funkcijām un līdz 6 bitiem simetriskām Būla funkcijām). Šajā darbā Montanaro arī izteica savus novērojumus par to, ka iepriekš visi precīzie kvantu algoritmi, kas uzlabo klasisko vaicājuma sarežģītību, kā vienīgo kvantisko sastāvdaļu izmanto tikai iepriekš pieminēto Doiča precīzo 2-bitu XOR algoritmu [3]. Viņš arī demonstrēja optimālu kvantu vaicājumu algoritmu 4-bitu Būla funkcijai, kurai neeksistē optimāls algoritms izmantojot Doiča precīzā kvantu 2-bitu XOR izsaukumus.

Pēc tam sekoja [5], kurā, izmantojot jaunu metodi, kas nebalstījās uz kvantu XOR izsaukumu, tika iegūts optimāls algoritms Būla funkciju klasei, konkrēti, parādīja EXACT_k^n un THRESHOLD_k^n optimālas precīzās kvantu vaicājumu sarežģītības algoritmu.

Saskaroties ar algoritmiskiem uzdevumiem klasiskajā skaitļošanā, ir noderīgi zināt dažādus paņēmienus, ar kuriem var mēģināt risināt problēmas, piemēram, dinamiskā programmēšana ir labs paņēmiens problēmu risināšanai ar visai konkrētu struktūru, tāpēc ne visām problēmām ar kuras parādās algoritmu izstrādē, to var pielietot. Līdzīgi var skatīties uz precīzo kvantu algoritmu izstrādi. XOR pielietošanas paņēmiens ir vienīgā ļoti labi izpētītā metode, kas parādās daudzos pielietojumos precīzo kvantu algoritmu konstrukcijā ([4, §1]). Šī iemesla dēļ ir ievērojama motivācija pētīt precīzo kvantu algoritmu konstrukciju paņēmienus "virzienos", kas ir atšķirīgi no XOR paņēmiena izmantošanas.

Viens paraugs šādai pētniecības virzībai ir paņēmiens, kas parādās darbā [5]. Tajā ir izmantota cita pieeja algoritma konstrukcijai, kuru ir vērts analizēt un saprast paņēmiena vispārināšanas iespējas un ierobežojumus.

Šī darba vispārīgais mērķis ir tieši analizēt iepriekšminētā paņēmiena īpašības un censties to vispārināt, vai pamatot, ka to nav iespējams izdarīt.

1. nodaļā tiek aprakstītas pamatzināšanas, kuras ir nepieciešamas darba izpratnei. 2. nodaļā tiek konspektīvi aprakstīti kvantu algoritmi, un analizētas īpašības un vispārināšanas iespējas. 3. nodaļā tiek uzsākts apraksts par vispārīgu viena kvantu vaicājuma izsaukumu modeli. 4. nodaļā tiek stingri nodefinēts relaksēts modelis, kas ir spēcīgāks par vispārīgu viena kvantu vaicājuma izsaukumu modeli. 5. nodaļā tiek apkopoti secinājumi un turpmākās idejas, ko virzīt.

1 Ieskats nepieciešamajās priekšzināšanas

1.1 Būla funkcijas

Par **Būla mainīgo** jeb **bitu** x_1 sauksim mainīgo, kurš var pieņemt vienu no divām vērtībām, šajā darbā tās būs vai nu $\{\pm 1\}$ vai $\{0,1\}$. Standarta pāreja no $x_1 \in \{0,1\}$ uz $\hat{x}_1 \in \{\pm 1\}$ ir $\hat{x}_1 = (-1)^{x_1}$.

Par Būla ieejas vārdu x garumā n sauksim komplektu no atsevišķiem konkrētas reprezentācijas Būla mainīgajiem jeb bitiem $x_1, x_2, \ldots, x_n$, un apzīmēsim ar x.

Definīcija 1. n-Būla mainīgo ieejas vārda $x \in \{0,1\}^n$ **Heminga svars**, ko apzīmēsim ar $|x|$ ir "1" skaits.

Definīcija 2. Būla funkcija f tiek definēta kā n Būla mainīgo argumentu funkcija, kas izejā arī dod Būla mainīgo $f : B^n \to A$, kur B, A - Būla mainīgie. Šajā darbā parādīsies Būla funkcijas reprezentācijās gan ar $\{\pm 1\}$, gan $\{0,1\}$, piemēram, $f : \{\pm 1\}^n \to \{0,1\}$.

Definīcija 3. Būla funkcija ir **simetriska**, ja tās vērtība nav atkarīga no ieejas bitu secības.

Definēsim jēdzienu, kas ļaus divas vienāda ieejas vārda izmēra Būla funkcijas uzskatīt par ekvivalentām (dažādās nozīmēs), ja tām ir nebūtiskas atšķirības, piemēram, ieejas bitu pārkārtojumi, vai ieejas bitu noliegumi.

Definīcija 4. Divas n-mainīgo Būla funkcijas sauc par **NP-ekvivalentām**, ja pie visiem ieejas vārdiem tās atšķiras tikai ar ieejas mainīgo pārkārtojumiem vai to loģiskajiem noliegumiem.

Definīcija 5. Par n-mainīgo Būla funkciju **NP-ekvivalences klasēm** sauc visu n-mainīgo Būla funkciju sadalījumu pa savstarpēji nešķeļošām kopām, kur katrā no tām visas funkcijas ir savstarpēji NP-ekvivalentas.

Definīcija 6. Divas n-mainīgo Būla funkcijas sauc par **NPN-ekvivalentām**, ja pie visiem ieejas vārdiem tās atšķiras tikai ar ieejas mainīgo pārkārtojumiem, loģiskajiem noliegumiem vai izejas mainīgā noliegumu.

Definīcija 7. Par n-mainīgo Būla funkciju **NPN-ekvivalences klasēm** sauc visu n-mainīgo Būla funkciju sadalījumu pa savstarpēji nešķeļošām kopām, kur katrā no tām visas funkcijas ir savstarpēji NPN-ekvivalentas.

1.2 Lineārā algebra

Par lietotajām lineārās algebras pamatzināšanām sīkāk var skatīt [6].

Šajā darbā apskatītie vektori un lineāras transformācijas būs no kompleksās lineārās telpas, ja vien tas netiek atsevišķi atrunāts. Kompleksu (kolonas) vektoru $|a\rangle$ apzīmēsim ar

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix}.$$

Visām skaitļu struktūrām matricas formā (lineārām transformācijām, kolonas vektoriem, rindas vektoriem) par to **Ermita saistīto** jeb **duālo** objektu sauksim tā transponēto objektu ar kompleksi saistītajām vērtībām un apzīmēsim sekojoši

objekts	Ermita saistītais
U	$U^\dagger$
$\|a\rangle$	$\|a\rangle^\dagger = \langle a\|$
$\langle b\|$	$\langle b\|^\dagger = \|b\rangle$

Definīcija 8. Par vienādas dimensijas vektoru $|a\rangle$ un $|b\rangle$ **skalāro reizinājumu** sauksim kompleksu skaitli un apzīmēsim to ar $\langle a|b\rangle$ vai $\langle a, b\rangle$ un

$$\langle a, b\rangle = \langle a| \cdot |b\rangle = \begin{pmatrix} a_1^* & a_2^* & \dots & a_n^* \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

.

Definīcija 9. Par vektora $|\psi\rangle$ **normu** sauksim reālu pozitīvu skaitli un apzīmēsim to ar $||\,|\psi\rangle\,||$ vai vienkārši $||\psi||$ un $||\psi|| = \sqrt{\langle\psi, \psi\rangle}$

Definīcija 10. Lineāru transformācija U sauksim par unitāru, ja tai izpildās $UU^\dagger = I$, kur I ir vienības matrica.

1.3 Kvantu skaitļošana

Smalkākam ievadam kvantu mehānikā tiek norādīta atsauce uz [7], kvantu skaitļošanai – [8].

Kvantu skaitļošanā (un kvantu mehānikā) pamatelements ir sistēmas **kvantu stāvoklis**, ko mēdz apzīmēt ar $|\psi\rangle$, un kas raksturo sistēmas stāvokli.

Formāli, $|\psi\rangle$ pieder Hilberta telpai (kvantu skaitļošanā, kur darbojamies ar galīgu dimensionalitāti, tā ir unitāra telpa), un to var uzskatīt par vektoru $|\psi\rangle \in \mathbb{C}^n$.

Telpas bāzes stāvokļus apzīmēsim ar $|1\rangle, |2\rangle, \dots, |n\rangle$, tiek pieņemts, ka tie ir normēti vektori $\langle i, i\rangle = 1$.

Jebkuru kvantu stāvokli šajā telpā var izteikt kā lineāru kombināciju no telpas bāzes stāvokļiem:

$$|\psi\rangle = a_1|1\rangle + a_2|2\rangle + \dots + a_n|n\rangle\,,$$

kur $a_i \in \mathbb{C}$ un $|a_1|^2 + |a_2|^2 + \dots + |a_n|^2 = 1$.

Lai pārietu no viena kvantu stāvokļa uz nākamo, pieejamais rīks kvantu skaitļošanā ir unitāra transformācija U:

$$|a\rangle \xrightarrow{U} |b\rangle$$

Atbilstošā algebriskā sakarība šai stāvokļu pārejai ir

$$|b\rangle = U|a\rangle\,.$$

Nākamajā sadaļā par vaicājumu sarežģītību parādās īpašas simboliskas unitāras matricas, ar kuru palīdzību ir iespējams stāvoklī iekodēt algoritma ieejas datu vērtības - Būla mainīgos $x_1, x_2, \ldots, x_n$. Šāda unitāra transformācija ir diagonālmatrica Q un par piemēru var būt formā:

$$Q = \begin{pmatrix} x_1 & 0 & \ldots & 0 \\ 0 & x_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x_n \end{pmatrix},$$

kur $x_i \in \{\pm 1\}$.

Definīcija 11. Mērījums (standartbāzē) ir darbība, kuras rezultātā ar varbūtību $|a_i|^2$ stāvoklis pārtop par (kolapsē uz) $|i\rangle$, jeb no skaitļošanas viedokļa, mēs uzzinām stāvokļa indeksu i.

Gadījumā, ja stāvokļu superpozīcijā $a_i = 0$, bāzes stāvokli $|i\rangle$ mērījuma rezultātā nav iespējams iegūt. Precīzos kvantu algoritmos mērījuma brīdī būs svarīga tikai atšķirība starp $a_i = 0$ un $a_i \neq 0$.

1.3.1 Vaicājumu sarežģītības modeļi

Plašāks pārskats par vaicājumu sarežģītībām ir atrodams [9].

Deterministiskās vaicājuma sarežģītības modelis / lēmumkoka modelis

Par lēmumkoku sauc koku ar sakni, kura katrai ne-lapas virsotnei piekārtots ieejas bits x_i ($i \in \{1, 2, \ldots, n\}$). Ne-lapas virsotnei ir tieši divi bērni, un katrai lapai ir piekārtota vērtība 0 vai 1. Lēmumkoks aprēķina konkrētas Būla funkcijas vērtību sekojoši. Sākuma stāvoklis ir saknes virsotnē un katrā solī, kamēr nav sasniegta lapas virsotne, uzzinot tābrīža stāvokļa virsotnes piekārtotā bita vērtību x_i, atkarībā no x_i izvēlas kreiso vai labo bērnu uz kuru pārvietoties. Kad ir sasniegta lapas virsotne, izdod tai piekārtoto vērtību.

Lēmumkoks aprēķina Būla funkciju $f : \{0,1\}^n \to \{0,1\}$, ja pie katra ieejas vārda x lēmumkoks izdod $f(x)$ – pareizo Būla funkcijas vērtību.

Definīcija 12. Par Būla funkcijas f **lēmumkoka sarežģītību** sauc par minimālo lēmumkoka dziļumu no tiem lēmumkokiem, kuri aprēķina f, un to apzīmē ar $D(f)$.

Vispārīgais kvantu vaicājumu sarežģītības modelis

Ja lēmumkoku modelī mēs interesējamies par lēmumkoku ar minimālo dziļumu, kas pareizi aprēķina doto Būla funkciju, tad kvantu vaicājumu modelī mēs interesējamies par to, ar kādu mazāko vaicājumu matricu izsaukumu skaits ir nepieciešams, lai būtu pietiekama informācija funkcijas vērtības noteikšanai veicot mērījumu/mērījumus (precīzi, vai ar ierobežotu kļūdas varbūtību).

Kvantu vaicājumu modelī pirms un pēc katra vaicājuma ir pieļaujams, ka tiek veikta unitāra transformācija (neatkarīga no ieejas bitiem). k-vaicājumu gadījumā sākuma stāvoklim secīgi tiek pielietotas sekojošas transformācijas:

$$U_1, Q, U_2, Q, \ldots, U_k, Q, U_{k+1}\ ,$$

kur U_i ir brīvi izvēlamas unitāras transformācijas un vaicājuma transformācija Q ir formā

$$Q = \begin{pmatrix} x_{i_1} & 0 & \dots & 0 \\ 0 & x_{i_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x_{i_m} \end{pmatrix},$$

kur $i_j \in 0, 1, 2, \dots, n$, $x_0 \equiv 1$ ir konstantais loceklis un pārējie $x_1, x_2, \dots, x_n$ ir ieejas biti, kas pieņem vērtības $x_i \in \{\pm 1\}$. Un pēc šīm $2k+1$ transformācijām tiek veikts mērījums (standartbāzē). Katram bāzes stāvoklim ir piekārtota funkcijas vērtība (līdzīgi kā lapām lēmumkokā). Šāds kvantu algoritms aprēķina Būla funkcijas $f : \{\pm 1\}^n \to \{0, 1\}$, ja pie katra ieejas vārda x algoritms atgriež pareizo funkcijas vērtību.

Definīcija 13. Par Būla funkcijas f **precīzo kvantu vaicājumu sarežģītību** sauc mazāko nepieciešamo vaicājumu skaitu k, ka eksistē kvantu algoritms, kurš ar k vaicājumiem un varbūtību $P = 1$ katram ieejas vārdam pareizi izrēķina f vērtību. Precīzo kvantu vaicājumu sarežģītību apzīmē ar $Q_E(f)$.

Paritātes lēmumkoks

Liela grupa literatūrā atrodamo precīzo kvantu vaicājumu algoritmu, piemēram, [10–12], tiek izpildīti balstoties tikai uz Doiča XOR algoritmu divu ieejas bitu paritātes aprēķināšanai. vienā vaicājumā un neizmanto nekādas citas pieejamos kvantu vaicājumu iespējas. Gluži kā [4, §3.1], definēsim kvantu vaicājumu modeli tikai balstoties uz (klasisko) lēmumkoka modeli ar pieeju kvantu XOR vaicājuma izsaukumam kā vienam vaicājuma soli.

Definīcija 14. Par **paritātes lēmumkoka sarežģītību** sauksim vaicājuma sarežģītību lēmumkoka modelim ar vienīgo izmaiņu lēmumkoka struktūrā, ka katrā virsotnē ir atļauts izraudzīties, vai noskaidrot viena ieejas bita vērtību x_i (kā parastajā lēmumkokā), vai arī uzzināt paritāti $\mathrm{XOR}(x_i, x_j)$ jebkuram bitu pārim (x_i, x_j).

Apzīmēsim Būla funkcijas f paritātes lēmumkoka sarežģītību ar $D_{\mathrm{XOR}}(f)$.

2 Esošie rezultāti

[4] Būla funkciju klase f_n, kurai $D_{\text{XOR}}(f_n) > Q_E(f_n)$. Vēlāk parādījās viens no retiem precīziem kvantu algoritmiem Būla funkciju aprēķinam, kas nebalstās uz XOR izsaukuma [5]. Līdz ar to, ir skaidrs pamats veikt algoritma paņēmiena sīkāku analīzi.

Īsi tiks aprakstīti [5] esošie kvantu algoritmi specifisko Būla funkciju aprēķinam.

2.1 Precīzā kvantu vaicājumu sarežģītība Būla funkcijām EXACT un THRESHOLD

Definēsim sekojošas Būla funkcijas

$$\text{EXACT}_k^n(x) \quad = \begin{cases} 1, \text{ ja } |x| = k \\ 0, \text{ citādi} \end{cases}$$

$$\text{THRESHOLD}_k^n(x) = \begin{cases} 1, \text{ ja } |x| \geq k \\ 0, \text{ citādi} \end{cases}$$

2.1.1 EXACT_k^n

Apzīmējam $k = m$ un definējam U_1.

$$|0\rangle \xrightarrow{U_1} \sum_{i=1}^{2m} \frac{1}{\sqrt{2m}}|i\rangle \xrightarrow{Q} \sum_{i=1}^{2m} \frac{\hat{x}_i}{\sqrt{2m}}|i\rangle$$

Definējam U_2, ka visiem $i \in [2m]$:

$$U_2|i\rangle = \sum_{j>i} \frac{1}{\sqrt{2m}}|i,j\rangle - \sum_{j<i} \frac{1}{\sqrt{2m}}|j,i\rangle + \frac{1}{\sqrt{2m}}|0\rangle\,.$$

U_i izmērs ir $(2m+n+1) \times (2m+n+1)$, un nav vajadzības pārbaudīt skalāro reizinājumu, jo no lineārās algebras ir labi zināms, ka eksistē no uzrādītajām matricas rindiņām neatkarīgi normēti vektori, kas atbilstu $|i,j\rangle$, lai aizpildītu pilno $rank(U_i) = 2m+n+1$.

Vēl pielietojot tagad transformāciju U_2, rezultējošais kvantu stāvoklis ir:

$$\sum_{i=1}^{2m} \frac{\hat{x}_i}{\sqrt{2m}}|i\rangle \xrightarrow{U_2} \sum_{i=1}^{2m} \frac{\hat{x}_i}{2m}|0\rangle + \sum_{i<j} \frac{\hat{x}_i - \hat{x}_j}{2m}|i,j\rangle\,.$$

Algoritmā, kā publikācijā aprakstīts, tiek darīts sekojoši:

(a) ja tiek nomērīts $|0\rangle$, tad $\sum_{i=1}^{2m} \hat{x}_i \neq 0$ jeb $|\{i|\hat{x}_i = 1\}| \neq |\{i|\hat{x}_i = -1\}|$;

(b) ja tiek nomērīts $|i,j\rangle$, tad $\hat{x}_i \neq \hat{x}_j$.

Un abos gadījumos tiek iegūta informācija, kas ir derīga, lai rekursīvi reducētu problēmu uz tās stingri mazāku gadījumu:

(a) $EXACT_m^{2m} = 0$, jo bitu vērtību sadalījums nav precīzi uz pusēm $\sum\limits_{i:x_i=0} \hat{x}_i \neq -\sum\limits_{i:x_i=1} \hat{x}_i$;

(b) $EXACT_m^{2m}(x) = EXACT_{m-1}^{2m-2}(x \backslash \{x_i, x_j\})$.

2.1.2 THRESHOLD$_k^n$

Sākumā pilnīgi analoģiski EXACT$_k^n$ gadījumam, tiek sagatavots vienmērīgi pa bāzes stāvokļiem sadalīts stāvoklis ar U_1 un tad pielietots vaicājuma izsaukums Q:

$$|0\rangle \xrightarrow{U_1} \sum_{i=1}^{2m+1} \frac{1}{\sqrt{2m+1}}|i\rangle \xrightarrow{Q} \sum_{i=1}^{2m+1} \frac{\hat{x}_i}{\sqrt{2m+1}}|i\rangle$$

Transformācija, kas panāk nepieciešamo stāvokli:

$$|i\rangle \xrightarrow{U_2} \sum_{j>i} \frac{\sqrt{2m-1}}{2m}|i,j\rangle - \sum_{j<i} \frac{\sqrt{2m-1}}{2m}|j,i\rangle + \sum_{j\neq i} \frac{1}{2m}|j\rangle$$

To pielietojot pēc vaicājuma Q atstātajam stāvoklim, iegūstam sekojošu stāvokli:

$$\sum_{i=1}^{2m+1} \frac{\hat{x}_i}{\sqrt{2m+1}}|i\rangle \xrightarrow{U_2} \sum_{i=1}^{2m+1} \sum_{j\neq i} \frac{\hat{x}_j}{2m\sqrt{2m+1}}|i\rangle + \sum_{i<j} \frac{(\hat{x}_i - \hat{x}_j)\sqrt{2m-1}}{2m\sqrt{2m+1}}|i,j\rangle$$

Pēc mērījuma kolapsējot uz konkrētu bāzes stāvokli, iespējami divi varianti:

(a) ja nomēram $|i\rangle$, tad ir zināms, ka vārdā $x\backslash\{x_i\}$ bitu ar vērtību "0" un bitu ar vērtību "1" skaiti atšķiras vismaz par 2. Tāpēc izmetot no ieejas vārda x_i un jebkuru citu patvaļīgu bitu x_j $(j \neq i)$, vairākuma vērtība nemainīsies;

(b) ja nomēram $|i,j\rangle$, tad x_i un x_j ir dažādi, tos izmetot arī vairākuma vērtība nemainīsies.

Un abos gadījumos THRESHOLD$_{m+1}^{2m+1}(x)$ = THRESHOLD$_{m-1}^{2m-1}(x\backslash\{x_i, x_j\})$.

2.2 EXACT un THRESHOLD kvantu algoritmu kopīgās īpašības un paņēmieni

Var ievērot, ka izveidotās bāzes stāvokļu superpozīcijās ieejas bitu $\hat{x}_i$ lineāras kombinācijas pie katra bāzes stāvokļa ir divās formās (neņemot vērā normētībai nepieciešamos amplitūdu koeficientus):

$$\sum_{i\in S} \hat{x}_i|j\rangle \text{ un } (\hat{x}_i - \hat{x}_j)\,|i,j\rangle \ ,$$

kur S ir kāda izraudzīta indeksu apakškopa.

Viegli saprast, ka mērījuma rezultātā, piemēram, kolapsējot stāvoklī $|i,j\rangle$, tiek iegūti indeksi diviem bitiem, par kuriem zināms, ka tie ir savā starpā dažādi $x_i \neq x_j$. Toties nomērot stāvokli ar amplitūdu formā $\sum_i \hat{x}_i$, uzreiz sniedz informāciju, lai vai nu zinātu funkcijas vērtību (EXACT gadījumā $= 0$) vai arī, ka neieskaitot x_i pārējo bitu kopā $x \backslash \{x_i\}$ "1" un "0" skaiti atšķiras vismaz par 2 (THRESHOLD gadījumā un varam to rekursīvi reducēt uz THRESHOLD ar 2 bitiem mazāku ieejas vārdu).

Labākai izpratnei, apskatīsim konkrētu beigu superpozīcijas piemēru – EXACT_2^4 bāzes stāvokļu amplitūdas (kā ieejas bitu lineāras kombinācijas), kad tās pieņems 0 vērtību, ir norādītas tabulā 2.1.

Tabula 2.1: EXACT_2^4 kvantu algoritma beigu stāvokļa superpozīcijas bāzes stāvokļu koeficientu vērtības. Tukšajās ailītēs ir nenulles vērtība.

$x_4x_3x_2x_1$	$\hat{x}_1+\hat{x}_2$ $+\hat{x}_3+\hat{x}_4$	$\hat{x}_1-\hat{x}_2$	$\hat{x}_1-\hat{x}_3$	$\hat{x}_1-\hat{x}_4$	$\hat{x}_2-\hat{x}_3$	$\hat{x}_2-\hat{x}_4$	$\hat{x}_3-\hat{x}_4$	EXACT_2^4
0000		0	0	0	0	0	0	0
0001					0	0	0	0
0010			0	0			0	0
0011	0	0					0	1
0100		0		0		0		0
0101	0		0			0		1
0110	0			0	0			1
0111		0	0		0			0
1000		0	0		0			0
1001	0			0	0			1
1010	0		0			0		1
1011		0		0		0		0
1100	0	0					0	1
1101			0	0			0	0
1110					0	0	0	0
1111		0	0	0	0	0	0	0

Kvantu mērījuma rezultāts (bāzes stāvoklis) atbilst tabulā 2.1 kādai no kolonām, turklāt pie katra ieejas vārda var tikt iegūta tikai kāda (no četrām) tabulas rindiņas šūnām ar nenulles vērtību tajā. No otras puses, ja mēs nezinām ieejas vārdu, tad uzzinot kura kolona ir tikusi nomērīta, automātiski var izslēgt ieejas vārdus, kuru atbilstošās šūnas ir ar nulles vērtību. Konkrētā gadījumā visas kolonas izņemot pirmo satur tieši pusi no šūnām ar nulli tajā - kuru atbilstošos rindiņu ieejas vārdus varam izslēgt. Pirmā kolona ir īpaša ar to, ka šūnā ir nulles vērtība tad un tikai tad, ja atbilstošā funkcijas vērtība $\text{EXACT}_2^4(x) = 1$.

Ja pretendējam vispārināt šo paņēmienu uz citiem vaicājumiem ar līdzīgiem polinomiem kolonās, tad svarīgs aspekts, ko ņemt vērā ir tas, ka nulles vērtību skaits ir tas faktors, kas nosaka, cik daudz ieejas vārdu tiek atmesti mērījuma rezultātā. Jo vairāk nuļļu ir nomērītajā kolonā, jo par vairāk potenciālajiem ieejas vārdiem varam pateikt, ka faktiskais ieejas vārds nav viens no tiem.

Cits aspekts ir tas, ka ne obligāti izpildot vairākus šāda tipa vaicājumus ir nepieciešams potenciālo ieejas vārdu komplektu kopu reducēt līdz vienam elementam – ja aprēķināmās funkcijas vērtība visiem atlikušajiem iespējamiem ieejas vārdiem ir vienāda, varam sniegt atbildi – funkcijas vērtību.

Līdz šim nav pieminēts aspekts, ka konstruējot kvantu vaicājumu, iespējas uzkonstruēt lineārus polinomus no ieejas bitiem, ir ierobežotas ar iespējām, ko sniedz unitāras transformācijas. Tātad kvantu vaicājuma lineāriem polinomiem ir niepieciešams, lai tos būtu iespējams nonormēt (saglabājot normu pie visiem ieejas vārdiem), bet jāpiebilst, ka iespējams tas nav pietiekams nosacījums, lai jebkura lineāra transformācija, ar kuru iegūti interesējošie lineāru polinomu komplekti, būtu unitāra vai arī viegli pārveidojama par unitāru.

3 Viena kvantu vaicājuma izsaukumu lēmumkoks

Iepriekš aprakstītos EXACT un THRESHOLD algoritmos izmantotos paņēmienus var vispārināt dažādos virzienos. Viens veids no tādiem būtu interesēties tikai par viena kvantu vaicājuma iespējām.

Tā kā liela daļu literatūrā atrodamo precīzo kvantu algoritmu iekļaujas paritātes lēmumkoka modelī, kā arī ir uzrādītas Būla funkciju klases, kurām neeksistē optimālu precīzie kvantu algoritmi, kas iekļautos paritātes lēmumkoka modelī, tad ir pamats aplūkot plašākus modeļus par paritātes lēmumkoku, bet kas tomēr būtu vienkāršāki un vieglāk pētāmi par precīzu kvantu vaicājumu vispārīgo modeli. Tas būtu daudzsološs solis, gadījumā, ja šajā modelī jau būtu automātiski zināms kāds algoritms, kurš parāda tā pārākumu pār paritātes lēmumkoku. Nav garantijas, ka tāds skaitļošanas modelis nekļūst spēcīgāks par kvantu skaitļošanas, bet tomēr iegūstot jebkādu negatīvu rezultātu par to, ko šis modelis nespēj aprēķināt, automātiski pierāda, ka to nespēj arī paritātes lēmumkoka modelis, jo tas būtu tad vājāks skaitļošanas modelis.

Tādu modeli tagad ieviesīsim, kurā iekļausies EXACT un THRESHOLD piedāvātie kvantu aprēķinu algoritmi [5].

Vispārīgāks kvantu vaicājuma modelis ar jebkādām unitārām transformācijām ir pārāk plašs, lai to būtu pietiekami viegli analizēt, tāpēc interesēsimies par vienu kvantu vaicājumu un kādu informāciju tādā veidā varam iegūt, kas palīdzētu jaunu kvantu algoritmu konstrukcijai Būla funkciju aprēķināšanai.

Vispārīgākajā formā viena vaicājuma rezultātā iegūtais kvantu stāvoklis ir

$$|p\rangle = U\,Q\,U_0\,|\psi\rangle\ ,$$

kur $|\psi\rangle$ ir sākuma stāvoklis, U_0 un U ir patvaļīgas unitāras transformācijas, Q - kvantu vaicājums. Pierādīsim, ka

Lemma 1. *Ja ir doti divi patvaļīgi normēti vektori $|a\rangle, |b\rangle \in \mathbb{C}^n$ ($||a||^2 = ||b||^2 = 1$), tad vienmēr eksistē unitāra transformācija U, kas pārveido $|a\rangle \xrightarrow{U} |b\rangle$.*

Pierādījums. Ja $|\langle a|b\rangle| = 1$, tad $U = e^{\mathrm{i}\alpha} I$, kur $\alpha = \mathrm{Arg}(\langle a|b\rangle)$. Citādi, $|\langle a|b\rangle| < 1$, un varam pielietot Hausholdera transformācijas (Householders reflection) versiju kompleksajā telpā, kas būs formā

$$U = e^{\mathrm{i}\alpha}\left(I - 2\frac{|\varphi\rangle\langle\varphi|}{||\varphi||^2}\right),$$

kur $|\varphi\rangle = |a\rangle - e^{-\mathrm{i}\alpha}|b\rangle$. Viegli pārliecināties, ka $||\varphi||^2 > 0$ un $U|a\rangle = |b\rangle$, kā arī tas, ka $U^\dagger U = I$. □

Tas nozīmē, ka pilnīgi vispārīgu vienu kvantu vaicājumu vienkāršības labad, varam apskatīt formā $UQ|\alpha\rangle$, kur U ir patvaļīga unitāra transformācija un $|\alpha\rangle$ ir izvēlams sākuma stāvoklis ar nosacījumu $||\alpha||^2 = 1$.

Izmantotā kvantu stāvokļu darba telpa ir izmērā m, un kvantu vaicājumam vispārīgākajā formā k-tais bits $x_k \in \{\pm 1\}$ var parādīties nevienā, vienā, kā arī vairākās Q matricas pozīcijās. Ļaujam $i_j \in \{0, 1, 2, \ldots, n\}$, kur $i_j \neq 0$ atbilst vienam no n ieejas bitiem $x_1, x_2, \ldots, x_n$ un $i_j = 0$ atbilst x_0, kas ir konstantais ieejas bits, kas vienmēr pieņems vērtību $x_0 = 1$.

$$|\alpha\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{pmatrix} \in \mathbb{C}^m$$

$$Q = \begin{pmatrix} x_{i_1} & 0 & \ldots & 0 & 0 \\ 0 & x_{i_2} & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & \ldots & x_{i_{m-1}} & 0 \\ 0 & 0 & \ldots & 0 & x_{i_m} \end{pmatrix}$$

$$U = \begin{pmatrix} U_{11} & U_{12} & \ldots & U_{1m} \\ U_{21} & U_{22} & \ldots & U_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ U_{m1} & U_{m2} & \ldots & U_{mm} \end{pmatrix}$$

$$Q, U, U_0 \in \mathbb{C}^{m \times m}$$

Pēc transformācijām rezultējošais vektors ir

$$|p\rangle = U\,Q\,|\alpha\rangle = \begin{pmatrix} U_{11}x_{i_1}\alpha_1 + U_{12}x_{i_2}\alpha_2 + \cdots + U_{1m}x_{i_m}\alpha_m \\ U_{21}x_{i_1}\alpha_1 + U_{22}x_{i_2}\alpha_2 + \cdots + U_{2m}x_{i_m}\alpha_m \\ \vdots \\ U_{m1}x_{i_1}\alpha_1 + U_{m2}x_{i_2}\alpha_2 + \cdots + U_{mm}x_{i_m}\alpha_m \end{pmatrix} = \begin{pmatrix} p_1(x) \\ p_2(x) \\ \vdots \\ p_m(x) \end{pmatrix} .$$

Ja savelkam kopā koeficientus pie katra x_i, tad saīsināti vektora komponentes atkarībā no ieejas bitiem varam pārrakstīt formā

$$p_i(x) = \sum_{j=1}^{n} a_{ij}x_j - b_i\,.$$

Lai šāda sistēma atbilstu kvantu mehānikas pamatpostulātiem, viens no nepieciešamajiem nosacījumiem noteikti būtu

$$\sum_{i=1}^{m} |p_i(x)|^2 = 1.$$

Bet pie šī nosacījuma nav triviāli redzamas garantijas, ka izraugoties patvaļīgu $|p\rangle$, tikai ierobežotu ar nosacījumu $|p|^2 = 1$, eksistēs unitāra transformācija U, ar kuru varēs panākt jebkuru patvaļīgu normētu beigu stāvokli.

Ja vienkāršākai analīzei relaksējam U unitaritātes nosacījumu, un tikai par to, kad $p_i(x)$ pieņems vērtību $p_i(x) = 0$ un kad ne – $p_i(x) \neq 0$, tad

$$\sum_{j=1}^{n} |p_j(x)|^2 = 0 \iff \sum_{j=1}^{n} q_j(x)^2 = 0 \text{ un } \sum_{j=1}^{n} r_j(x)^2 = 0$$

un kā varēs redzēt turpmākajā analīzē, šo loģisko konjunkciju būs iespējams modelēt ar citu paņēmienu, tāpēc nezaudējot vispārīgumu, varam uzskatīt, ka visi lineārie polinomi $p_i(x)$ ir ar reāliem koeficientiem.

Apskatīsim, vai U unitaritātes nosacījumu ir iespējams vienkāršot vienam kvantu vaicājumam $|p\rangle = UQ|z\rangle$. Kā vienkāršu gadījumu apskatīsim, ka $||p|| = ||z|| = 1$ un vaicājums Q ir formā

$$Q = \begin{pmatrix} x_1 & 0 & \dots & 0 & 0 \\ 0 & x_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & 0 \\ 0 & 0 & \dots & x_{n-1} & 0 \\ 0 & 0 & \dots & 0 & x_n \end{pmatrix},$$

t.i., darba telpas izmērs sakrīt ar ieejas bitu skaitu.

Interpretējot transformāciju kā kolonas vektoru komplektu

$$U = \begin{pmatrix} | & | & & | \\ v_1 & v_2 & \dots & v_n \\ | & | & & | \end{pmatrix},$$

varam izrakstīt

$$|p\rangle = UQ|z\rangle = \begin{pmatrix} | & | & & | \\ x_1 v_1 & x_2 v_2 & \dots & x_n v_n \\ | & | & & | \end{pmatrix} |z\rangle = \sum_{i=1}^{n} x_i z_i \begin{pmatrix} | \\ v_i \\ | \end{pmatrix}$$

$$||p||^2 = \langle p|p\rangle = \left(\sum_{i=1}^{n} x_i z_i^* \langle v_i|\right)\left(\sum_{j=1}^{n} x_j z_j^* |v_j\rangle\right) = \sum_{i=1}^{n} x_i^2 z_i^* z_i ||v_i||^2 + \sum_{1\le i<j\le n} x_i x_j (z_i^* z_j \langle v_i|v_j\rangle + z_j^* z_i \langle v_j|v_i\rangle)$$

$$= \sum_{i=1}^{n} |z_i|^2 ||v_i||^2 + \underbrace{\sum_{1\le i<j\le n} x_i x_j 2\Re(z_i^* z_j \langle v_i|v_j\rangle)}_{0} = 1$$

Tā kā visiem $x_i \in \{\pm 1\}$ un izteiksmei $||p||^2 \equiv 1$ ir jābūt konstantai (neatkarīgai) no x_i, tad $\Re(z_i^* z_j \langle v_i|v_j\rangle) = 0$. Citiem vārdiem $z_i^* z_j \langle v_i|v_j\rangle$ ir tīri imaginārs. Ja nosacījums būtu, ka $\langle v_i|v_j\rangle = 0$ tad mēs automātiski būtu ieguvuši ortogonalitātes nosacījumu. Ja apskatam gadījumu, kad $|z\rangle \in \mathbb{R}^n$, tad $z_i^* z_j \langle v_i|v_j\rangle = 0$ un no kā izriet, ka visiem $i \neq j \wedge |z_i|, |z_j| > 0 \implies \langle v_i|v_j\rangle = 0$. Tā kā $\{z_i\}$ jābūt neatkarīgam no $\{v_i\}$ un $\sum_i |z_i|^2 = 1$, tad $\sum_i ||v_i||^2 = 1$. Redzams, ka tomēr ir nepieciešami vēl citi nosacījumi bez $||p|| = ||z|| = 1$, lai U transformācija būtu unitāra.

4 Lineāru polinomu komplektu mērījumu modelis

Kā sadaļā 2.2 tika analizēts, tad doto kvantu algoritmu specifika bija tajā, ka tika uzkonstruēti lineāru polinomu komplekti, no kuriem katrs polinoms lielai daļai ieejas vārdu pieņēma vērtību 0.

Šajā nodaļā formāli definēsim modeli, kura aspektus pētīsim tālākā darbā daļā.

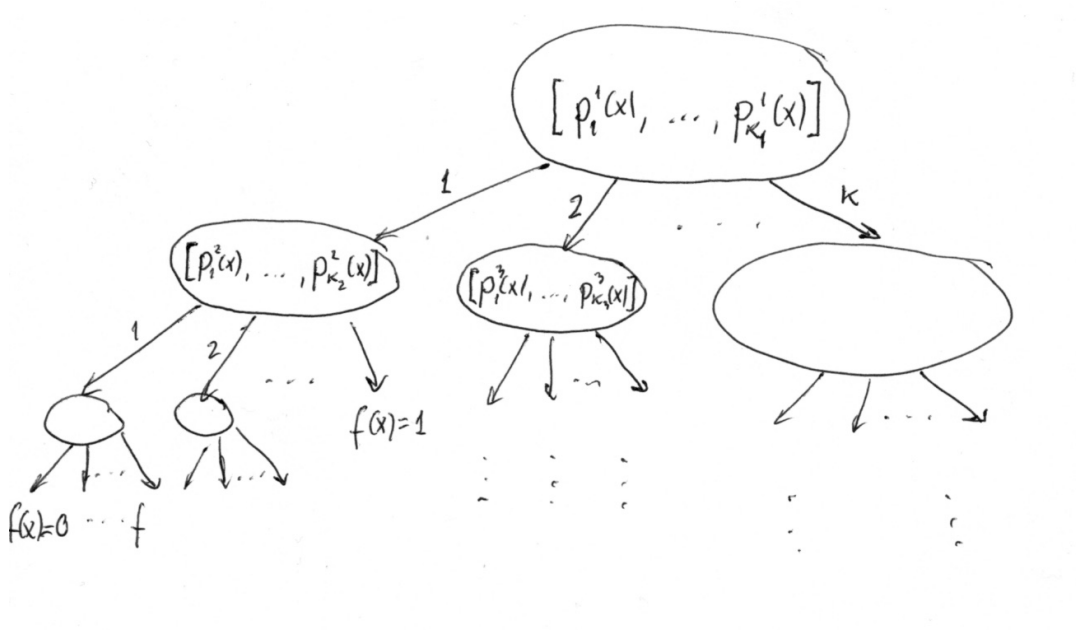
4.1 Modeļa definīcija un salīdzinājums

Darbā no šī brīža, apskatīsim ieejas vārdu sastāvam no bitiem ± 1 reprezentācijā, t.i., $x_i \in \{\pm 1\}$.

Formalizēsim modeli sekojoši:

Definīcija 15. Kortežu ar k elementiem, kur katrs no tiem ir lineārs polinoms no n ieejas bitiem $x_i \in \{\pm 1\}$, kur $i \in \{1, 2, \ldots, n\}$, sauksim par **lineāru polinomu komplektu** (jeb LPK)

$$[\, p_1(x), p_2(x), \ldots, p_k(x) \,].$$



Att. 4.1: Lineāru polinomu komplektu lēmumkoks (LPKL)

Definīcija 16. Par **lineāru polinomu komplektu lēmumkoku** (LPKL) sauksim lēmumkoku, kura katrai lēmumkoka virsotnei tiek piekārtots LPK $[\, p_1(x), p_2(x), \ldots, p_k(x) \,]$ (ar kompleksiem

koeficientiem), katrai lēmumkoka ne-lapas virsotnei ir tieši k bērni, un katrā ne-lapas virsotne pāriet uz vienu no virsotnes bērniem $j \in \{l \in [k] \,|\, p_l(x) \neq 0\}$, ar īpašību, ka šī bērna apakškoks ir visdziļākais, t.i., tiek iegūts indeks vienam no polinomiem, kuri pie esamā ieejas vārda nepieņem nulles vērtību. Katrai lapas virsotnei ir piekārtota vērtība 0 vai 1, un nonākot lapas virsotnē, lēmumkoks izdod šai virsotnei piekārtoto vērtību.

Ja pie katra no Būla funkcijas f ieejas vārdiem x LPKL izdod vērtību $f(x)$, tad LPKL aprēķina f.

Definīcija 17. Par LPKL sarežģītību Būla funkcijai f sauksim minimālā dziļuma LPKL, kas aprēķina f, un apzīmēsim to ar LPKL(f).

Definīcija 18. Lēmumkoka modeli L_1 sauksim **spēcīgāku par** lēmumkoka modeli L_2, ja visām Būla funkcijām f, L_1 sarežģītība funkcijai f ir mazāka vai vienāda ar L_2 sarežģītību funkcijai f.

Teorēma 2. *LPKL modelis ir spēcīgāks par paritātes lēmumkoka modeli.*

Pierādījums. Zinot vaicājumu algoritmu paritātes lēmumkokam, pierādīsim, ka katram vaicājumam atbilst analogs LPKL. Katrs solis var būt

(a) bita x_i vaicājums - šajā gadījumā izveidojam polinoma komplektu sastāvam no $p_1(x) = 1 + x_i$, $p_2(x) = 1 - x_i$. Acīmredzami, ka atkarībā no x_i vērtības, viens no polinomiem pieņems $p_i(x) = 0$ un otrs $p_j(x) \neq 0$, un abos gadījumos viennozīmīgi būs zināma x_i vērtība.

(b) paritātes $x_i \oplus x_j$ vaicājums - izveidojam $p_1(x) = x_i - x_j$, $p_2(x) = x_i + x_j$. Līdzīgi arī šajā gadījumā pie katra ieejas vārda viens no polinomiem pieņems nulles vērtību, otrs nē, kā arī tiks viennozīmīgi noteikta paritāte $x_i \oplus x_j$, uzzinot, kurš polinoms ir ar nenulles vērtību.

□

4.2 LPKL atsevišķa polinoma analīze

Apskatīsim atsevišķa lineāra polinoma īpašības, kas ir svarīgas LPKL pielietojumā.

Definīcija 19. Par lineāra polinoma $p(x)$ **raksturojošo Būla funkciju** sauksim tādu Būla funkciju $f(x)$, kurai izpildās:

$$f(x) = \begin{cases} 0, \text{ ja } p(x) = 0 \\ 1, \text{ ja } p(x) \neq 0 \end{cases}$$

Lemma 3. *Ja LPKL jebkuras virsotnes LPK jebkuru polinomu aizstāj ar citu polinomu, ka to raksturojošās Būla funkcijas sakrīt, tad tas nekādīgi neizmaina LPKL vai arī tā izpildes gaitu atkarībā no ieejas vārda.*

Pierādījums. Acīmredzami pēc definīcijām. □

Līdz ar to varam ieviest polinomu ekvivalenci.

Definīcija 20. Lineārus polinomus sauksim par ekvivalentiem (LPKL modeļa ietvaros), ja to raksturojošās Būla funkcijas sakrīt.

Definīcija 21. Šī darba ietvaros par triviāliem sauksim tādus lineārus polinomus, kuru raksturojošā Būla funkcija $f(x) \equiv c$, kur $c \in \{0, 1\}$.

Ja vienkāršos gadījumos apskatām lineārus polinomus ar kompleksiem algebriskiem koeficientiem, un apskatām homogēno gadījumu (nehomogēnajam ir līdzīgs intuitīvs spriedums), tad ir skaidrs, ka, piemēram, koeficients $\sqrt{2}$ un $\sqrt{3}$ ar jebkādiem papildus racionāliem reizinātājiem nedos summā 0, līdz ar to intuitīvi būtu saprātīgi savilkt iracionāli līdzīgos saskaitāmos kopā un tikai, ja polinoma katra no šādām savilktajām grupām pieņemtu 0 vērtību, polinoms summāri dotu 0 vērtību. Tādu grupu analogu veselajos skaitļos varētu izveidot, piereizinot pietiekami lielu reizinātāju daļai polinoma mainīgo, tādā veidā panākot loģisko konjunkciju starp nosacījumiem, ka katras grupas summai jābūt 0.

Hipotēze 4. *Lineāri polinomi ar kompleksiem koeficientiem LPKL modeļa ietvaros ir ekvivalenti lineāriem polinomiem ar veseliem koeficientiem.*

Varam to sadalīt sekojoši:

$$p(x) = q(x) + \mathrm{i}r(x)\,,$$

kur $q(x)$ un $r(x)$ ir polinomi ar reāliem koeficientiem. Nosacījums $p(x) = 0$ izpildīsies tad un tikai tad, ja reizē $q(x) = 0$ un $r(x) = 0$.

Tālāk tiks apskatīts vienkārši skaitliski apskatāms viena polinoma gadījums

4.2.1 Veselo skaitļu koeficientu lineāri polinomi

Aplūkosim vienkāršāku gadījumu, kur lineāra polinoma koeficienti ir veseli skaitļi. Tad

$$p(x) = a_1x_1 + a_2x_2 + \cdots + a_nx_n - b\,,$$

kur $a_i, b \in \mathbb{Z}$ un $x_i \in \{\pm 1\}$.

Ja apskatām šī polinoma raksturīgo Būla funkciju f, tad ir skaidrs, ka

(a) gadījums $a_i = 0$ nozīmē, ka f ir neatkarīga no x_i bita;

(b) a_i zīmes maiņa polinomā uz $-a_i$ atbilst f ieejas bita negācijai; līdzīgi arī b zīmes maiņa veic negāciju Būla funkcijas visām ieejām;

(c) polinoma a_i koeficientu permutācijas atbilst f ieejas bitu permutācijām.

Tā kā koeficientu zīmju maiņu un permutāciju rezultātā netiek iziets ārpus konkrētas NP-ekvivalences klases, nezaudējot vispārīgumu, varam interesēties tikai par nenegatīviem koeficientiem, kuri sakārtoti ne-dilstošā secībā.

4.2.2 Skaitliskie aprēķini

Lai sekmētu labāku izpratni par problēmu, tika uzrakstīta programma C++ valodā, kas ar pilno pārlasi atrod atšķirīgu raksturojošo Būla funkciju lineāros polinomus ar veseliem koeficientiem, ar koeficienta vērtību a_i līdz 32, un tika iegūta sekojoši rezultāti.

No pilnajām tabulām (ne visas ir attēlotas) var redzēt, ka lineāru polinomu raksturojošo Būla funkciju ar mazāko Heminga svaru (lielāko nuļļu skaitu) ir pie polinoma ar visiem 1 koeficientiem.

Tabula 4.1: 1-bita netriviālā raksturīgā Būla funkcija (1)

	$f_i(000)\dots f_i(111)$	a_1	b	Raksturojošā Būla funkcija
f_1	10	1	0	$NAND(x_1)$

Tabula 4.2: 2-bitu netriviālās raksturīgās Būla funkcijas (kopā 3)

$f_i(000)\dots f_i(111)$	a_1	a_2	b	Raksturojošā Būla funkcija
0111	1	1	2	
1001	1	1	0	
1011	1	2	1	

Tabula 4.3: 3-bitu raksturīgo Būla dažādās funkcijas (kopā 6)

	$f_i(000)\dots f_i(111)$	a_1	a_2	a_3	b	Raksturojošā Būla funkcija
f_1	11111110	1	1	1	3	$NAND(x_1, x_2, x_3)$
f_2	11110111	1	1	3	1	$OR(NAND(x), AND(x_1 = x_2, x_1 \neq x_3))$
f_3	11111101	1	2	2	3	$NAND(x_1 \neq x_2, x_2 = x_3, x_1 = c)$
f_4	11100111	1	1	2	0	$NAND(x_1 = x_2, x1 \neq x_3)$
f_5	11101011	1	2	2	1	$NAND(x_1 = c, x2 \neq x_3)$
f_6	11101001	1	1	1	1	$x_1 * x_2 * x_3 == c$

Tabula 4.4: Izlase no 4-bitu raksturīgo Būla dažādām funkcijām (kopā 18)

$f_i(0000)\dots f_i(1111)$	a_1	a_2	a_3	a_4	b
1111111111111110	1	1	1	1	4
1111111111100111	1	1	2	3	3
1111111111100111	1	1	2	3	3
1111110111011111	1	2	3	3	1
1111111111111001	1	1	2	2	4
1111110110111111	1	2	2	3	0
1111111010011111	1	1	2	3	1
1111111011101001	1	1	1	1	2
1110100110010111	1	1	1	1	0

Tabula 4.5: Izlase no 5-bitu raksturīgo Būla dažādām funkcijām (kopā 64)

$f_i(000000)\dots f_i(111111)$	a_1	a_2	a_3	a_4	a_5	b
11111110111010011001011101111111	1	1	1	1	2	0
11111110111010011111010011001011	1	1	1	1	1	1

Tabula 4.6: Izlase no 6-bitu raksturīgo Būla dažādām funkcijām (kopā 399)

$f_i(000000)\dots f_i(111111)$	$a_1\ a_2\ a_3\ a_4\ a_5\ a_6$	b
11111111111111101111111011101001111010011001011110010111011111111	1 1 1 1 1 2	1
11111111111111101111111011101001111111011101001111010011010111	1 1 1 1 1 1	2
11111110111010011110100110010111111010011001011110010111011111111	1 1 1 1 1 1	0

Hipotēze 5. *n ieejas bitu polinoms ar mazāko raksturojošā polinoma Heminga svaru ir ar koeficientiem* $a_i = 1$ *un* $b = 0$ *vai* 1. *Heminga svars* $= \binom{n}{\lfloor n/2 \rfloor}$.

Ja šī hipotēze izpildītos, būtu iespēja tālāk virzīt ideju, ka iespējams praktiski noderīgie polinomu komplekti priekš Būla funkciju klasēm (lieliem n) noderīgas ir tikai konstrukcijas ar $x_i \pm x_j$ *polinomiem, kā arī* $\sum_i x_i$ *polinomiem, kā ir ticis izmantots [5] darbā.*

5 Rezultāti un secinājumi

Darbā ir formāli definēts jauns lēmumkoka-tipa modelis, kas ir klasisks lēmumkoka modelis, izmantojot viena kvantu vaicājuma izsaukumu, un ir izteiktas hipotēzes par pamatots, ka tas ir spēcīgāks par paritātes lēmumkoka modeli.

Skaitliskie aprēķini izveidotajā LPKL modelī liecina par iespēju pierādīt, ka nedaudz vispārīgākā modelī par paritātes lēmumkoku (klasiskie vaicājumi ar Doiča XOR izsaukumiem) ievērojami lielākas skaitļošanas iespējas nav. Uzsākta šī modeļa dažādu īpašību analīze, kā arī veikti skaitliskie aprēķini, labākai modeļa izpratnei.

Ir izteiktas vairākas hipotēzes, kurām varētu meklēt pretpiemērus vai mēģināt pierādīt.

Ir neskaitāmi virzieni, kuros

Kas vēl netika pagūts - mēģināt pielietot hiperkuba/ģeometriskās interpretācijas un zināmos faktus, lai pateiktu ko par hiperplakņu šķēlumiem ar tiem.

Izmantotā literatūra un avoti

[1] D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 400(1818):97–117, jul 1985. ISSN 1364-5021. doi: 10.1098/rspa.1985.0070. URL http://rspa.royalsocietypublishing.org/cgi/doi/10.1098/rspa.1985.0070.

[2] D. Deutsch and R. Jozsa. Rapid Solution of Problems by Quantum Computation. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 439(1907): 553–558, 1992. ISSN 1364-5021. doi: 10.1098/rspa.1992.0167. URL http://rspa.royalsocietypublishing.org/cgi/doi/10.1098/rspa.1992.0167.

[3] Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Quantum Algorithms Revisited. pages 339–354, 1997. ISSN 1364-5021. doi: 10.1098/rspa.1998.0164. URL http://arxiv.org/abs/quant-ph/9708016{%}0Ahttp://dx.doi.org/10.1098/rspa.1998.0164.

[4] Ashley Montanaro, Richard Jozsa, and Graeme Mitchison. On Exact Quantum Query Complexity. Algorithmica, 71(4):775–796, 2015. ISSN 14320541. doi: 10.1007/s00453-013-9826-8.

[5] Andris Ambainis, Jānis Iraids, and Juris Smotrovs. Exact quantum query complexity of EXACT and THRESHOLD. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10139 LNCS:243–255, feb 2013. ISSN 16113349. doi: 10.1007/978-3-319-51963-0_19. URL http://arxiv.org/abs/1302.1235.

[6] Roger A. Horn and Charles R. Johnson. Matrix analysis. 2013. ISBN 978-0-521-54823-6. doi: 10.1002/1521-3773(20010316)40:6<9823::AID-ANIE9823>3.3.CO;2-C. URL www.cambridge.org/9780521548236.

[7] J. J. Sakurai and Richard L. Liboff. Modern Quantum Mechanics, 1986. ISSN 0002-9505. URL http://aapt.scitation.org/doi/10.1119/1.14491.

[8] Michael a. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information. Book, page 706, 2011. doi: 10.2277/0521635039.

[9] Harry Buhrman and Ronald De Wolf. Complexity measures and decision tree complexity: A survey. Theoretical Computer Science, 288(1):21–43, 2002. ISSN 03043975. doi: 10.1016/S0304-3975(01)00144-X.

[10] Alina Dubrovska Vasilieva and Taisija Mischenko-Slatenkova. Computing Boolean Functions: Exact Quantum Query Algorithms and Low Degree Polynomials. jul 2006. URL http://arxiv.org/abs/quant-ph/0607022.

[11] Alina Vasilieva. Quantum Query Algorithm Constructions for Computing AND, OR and MAJORITY Boolean Functions. page 24, 2007. URL http://arxiv.org/abs/0710.5592.

[12] Alina Vasilieva. Exact Quantum Query Algorithm for Error Detection Code Verification. apr 2009. URL http://arxiv.org/abs/0904.3660.

[13] Andris Ambainis. New Developments in Quantum Algorithms. pages 1–4, 2010. doi: 10.1007/978-3-642-15155-2_1. URL http://arxiv.org/abs/1006.4014{%}0Ahttp://dx.doi.org/10.1007/978-3-642-15155-2{_}1.

[14] Daowen Qiu and Shenggen Zheng. Characterizations of symmetrically partial Boolean functions with exact quantum query complexity. 2016. URL http://arxiv.org/abs/1603.06505.

[15] S. A. Grillo and F. L. Marquezino. Quantum Query as a State Decomposition. pages 1–30, 2016. URL http://arxiv.org/abs/1602.07716.

[16] Shenggen Zheng, Lvzhou Li, Daowen Qiu, and Jozef Gruska. Promise problems solved by quantum and classical finite automata. Theoretical Computer Science, 666(November):48–64, 2017. ISSN 03043975. doi: 10.1016/j.tcs.2016.12.025.

[17] Shenggen Zheng and Daowen Qiu. From Quantum Query Complexity to State Complexity. pages 1–15, 2014. URL http://arxiv.org/abs/1407.7342.

[18] Jozef Gruska, Daowen Qiu, and Shenggen Zheng. Potential of Quantum Finite Automata with Exact Acceptance. International Journal of Foundations of Computer Science, 26(03): 381–398, 2015. ISSN 0129-0541. doi: 10.1142/S0129054115500215. URL http://www.worldscientific.com/doi/abs/10.1142/S0129054115500215.

[19] Jozef Gruska, Daowen Qiu, and Shenggen Zheng. Generalizations of the distributed Deutsch-Jozsa promise problem. Mathematical Structures in Computer Science, 27(3):311–331, 2017. ISSN 09601295. doi: 10.1017/S0960129515000158.

[20] Gatis Midrij. Exact quantum query complexity for total Boolean functions. Contract, 11234 (01):1–5, 1999.

[21] Andris Ambainis. Understanding Quantum Algorithms via Query Complexity. pages 1–20, 2017. URL http://arxiv.org/abs/1712.06349.

[22] Daowen Qiu and Shenggen Zheng. Characterizations of symmetrically partial Boolean functions with exact quantum query complexity. pages 1–33, 2016. URL http://arxiv.org/abs/1603.06505.

[23] Andris Ambainis, Arturs Backurs, Juris Smotrovs, and Ronald de Wolf. Optimal quantum query bounds for almost all Boolean functions. Stacs'13, 1(255961):8, 2013. ISSN 18688969. doi: 10.4230/LIPIcs.STACS.2013.446. URL http://arxiv.org/abs/1208.1122.

[24] Alina Dubrovska and Taisija Mischenko-Slatenkova. Computing Boolean Functions: Exact Quantum Query Algorithms and Low Degree Polynomials. page 11, 2006. URL http://arxiv.org/abs/quant-ph/0607022.

[25] Andris Ambainis, Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha, and Juris Smotrovs. Separations in Query Complexity Based on Pointer Functions. 117543:1–25, 2015. ISSN 1433-8092. doi: 10.1145/2897518.2897524. URL http://arxiv.org/abs/1506.04719.

[26] *Andris Ambainis. Superlinear advantage for exact quantum algorithms. Proceedings of the 45th annual ACM symposium on Symposium on theory of computing - STOC '13, 45(600700): 617–631, 2013. ISSN 07378017. doi: 10.1137/130939043. URL* http://dx.doi.org/10.1137/130939043{%}5Cnhttp://dl.acm.org/citation.cfm?doid=2488608.2488721.

[27] *Andris Ambainis, Jozef Gruska, and Shenggen Zheng. Exact quantum algorithms have advantage for almost all Boolean functions. pages 1–17, 2014. ISSN 15337146. URL* http://arxiv.org/abs/1404.1684.

[28] *Andrejs Vihrovs. Datorikas fakultāte Precīzi kvantu algoritmi ar minimālu vaicājumu skaitu Maģistra darbs.*

[29] *Andris Ambainis, Jozef Gruska, and Shenggen Zheng. Exact quantum algorithms have advantage for almost all Boolean functions. pages 1–15, apr 2014. ISSN 15337146. URL* http://arxiv.org/abs/1404.1684.

Maģistra darbs "Precīzie kvantu algoritmi, izmantojot 1-kvantu-vaicājuma izsaukumus" izstrādāts LU Datorikas fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: Zigmārs Rupenheits

_____ _____
(paraksts) *(datums)*

Rekomendēju darbu aizstāvēšanai.
Vadītājs: prof. Dr.dat. Juris Smotrovs

_____ _____
(paraksts) *(datums)*

Recenzents: doc. Dr.dat. Aleksandrs Belovs

_____ _____
(paraksts) *(datums)*

Darbs iesniegts _____
(datums)

_____
(darbu pieņēma)

Darbs aizstāvēts maģistra gala pārbaudījuma komisijas sēdē

_____ *prot. Nr.* _____, *vērtējums*_____
(datums)

Komisijas sekretārs/-e: _____ _____
(Vārds, Uzvārds) *(paraksts)*