LATVIJAS UNIVERSITĀTE

LELDE LĀCE

KVANTU VAICĀJOŠIE ALGORITMI

Promocijas darbs
datorzinātņu doktora (Dr.sc.comp.) zinātniskā grāda iegūšanai

Nozare: datorzinātnes
Apakšnozare: datorzinātņu matemātiskie pamati

Zinātniskais vadītājs:
profesors, Dr.habil.math.
RŪSIŅŠ MĀRTIŅŠ FREIVALDS

Rīga – 2008

ANOTĀCIJA

Kvantu skaitļošana ir datorzinātņu apakšnozare, kurā tiek izmantotas kvantu mehānikas īpatnības, lai efektīvāk risinātu skaitļošanas uzdevumus. Šajā darbā tiek aplūkoti kvantu vaicājošie algoritmi Bula funkciju rēķināšanai.

Darba sākumā tiek pierādīti kvantu algoritmu apakšējie novērtējumi dažādām funkcijām, kas apraksta grafu problēmas. Promocijas darba galvenais uzdevums ir izveidot efektīvus kvantu vaicājošos algoritmus. Ir nodefinēts kā veidot precīzus kvantu vaicājošos algoritmus ar sarežģītību n-1, 2n/3 un n/2. Darba turpinājumā tiek analizēti nedeterminētie kvantu algoritmi ar vienu jautājumu, to veidošanas iespējas un īpašības. Promocijas darbā tiek definēts jauns kvantu vaicājošo algoritmu veids - kvantu vaicājošie algoritmi ar pēcatlasi un tiek pierādīta šo algoritmu saistība ar nedeterminētajiem kvantu vaicājošajiem algoritmiem.

ANNOTATION

Quantum computing is the subfield of computer science that aims to employ effects of quantum mechanics to efficiently perform computational tasks. The main research object of this work is quantum query model to compute Boolean functions.

At first we prove higher lower bounds of quantum query algorithms for some of graph problems. Main purpose of the research is to find quantum query algorithms with complexity lower than deterministic one. The work presents a set of new exact quantum algorithms with quantum query complexity n-1, 2n/3 and n/2. We construct some nondeterministic quantum query algorithms with complexity 1 for Boolean functions with 2, 4 and 2n variables and study some properties of these functions. We propose definition of postselection quantum query algorithm and we propose one method how to make postselection quantum query algorithms.

SATURS

IEVADS

Kvantu algoritmi bieži spēj veikt aprēķinus ātrāk par to klasiskajiem līdziniekiem. Kvantu algoritmu priekšrocība rodas izmantojot kvantu mehānisko superpozīciju un interferenci. Vaicājošie algoritmi ir vienkāršākais modelis Bula funkciju rēķināšanai. Veidojot algoritmu, ir zināma konkrētā funkcija, bet mainīgie ir ievietoti „melnajā kastē" un to vērtības var uzzināt uzdodot jautājumus „melnajai kastei" par konkrētu mainīgo. Algoritmam darbības beigās ir jāizdod pareizā funkcijas vērtība. Uzdevums ir izveidot algoritmus ar iespējami mazāku jautājumu skaitu. Ja aplūko kvantu vaicājošos algoritmus, tad ir nepieciešams atrast algoritmus, kas būtu labāki par šīs pašas funkcijas determinētajiem algoritmiem.

Darba pirmā nodaļa ir veltīta kvantu algoritmu apakšējo novērtējumu iegūšanai. Apakšējie novērtējumi ir veids, kā noskaidrot dotās funkcijas iespējamā kvantu vaicājošā algoritma parametrus. Apakšējā novērtējuma iegūšana gan vēl nenodrošina iespēju šādu algoritmu izveidot.

Darba otrajā nodaļā tiek aplūkoti veidi, kā varētu izveidot jaunus kvantu vaicājošos algoritmus dotām funkciju kopām. Galvenā problēma ir atrast atbilstošus bāzes algoritmus.

Promocijas darba trešā nodaļa ir veltīta konkrētiem kvantu algoritmiem. Ir nodefinēts kā veidot precīzus kvantu vaicājošos algoritmus ar sarežģītību n-1, 2n/3 un n/2. Doto teorēmu pierādījumos ir izmantotas otrās nodaļas teorēmas. Ir izveidots arī kvantu vaicājošais algoritms ar kļūdas varbūtību, kas spēj aprēķināt vienu no pirmajā nodaļā aprakstīto grafu problēmām ar iespējami labāko sarežģītību.

Darba turpinājumā tiek analizēti nedeterminētie kvantu algoritmi. Galvenā uzmanība tiek pievērsta nedeterminētajiem kvantu vaicājošajiem algoritmiem ar vienu jautājumu, tiek aplūkotas to veidošanas iespējas un meklētas tādas funkcijas, kurām būtu iespējams izveidot šādus algoritmus.

Promocijas darbā tiek definēts jauns kvantu vaicājošo algoritmu veids - kvantu vaicājošie algoritmi ar pēcatlasi un tiek pierādīta šo algoritmu saistība ar nedeterminētajiem kvantu vaicājošajiem algoritmiem.

1. KVANTU ALGORITMU APAKŠĒJIE NOVĒRTĒJUMI

1.1. Apakšējā novērtējuma iegūšanas metodes

Apakšējo novērtējumu iegūšana ir viens no paņēmieniem, kā iegūt salīdzinājumu ar citiem algoritmu veidiem. Ir lielas cerības, ka kvantu vaicājošie algoritmi varētu būt labāki salīdzinoši ar to determinētajiem un varbūtiskajiem līdziniekiem, jo kvantu vaicājošajos algoritmos tiek izmantotas jaunas iespējas. Tomēr no otras puses nav īsti skaidrs, cik lielu priekšrocību varētu iegūt izmantojot kvantu algoritmus. Izmantojot apakšējos novērtējumus, var iegūt vērtējumu kādi ir iespējamie labākie algoritmi.

Nodaļas pierādījumi ir balstīti uz divām A.Ambaiņa apakšējā novērtējuma iegūšanas teorēmām. Tāpat kā cita veida vaicājošajos algoritmos, arī kvantu vaicājošajos algoritmos pareizās atbildes varbūtība ir atkarīga no uzdoto jautājumu skaita. Dotās teorēmas nosaka nepieciešamo jautājumu skaitu, lai algoritms sniegtu pareizu atbildi ar pietiekoši labu varbūtību.

Vaicājošajos algoritmos tiek rēķinātas vairākmainīgo funkcijas, kur katram mainīgajam ir tikai divas vērtības – 0 vai 1. Funkcijas vērtība parasti arī ir 0 vai 1. Algoritma sarežģītība apraksta nepieciešamo jautājumu skaitu.

Aplūkojot determinētos vaicājošos algoritmus, to sarežģītība tiek novērtēta noskaidrojot funkcijas jūtīgumu. Tas raksturo sliktāko gadījumu, cik jautājumus ir nepieciešams uzdot, lai noskaidrotu funkcijas vērtību.

Teorēma A1: [29] *Ja* $f(x_1, x_2..x_n)$ *ir n {0,1} vērtīgu mainīgo funkcija, un kopas* $A \subset \{0,1\}^n$, $B \subset \{0,1\}^n$ *ir tādas, ka* $f(A)=1$, $f(B)=0$ *un*

- *katram* $x=(x_1..x_n) \in A$, *eksistē* $i \in \{1,...,n\}$ *vismaz skaitā m, tādi, ka* $(x_1, \ldots, x_{i-1}, 1-x_i, x_{i+1}, \ldots, x_n) \in B$,
- *katram* $x=(x_1..x_n) \in B$, *eksistē* $i \in \{1,...,n\}$ *vismaz skaitā m', tādi, ka* $(x_1, \ldots, x_{i-1}, 1-x_i, x_{i+1}, \ldots, x_n) \in A$,

tad $Q(f)=\Omega(\sqrt{mm'})$.

Darbā izmantotajās A.Ambaiņa apakšējā novērtējuma teorēmās tiek izmantoti nedaudz līdzīgi principi. Teorēmā A1 tiek meklētas divas ieejas mainīgo vērtību kopas, tādas, lai tās būtu maksimāli grūti atšķiramas. Katrai no šīm kopām ir piekārtota sava aprēķināmās funkcijas vērtība. Ieejas mainīgo vērtību kopas ir nepieciešams atrast tādas, lai katram to elementam būtu maksimāli daudz jūtīgo punktu, tas ir, nomainot jūtīgā punkta vērtību uz pretējo, jaunais elements piederētu otrai kopai. Teorēmā A1 kopas tiek meklētas tādas, lai

to elementi atšķirtos tikai vienu ieejas mainīgā vērtību. Ja dotajai funkcijai nav iespējams atrast šādas ieejas mainīgo kopas, tad apakšējā novērtējuma iegūšanai tiek izmantota teorēma A2.

Teorēma A2: [29] *Ja* $f(x_1, x_2..x_n)$ *ir n* $\{0,1\}$ *vērtīgu mainīgo funkcija, un kopas* $A \subset \{0,1\}^n$, $B \subset \{0,1\}^n$ *ir tādas, ka* $f(x) \neq f(y)$, *ja* $x \in A$ *un* $y \in B$ *un eksistē* $R \subset A \bullet B$ *tāda, ka*

- *katram* $x=(x_1..x_n) \in A$, *eksistē vismaz m atšķirīgi mainīgie* $y \in B$, *tādi, ka* $(x,y) \in R$,
- *katram* $x=(x_1..x_n) \in B$, *eksistē vismaz m' atšķirīgi mainīgie* $x \in A$, *tādi, ka* $A(x,y) \in R$,
- *katram* $x \in A$ *un* $i \in \{1,...n\}$ *nav vairāk kā l dažādi* $y \in B$ *tādi, ka* $(x,y) \in R$ *un* $x_i \neq y_i$,
- *katram* $y \in B$ *un* $i \in \{1,...n\}$ *nav vairāk kā l' dažādi* $x \in A$ *tādi, ka* $(x,y) \in R$ *un* $x_i \neq y_i$

tad $Q(f) = \Omega\left(\sqrt{\frac{mm'}{\max(ll')}}\right)$.

Šajā gadījumā kopu elementi var atšķirties vairāk kā par vienu mainīgā vērtību. Tomēr šajā situācijā ir jāanalizē arī šo atšķirīgo mainīgo savstarpējās atkarības. Kopumā ņemot, teorēma A1 ir vienkāršāka un vieglāk lietojama, tāpēc, ja bija iespējams, tad pierādījumos tika lietota šī teorēma. Lai pierādītu, ka iegūtie rezultāti ir maksimāli labākie, tika izmantota teorēma A3, kas ļauj pierādīt, ka ar šo metodi labākus rezultātus iegūt nevar.

Teorēma A3 *Neatkarīgi no kopām A un B ar teorēmas A1 palīdzību nav iespējams pierādīt labāku apakšējo novērtējumu kvantu vaicājošajiem algoritmiem, kā* $\sqrt{ND_0(f) \cdot ND_1(f)}$.

1.2. Apakšējo novērtējumu rezultāti

Dotajā nodaļā ir pierādīti apakšējie novērtējumi 17 dažādām problēmām:

1. Problēma par sadalīšanu trīsstūros [2] (*Partition into triangles*)
2. Problēma par sadalījumu frakcijās [2] (*Partition into cliques*)
3. Pāru izveidošanas problēma [2] (*Matching*)
4. Matricu paritātes vērtības noteikšana [2] (*Matrix Parity*)
4. Hamiltona cikla atrašanas problēma [4] (*Hamiltonian circuit*)
6. Virsotņu pārklājuma atrašanas problēma [4] (*Vertex cover*)
7. Dominējošās kopas atrašanas problēma [4] (*Dominating set*)
8. Virsotņu nokrāsošanas problēma [4] (*Chromatic number*)
9. Vienkrāsaina trīsstūra eksistences problēma [4] (*Monochromatic triangle*)
10. Minimums no maksimālās sadalīšanas pāros [7] (*Minimum maximal matching*)
11. Sadalīšana izomorfos apakšgrafos [7] (*Partition into isomorphic subgraphs*)
12. Sadalīšana Hamiltona apakšgrafos [7] (*Partition into Hamiltonian subgraphs*)
13. Dominējošo kopu skaita noskaidrošana [8] (*Domatic number*)
14. Problēma par Ahromatisko skaitli [7] (*Achromatic number*)
15. Problēma par Frakcijas atrašanu [7] (*Clique*)
16. Neatkarīgās kopas atrašanas problēma [7] (*Independent set*)
17. Pilnas zvaigznes atrašanas problēma [8] (*Full star*)

Šajā nodaļā izvērstā veidā tiek sniegti autores pierādītie kvantu vaicājošo algoritmu apakšējo novērtējumu pierādījumi. Katrai problēma ir aprakstīta atsevišķā apakšnodaļā. Tai tiek sniegts problēmas nostādījums un tālāk tiek pierādīts konkrētais apakšējais novērtējums. Visas aplūkotās problēmas tiek numurētas, bet katrai problēmai ir arī nosaukums. Nodaļas sākumā parādās arī problēmu angliskie nosaukumi un atsauces uz publikācijām, kurās dotie pierādījumi ir publicēti.

1.2.1. Problēma par sadalīšanu trīsstūros

Problēma-1:
Dots – Grafs $G=(V,E)$ un $|V|= 3k$, kur k ir vesels skaitlis.
Jautājums – Vai dotā grafa G virsotnes var sadalīt k nešķeļošās kopās $V_1,V_2, .. V_k$ tā, lai katra kopa satur tieši trīs virsotnes un katrai $V_i=\{u_i,v_i,w_i\}$, $1\le i\le k$, visas trīs šķautnes $\{u_i,v_i\},\{u_i,w_i\},\{v_i,w_i\}$ pieder E?

Lemma 1-1. *Ja grafā G=(V,E), |V|=3k ir k+1 virsotne, kas nav savstarpēji saistītas, tad šo grafu nevar sadalīt trīsstūros, atbilstoši paroblēmai-1.*

Pierādījums: Pierādīsim no pretējā. Pieņemam, ka grafā G ir iespējams atrisināt problēmu par sadalīšanu trīsstūros. Tātad eksistē k nešķeļošās virsotņu kopas V_1,V_2, .. V_k. Vismaz vienā no šīm virsotņu kopām ir jābūt divām no savstarpēji nesaistītajām virsotnēm, jo šo virsotņu skaits ir k+1. Tātad dotajai virsotņu kopai piesaistītās šķautnes neveido trīsstūri, un ir iegūta pretruna.

Lemma 1-2. *Ja grafs G=(V,E), |V|=3k, apmierina sekojošus nosacījumus:*

- *tajā ir k/2 savstarpēji nesaistītas (sarkanas) virsotnes,*
- *tajā ir k(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,*
- *pārējām (melnas) virsotnēm atbilstošais apakšgrafs ir pilns grafs, un visas melnās virsotnes ir savienotas ar sarkanajām un zilajām virsotnēm,*

tad doto grafu var sadalīt trīsstūros, atbilstoši problēmai-1.

Pierādījums: Veidosim virsotņu sadalījumu apakšgrafos sekojoši:

- katru sarkano virsotni iedalām atsevišķā kopā – k/2 apakškopas,
- katru savienoto zilo virsotņu pāri arī atsevišķā kopā – k/2 apakškopas,
- katrā kopā, kura satur sarkano virsotni pievienojam divas melnās virsotnes, katram zilo virsotņu pārim pievienojam vienu melno virsotni.

Šis sadalījums apakškopās apmierina problēmu par sadalīšanu trīsstūros, jo dotās apakškopas nešķeļas, un katrai atbilstošais apakšgrafs satur trīsstūri. Tātad dotajā grafā problēmas par sadalīšanu trīsstūros atbilde ir pozitīva.

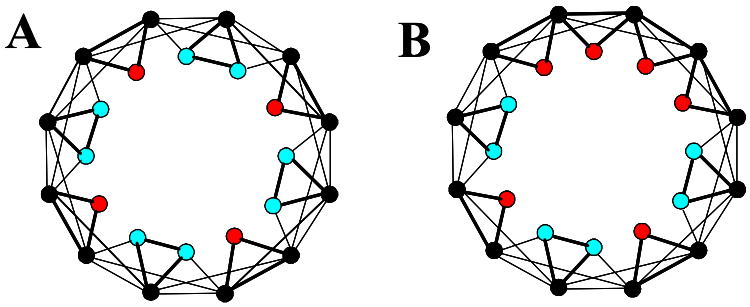
Lemma 1-3. *Ja grafs G=(V,E), |V|=3k, apmierina sekojošus nosacījumus:*

- *tajā ir k/2+2 savstarpēji nesaistītas (sarkanas) virsotnes,*
- *tajā ir k-2(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,*
- *pārējām (melnas) virsotnēm atbilstošais apakšgrafs ir pilns grafs, un visas melnās virsotnes ir savienotas ar sarkanajām un zilajām virsotnēm,*

tad doto grafu doto grafu var sadalīt trīsstūros, atbilstoši problēmai-1.

Pierādījums: Izveidosim sekojošu virsotņu apakškopu - visas sarkanās virsotnes (k/2+2), un pa vienai no katra zilo virsotņu pāra ((k-2)/2). Iegūtās virsotņu apakškopas izmērs ir k+1. Visas šīs virsotnes ir savstarpēji nesaistītas. No Lemmas 1-1 seko, ka doto grafu var sadalīt trīsstūros, atbilstoši problēmai-1.

Teorēma 1-1. *Problēmas par sadalīšanu trīsstūros atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*



1.2.1. att. **Kopu A un B piemērs problēmai par sadalīšanu trīsstūros**

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, kas apraksta Ambaiņa metodi, prasībām:

Kopa A satur visus grafus G, kas apmierina Lemmas 1-2 nosacījumus. Funkcijas vērtība, kas atbilst problēmai par sadalīšanu trīsstūros, ir 1. Tas seko no Lemmas 1-2. Kopa B satur visus grafus G', kas apmierina Lemmas 1-3 nosacījumus. Funkcijas vērtība, kas atbilst problēmai par sadalīšanu trīsstūros, ir 0. Zīmējumā 1.2.1. var redzēt divus grafus (šķautnes no melnajām virsotnēm nav pilnībā uzzīmētas), no kuriem viens pieder kopai A, bet otrs kopai B.

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams izmest vienu no šķautnēm, kas savieno zilās virsotnes. Šādu šķautņu skaits ir k/2, tātad m= O(n), jo k=n/3. Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu, kas piederētu kopai A, ir nepieciešams izveidot šķautni starp divām patvaļīgām sarkanajām virsotnēm. Pirmo sarkano virsotni ir iespējams izvēlēties k/2+2 veidos, otro k/2+1 veidos, un kopīgais dažādo iespējamo jauno šķautņu skaits ir (k/2+2)(k/2+1)/2. Tātad m'=O(n^2).

No teorēmas A1 seko, ka problēmas par sadalīšanu trīsstūros atrisināšanai ir nepieciešami $\Omega\sqrt{n \cdot n^2}$ =Ω($n^{1.5}$) kvantu jautājumi.

Teorēma 1-2. *Problēmas par sadalīšanu trīsstūros apakšējo novērtējumu kvantu gadījumā nav iespējams uzlabot lietojot Ambaiņa metodi.*

Pierādījums: Pierādījumā tiek izmantota Teorēma A3.
$ND_1(f) = O(n)$, jo pietiek parādīt, ka visas apakškopas satur trīsstūrus, tātad kopā ir nepieciešams aplūkot n šķautnes.
$ND_0(f) = O(n^2)$, jo ir nepieciešams noskaidrot, vai eksistē n/3+1 virsotne, kas nav savstarpēji saistītas ar šķautnēm, bet lai to noskaidrotu ir nepieciešamas pārbaudīt ((n/3+1)n/3)/2 šķautnes. Tātad $\sqrt{ND_1(f) \cdot ND_0(f)} = O(n^{1.5})$.

1.2.2. Problēma par sadalījumu frakcijās

Problēma-2:
Dots – Fiksēts vesels skaitlis q un grafs G=(V,E) un |V|= qk, kur k ir vesels skaitlis.
Jautājums – Vai dotā grafa G virsotnes var sadalīt k nešķeļošās kopās $V_1,V_2,..V_k$ tā, lai ja $1 \le i \le k$, tad katras kopas V_i noteiktais apakšgrafs ir pilns grafs un $|V_i|=q$?

Problēmu par sadalīšanu frakcijās var pierādīt balstoties un problēmas par trīsstūriem pierādījumu. Problēma par sadalīšanu trīsstūros ir problēmas par sadalīšanu frakcijās apakšgadījums, kur q=3. Pierādot problēmas par sadalīšanu frakcijās apakšējo novērtējumu ir nepieciešams izvēlēties tādu q, lai k būtu ar kārtu n. No šī nosacījuma seko, ka q ir ar kārtu konstante.

Teorēma 1-3. *Problēmas par sadalīšanu frakcijās atrisināšanai ir nepieciešami* $\Omega(n^{1.5})$ *kvantu jautājumi.*

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, kas apraksta Ambaiņa metodi, prasībām:

Kopa A satur visus grafus G, kas apmierina sekojošus nosacījumus:
- tajā ir k/2 savstarpēji nesaistītas (sarkanas) virsotnes,
- tajā ir k(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,
- pārējām (melnas) virsotnēm atbilstošais apakšgrafs ir pilns grafs, un visas melnās virsotnes ir savienotas ar sarkanajām un zilajām virsotnēm.

Funkcijas vērtība, kas atbilst problēmai par sadalīšanu frakcijās, ir 1. Virsotnes tiek sadalītas apakškopās šādā veidā. Sarkanās virsotnes tiek ievietotas katra savā apakškopā, Katrs zilo virsotņu pāris tiek ievietots savā apakškopā. Katrai sarkanajai virsotnei tiek pievienotas q-1 melnas virsotnes. Katram zilo virsotņu pārim tiek pievienotas q-2 melnās virsotnes. Visu izveidoto virsotņu kopu atbilstoši apakšgrafi ir pilni grafi, jo melnās virsotnes ir saistītas ar visām virsotnēm, un katrs savienotais zilo virsotņu pāris ir savā starpā savienots.

Kopa B satur visus grafus G', kas apmierina sekojošus nosacījumus.
- tajā ir k/2+2 savstarpēji nesaistītas (sarkanas) virsotnes,
- tajā ir k-2(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,
- pārējām (melnas) virsotnēm atbilstošais apakšgrafs ir pilns grafs, un visas melnās virsotnes ir savienotas ar sarkanajām un zilajām virsotnēm.

Funkcijas vērtība, kas atbilst problēmai par sadalīšanu frakcijās, ir 0. Dotajā gadījumā grafs satur k+1 savstarpēji nesaistītas virsotnes (visas sarkanās un pa vienai no katra zilo

virsotņu pāra). Tā kā ir nepieciešams izveidot k virsotņu apakškopas, tad vismaz divas no savstarpēji nesaistītajām virsotnēm nokļūs vienā apakškopā, kas līdz ar to nesaturēs pilnu grafu.

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams izmest vienu no šķautnēm, kas savieno zilās virsotnes. Šādu šķautņu skaits ir k/2, tātad m= O(n), jo k=O(n). Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu, kas piederētu kopai A, ir nepieciešams izveidot šķautni starp divām patvaļīgām sarkanajām virsotnēm. Pirmo sarkano virsotni ir iespējams izvēlēties k/2+2 veidos, otro k/2+1 veidos, un kopīgais dažādo iespējamo jauno šķautņu skaits ir (k/2+2)(k/2+1)/2. Tātad m'=O(n^2).

No teorēmas A1 seko, ka problēmas par sadalīšanu frakcijās atrisināšanai ir nepieciešami $\Omega\sqrt{n \cdot n^2}$ =Ω($n^{1.5}$) kvantu jautājumi.

Teorēma 1-4. *Problēmas par sadalīšanu frakcijās apakšējo novērtējumu kvantu gadījumā nav iespējams uzlabot lietojot Ambaiņa metodi.*

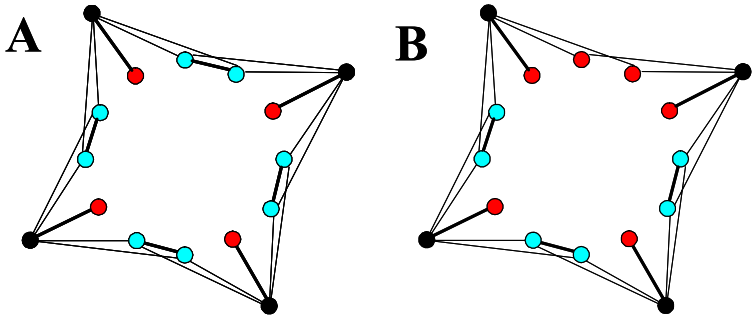
Pierādījums: Pierādījumā tiek izmantota Teorēma A3.
$ND_1(f)$ = O(n) , jo pietiek parādīt, ka visas apakškopas satur pilnus grafus, tātad kopā ir nepieciešams aplūkot q(q-1)n šķautnes, bet q=O(C).
$ND_0(f)$ = O(n^2) , jo ir nepieciešams noskaidrot, vai eksistē n/q+1 virsotne, kas nav savstarpēji saistītas ar šķautnēm, bet lai to parādītu ir nepieciešamas pārbaudīt ((n/q+1)n/q)/2 šķautnes.
Tātad $\sqrt{ND_1(f) \cdot ND_0(f)} = O(n^{1.5})$.

1.2.3. Pāru izveidošanas problēma

Problēma-3:
Dots – Grafs G=(V,E) un |V|= 2k, kur k ir vesels skaitlis.
Jautājums - Vai dotā grafa G virsotnes var sadalīt k nešķeļošos virsotņu pāros $P_1,P_2,\ldots,P_n$ tā, lai katram pārim $P_i = \{u_i,v_i\}$, $1 \le i \le n/2$, šķautne $\{u_i,v_i\}$ pieder E?

Problēmu par sadalīšanu pa pāriem arī var pierādīt balstoties un problēmas par trīsstūriem pierādījumu. Problēma par sadalīšanu pāros ir problēmas par sadalīšanu frakcijās apakšgadījums, kur q=2.

Teorēma 1-5. *Problēmas par sadalīšanu pa pāriem atrisināšanai ir nepieciešami* $\Omega(n^{1.5})$ *kvantu jautājumi.*



1.2.2. att. **Kopu A un B piemērs problēmai par sadalīšanu pāros**

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1 prasībām:

Kopa A satur visus grafus G, kas apmierina sekojošus nosacījumus:

- tajā ir k/2 savstarpēji nesaistītas (sarkanas) virsotnes,
- tajā ir k(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,
- pārējās (melnas) virsotnes (k/2) ir savienotas ar visām sarkanajām un zilajām virsotnēm.

Funkcijas vērtība, kas atbilst problēmai par sadalīšanu pa pāriem, ir 1. Virsotnes tiek sadalītas pāros šādā veidā. Sarkanās virsotnes tiek ievietotas katra savā pārī, Katrs zilo virsotņu pāris veido savu pāri. Katrai sarkanajai virsotnei tiek pievienotas vien melna virsotne. Katrs izveidotais virsotņu pāris ir savā starpā savienots.

Kopa B satur visus grafus G', kas apmierina sekojošus nosacījumus.

- tajā ir k/2+2 savstarpēji nesaistītas (sarkanas) virsotnes,
- tajā ir k-2(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,
- pārējās (melnas) virsotnes (k/2) ir savienotas ar visām sarkanajām un zilajām virsotnēm.

Funkcijas vērtība, kas atbilst problēmai par sadalīšanu pa pāriem, ir 0. Dotajā gadījumā grafs satur k+1 savstarpēji nesaistītas virsotnes (visas sarkanās un pa vieni no katra zilo virsotņu pāra). Tā kā ir nepieciešams izveidot k virsotņu pārus, tad vismaz divas no savstarpēji nesaistītajām virsotnēm nokļūs vienā pārī.

Zīmējumā 1.2.2. var redzēt divus grafus (šķautnes no melnajām virsotnēm nav pilnībā uzzīmētas), no kuriem viens pieder kopai A, bet otrs kopai B.

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams izmest vienu no šķautnēm, kas savieno zilās virsotnes. Šādu šķautņu skaits ir k/2, tātad m= O(n), jo k=O(n). Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par

grafu, kas piederētu kopai A, ir nepieciešams izveidot šķautni starp divām patvaļīgām sarkanajām virsotnēm. Pirmo sarkano virsotni ir iespējams izvēlēties k/2+2 veidos, otro k/2+1 veidos, un kopīgais dažādo iespējamo jauno šķautņu skaits ir (k/2+2)(k/2+1)/2. Tātad m'=$O(n^2)$.

No teorēmas A1 seko, ka problēmas par sadalīšanu pa pāriem atrisināšanai ir nepieciešami $\Omega\sqrt{n \cdot n^2}$ =$\Omega(n^{1.5})$ kvantu jautājumi.

Teorēma 1-6. *Problēmas par sadalīšanu pa pāriem apakšējo novērtējumu kvantu gadījumā nav iespējams uzlabot lietojot Ambaiņa metodi.*

Pierādījums: Pierādījumā tiek izmantota Teorēma A3.
$ND_1(f) = O(n)$, jo ir nepieciešams parādīt, ka visi pāri ir savienoti ar virsotnēm, tātad kopā ir nepieciešams pārbaudīt n/2 šķautnes.
$ND_0(f) = O(n^2)$, jo ir nepieciešams noskaidrot, vai eksistē n/2+1 virsotne, kas nav savstarpēji saistītas ar šķautnēm, bet lai to noskaidrotu ir nepieciešamas pārbaudīt ((n/2+1)n/2)/2 šķautnes.
Tātad $\sqrt{ND_1(f) \cdot ND_0(f)} = O(n^{1.5})$.

1.2.4. Matricu paritātes vērtības noteikšana

Problēma-4:
Dots – matrica M 2n×2n, $M_{ij} \in \{0,1\}$.
Jautājums - $\sum_{i=1,2n} \text{PARITY}(M_i) = n$?

Teorēma 1-7. *Problēmas par matricu paritātes atrisināšanai ir nepieciešami $\Omega(n^2)$ kvantu jautājumi.*

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1 prasībām:

Kopa A satur visas tādas matricas M, kurām ir n rindas ar n vieniniekiem katrā rindā (vienīnieki ir izvietoti patvaļīgās rindas kolonnās), un n rindas ar n+1 vienīnieku katrā rindā. Saskaitot šādas matricas visu rindu paritātes funkciju vērtību, tiek iegūts skaitlis n, neatkarīgi no tā, vai n ir pāra, vai nepāra skaitlis. Ja n ir pāra skaitlis, tad paritātes funkcijas vērtība ir 1 tajās rindās, kur ir n+1 vienīnieki, un 0 tajās rindas, kur ir n vienīnieki. Ja n ir nepāra skaitlis, tad paritātes funkcijai ir pretējas vērtības, bet paritātes funkciju summa abos gadījumos ir n.

Kopa B satur visas tādas matricas M', kurām ir n-1 rinda ar n vieniniekiem katrā rindā un n+1 rindu ar n+1 vieninieku katrā rindā. Šajā gadījumā paritātes funkciju summa ir n-1, ja n ir nepāra skaitlis un n+1, ja n ir pāra skaitlis. Tātad abos gadījumos šī vērtība nav n.

Lai jebkuru matricu M, kas pieder kopai A, pārveidotu par matricu M', kas pieder kopai B, ir jāizvēlas kāda no rindām, kurā ir n vieninieki un jānomaina patvaļīga šīs rindas 0 par 1. Rindu mēs varam izvēlēties n variantos, un pārveidojamo 0 arī var izvēlēties n variantos, tātad $m=n^2$. Lai jebkuru matricu M' no kopas B pārveidotu par matricu M no kopas A, ir jāizvēlas kāda no rindām ar n+1 vieninieku un patvaļīgs vieninieks ir jāpārveido par 0. Tātad arī $m'=n^2$.

No teorēmas A1 seko, ka problēmas par matricu paritātes noteikšanu atrisināšanai ir nepieciešami $\Omega\sqrt{n^2 \cdot n^2} = \Omega(n^2)$ kvantu jautājumi.
Dotajā gadījumā nav iespējams iegūt kvantu algoritma priekšrocību salīdzinot ar determinēto algoritmu, jo iegūtais sarežģītības novērtējums ir maksimāli iespējamais.

1.2.4. Hamiltona cikla atrašanas problēma

Problēma-5:
Dots - Grafs G=(V,E).
Jautājums – Vai grafs G satur Hamiltona ciklu (šķautņu cikls, kas iet caur visām grafa virsotnēm, caur katru tieši vienu reizi)?

Lemma 1-4. *Ja grafs G=(V,E), |V|=5k apmierina sekojošus nosacījumus:*

- *tajā ir k savstarpēji nesaistītas (sarkanas) virsotnes,*
- *tajā ir 2k(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,*
- *visas atlikušās 2k virsotnes (melnas) ir savienotas ar visām sarkanajām un visām zilajām virsotnēm,*

tad dotais grafs satur Hamiltona ciklu.

Pierādījums: Izvēlamies sekojošu virsotņu virkni: sarkana, melna, zilo virsotņu pāris, melna, sarkana utt. . Dotā virsotņu virkne apmierina Hamiltona cikla nosacījumus.

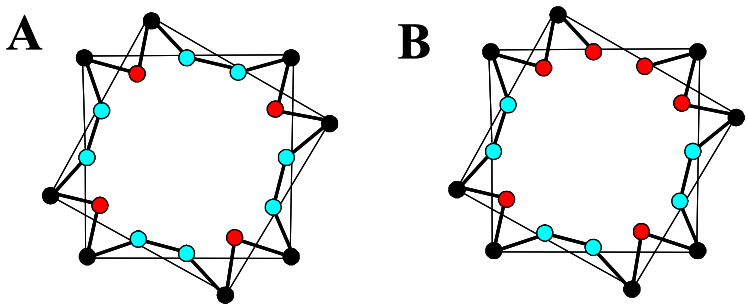
Lemma 1-5. *Ja grafs G=(V,E), |V|=5k apmierina sekojošus nosacījumus:*

- *tajā ir k+2 savstarpēji nesaistītas (sarkanas) virsotnes,*
- *tajā ir 2k-2(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,*
- *visas atlikušās 2k virsotnes (melnas) ir savienotas ar visām sarkanajām un visām zilajām virsotnēm,*

tad dotais grafs nesatur Hamiltona ciklu.

Pierādījums: Tā kā sarkanās virsotnes un zilo virsotņu pāri nav savā starpā savienoti, tad lai veidotos cikls ir nepieciešams starp katrām šīm virsotnēm (virsotņu pāriem) novietot vismaz vienu melno virsotni. Bet šādi savstarpēji nesavienoti apgabali ir: n+2 –sarkanās virsotnes, n-1 – zilo virsotņu pāri, kopā 2n+1. Bet melnās virsotnes ir tikai 2n, un tā kā nevienu virsotni nedrīkst lietot divas reizes, tad šajā grafā nav iespējams atrast Hamiltona ciklu.

Teorēma 1-8. *Problēmas par Hamiltona cikla atrašanu atrisināšanai ir nepieciešami* $\Omega(n^{1.5})$ *kvantu jautājumi.*



1.2.3. att. **Kopu A un B piemērs Hamiltona cikla atrašanas problēmai**

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:

Kopa A satur visus grafus G, kas apmierina Lemmas 1-4 nosacījumus. Funkcijas vērtība, kas atbilst problēmai par Hamiltona cikla atrašanu, ir 1. Kopa B satur visus grafus G', kas apmierina Lemmas 1-5 nosacījumus. Funkcijas vērtība, kas atbilst problēmai par Hamiltona grafa atrašanu, ir 0. Zīmējumā 1.2.3. var redzēt divus grafus (šķautnes no melnajām virsotnēm nav pilnībā uzzīmētas), no kuriem viens pieder kopai A, bet otrs kopai B. Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams izmest vienu no šķautnēm, kas savieno zilās virsotnes. Šādu šķautņu skaits ir n, tātad m= O(n), jo k=n/5. Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu, kas piederētu kopai A, ir nepieciešams izveidot šķautni starp divām patvaļīgām sarkanajām virsotnēm. Pirmo sarkano virsotni ir iespējams izvēlēties k+2 veidos, otro k+1 veidos, un kopīgais dažādo iespējamo jauno šķautņu skaits ir (k+2)(k+1)/2. Tātad m'=O(n^2).

No teorēmas A1 seko, ka problēmas par Hamiltona cikla atrašanu atrisināšanai ir nepieciešami $\Omega\sqrt{n \cdot n^2}$ =Ω($n^{1.5}$) kvantu jautājumi.

Teorēma 1-9. *Problēmas par Hamiltona cikla atrašanu apakšējo novērtējumu kvantu gadījumā nav iespējams uzlabot lietojot Ambaiņa metodi.*

Pierādījums: Pierādījumā tiek izmantota Teorēma A3.
$ND_1(f) = O(n)$, jo ir nepieciešams parādīt, ka dotā cikla virsotnes ir savienotas ar šķautnēm, tāpēc ir nepieciešams pārbaudīt n šķautnes.
$ND_0(f) = O(n^2)$, lai pierādītu, ka grafā neeksistē Hamiltona cikls ir nepieciešams pārbaudīt visas grafa virsotnes.
Tātad $\sqrt{ND_1(f) \cdot ND_0(f)} = O(n^{1.5})$.

1.2.6. Virsotņu pārklājuma atrašanas problēma

Problēma-6:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis K, tāds, ka $K \leq |V|$.
Jautājums – Vai šajā grafā G eksistē virsotņu pārklājums izmērā K vai mazāks? Tas ir vai eksistē virsotņu apakškopa $V' \subseteq V$ ar izmēru $|V'| \leq K$ tāda, ka katrai šķautnei $\{u,v\} \in E$ vismaz viena no virsotnēm pieder V'?

Lemma 1-6. *Ja grafs G=(V,E), |V|=n, K=n/4 apmierina sekojošus nosacījumus:*
- *tajā ir n/2 savstarpēji nesaistītas (melnas) virsotnes,*
- *tajā ir n/2 (sarkanas) virsotnes, kas ir pa pāriem savienotas,*

tad dotajā grafā var atrast virsotņu pārklājumu, atbilstošu problēmai-6.

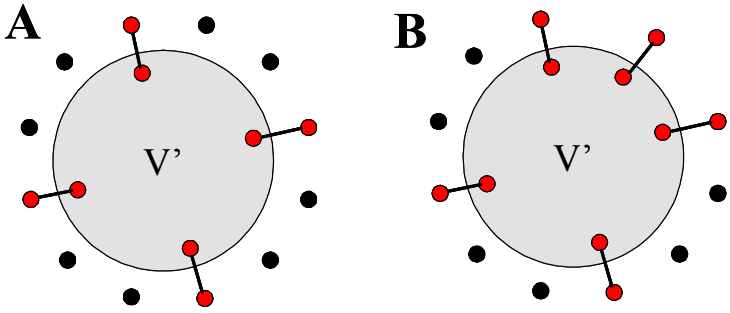
Pierādījums: Ja apakškopu veido ņemot no katra sarkanā virsotņu pāra vienu virsotni, tad tiek iegūta virsotņu apakškopa ar izmēru n/4, kas ir virsotņu pārklājums ar nepieciešamo izmēru.

Lemma 1-7. *Ja grafs G=(V,E), |V|=n, K=n/4 apmierina sekojošus nosacījumus:*
- *tajā ir n/2-2 savstarpēji nesaistītas (melnas) virsotnes,*
- *tajā ir n/2+2 (sarkanas) virsotnes, kas ir pa pāriem savienotas,*

tad dotajā grafā neeksistē virsotņu pārklājums, atbilstošs problēmai-6.

Pierādījums: Tā kā dotajā grafā ir n/2+2 sarkanas virsotnes, kas ir pa pāriem savienotas, tad grafā kopā ir n/4+1 šķautne. Vismaz vienam no katras šķautnes galapunktam ir jāpieder izvēlētajai virsotņu apakškopai, tātad tās minimālais izmērs ir n/4+1, bet tas ir lielāks par prasīto izmēru.

Teorēma 1-10. *Problēmas par virsotņu pārklājuma atrašanu atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*



1.2.4. att. **Kopu A un B piemērs problēmai par virsotņu pārklājumu**

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:
Kopa A satur visus grafus G, kas apmierina Lemmas 1-6 nosacījumus. Kopa B satur visus grafus G', kas apmierina Lemmas 1-7 nosacījumus. Zīmējumā 1.2.4. var redzēt divus grafus, no kuriem viens pieder kopai A, bet otrs kopai B.

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams savienot divas patvaļīgas melnās virsotnes. Šādu virsotņu skaits ir n/2, starp šādām virsotnēm šķautnes ir iespējams novilkt n/2(n/2-1)/2 dažādos veidos tātad m= $O(n^2)$.
Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu, kas piederētu kopai A, ir nepieciešams izmest vienu šķautni. Grafā ir n/4+1 šķautne, tātad m'=O(n).

No teorēmas A1 seko, ka problēmas par virsotņu pārklājuma atrašanu atrisināšanai ir nepieciešami $\Omega\sqrt{n^2 \cdot n}$ =$\Omega(n^{1.5})$ kvantu jautājumi.

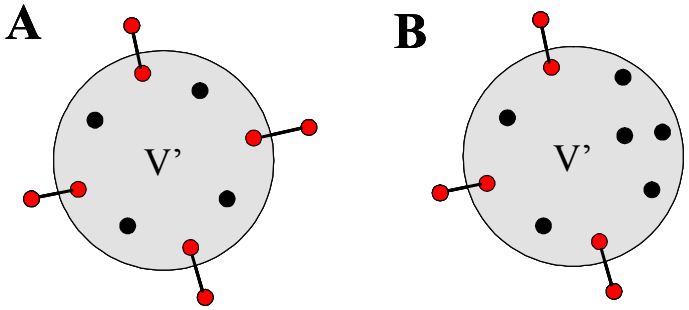
Teorēma 1-11. *Problēmas par virsotņu pārklājuma atrašanu apakšējo novērtējumu kvantu gadījumā nav iespējams uzlabot lietojot Ambaiņa metodi.*

Pierādījums: Pierādījumā tiek izmantota Teorēma A3.
$ND_1(f) = O(n^2)$, jo ir nepieciešams pārbaudīt visas šķautnes, lai parādītu virsotņu pārklājuma problēmas atrisinājumu.
$ND_0(f) = O(n)$, lai pierādītu, ka grafā neeksistē virsotņu pārklājums ar doto izmēru K ir pietiekams parādīt, ka eksistē lielāks virsotņu pārklājums.
Tātad $\sqrt{ND_1(f) \cdot ND_0(f)} = O(n^{1.5})$.

1.2.7. Dominējošās kopas atrašanas problēma

Problēma-7:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis K, tāds, ka K≤|V|.
Jautājums – Vai šajā grafā G eksistē Dominējošā virsotņu kopa ar izmēru K vai mazāku? Tas ir vai eksistē virsotņu apakškopa V'⊆V ar izmēru |V'|≤K tāda, ka visiem u∈V-V' eksistē v∈V', kurai {u,v}∈E?

Teorēma 1-12. *Problēmas par Dominējošās kopas atrašanu atrisināšanai ir nepieciešami* $\Omega(n^{1.5})$ *kvantu jautājumi.*



1.2.5. att. **Kopu A un B piemērs problēmai par Dominējošās kopas atrašanu**

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1 prasībām:

Kopa A satur visus grafus G, kas apmierina sekojošus nosacījumus:

- tajā ir n/3 savstarpēji nesaistītas (melnas) virsotnes,
- tajā ir 2n/3(sarkanas) virsotnes, kas ir pa pāriem savienotas,
- K=2n/3.

Funkcijas vērtība, kas atbilst problēmai par Dominējošās kopas atrašanu, ir 1. Dominējošā kopa tiek veidota no visām melnajām virsotnēm, tām pievienojot pa vienai virsotnei no katra sarkanā virsotņu pāra. Šīs kopas izmērs ir 2n/3, un tā apmierina Dominējošai kopai uzliktos nosacījumus.

Kopa B satur visus grafus G', kas apmierina sekojošus nosacījumus.

- tajā ir n/3+2 savstarpēji nesaistītas (melnas) virsotnes,
- tajā ir n/3-2(sarkanas) virsotnes, kas ir pa pāriem savienotas,
- K=2n/3.

Funkcijas vērtība, kas atbilst problēmai par Dominējošās kopas ar doto izmēru atrašanu, ir 0. Dotajā gadījumā minimālā Dominējošā kopa ir ar izmēru 2n/3+1, jo šajā kopā ir jābūt visām melnajām virsotnēm un vismaz pa vieni no katra sarkano virsotņu pāra. Bet 2n/3+1ir lielāks par2n/3. Zīmējumā 1.2.5. var redzēt divus grafus, no kuriem viens pieder kopai A, bet otrs kopai B.

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams izmest vienu no šķautnēm, kas savieno sarkanās virsotnes. Šādu šķautņu skaits ir n/3, tātad m= O(n). Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu, kas piederētu kopai A, ir nepieciešams izveidot šķautni starp divām patvaļīgām melnajām virsotnēm. Kopīgais dažādo iespējamo jauno šķautņu skaits ir (n/3+2)(n/3+1)/2. Tātad m'=O(n^2).

No teorēmas A1 seko, ka problēmas par Dominējošās kopas atrašanu atrisināšanai ir nepieciešami $\Omega\sqrt{n \cdot n^2}$ =Ω($n^{1.5}$) kvantu jautājumi.

Teorēma 1-13. *Problēmas par Dominējošās kopas atrašanu apakšējo novērtējumu kvantu gadījumā nav iespējams uzlabot lietojot Ambaiņa metodi.*

Pierādījums: Pierādījumā tiek izmantota Teorēma A3.
$ND_1(f) = O(n^2)$, lai pierādītu, ka izvēlētā kopa atbilst Dominējošās kopas nosacījumiem ir nepieciešams pārbaudīt visas šķautnes, kuru galapunkti atrodas ārpus šīs kopas. $ND_0(f) = O(n)$, lai pierādītu, ka dotajā grafā nevar izveidot Dominējošo kopu ar doto izmēru, pietiek pierādīt, ka minimālais Dominējošās kopas izmērs ir lielāks par doto.
Tātad $\sqrt{ND_1(f) \cdot ND_0(f)} = O(n^{1.5})$.

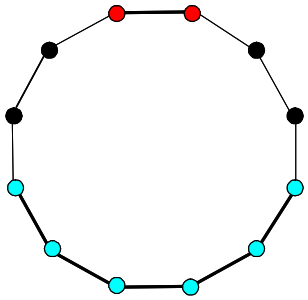
1.2.8. Virsotņu nokrāsošanas problēma

Problēma-8:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis k, tāds, ka k≤|V|.
Jautājums – vai eksistē tāda funkcija f: V→{1,2,…k}, ka f(u)≠f(v) , ja {u,v}∈E?

Lemma 1-8. *Ja grafs G_1 satur vienu ciklu un grafs G_2 satur divus ciklus, tad šo grafu atšķiršanai būs nepieciešami Ω($n^{1.5}$) kvantu jautājumi.*

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A2 prasībām:

Kopa A satur visus tādus grafus G=(V,E), |V|=n, kas satur tikai Hamiltona ciklu. Kopa B satur grafus G', kas apmierina sekojošus nosacījumus. Katrs grafs G' ir veidots kā apvienojums no diviem grafiem G''=(V'',E''), |V''|=O(n), kuri abi grafi satur tikai Hamiltona ciklus.



1.2.6. att. **Kopas A piemērs Lemmai 1-8**

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams veikt divas darbības. Izvēlamies vienu patvaļīgu šķautņu (iezīmētas sarkanās virsotnes) un izdzēšam šo šķautni. Šai darbībai ir iespējami n dažādi varianti. Atzīmējam ar zilu krāsu tās virsotnes, kas atrodas pretī izmestajai virsotnei tā, lai šķautņu skaits būtu n/3. Tad izmetam vienu no šīm šķautnēm. To ir iespējams izdarīt n/3 dažādos veidos. Katru no palikušajām šķautņu virknēm apvienojam ciklā. Tātad $m=n*n/2=O(n^2)$.

Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu G, kas piederētu kopai A, ir nepieciešams katrā no grafa G' esošajiem cikliem izmest vienu šķautni, un apvienot iegūtos šķautņu fragmentus vienā ciklā. Šādas darbības ir iespējams veikt $\sim n^2$ dažādos veidos, jo katrs no cikliem ir ar kārtu n. Tātad $m'=O(n^2)$.

Vēl ir nepieciešams atrast max(l*l'). Katrai šķautnei, kas tiek izmesta pirmajā solī l=n/3, jo to var izdarīt n/3 dažādās kombinācijās ar citām šķautnēm, bet l'=const, jo šo šķautni var atjaunot tikai konstantā skaitā variantu. Katrai šķautnei, kas tiek izveidota pirmajā solī l=const, bet l'=O(n), jo mēs varam šo šķautni izmest kombinācijā ar visām citām šķautnēm no otra cikla. Tātad max(l*l')=O(n).

No teorēmas A2 seko, ka dotās problēmas atrisināšanai ir nepieciešami $\Omega\sqrt{\frac{n^2 * n^2}{n}}=\Omega(n^{1.5})$ kvantu jautājumi.

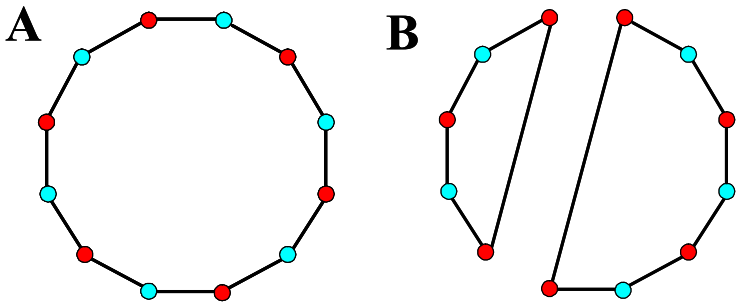
Lemma 1-9. *Ja grafs G=(V,E), |V|=2n satur tikai Hamiltona ciklu, tad šī grafa virsotnes var nokrāsot, atbilstoši problēmai-8, ja krāsu skaits ir 2.*

Pierādījums: Virsotnes ir jānokrāso divās krāsās ejot pa doto Hamiltona ciklu un mainot šīs krāsas pēc kārtas. Dotais virsotņu krāsojums apmierinās virsotņu nokrāsošanas problēmu.

Lemma 1-10. *Ja grafs G(V,E), |V|=2n+1 satur tikai Hamiltona ciklu, tad šī grafa virsotnes nevar nokrāsot, atbilstoši problēmai-8, ja krāsu skaits ir 2.*

Pierādījums: Lai arī kā virsotnes tiktu nokrāsotas, būs vismaz divas vienas krāsas virsotnes, kas būs savienotas ar šķautni.

Teorēma 1-14. *Problēmas par virsotņu nokrāsošanu atrisināšanai ir nepieciešami* $\Omega(n^{1.5})$ *kvantu jautājumi.*



1.2.7. att. **Kopu A un B piemērs problēmai par virsotņu nokrāsošanu**

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:

Kopa A satur visus grafus G, kas apmierina Lemmas 1-9 nosacījumus. Kopa B satur visus grafus G', kas ir veidoti apvienojot divus grafus $G_1=(V_1,E_1)$ un $G_2=(V_2,E_2)$, kuri apmierina Lemmas 1-10 nosacījumus un $|V_1|+|V_2|=|V|$ un $O(|V_1|)=O(|V|)$ un $O(|V_2|)= O(|V|)$. Zīmējumā 1.2.7. var redzēt divus grafus, no kuriem viens pieder kopai A, bet otrs kopai B.

No Lemmas 1-8. seko, ka virsotņu nokrāsošanas problēmas atrisināšanai ir nepieciešami $\Omega\sqrt{n^2 \cdot n} = \Omega(n^{1.5})$ kvantu jautājumi.

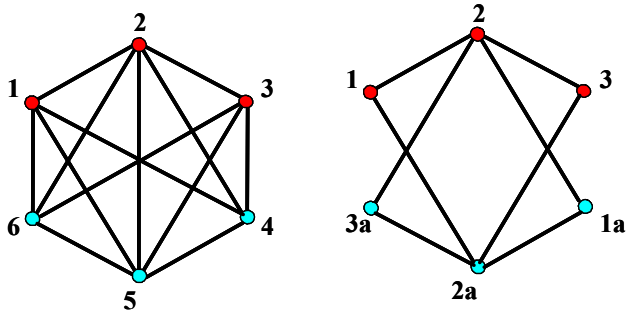
Teorēma 1-15. *Problēmas par virsotņu nokrāsošanu apakšējo novērtējumu kvantu gadījumā nav iespējams uzlabot lietojot Ambaiņa metodi.*

Pierādījums: Pierādījumā tiek izmantota Teorēma A3.
$ND_1(f) = O(n^2)$, jo ir nepieciešams pārbaudīt visas šķautnes, lai parādītu, ka dotais virsotņu nokrāsojums atbilst prasībām.
$ND_0(f) = O(n)$, lai pierādītu, ka dota grafu nevar nokrāsot divās krāsās, ir pietiekams, ja šajā grafā tiek uzrādīts cikls ar nepāra skaitu šķautņu.
Tātad $\sqrt{ND_1(f) \cdot ND_0(f)} = O(n^{1.5})$.

1.2.9. Vienkrāsaina trīsstūra eksistences problēma

Problēma-9:
Dots - Grafs G=(V,E).
Jautājums – Vai eksistē tāds grafa G šķautņu kopas E sadalījums divās nešķeļošās apakškopās E_1, E_2 tāds, ka ne $G_1=(V,E_1)$, ne $G_2=(V,E_2)$ nesatur trīsstūri?

Grafs G=(V,E), |V|=3n tiek veidots sekojoši. Visas grafa virsotnes tiek sadalītas trijniekos. Katrs no šiem trijniekiem tiek savienots ar citiem trijniekiem vienā no dotajiem veidiem (zīmējums 1.2.8.) . Katrs no šiem trijniekiem nesatur trīsstūri. Apakškopas E_1 un E_2 tiks veidotas neizjaucot šos trijniekus.

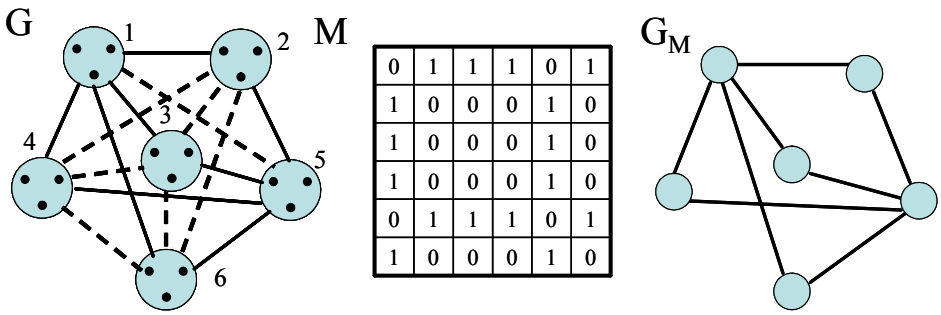


1.2.8. att. **Kopu A un B piemērs problēmai par vienkrāsaina trīsstūra eksistenci**

Lemma 1-11. *Ja vienkrāsainā trijstūra problēma nav atrisināma šādā grafa sadalījumā trijniekus, tad tā nav atrisināma arī citā sadalījumā trijniekos.*

Pierādījums: Ja tiek savā starpā mainīta kāda no virsotnēm 1,2,3 ar kādu no virsotnēm 4,5,6, tad vismaz vienā no jaunizveidotajiem virsotņu trijniekiem būs trīsstūris, vai arī problēmas atrisinājums nemainīsies. Ja tiek mainītas savā starpā kādas no virsotnēm 1,2,3 ar 1a,2a,3a, tad vienkrāsainā trijstūra problēmas atrisinājums nemainās.

Tātad pietiek pierādīt apakšējo novērtējumu pēc dotā principa veidotos grafos. Katram grafam G tiek piekārtota matrica M, kas tiek veidota sekojoši. Matricā ir tik rindu un kolonnu, cik grafā G trijnieku, t.i. |V|/3. Matricā m_{ij} vērtība ir 1, ja trijnieks v_i ir savienots ar trijnieku v_j pirmajā savienošanas veidā. Ja trijnieki ir savienoti otrajā savienošanas veidā, tad matricā atbilstošajā vietā ir 0. Izmantojot iegūto matricu M, tiek izveidots grafs G_M. Grafa G_M veidošanas piemēru var redzēt zīmējumā 1.2.9.



1.2.9. att. **Vienkrāsainā trīsstūra problēmas reducēšana un virsotņu nokrāsošanu**

Lemma 1-12. *Ja grafā G_M ir atrisināma virsotņu nokrāsošanas problēma divu krāsu gadījumam, tad atbilstošajā grafā G ir atrisināma vienkrāsainā trijstūra problēma.*

Pierādījums: Katra grafa G_M virsotne atbilst grafa G virsotņu trijniekam. Tātad, ja grafā G_M ir atrisināma virsotņu nokrāsošanas problēma divu krāsu gadījumā, tad var grafa G_M virsotnes nokrāsot divās krāsās tā, lai divas vienā krāsā nokrāsotas virsotnes nebūtu saistītas. Vienā virsotņu apakškopā ir jāliek tie grafa G virsotņu trijnieki, kuriem atbilstošās virsotnes grafā G_M ir nokrāsotas vienā krasā. Tātad vienā apakškopā ir nonākuši tikai tādi virsotņu trijnieki, kas ir savienoti savā starpā otrajā savienošanas veidā. Tas nozīmē, ka šajā apakškopā nav trijnieku.

Lemma 1-13. *Ja grafā G_M nav atrisināma virsotņu nokrāsošanas problēma divu krāsu gadījumam, tad atbilstošajā grafā G nav atrisināma vienkrāsainā trijstūra problēma.*

Pierādījums: Pieņemsim, ka grafā G ir atrisināma vienkrāsainā trijstūra problēma, ja virsotņu sadalījums trijniekos ir savādāks. Tomēr Lemmā 1-11 ir pieradīts, ka mainot trijnieku sadalījumu nav iespējams uzlabot vienkrāsainā trijstūra problēmas atrisinājumu, tātad arī šī problēma ir atrisināma arī tajā trijnieku sadalījumā, kas atbilst grafam G_M. Bet tad ir atrisināma arī virsotņu nokrāsošanas problēma grafa G_M. Tiek iegūta pretruna ar pieņemto.

Teorēma 1-16. *Problēmas par vienkrāsaino trijstūri atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*

Pierādījums: No Lemmām 1-12 un 1-13 seko, ka vienkrāsainā trijstūra problēmas sarežģītība ir ekvivalenta problēmas par virsotņu nokrāsošanu sarežģītībai. Tātad sarežģītība ir $\Omega(n^{1.5})$.

1.2.10. Minimuma no maksimālās savienošanas pa pāriem noskaidrošana

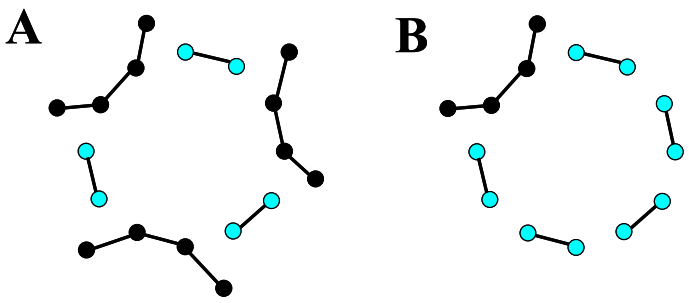
Problēma-10:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis K, tāds, ka K≤|V|.
Jautājums – Vai eksistē tāda grafa G šķautņu apakškopa E'⊆ E ar izmēru K vai mazāku tāda, lai E' ir maksimālais savienojums pa pāriem? Tas ir, neeksistē divas E' šķautnes ar kopīgu galapunktu, un katrai šķautnei no E-E' ir kopīgs galapunkts ar kādu no kopas E' šķautnēm.

Lemma 1-14. *Ja grafs G=(V,E), |V|=6n, K=2n apmierina sekojošus nosacījumus:*

- *tajā ir 2n pa pāriem saistītas (zilas) virsotnes,*
- *tajā ir 4n (melnas) virsotnes, kas ir sadalītas grupās pa četri, un katra virsotņu grupa ir savienota ar trīs šķautnēm (•-•-•-•),*

tad dotajā grafā ir atrisināma problēma par minimumu no maksimālās savienošanas pa pāriem .

Pierādījums: Apakškopa E' tiek veidota sekojoši, tajā tiek apvienotas visas šķautnes, kas savieno zilās virsotnes (n šķautnes) un vidējas šķautnes no katras melno virsotņu grupas (n virsotnes). Tiek iegūta šķautņu kopa ar izmēru 2n, kas apmierina minimuma no maksimālās savienošanas pa pāriem problēmu.



1.2.10. att. **Kopu A un B piemērs problēmai-10**

Lemma 1-15. *Ja grafs G=(V,E), |V|=6n, K=2n apmierina sekojošus nosacījumus:*

- *tajā ir 2n+4 pa pāriem saistītas (zilas) virsotnes,*
- *tajā ir 4n-4 (melnas) virsotnes, kas ir sadalītas grupās pa četri, un katra virsotņu grupa ir savienota ar trīs šķautnēm (•-•-•-•),*

tad dotajā grafā nav atrisināma problēma par minimumu no maksimālās savienošanas pa pāriem .

Pierādījums: Ārpus kopas E' var palikt tikai divas malējās šķautnes no katras melno virsotņu grupas. Visas pārējās šķautnes ir nepieciešams apvienot kopā E'. Tātad kopas E' izmērs ir 2n+1 (n+2 no zilajām virsotnēm un n-1 vidējās no melnajām virsotņu kopām).

Iegūtās kopas izmērs ir lielāks par prasīto K vērtību, tātad grafā nav atrisināma problēma par minimumu no maksimālās savienošanas pa pāriem .

Teorēma 1-17. *Problēmas par minimumu no maksimālās savienošanas pa pāriem atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:

Kopa A satur visus grafus G, kas apmierina Lemmas 1-14 nosacījumus. Kopa B satur visus grafus G', kas apmierina Lemmas 1-15 nosacījumus. Zīmējumā 1.2.10. var redzēt divus grafus, no kuriem viens pieder kopai A, bet otrs kopai B.

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams izmest vidējo šķautni kādā no melno virsotņu četriniekiem. Šādu četrinieku skaits ir n, tātad m= O(n). Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu, kas piederētu kopai A, ir nepieciešams savienot ar šķautni jebkuras divas zilās virsotnes. To var izdarīt (2n+4)(2n+2)/2 dažādos veidos, tātad m'=$O(n^2)$.
No teorēmas A1 seko, ka problēmas par minimumu no maksimālās savienošanas pa pāriem atrisināšanai ir nepieciešami $\Omega\sqrt{n^2 \cdot n} = \Omega(n^{1.5})$ kvantu jautājumi.

Teorēma 1-18. *Problēmas par minimumu no maksimālās savienošanas pa pāriem apakšējo novērtējumu kvantu gadījumā nav iespējams uzlabot lietojot Ambaiņa metodi.*

Pierādījums: Pierādījumā tiek izmantota Teorēma A3.
$ND_1(f) = O(n^2)$, jo ir nepieciešams pārbaudīt visas šķautnes, lai parādītu, ka izvēlētā šķautņu apakškopa apmierina minimuma no maksimālās savienošanas pa pāriem prasības.
$ND_0(f) = O(n)$, jo ir jāuzrāda K+1 virsotne, no kuras iziet divas šķautnes.
Tātad $\sqrt{ND_1(f) \cdot ND_0(f)} = O(n^{1.5})$

1.2.11. Sadalīšana izomorfos apakšgrafos

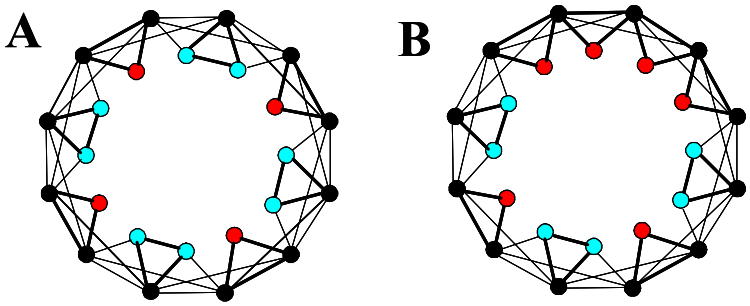
Problēma-11:
Dots - Grafs G=(V,E) un H=(V',E') , kur |V|=q|V'| un q ir vesels pozitīvs skaitlis.
Jautājums – Vai grafa G virsotnes var sadalīt q nešķeļošās kopās $V_1, V_2, .. V_q$ tā, lai katram i, $1 \le i \le q$, kopas V_i noteiktais apakšgrafs ir izomorfs ar H?

Teorēma 1-19. *Problēmas par sadalīšanu izomorfos apakšgrafos atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*

Pierādījums: Problēmas par sadalīšanu izomorfos apakšgrafos apakšējais novērtējums ir vienāds ar problēmas par sadalīšanu trīsstūros apakšējo novērtējumu. Ja ņem H=(V',E'), V'={u,v,w} un E'={{u,v},{v,w}, {w,u}}, tad problēma par sadalīšanu izomorfos apakšgafos reducējas uz problēmu par sadalīšanu trīsstūros. Tātad problēmas par sadalīšanu izomorfos apakšgrafos atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.

1.2.12. Problēma par sadalīšana Hamiltona apakšgrafos

Problēma-12:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis K, tāds, ka K≤|V|.
Jautājums – Vai grafa G virsotnes var sadalīt k≥K nešķeļošās kopās $V_1, V_2, .. V_k$ tā, lai katra V_i saturētu vismaz trīs virsotnes un katras kopas V_i noteiktais apakšgrafs saturētu Hamiltona ciklu?



1.2.11. att. **Kopu A un B piemērs problēmai par sadalīšanu Hamiltona apakšgrafos**

Teorēma 1-20. *Problēmas par sadalīšanu Hamiltona apakšgrafos atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*

Pierādījums: Ja grafs *G=(V,E), |V|=3k=n* apmierina sekojošus nosacījumus (grafs zīmējuma 1.2.11. kreisajā pusē):

- tajā ir k/2 savstarpēji nesaistītas (sarkanas) virsotnes,
- tajā ir k(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,
- pārējām (melnas) virsotnēm atbilstošais apakšgrafs ir pilns grafs, un visas melnās virsotnes ir savienotas ar sarkanajām un zilajām virsotnēm,

tad problēma par sadalīšanu Hamiltona apaksgrafos ir atrisināma. Virsotņu sadalījums tiek veidots sekojoši. Vienā kopā ievieto divas zilās virsotnes un vienu melno virsotni, vai vienu sarkano virsotni un divas melnās virsotnes. Katra no šīm virsotņu kopām saturēs trīsstūri, kas dotajā kopu apjomā ir arī Hamiltona cikls.

Ja grafs *G=(V,E), |V|=3k=n* apmierina sekojošus nosacījumus (grafs zīmējuma 1.2.11. labajā pusē):

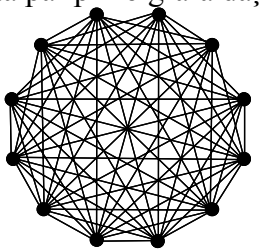
- tajā ir k/2+2 savstarpēji nesaistītas (sarkanas) virsotnes,
- tajā ir k-2(zilas) virsotnes, kas ir pa pāriem savienotas un nav savienotas ar sarkanajām virsotnēm,
- pārējām (melnas) virsotnēm atbilstošais apakšgrafs ir pilns grafs, un visas melnās virsotnes ir savienotas ar sarkanajām un zilajām virsotnēm,

tad problēma par sadalīšanu Hamiltona apaksgrafos nav atrisināma, jo katru sarkano virsotni un katru zilo virsotņu pāri ir nepieciešams ievietot savā apakškopā un melno virsotņu skaits ir nepietiekams, lai katrā apakškopā būtu vismaz trīs virsotnes. Apakškopu skaits ir k/2+2+(k-2)/2=k+1, bet melno virsotņu skaits ir 2k. Tātad problēma par sadalīšanu Hamiltona apakšgrafos reducējas uz problēmu par sadalīšanu trīsstūros un problēmas atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.

1.2.13. Dominējošo kopu skaita noskaidrošana

Definīcija: ***Cn-m*** *ir n virsotņu grafs, kurš tiek izveidots no pilna grafa, izmetot m šķautnes tā, lai izmestajām šķautnēm nebūtu kopīgu galapunktu.*

Katru grafu Cn-m var izvietot sekojoši – zīmējums 1.2.12. Grafa apakšējā daļa, kura nesatur izmestās šķautnes tiek saukta par pilno grafa daļu.



1.2.12. att. **Grafa Cn-m izvietojums**

Lemma 1-16. *Ja m=O(n) tad grafa Cn-m un grafa Cn-(m+1) atšķiršanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:
Kopa A satur visus grafus Cn-m. Visi šie grafi ir savā starpā izomorfi. Kopa B satur visus grafus Cn-(m+1).

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams atvienot vienu no grafa pilnās daļas virsotnēm. Tātad $m=O(n^2)$. Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu G, kas piederētu kopai A, ir nepieciešams savienot divas nesavienotās virsotnes. Tātad m'=O(n).

No teorēmas A1 seko, ka problēmas par minimumu no maksimālās savienošanas pa pāriem atrisināšanai ir nepieciešami $\Omega\sqrt{n^2 \cdot n} = \Omega(n^{1.5})$ kvantu jautājumi.

Problēma-13:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis K, tāds, ka K≤|V|.
Jautājums - Vai grafa G virsotnes var sadalīt k≥K nešķeļošās kopās $V_1, V_2, .. V_k$ tā, lai katra V_i būtu grafa G Dominējošā kopa? (Dominējošā kopa ir virsotņu apakškopa V' tāda, ka visiem u∈V-V' eksistē v∈V', kurai {u,v}∈E.)

Lemma 1-17. *Dominējošo kopu skaita problēma ir atrisināma jebkurā grafā Cn-m ja* $m \leq K \leq n-m$.

Pierādījums: Virsotnes tiek sadalītas kopās sekojoši:

- katrs virsotņu pāris, kas nav savienots ar šķautni – atsevišķā kopā (m kopas).
- atlikušās virsotnes var tikt sadalītas pa kopām vairākos veidos. Tās var tikt pievienotas jau izveidotajām kopām (nepalielinot kopu skaitu) vai tas var tikt ievietotas jaunās kopās (maksimālais kopu skaits ir n-2m).

Katra no šādi izveidotajām kopām ir dotā grafa Dominējošā virsotņu kopa. Maksimālais šādu kopu skaits ir n-m. Ja $m \leq K \leq n-m$, tad Dominējošo kopu skaitļa problēma ir atrisināma.

Lemma 1-18. *Dominējošo kopu skaita problēma nav atrisināma grafā Cn-(m+1) ja* $K \geq n-m$.

Pierādījums: Virsotnes tiek sadalītas kopās tāpat kā Lemmā 1-17. Maksimālais kopu skaits ir n-(m+1), bet tas ir mazāks par K.

Teorēma 1-21. *Problēmas par Dominējošo kopu skaitu atrisināšanai ir nepieciešami* $\Omega(n^{1.5})$ *kvantu jautājumi.*

Pierādījums: Ja K = n-m, tad Dominējošo kopu skaita problēma ir atrisināma grafā Cn-m, kas seko no Lemmas 1-17, bet nav atrisināma grafā Cn-(m+1), kas seko no Lemmas 1-18. Bet Lemma 1-16 apgalvo, ka dotie grafi ir atšķirami ar $\Omega(n^{1.5})$ kvantu jautājumiem, tātad problēmas par Dominējošo kopu skaitu atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.

1.2.14. Problēma par Ahromatisko skaitli

Problēma-14:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis K, tāds, ka K≤|V|.
Jautājums - Vai grafa G virsotnes var sadalīt k≥K nešķeļošās kopās $V_1,V_2, .. V_k$ tā, lai katra V_i būtu grafa G Natkarīgā kopa, un jebkuram divu dažādu virsotņu kopu pārim V_i,V_j, $V_i \cup V_j$ nebūtu grafa G Neatkarīgā kopa (tāda grafa virsotņu apakškopa, ka jebkuras divas šīs apakškopas virsotnes nav savienotas ar šķautni) ?

Teorēma 1-22. *Problēmas par Ahromatisko skaitli atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:
Kopa A satur visus grafus Cn-m. Virsotnes var tikt sadalītas kopās sekojoši:

- katrs nesavienoto virsotņu pāris sava kopā (m kopas)
- katra atlikusī virsotne savā kopā (n-2m kopas).

Šis sadalījums kopās (n-m kopas) apmierina Ahromatiskā skaitļa problēmu, ja K= n-m, un šis ir vienīgais iespējamais sadalījums dotajai problēmai.

Kopa B satur visus grafus Cn-(m+1). Virsotnes tiek dalītas kopās tāpat kā kopas A gadījumā. Vienīgais sadalījums kopās satur n-(m+1) kopu, bet ja K=n-m, tad Ahromatiskā skaitļa problēma nav atrisināma, jo ir jāizveido vismaz n-m kopas.

No Lemmas 1-16 seko, ka kopu A un B atšķiršanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi. No teorēmas A1 seko, ka problēmas par Ahromatisko skaitli atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.

1.2.15. Problēma par Frakcijas atrašanu

Problēma-15:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis k, tāds, ka K≤|V|.
Jautājums – Vai grafs G satur Frakciju, kuras izmērs ir K vai lielāks? Tas ir vai grafā G eksistē virsotņu apakškopa V'⊆V ar izmēru |V'|≤|V| tāda, ka katras divas šīs apakškopas V' virsotnes ir savienotas ar šķautni no E?

Teorēma 1-23. *Problēmas par Frakcijas atrašanu atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi.*

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:
Kopa A satur visus grafus Cn-m. Šajā gadījumā maksimālais Frakcijas izmērs ir n-m. Frakcija tiek veidota sekojoši – tajā ietilpst visa grafa Cn-m pilnā daļa (n-2m virsotnes) un viena virsotne no katra nesavienoto virsotņu pāra. Izveidotās kopas izmērs ir n-m. Ja K= n-m, tad problēma par Frakcijas atrašanu ir atrisināma.

Kopa B satur visus grafus Cn-(m+1). Maksimālais Frakcijas izmērs ir n-(m+1). Ja K=n-m, tad problēma par Frakcijas atrašanu nav atrisināma.

No Lemmas 1-16 seko, ka kopu A un B atšķiršanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi. No teorēmas A1 seko, ka problēmas par Frakcijas atrašanu atrisināšanai ir nepieciešami $\Omega(n^{1.5})$ kvantu jautājumi

1.2.16. Neatkarīgās kopas atrašanas problēma

Problēma-16:
Dots - Grafs G=(V,E), vesels pozitīvs skaitlis K, tāds, ka K≤|V|.
Jautājums - Vai grafs G satur Neatkarīgo kopu, kuras izmērs ir K vai lielāks? Tas ir vai grafā G eksistē virsotņu apakškopa V'⊆V ar izmēru |V'|≤|V| tāda, ka jebkuras divas šīs apakškopas V' virsotnes nav savienotas ar šķautni ?

Lemma 1-19. *Ja grafs G=(V,E), |V|=3n, K=2n apmierina sekojošus nosacījumus:*
- *tajā ir n melnas savstarpēji nesaistītas virsotnes,*
- *tajā ir 2n sarkanas pa pāriem savienotas virsotnes,*

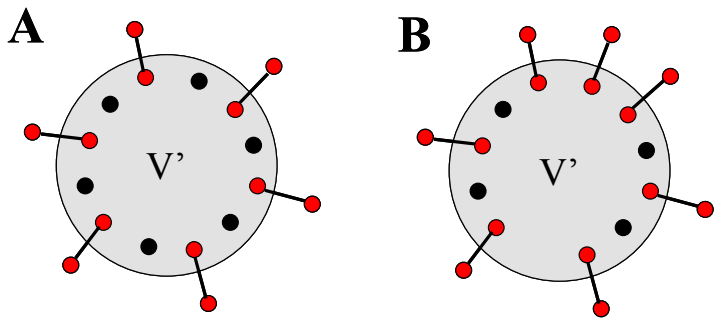
tad Neatkarīgās kopas atrašanas problēma ir atrisināma.

Pierādījums: Neatkarīgo kopu ar var izveidot sekojoši. Tajā tiek ievietotas visas melnās virsotnes un pa vienai virsotnei no katra sarkano virsotņu pāra. Izveidotās kopas izmērs ir 2n. Tātad Neatkarīgās kopas atrašanas problēma ir atrisināma.

Lemma 1-20. *Ja grafs G=(V,E), |V|=3n, K=2n apmierina sekojošus nosacījumus:*
- *tajā ir n-2 melnas savstarpēji nesaistītas virsotnes,*
- *tajā ir 2n+2 sarkanas pa pāriem savienotas virsotnes,*

tad Neatkarīgās kopas atrašanas problēma nav atrisināma.

Pierādījums: Maksimālais Neatkarīgās kopas izmērs dotajā gadījumā ir 2n-1, jo kopā var ievietot visas melnās virsotnes, bet no katra sarkano virsotņu pāra tikai pa vienai. Tā kā izveidotās kopas izmērs ir mazāks par K, tad Neatkarīgās kopas atrašanas problēma nav atrisināma.



1.2.13. att. **Kopu A un B piemērs Neatkarīgās kopas atrašanai**

Teorēma 1-24 *Problēmas par Neatkarīgās kopas atrašanu atrisināšanai ir nepieciešami* $\Omega(n^{1.5})$ *kvantu jautājumi.*

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:
Kopa A satur visus grafus G, kas apmierina Lemmas 1-19 nosacījumus. Kopa B satur visus grafus G', kas apmierina Lemmas 1-20 nosacījumus. Zīmējumā 1.2.13. var redzēt divus grafus, no kuriem viens pieder kopai A, bet otrs kopai B.

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams savienot kādu melno virsotņu pāri. To var izdarīt (n-2)(n-3)/2 dažādos veidos, tātad $m=O(n^2)$. Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu, kas piederētu kopai A, ir nepieciešams izmest vienu no sarkanās virsotnes savienojošajām šķautnēm. Šādu šķautņu ir n, tātad m'=O(n).

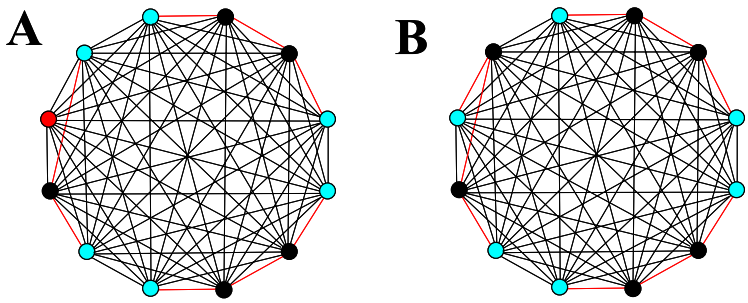
No teorēmas A1 seko, ka problēmas par Neatkarīgās kopas atrašanu atrisināšanai ir nepieciešami $\Omega\sqrt{n^2 \cdot n} = \Omega(n^{1.5})$ kvantu jautājumi.

1.2.17. Pilnas zvaigznes atrašanas problēma

Problēma-17:
Dots - Grafs G=(V,E).
Jautājums – Vai grafs G satur tādu virsotni v* ka, visām virsotnēm $u \subseteq V-v^*$ - šķautne $\{u,v^*\} \in E$?

Definīcija: Teiksim, ka virsotnei ir tips v_n , ja tā ir savienota ar visām pārējām virsotnēm, tips v_{n-1} , ja virsotne ir savienota ar visām pārējām virsotnēm, izņemot vienu, tips v_{n-2} , ja virsotne ir savienota ar visām pārējām virsotnēm, izņemot kādas divas virsotnes.

Teorēma 1-24 *Problēmas par pilnas zvaigznes atrašanu atrisināšanai ir nepieciešami* $\Omega(n)$ *kvantu jautājumi.*



1.2.14. att. **Kopu A un B piemērs pilnas zvaigznes atrašanai**

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, prasībām:
Kopa A satur visus grafus, kas satur vienu virsotni ar tipu v_n (sarkana), n/2 virsotnes ar tipu v_{n-1}(zila) un n/2-1 virsotni ar tipu v_{n-2}(melna). Šajos grafos ir atrisināma pilnas zvaigznes atrašanas problēma, jo virsotne ar tipu v_n atbilst virsotnei v* izvirzītajām prasībām.

Kopa B satur visus grafus, kas satur n/2 virsotnes ar tipu v_{n-1} (zila) un n/2 virsotnes ar tipu v_{n-2} (melna). Šajos grafos problēma par pilnas zvaigznes atrašanu nav atrisināma

Zīmējumā 1.2.14. var redzēt divus grafus, no kuriem viens pieder kopai A, bet otrs kopai B. Virsotnes ar tipu v_n ir attēlotas sarkanā krāsā, virsotnes ar tipu v_{n-1} – zilā, bet virsotnes ar tipu v_{n-2} – melnā krasā. Neeksistējošās šķautnes ir attēlotas sarkanā krāsā.

Lai jebkuru grafu G, kas pieder kopai A, pārveidotu par grafu G', kas piederētu kopai B, ir nepieciešams izmest vienu šķautni, kas savieno virsotni ar tipu v_n ar kādu virsotni ar tipu v_{n-1}. Katrai no šīm virsotnēm tips samazināsies par vienu. To var izdarīt n-2 dažādos veidos, tātad m=O(n). Lai jebkuru grafu G', kas pieder kopai B, pārveidotu par grafu, kas piederētu kopai A, ir nepieciešams izvēlēties vienu no virsotnēm ar tipu v_{n-1} un pārveidot to par virsotni ar tipu v_n, izveidojot trūkstošo šķautni. Virsotņu ir tipu v_{n-1} ir n/2, tātad m'=O(n).

No teorēmas A1 seko, ka problēmas par pilnas zvaigznes atrašanu atrisināšanai ir nepieciešami $\Omega\sqrt{n \cdot n} = \Omega(n)$ kvantu jautājumi.

2. KVANTU ALGORITMU VEIDOŠANAS PRINCIPI

2.1. Kvantu vaicājošie algoritmi

Vaicājošie algoritmi ir algoritmu veids, kas ir domāts Bula funkciju rēķināšanai. Katrs algoritms tiek veidots kādas konkrētas funkcijas rēķināšanai. Funkcijas mainīgo vērtības nav zināmas, tās atrodas „melnajā kastē". Algoritms var uzdot jautājumu un uzzināt konkrēta mainīgā vērtību. Veidojot algoritmus mērķis ir izveidot tos ar iespējami mazāko jautājumu skaitu. Vēsturiski sākotnēji tika analizēti determinētie, varbūtiskie un nedeterminētie vaicājošie algoritmi. Visi šie algoritmi tiek veidoti koka veidā. Šajā darbā tiek aplūkots nākošais solis vaicājošajos algoritmos- kvantu vaicājošie algoritmi. Teorētiskais kvantu vaicājošā algoritma modelis ir ņemts no darbiem Gruska [24] and Nielsen and Chuang [26]

Darbā tiek izmantots šāds kvantu vaicājošo algoritmu modelis. Kvantu vaicājošais algoritms ir virkne, kas sastāv no unitārām transformācijām un jautājumiem.

$U_0 \rightarrow O \rightarrow U_1 \rightarrow O \rightarrow \ldots \rightarrow U_{T-1} \rightarrow O \rightarrow U_T$

Šajā virknē U_0, U_1, …, U_T ir patvaļīgas unitāras transformācijas, kas nav atkarīgas no mainīgo vērtībām. Savukārt O ir vaicājumu transformācijas, kur tiek uzdoti jautājumi par konkrētu mainīgo vērtībām . Algoritms sāk darbu stāvoklī $|0\rangle$, tālāk tiek pielietotas transformācijas U_0, O_x ,..., O_x, U_T un beigās tiek veikts mērījums.

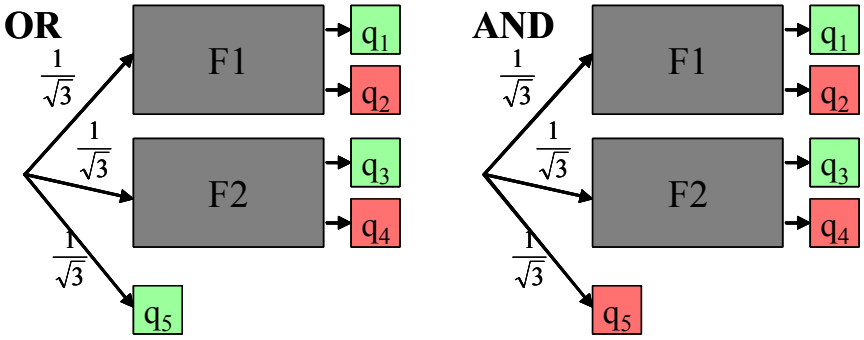
Jautājuma uzdošana notiek sekojošā veidā. Ja pirms jautājuma veikšanas algoritma stāvoklis bija $|\psi\rangle = \sum_i a_i |i\rangle$, tad pēc jautājuma uzdošanas algoritma stāvoklis pārvēršas par $|\phi\rangle = \sum_i (-1)^{x_{ki}} a_i |i\rangle$. Definējot jautājumu ir iespējams brīvi izvēlēties katrai amplitūdai piesaistīto mainīgo x_{ki}. Ja ir nepieciešams, tad var izveidot arī tādus jautājumus, kuru rezultātā amplitūdas zīmes maiņa notiek, ja mainīgā vērtība ir 0, bet ja mainīgā vērtība ir 1, tad amplitūdas zīme nemainās.

2.2. Rezultāti

Dotajā nodaļā ir aplūkoti vairāki kvantu algoritmu veidošanas principi. Dažas no šīm teorēmām tiek iemantotas konkrētu algoritmu veidošanā, bet dažas pierāda tikai teorētiskus algoritmu veidošanas principus.

2.2.1. Algoritmi izmantojot funkcijas OR un AND

Teorēma 2-1. *Ja patvaļīgu funkciju $f(x_1, x_2, \ldots, x_n)$ var izteikt kā $f(x_1, x_2, \ldots, x_n) = f_1(x_1, x_2, \ldots, x_n)$ OR $f_2(x_1, x_2, \ldots, x_n)$, un eksistē kvantu vaicājošais algoritms F_1, kas rēķina funkciju f_1 ar varbūtību 1 un kuram uzdoto jautājumu skaits ir k_1, un kvantu vaicājošais algoritms F_2, kas rēķina funkciju f_2 ar varbūtību 1 un kuram uzdoto jautājumu skaits ir k_2, tad eksistē kvantu vaicājošais algoritms F, kas rēķina funkciju f ar varbūtību 2/3 un uzdoto jautājumu skaits ir $k = max(k_1,k_2)$.*



2.2.1. att. **Kvantu vaicājošo algoritmu apvienošana**

Pierādījums: Algoritmu veido izmantojot 2.2.1. zīmējuma kreisajā pusē attēloto shēmu. 2.2.1. tabulā ir redzami amplitūdu sadalījumi pirms mērījumu izdarīšanas. Zaļā krāsā ir attēloti stāvokļi, kas atbilst funkcijas vērtībai 1, sarkanā- funkcijas vērtībai 0. Ja funkciju f_1 un f_2 vērtības ir 1, tad pareizā atbilde tiek sniegta ar varbūtību 1, pārējos gadījumos pareizās atbildes varbūtība ir 2/3. Tā kā abi algoritmi tiek veikti paralēli, tad kopējais jautājumu skaits ir maksimālais no abu algoritmu jautājuma skaita.

f_1 f_2	f	q_1	q_2	q_3	q_4	q_5
0 0	0	0	$1/\sqrt{3}$	0	$1/\sqrt{3}$	$1/\sqrt{3}$
0 1	1	0	$1/\sqrt{3}$	$1/\sqrt{3}$	0	$1/\sqrt{3}$
1 0	1	$1/\sqrt{3}$	0	0	$1/\sqrt{3}$	$1/\sqrt{3}$
1 1	1	$1/\sqrt{3}$	0	$1/\sqrt{3}$	0	$1/\sqrt{3}$

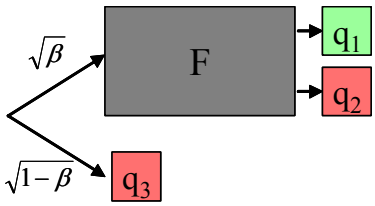
Tabula 2.2.1.

Teorēma 2-2. *Ja patvaļīgu funkciju $f(x_1, x_2, \ldots,x_n)$ var izteikt kā $f(x_1, x_2, \ldots,x_n) = f_1(x_1, x_2, \ldots,x_n)$ AND $f_2(x_1, x_2, \ldots,x_n)$, un eksistē kvantu vaicājošais algoritms F_1, kas rēķina funkciju f_1 ar varbūtību 1 un kuram uzdoto jautājumu skaits ir k_1, un kvantu vaicājošais algoritms F_2, kas rēķina funkciju f_2 ar varbūtību 1 un kuram uzdoto jautājumu skaits ir k_2, tad eksistē kvantu vaicājošais algoritms, kas rēķina funkciju f ar varbūtību 2/3 un uzdoto jautājumu skaits ir $k = max(k_1,k_2)$.*

Pierādījums: Algoritmu veido izmantojot 2.2.1. zīmējuma labajā pusē attēloto shēmu. Pārējais pierādījums ir analoģisks 2-1. teorēmas pierādījumam.

2.2.2. Kopējās pareizās atbildes varbūtības izlīdzināšana

Teorēma 2-3. *Ja eksistē patvaļīga funkcija $f(x_1, x_2, \ldots,x_n)$ un tai eksistē kvantu vaicājošais algoritms F, kas ja funkcijas vērtība ir 1, dod pareizu atbildi ar varbūtību 1, un ja funkcijas vērtība ir 0, dod pareizu atbildi ar varbūtību v, tad eksistē kvantu vaicājošais algoritms F_b , kas rēķina funkciju f ar varbūtību 1/(2-v),un kura jautājumu skaits ir vienāds ar kvantu vaicājošā algoritma F jautājuma skaitu.*

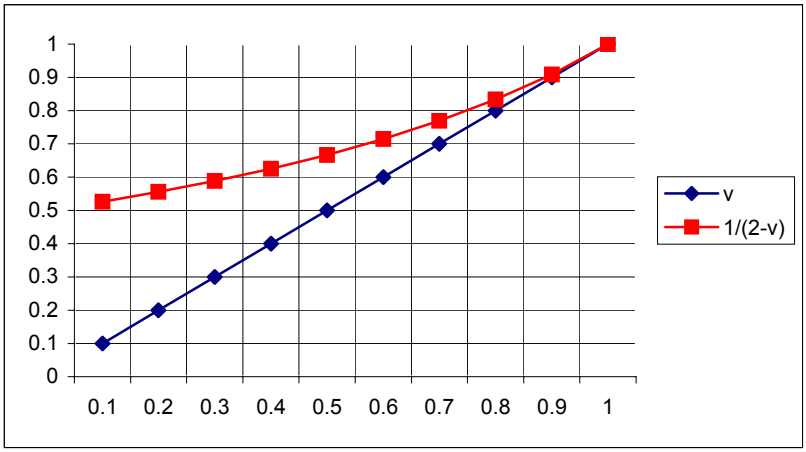


2.2.2. att. **Algoritma kopējās varbūtības izlīdzināšana**

Pierādījums: Algoritmu veido izmantojot 2.2.2. zīmējumā redzamo shēmu. Mainīgais β = 1/(2-v), līdz ar to 1-β ir vienāds ar 1-1/(2-v) vai pārveidojot (1-v)/(2-v). Ja algoritms F pie funkcijas vērtības 0 dod pareizu atbildi ar varbūtību v, tas nozīmē, ka pirms mērījuma veikšanas atbilstošajā stāvoklī ir amplitūda $\sqrt{v}$. 2.2.2. tabulā ir redzami amplitūdu sadalījumi jaunajā algoritmā pirms mērījumu veikšanas. Ir redzams, ka pēc mērījuma veikšanas pareizās atbildes varbūtība abos gadījumos ir 1/(2-v), kas ir lielāka par v.

f	q1	q2	q3
0	$\sqrt{\frac{1}{2-v}} * \sqrt{1-v} = \sqrt{1-\frac{1}{2-v}}$	$\sqrt{\frac{1}{2-v}} * \sqrt{v} = \sqrt{\frac{v}{2-v}}$	$\sqrt{1-\frac{1}{2-v}}$
1	$\sqrt{\frac{1}{2-v}}$	0	$\sqrt{1-\frac{1}{2-v}}$

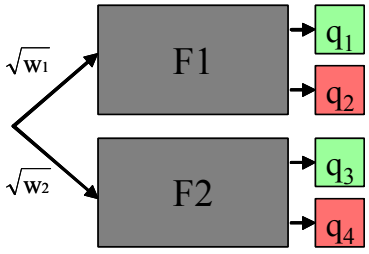
Tabula 2.2.2.



Dotajā grafikā ir attēlota uzlabotā varbūtība atkarībā no sākotnējās varbūtības v. Ja v vērtība ir tuva nullei, tad kopējā algoritma pareizās atbildes varbūtība ir nedaudz pāri 1/2. Ja v vērtība tuvojas 1, tad kopējā pareizās atbildes varbūtība arī tuvojās 1. Dotā metode neuzlabo kopējo pareizās atbildes atpazīšanas intervālu, tas tiek tikai izlīdzināts.

2.2.3. Funkcija ar divām neatkarīgām mainīgo vērtību kopām

Teorēma 2-4. *Ja eksistē funkcija $f(x_1, x_2, \ldots, x_n)$, un eksistē divi kvantu vaicājošie algoritmi F1 un F2 ar sekojošam īpašībām: Ir divas mainīgo $x_1, x_2, \ldots, x_n$ vērtību kopas kk_1 un kk_2 tādas, ka šīs kopas nešķeļas un šo kopu apvienojums dod visas iespējamās mainīgo vērtību kombinācijas. Kvantu vaicājošais algoritms F1 rēķina funkciju $f(x_1, x_2, \ldots, x_n)$ vērtību kopai kk_1 ar varbūtību 1, un kopai kk_2 ar varbūtību $1-v_1$ ar k_1 jautājumiem. Un kvantu vaicājošais algoritms F2 rēķina funkciju $f(x_1, x_2, \ldots, x_n)$ vērtību kopai kk_2 ar varbūtību 1, un kopai kk_1 ar varbūtību $1-v_2$ ar k_2 jautājumiem. Tad eksistē kvantu vaicājošais algoritms, kas rēķina funkciju $f(x_1, x_2, \ldots, x_n)$ ar $\max(k_1,k_2)$ jautājumiem un varbūtību $1-v_1*v_2/(v_1+v_2)$.*



2.2.3. att. **Algoritms 2-4. teorēmai**

Pierādījums: Kvantu vaicājošo algoritmu veido pēc 2.2.3. zīmējuma parauga. $w_1=v_2/(v_1+v_2)$ un $w_2=v_1/(v_1+v_2)$. 2.2.3. tabulā ir redzamas amplitūdu vērtības gadījumā, ja funkcijas f vērtība ir 1. 2.2.4. tabulā ir redzami izveidotā kvantu vaicājošā algoritma pieļautās kļūdas un pareizās atbildes varbūtības pēc mērījuma veikšanas. Ja $v_1=v_2$, tad ir redzams, ka kopējā kļūdas varbūtība samazinās uz pusi.

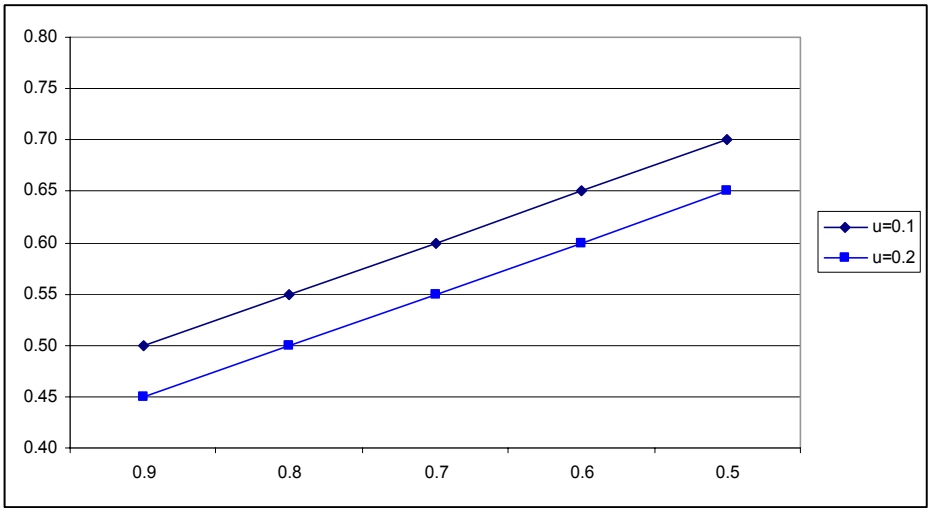
Mainīgie	q1	q2	q3	q4
kk1	$\sqrt{\frac{v_2}{v_1+v_2}}$	0	$\sqrt{\frac{v_2(1-v_1)}{v_1+v_2}}$	$\sqrt{\frac{v_2 v_1}{v_1+v_2}}$
kk2	$\sqrt{\frac{v_1(1-v_2)}{v_1+v_2}}$	$\sqrt{\frac{v_2 v_1}{v_1+v_2}}$	$\sqrt{\frac{v_1}{v_1+v_2}}$	0

Tabula 2.2.3.

Mainīgie	F1-kļūda	F2-kļūda	Pareizās atbildes varbūtība
kk1	0	$v_1 * v_2/(v_1+v_2)$	$1-v_1*v_2/(v_1+v_2)$
kk2	$v_2 * v_1/(v_1+v_2)$	0	$1-v_1*v_2/(v_1+v_2)$

Tabula 2.2.4.

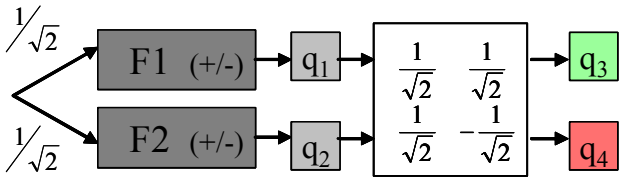
Ir iespējams lietot šo paņēmienu arī situācijai, kad labākā varbūtība nav precīzi 1. Pieņemsim, ka kļūda ir maza un apzīmēsim to ar u. Pieņemsim, ka lielākās kļūdas varbūtība arī abiem algoritmiem ir vienāda. Nākamajā grafikā ir redzama kopējās pareizās varbūtības atkarība no kļūdas v (x ass). Varbūtība tiek aprēķināta pēc formulas 1-(v+u)/2. Šādu pieeju var lietot, ja v+u ir mazāks par 1. Ja ir vairāk kā divas neatkarīgas mainīgo vērtību kopas ar atbilstošajiem algoritmiem, tad arī var veidot līdzīgas konstrukcijas, tikai tādā gadījumā kļūdas samazinājums būs atkarīgs no kopu un algoritmu skaita, bet jau trīs algoritmu gadījumā ieguvums ir tikai apmēram 1/3.



2.2.4. Funkciju apvienošana izmantojot Paritātes funkciju

Teorēma 2-5. *Ja patvaļīgu funkciju $f(x_1, x_2, \ldots, x_n)$ var izteikt kā $f(x_1, x_2, \ldots, x_n) = f1(x_1, x_2, \ldots, x_n)$ XOR $f2(x_1, x_2, \ldots, x_n)$, un eksistē kvantu vaicājošais algoritms F1, kas rēķina funkciju f1 sekojoši: kuram ir viens izejas stāvoklis kurā, ja funkcijas vērtība ir viens, automāts nonāk ar amplitūdu 1, un ja funkcijas vērība ir 0 automāts nonāk ar amplitūdu –1, un kuram uzdoto jautājumu skaits ir k_1, un eksistē kvantu vaicājošais algoritms F2, kas rēķina funkciju f2 sekojoši: kuram ir viens izejas stāvoklis kurā, ja funkcijas vērtība ir viens, automāts nonāk ar amplitūdu 1, un ja funkcijas vērība ir 0 automāts nonāk ar amplitūdu –1, un kuram uzdoto jautājumu skaits ir k_2, tad eksistē kvantu vaicājošais algoritms, kas rēķina funkciju f ar varbūtību 1 un uzdoto jautājumu skaits ir $k = max(k_1,k_1)$.*

Pierādījums Kvantu vaicājošo algoritmu veido pēc 2.2.4. zīmējuma parauga. 2.2.5. tabulā ir redzami kvantu vaicājošā algoritma amplitūdu sadalījumi pa stāvokļiem un mērījumu rezultāti.



2.2.4. att. **Algoritms 2-5. teorēmai**

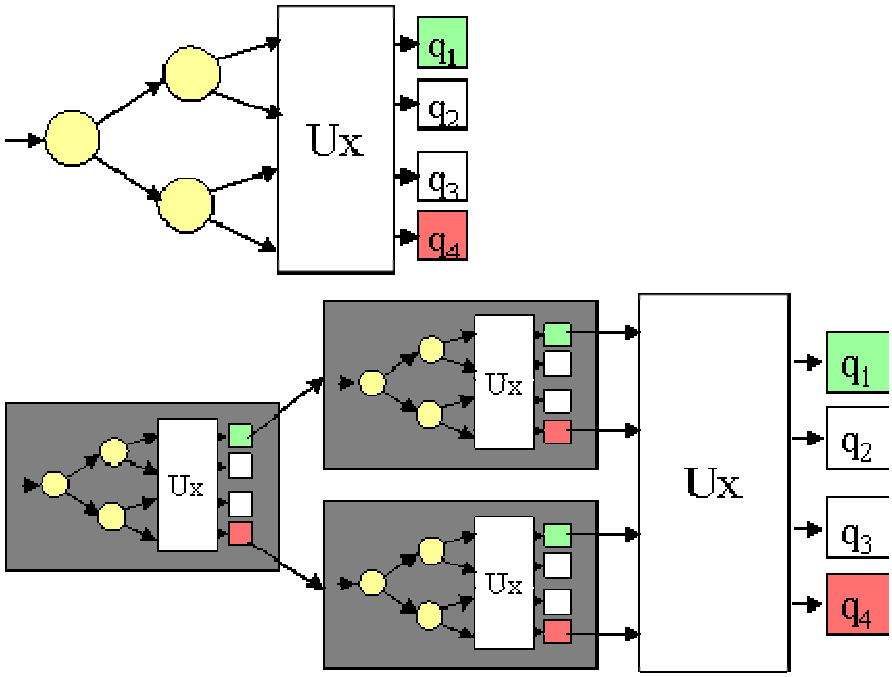
F1	F2	q_1	q_2	q_3	q_4	0	1
0	0	$-\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$	-1	0	0	1
0	1	$-\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$	0	-1	1	0
1	0	$\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$	1	0	1	0
1	1	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$	0	1	0	1

Tabula 2.2.5.

2.2.5. Algoritmi ar jautājumiem bez amplitūdu apgriešanas

Teorēma 2-6. *Ja eksistē funkcija $f(x_1, x_2, \ldots, x_n)$, un šai funkcijai eksistē kvantu vaicājošais algoritms F, kas rēķina šo funkciju ar varbūtību 1, nelietojot amplitūdas zīmes maiņu veicot jautājumu, un kvantu vaicājošajam algoritmam jautājumu skaits ir k, un tam ir tikai viens akceptējošais un noraidošais stāvoklis, tad funkcijai $ff(x_1, x_2, \ldots, x_{n*n}) = f(f(x_1, x_2 \ldots, x_n), f(x_{n+1}, \ldots, x_{2*n}), \ldots f(x_{(n-1)*n+1}, \ldots, x_{n*n}))$ eksistē kvantu vaicājošais algoritms , kas rēķina šo funkciju ar k^2 jautājumiem ar varbūtību 1.*

Pierādījums: Funkcijas ff kvantu vaicājošais algoritms FF ir jābūvē sekojoši: Ņem kvantu vaicājošo algoritmu F, kas rēķina funkciju f, un izveido no tā "orākulu", akceptējošos un noraidošos zarus veidojot par orākula atbildēm. Tad šos jaunizveidotos orākulus ievieto algoritmā F parasto orākulu vietā. Kvantu vaicājošais algoritms FF rēķina funkciju ff, tas seko no koka konstrukcijas. Tā kā koka f dziļums ir k, un katrs jaunizveidotais orākuls arī ir dziļumā k, tad kopējais varbūtiskā vaicājošā algoritma jautājuma skaits ir $k*k=k^2$. Jaunizveidotā kvantu vaicājošā algoritma varbūtība arī ir 1. 2.2.5. zīmējumā ir redzama 2.6. teorēmas kvantu vaicājošā algoritma konstruēšanas shēma gadījumā, ja n=3 un k = 2, fiktīvai funkcijai.

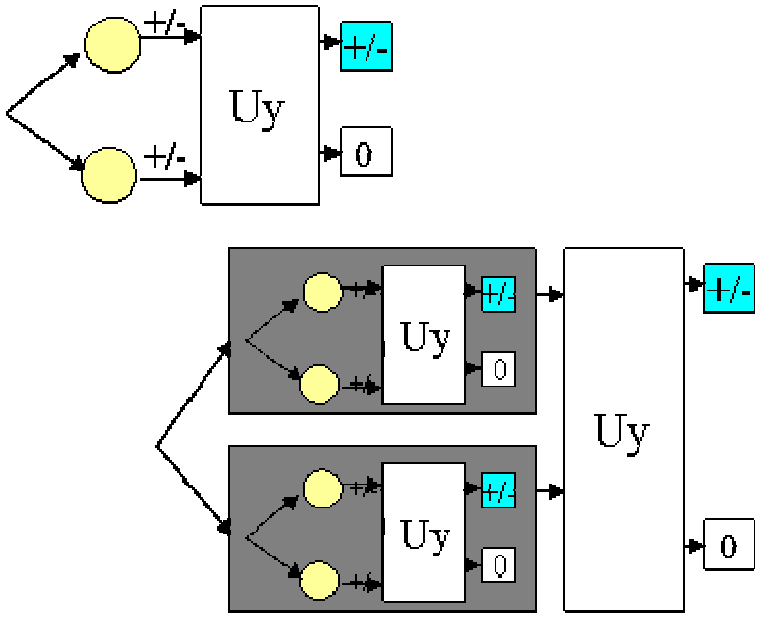


2.2.5. att. **Algoritma veidošanas shēma 2-6. teorēmai**

2.2.6. Algoritmi ar jautājumiem ar amplitūdu apgriešanu

Teorēma 2-7. *Ja eksistē funkcija $f(x_1, x_2, \ldots, x_n)$, un šai funkcijai eksistē kvantu vaicājošais algoritms F, kas rēķina šo funkciju sekojoši: Kuram ir viens izejas stāvoklis kurā, ja funkcijas vērtība ir viens, automāts nonāk ar amplitūdu 1, un ja funkcijas vērība ir 0 automāts nonāk ar amplitūdu –1, un visos orākulu jautājumos notiek amplitūdu apgriešana, un kvantu vaicājošajam algoritmam jautājumu skaits ir k. Tad funkcijai $ff(x_1, x_2, \ldots, x_{n*n}) = f(f(x_1, x_2 \ldots, x_n), f(x_{n+1}, \ldots, x_{2*n}), \ldots f(x_{(n-1)*n+1}, \ldots, x_{n*n}))$ eksistē kvantu vaicājošais algoritms , kas rēķina šo funkciju ar k^2 jautājumiem arī ar vienu izejas stāvokli un tādiem pašiem nosacījumiem kā F.*

Pierādījums: Kvantu vaicājošo algoritmu veido pēc 2.2.6. zīmējuma parauga. Dotajā piemērā bāzes algoritmam ir nepieciešams tikai viens jautājums (dziļumā), tātad arī izveidotajam algoritmam būs tikai viens jautājums. Ja jautājumu skaits ir lielāks par viens, tad kopējais jautājumu skaits ir k^2, jo algoritms tiek veidots rekursīvi.

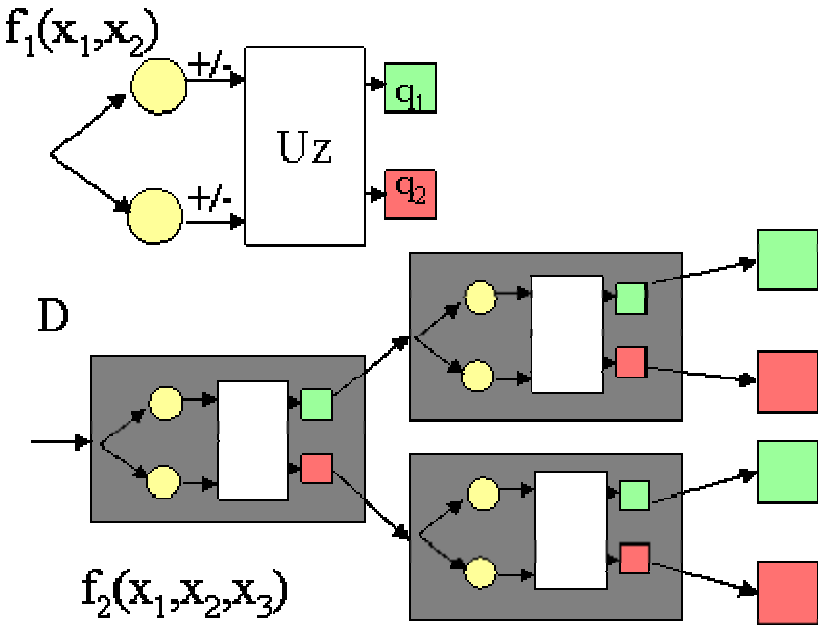


2.2.6. att. **Algoritma veidošanas shēma 2-7. teorēmai**

Jauniegūtā funkcija apmierina 2-5. teorēmas nosacījumus, tātad var izveidot jaunu funkciju, fff = ff XOR ff, kurai būs varbūtība 1 un jautājumu skaits vienāds ar funkcijas ff jautājumu skaitu.

2.2.7. Kvantu un determinēto algoritmu apvienošana

Teorēma 2-8. [5] *Ja eksistē Q – precīzs kvantu vaicājošais algoritms, kas rēķina funkciju $f_1(x_1,...x_m)$ uzdodot k_1 jautājumu, un šim algoritmam ir divas izejas (0,1). Un atbilstošā determinētā algoritma jautājumu skaits ir k_2 ($(k_2>k_1)$. Un ja eksistē D – determinēts reversējams vaicājošais algoritms, kas rēķina funkciju $f_2(x_1,...x_n)$ uzdodot n jautājumus. Tad eksistē kvantu vaicājošais algoritms, kas rēķina funkciju $f_2(f_1(x_1,...x_m), f_1(x_{m+1},...x_{2m}),...f_1(x_{(n-1)m+1},...x_{nm}))$ ar varbūtību 1, uzdodot k_1n jautājumus un atbilstošajam determinētajam algoritmam ir nepieciešami k_2n jautājumi.*

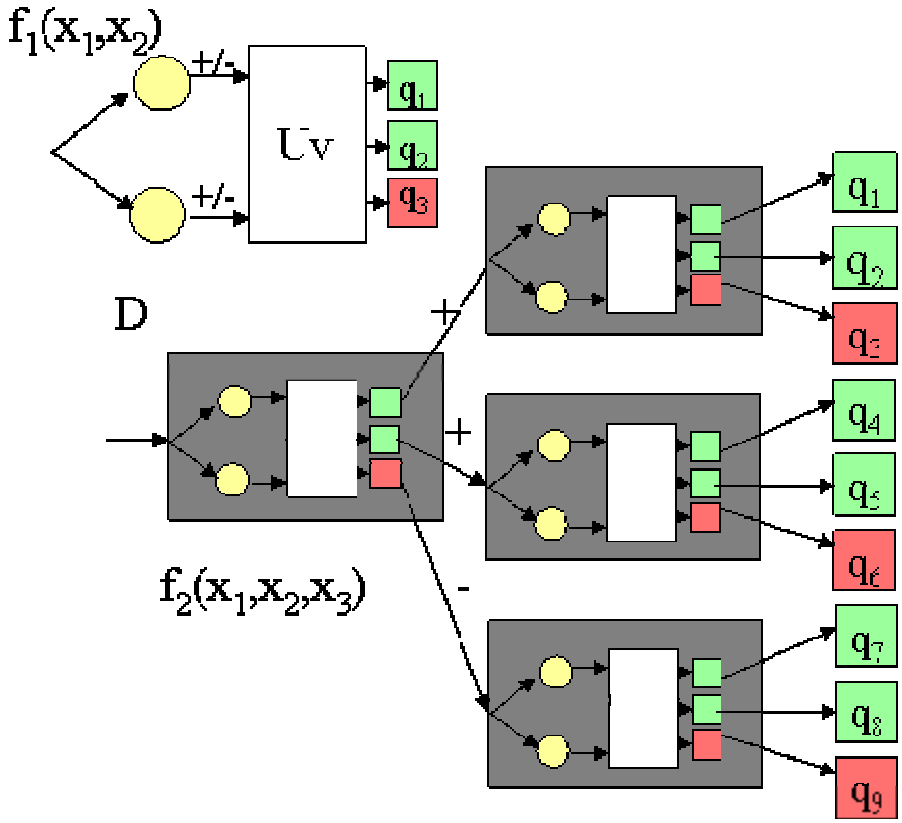


2.2.7. att. **Algoritma veidošanas shēma 2-8. teorēmai**

Pierādījums: Algoritma veidošanas shēma ir parādīta 2.2.7. zīmējumā. Tiek ņemts determinētais algoritms D un katrā šī algoritma jautājumā tiek ievietots bāzes kvantu vaicājošais algoritms ar atbilstošajiem mainīgajiem. Kvantu algoritma izejas tiek savienotas ar determinētā algoritma izejām. Šādā veidā tiek iegūts kvantu vaicājošais algoritms, kas rēķina funkciju f_2, uzdodot k_1n jautājumus. Tā kā bāzes kvantu vaicājošais algoritms ir precīzs, kas nozīmē, ka tas dod pareizo atbildi ar varbūtību 1, tātad arī jaunveidotajam algoritmam būs varbūtība 1, Determinēto algoritmu funkcijai var veidot līdzīgi, bet tam būs nepieciešami k_2n jautājumi.

Teorēma 2-9. [6] *Ja eksistē Q- precīzs kvantu vaicājošais algoritms, kas rēķina funkciju $f_1(x_1,...x_m)$ uzdodot k_1 jautājumu. Un atbilstošā determinētā algoritma jautājumu skaits ir k_2 ($(k_2>k_1)$. Un ja eksistē D – determinēts reversējams vaicājošais algoritms, kas rēķina funkciju $f_2(x_1,...x_n)$ uzdodot n jautājumus. Tad eksistē kvantu vaicājošais algoritms, kas rēķina funkciju $f_2(f_1(x_1,...x_m),f_1(x_{m+1},...x_{2m}),...f_1(x_{(n-1)m+1},...x_{nm}))$ ar varbūtību 1, uzdodot $k_1 n$ jautājumus un atbilstošajam determinētajam algoritmam ir nepieciešami $k_2 n$ jautājumi.*

Pierādījums: Algoritms tiek veidots pēc līdzīga principa, kā iepriekšējās teorēmas gadījumā. Ja kvantu vaicājošajam algoritmam ir vairāk kā divas izejas, tad veidojot kopējo algoritmu determinētajam algoritmam tiek pavairota attiecīgā izeja. Tā kā katrs jaunizveidotais zars ir neatkarīgs, tos nav nepieciešams tālāk apvienot, tad šādā veidā ir iespējams izveidot attiecīgo kvantu vaicājošo algoritmu. 2.2.8. zīmējumā ir parādīts piemērs situācijai, kad bāzes kvantu vaicājošajam algoritmam ir divas izejas, kas atbilst funkcijas vērtībai 1. Ja bāzes algoritms funkcijas vērtībai 1, nonāk stāvoklī q_1 ar amplitūdu $1/\sqrt{3}$ un stāvoklī q_2 ar amplitūdu $\sqrt{2}/\sqrt{3}$, tad kopējā pareizās atbildes varbūtība ir 1. Tad piemērā attēlotais algoritms nonāks beigu stāvokļos q_1, q_2, q_4 un q_5 ar atbilstošajām amplitūdām - $1/3$, $\sqrt{2}/3$, $\sqrt{2}/3$ un $2/3$. Pēc beigu mērījuma veikšanas pareizās atbildes varbūtība ir 1.



2.2.8. att. **Algoritma veidošanas shēma 2-9. teorēmai**

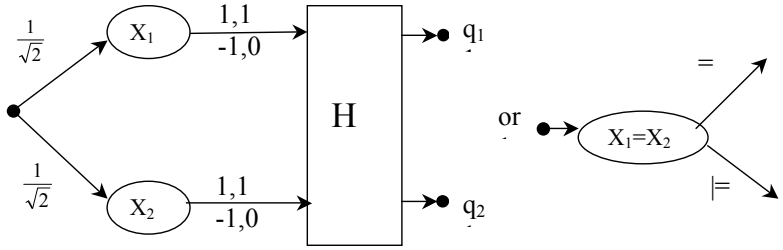
3. KVANTU ALGORITMI KONKRĒTĀM FUNKCIJĀM

3.1. Zināmie kvantu algoritmi

Definīcija [28] *Kvantu algoritmu sauc par **precīzu**, ja tas vienmēr dod pareizu rezultātu ar varbūtību 1.*

Definīcija [28] *Kvantu algoritmu sauc par algoritmu ar **kļūdas varbūtību**, ja aprēķinu rezultāts ir vienāds ar varbūtību vismaz 1-δ, fiksētam δ<1/2.*

Populārākais precīzais kvantu vaicājošais algoritms ir funkcijai XOR/PARITY. Šis algoritms ir attēlots 3.1.1. zīmējumā. Kvantu gadījumā šim algoritmam ir nepieciešams tikai viens jautājums, ja ir divi mainīgie. Determinētajā gadījumā ir jāuzdod divi jautājumi. Liela daļa no konstruētajiem precīzajiem algoritmiem balstās uz šo pamatalgoritmu.



3.1.1. att. **Kvantu algoritms funkcijai PARITY**

Veidojot jaunus kvantu vaicājošos algoritmus ar kļūdu bieži tiek izmantota Grovera amplitūdu palielināšanas metode [21]. Šī metode tiek izmantota n mainīgo funkcijas OR rēķināšanai ar $\sqrt{n}$ jautājumiem. Bet šo metodi ir iespējams pielietot arī citās līdzīgās situācijās. Ja eksistē algoritms, kas izdod pareizo atbildi ar varbūtību 1/n, tad atkārtojot šo algoritmu $\sqrt{n}$ reizes ir iespējams pietiekoši palielināt pareizās atbildes varbūtību.

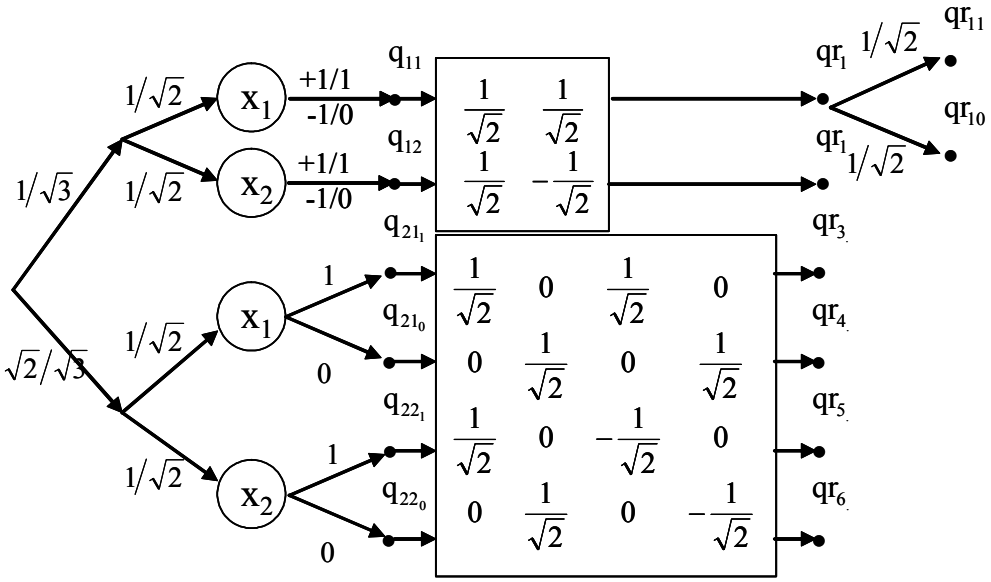
3.2. Izveidotie kvantu algoritmi

Dotā nodaļa satur dažādus konkrētus autores izveidotus kvantu algoritmus dažādām funkcijām. Nodaļā ir pārstāvēti gan precīzie kvantu vaicājošie algoritmi- tādi, kas dod pareizu atbildi ar varbūtību 1, gan arī kvantu vaicājošie algoritmi ar kļūdu. Tiek sniegti arī algoritmu darbības pareizības pierādījumi.

3.2.1. Kvantu vaicājošie algoritmi ar vienu jautājumu

Teorēma 3-1. [1] *Ir iespējams izveidot kvantu vaicājošo algoritmu, kas rēķina funkciju OR no diviem mainīgajiem ar vienu jautājumu un varbūtību 5/6.*

Pierādījums: Zīmējumā 3.2.1. ir redzams izveidotais kvantu vaicājošais algoritms.



3.2.1. att. **Kvantu algoritms funkcijai OR**

Amplitūdu sadalījums dažādām mainīgo vērtībām pēc jautājuma uzdošanas ir redzams tabulā 3.2.1.

x_1x_2	q_{11}	q_{12}	q_{211}	q_{210}	q_{221}	q_{220}
0 0	$-1/\sqrt{6}$	$-1/\sqrt{6}$	0	$+1/\sqrt{3}$	0	$+1/\sqrt{3}$
0 1	$-1/\sqrt{6}$	$+1/\sqrt{6}$	0	$+1/\sqrt{3}$	$+1/\sqrt{3}$	0
1 0	$+1/\sqrt{6}$	$-1/\sqrt{6}$	$+1/\sqrt{3}$	0	0	$+1/\sqrt{3}$
1 1	$+1/\sqrt{6}$	$+1/\sqrt{6}$	$+1/\sqrt{3}$	0	$+1/\sqrt{3}$	0

Tabula 3.2.1.

Tālāk tiek pielietas divas unitāras transformācijas. Algoritma augšējā daļā tiek izmantota Adamāra otrās pakāpes transformācija, bet otra lietotā ceturtās pakāpes transformācija ir izveidota izmantojot divas otrās pakāpes Adamāra transformācijas. Amplitūdu sadalījums pēc šo transformāciju veikšanas ir redzams 3.2.2. tabulā. Stāvokļi q_2, q_3, q_5 un q_6 būs akceptējošie stāvokļi, kas atbildīs funkcijas vērtībai 1. Stāvoklis q_4 būs noraidošais stāvoklis, kas atbildīs funkcijas vērtībai 0. Lai iegūtu nepieciešamo akceptēšanas varbūtību stāvokli q_1 ir nepieciešams sadalīt divos vienādas amplitūdas stāvokļos, no kuriem viens būs akceptējošais, bet otrs noraidošais.

X_1x_2	q_1	q_2	q_3	q_4	q_5	q_6
0 0	$-1/\sqrt{3}$	0	0	$+\sqrt{2}/\sqrt{3}$	0	0
0 1	0	$-1/\sqrt{3}$	$+1/\sqrt{6}$	$+1/\sqrt{6}$	$-1/\sqrt{6}$	$+1/\sqrt{6}$
1 0	0	$+1/\sqrt{3}$	$+1/\sqrt{6}$	$+1/\sqrt{6}$	$+1/\sqrt{6}$	$-1/\sqrt{6}$
1 1	$+1/\sqrt{3}$	0	$+\sqrt{2}/\sqrt{3}$	0	0	0

Tabula 3.2.2.

Veicot beigu stāvokļu mērījumus pareizā atbilde tiek iegūta ar varbūtību 5/6.

x_1x_2	q_{10}	q_{11}	q_2	q_3	q_4	q_5	q_6
0 0	1/6	1/6	0	0	2/3	0	0
0 1	0	0	1/3	1/6	1/6	1/6	1/6
1 0	0	0	1/3	1/6	1/6	1/6	1/6
1 1	1/6	1/6	0	2/3	0	0	0

Tabula 3.2.3.

Teorēma 3-2. [1] *Ir iespējams izveidot kvantu vaicājošo algoritmu, kas rēķina funkciju AND no diviem mainīgajiem ar vienu jautājumu un varbūtību 5/6.*

Pierādījums: Algoritms tiek veidots uz iepriekšējā algoritma bāzes, mainot tikai baigu stāvokļiem piekārtotās funkcija vērtības. Šajā gadījumā akceptējošie stāvoklis ir tikai q_3, noraidošie stāvokļi ir – q_2, q_4, q_5 un q_6. Bet stāvokļa q_1 amplitūda, tāpat kā iepriekšējā gadījumā, tiek sadalīta vienādi uz akceptējošo un noraidošo stāvokli. Tabulā 3-4. ir redzams atbilstošais amplitūdu sadalījums un atzīmētie akceptējošie un noraidošie stāvokļi.

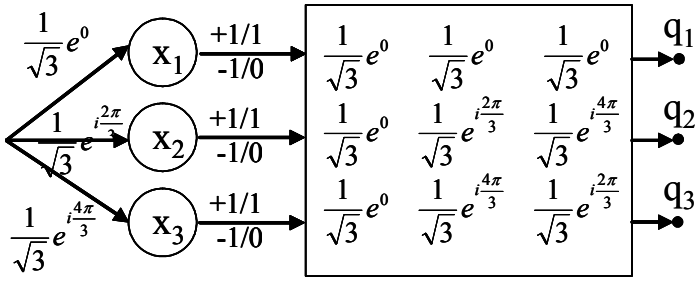
X_1x_2	q_1	q_2	q_3	q_4	q_5	q_6
0 0	$-1/\sqrt{3}$	0	0	$+\sqrt{2}/\sqrt{3}$	0	0
0 1	0	$-1/\sqrt{3}$	$+1/\sqrt{6}$	$+1/\sqrt{6}$	$-1/\sqrt{6}$	$+1/\sqrt{6}$
1 0	0	$+1/\sqrt{3}$	$+1/\sqrt{6}$	$+1/\sqrt{6}$	$+1/\sqrt{6}$	$-1/\sqrt{6}$
1 1	$+1/\sqrt{3}$	0	$+\sqrt{2}/\sqrt{3}$	0	0	0

Tabula 3.2.4.

Veicot beigu stāvokļu mērījumus pareizā atbilde tiek iegūta ar varbūtību 5/6.

Teorēma 3-3. [1] *Ir iespējams izveidot kvantu vaicājošo algoritmu, kas rēķina funkciju* $(x_1 \wedge x_2 \wedge x_3) \vee (\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3})$ *no trim mainīgajiem ar vienu jautājumu un varbūtību 8/9.*

Pierādījums: Zīmējumā 3.2.2. ir redzams izveidotais kvantu vaicājošais algoritms.



3.2.2. att. **Kvantu algoritms funkcijai** $(x_1 \wedge x_2 \wedge x_3) \vee (\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3})$

Tiek izveidots amplitūdu sadalījums $\frac{1}{\sqrt{3}}e^{0}$, $\frac{1}{\sqrt{3}}e^{i\frac{2\pi}{3}}$, $\frac{1}{\sqrt{3}}e^{i\frac{4\pi}{3}}$. Katrā zarā tiek uzdots jautājums par vienu no x_i. Atkarībā no x_i vērtības mainās amplitūdas zīme. Pēc tam tiek pielietota trešās kārtas Furjē transformācija. Tabulā 3-4. ir redzams amplitūdu sadalījums pēc transformācijas veikšanas.

$x_1\ x_2\ x_3$	q_1	q_2	q_3
0 0 0	$-\frac{1}{3}e^{0}-\frac{1}{3}e^{i\frac{2\pi}{3}}-\frac{1}{3}e^{i\frac{4\pi}{3}}$	$-\frac{1}{3}e^{0}-\frac{1}{3}e^{i\frac{4\pi}{3}}-\frac{1}{3}e^{i\frac{2\pi}{3}}$	$-\frac{1}{3}e^{0}-\frac{1}{3}e^{0}-\frac{1}{3}e^{0}$
0 0 1	$-\frac{1}{3}e^{0}-\frac{1}{3}e^{i\frac{2\pi}{3}}+\frac{1}{3}e^{i\frac{4\pi}{3}}$	$-\frac{1}{3}e^{0}-\frac{1}{3}e^{i\frac{4\pi}{3}}+\frac{1}{3}e^{i\frac{2\pi}{3}}$	$-\frac{1}{3}e^{0}-\frac{1}{3}e^{0}+\frac{1}{3}e^{0}$
0 1 1	$-\frac{1}{3}e^{0}+\frac{1}{3}e^{i\frac{2\pi}{3}}+\frac{1}{3}e^{i\frac{4\pi}{3}}$	$-\frac{1}{3}e^{0}+\frac{1}{3}e^{i\frac{4\pi}{3}}+\frac{1}{3}e^{i\frac{2\pi}{3}}$	$-\frac{1}{3}e^{0}+\frac{1}{3}e^{0}+\frac{1}{3}e^{0}$
1 1 1	$\frac{1}{3}e^{0}+\frac{1}{3}e^{i\frac{2\pi}{3}}+\frac{1}{3}e^{i\frac{4\pi}{3}}$	$\frac{1}{3}e^{0}+\frac{1}{3}e^{i\frac{4\pi}{3}}+\frac{1}{3}e^{i\frac{2\pi}{3}}$	$\frac{1}{3}e^{0}+\frac{1}{3}e^{0}+\frac{1}{3}e^{0}$

Tabula 3.2.4.

Pēc mērījuma veikšanas tiek iegūts tabulā 3-5. redzamais rezultāts. Ja visu x_i vērtības ir vienādas, tad algoritms izdod vērtību 1 ar varbūtību 1. Visos citos gadījumos pareizās atbildes (0) varbūtība ir 8/9.

$x_1\ x_2\ x_3$	q_1	q_2	q_3
0 0 0	0	0	1
0 0 1	4/9	4/9	1/9
0 1 1	4/9	4/9	1/9
1 1 1	0	0	1

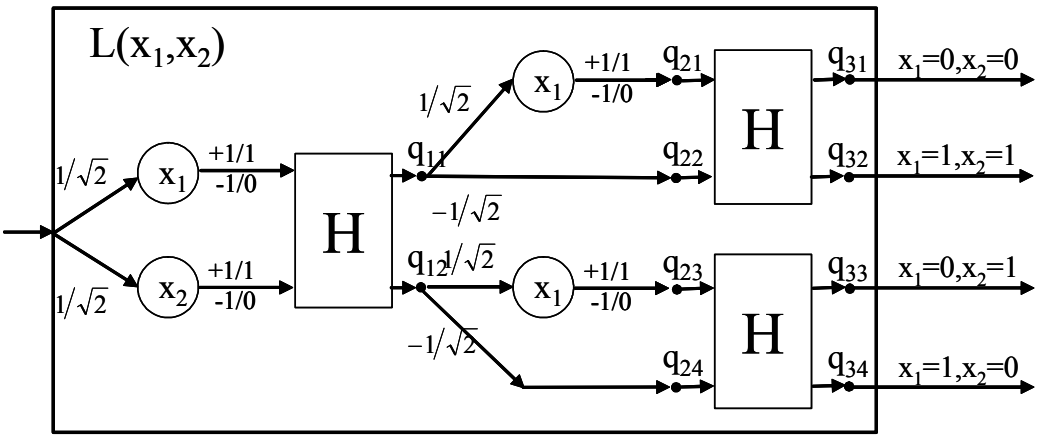
Tabula 3.2.5.

Tā kā dotajam algoritmam pareizās atbildes varbūtība, kad funkcijas vērtība ir 1, ir 1, un kad funkcijas vērtība ir 0 ir 8/9, tas ir abos gadījumos nav vienāda. Tad izmantojot 2-3. teorēmu var izveidot kvantu vaicājošo algoritmu, kas dod pareizu atbildi visos gadījumos ar varbūtību 9/10, kas ir nedaudz lielāka, kā sākotnējā.

3.2.2. Kvantu vaicājošie algoritmi grafu funkcijām

Lemma 3-1. [8] *Eksistē precīzs kvantu vaicājošais algoritms L, ar diviem jautājumiem un šim algoritmam ir četras izejas ar pozitīvām amplitūdām.*

Pierādījums: 3.2.3. zīmējumā ir redzams kvantu vaicājošais algoritms, kuram ir visas nepieciešamās īpašības. Dotajam kvantu vaicājošajam algoritmam ir četras izejas, un tiek uzdoti divi jautājumi. Visās algoritma izejās iz pozitīvas amplitūdas, un tas spēj atšķirt visus x_1 un x_2 vērtību gadījumus. Šis algoritms ir ekvivalents determinētam algoritmam, kas sadala divus mainīgos pa vērtībām. 3.2.6. tabulā var izsekot amplitūdu maiņām dotajā algoritmā, un pārliecināties, ka tas strādā pareizi.



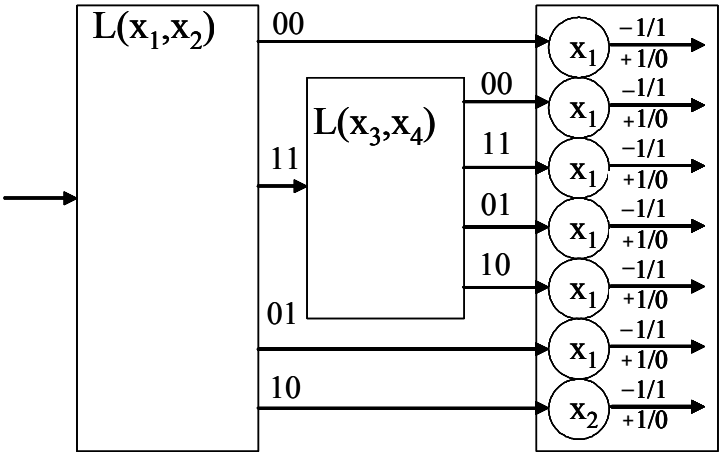
3.2.3. att. **Kvantu vaicājošais algoritms mainīgo vērtību atšķiršanai**

$x_1\,x_2$	q_{11}	q_{12}	q_{21}	q_{22}	q_{23}	q_{24}	q_{31}	q_{32}	q_{33}	q_{34}
0 0	-1	0	$1/\sqrt{2}$	$1/\sqrt{2}$	0	0	1	0	0	0
0 1	0	-1	0	0	$1/\sqrt{2}$	$1/\sqrt{2}$	0	0	1	0
1 0	0	1	0	0	$1/\sqrt{2}$	$-1/\sqrt{2}$	0	0	0	1
1 1	1	0	$1/\sqrt{2}$	$-1/\sqrt{2}$	0	0	0	1	0	0

Tabula 3.2.6.

Teorēma 3-4. [8] *Eksistē kvantu vaicājošais algoritms, kas atrisina Pilnas zvaigznes problēmu (Vai grafs G satur tādu virsotni v* ka, visām virsotnēm u $\subseteq$ V-v* - šķautne {u,v*} $\in$E?), izmantojot tikai n jautājumus.*

Pierādījums: Dotais algoritms tiek veidots izmantojot algoritmu L. Grafā ir n virsotnes, un katra grafa virsotne tiek apstrādāta ar amplitūdu $1/\sqrt{n}$. Ir nepieciešams pārbaudīt, vai dotajai virsotnei ir šķautnes uz visām pārējām virsotnēm. Ja virsotņu skaits ir četri, tad zīmējumā 3.2.4. ir redzams viena zara algoritms.



3.2.4. att. **Kvantu algoritma zars 3-4. teorēmai**

Pēc pēdējā jautājuma uzdošanas, ja dotajai virsotnei ir šķautnes uz visām pārejām virsotnēm, tad dotajā zarā ir viena izeja ar negatīvu amplitūdu (trešā no augšas) un pārējas izejas ar nulles amplitūdu. Ja virsotnei nav šķautnes uz visam pārejām virsotnēm, tad ir viena izeja ar pozitīvu amplitūdu un pārējās izejas ar nulles amplitūdu.

Tālāk tiek lietots Grovera amplitūdu palielināšanas algoritms, lai palielinātu pareizās atbildes varbūtību. Grovera algoritma tiek lietots tikai pēdējais kvantu algoritma daļa. Pirmajā algoritma daļā ir nepieciešami n jautājumi. Amplitūdu palielināšanas metodei ir nepieciešami $\sqrt{n}$ jautājumi, jo pirms šīs metodes veikšanas pareizās atbildes amplitūda ir $1/\sqrt{n}$. Tātad, kopējais jautājumu skaits ir O(n).

1-24. teorēmā ir pierādīts šīs problēmas apakšējais novērtējums, kas sakrīt ar dotajā algoritmā nepieciešamo jautājumu skaitu. Tātad izveidoto algoritmu nav iespējams uzlabot.

3.2.3. Precīzi kvantu vaicājošie algoritmi ar n-1 jautājumu

Teorēma 3-5. [5] *Ja $f(x_1,...x_n)$ ir Bula funkcija un ja $x_1=x_2=...x_n=0$ tad funkcijas vērtība ir 1. Bet ja viena no x_i vērtībām ir 1, tad funkcijas vērtība ir 0. Tad funkcijas determinētajam algoritmam ir nepieciešami n jautājumi.*

Pierādījums: Ja ir noskaidrotas n-1 mainīgā vērtības un tās visas ir 0, tad ir nepieciešams noskaidrot arī atlikušā mainīgā vērtību, lai noteiktu funkcijas vērtību.

Definīcija: *Ja $x_1,...\ ,x_n$ ir Bula funkcijas mainīgie, tad starpība **Dif(i)** starp diviem mainīgajiem x_i un x_{i+1} tiek definēta:*

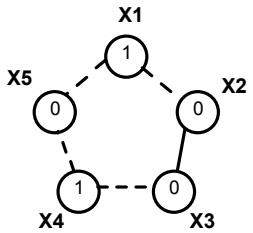
$$Dif(i)=\begin{cases}0, x_i = x_{i+1(\mathrm{mod}\,n)}\\ 1, x_i \neq x_{i+1(\mathrm{mod}\,n)}\end{cases}$$

Definīcija: *Ja $x_1,...\ ,x_n$ ir Bula funkcijas mainīgie un Dif(i) ir atbilstošās starpības, tad:*

$$DifSum(x_1,...x_n)=\sum_{i=1,n} Dif(i)$$

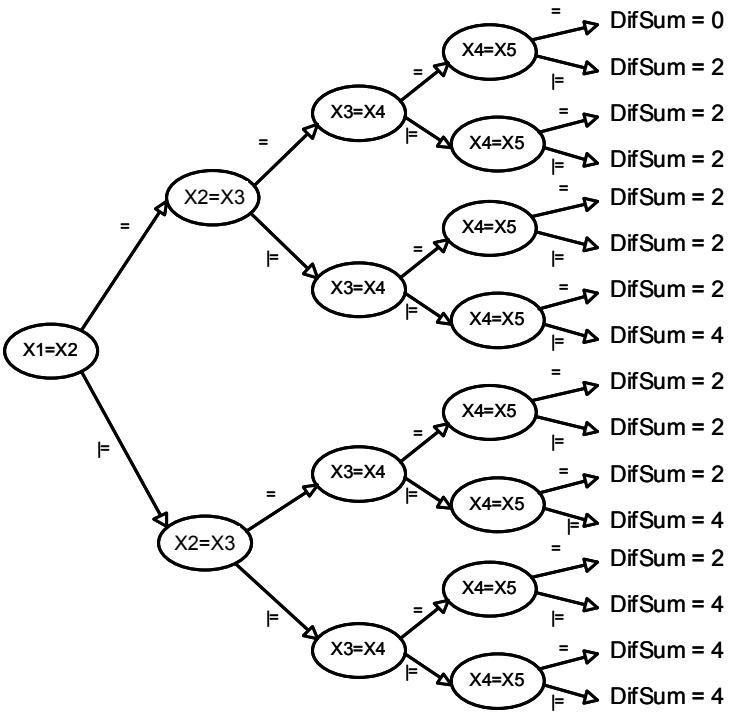
Teorēma 3-6. [5] *Ja $x_1,...\ ,x_n$ ir Bula funkcijas mainīgie un $n=2k+1$ tad DifSum $\in$ {0,2,4..,n-1}, t.i. neatkarīgi no mainīgo vērtībām, DifSum vērtības var būt tikai pāra skaitļi.*

Pierādījums: 3.2.5. zīmējumā ir redzams piecu mainīgo gadījums. Ja starpība starp diviem blakus esošiem mainīgajiem ir 0 (mainīgie ir vienādi), tad zīmējumā tas tiek attēlots ar nepārtrauktu līniju. Ja starpība ir 1, tad tas tiek attēlots kā raustīta līnija. Virsotnes ir izvietotas pa apli un starpības parādās šķautņu formā, kas izkārtotas pa apli. Ir skaidri redzams, ka nevar izveidot piecas raustītās šķautnes, tad vienam mainīgajam reizē būtu jābūt divām dažādām vērtībām. Ja mēģina izveidot tikai vienu raustīto šķautni, tad lai visas pārējās būtu nepārtrauktas, atkal sanāk vienam mainīgajam pretrunīgas vērtības. Arī pārējo nepāra skaita šķautņu gadījumos rodas pretrunas.



3.2.5. att. **Mainīgo starpību attēlošana grafa formā**

3.2.6. zīmējumā ir redzams precīzs kvantu vaicājošais algoritms, kurš var atšķirt dažādas *DifSum* vērtības. Šim algoritmam ir četri jautājumi, katru divu mainīgo salīdzināšana prasa tikai vienu kvantu jautājumu. Šis algoritms satur Paritātes aprēķināšanas algoritmus kā sastāvdaļas. Dažus zarus šajā algoritmā varētu veidot arī ar mazāk jautājumiem, bet maksimālais dziļums ir četri.



3.2.6. att. **Algoritms DifSum vērtību noteikšanai**

Aplūkosim n mainīgo Bula funkciju.

$$H_1(x_1,\ldots x_n)=\begin{cases}1, DifSum(x_1,\ldots x_n)=0\\ 0, DifSum(x_1,\ldots x_n)>0\end{cases}$$

Teorēma 3-7. [5] *Ir iespējams izveidot kvantu vaicājošo algoritmu, kas rēķina funkciju H_i ar n-1 vienu jautājumu un varbūtību 1. Atbilstošajam determinētajam algoritmam ir nepieciešami n jautājumi.*

Pierādījums: Kvantu vaicājošais algoritms tiek veidots līdzīgi piecu mainīgo gadījumam. Izveidotajam algoritmam ir n-1 jautājumi. Tai algoritma izejai, kas atbilst DifSum=0, tiek piekārtota vērtība 1, pārējām izejām – 0. Šis algoritms rēķina Bula funkciju H_1 . Dotā funkcija atbilst teorēmas 3-5. nosacījumiem, tātad determinētam vaicājošam algoritmam ir nepieciešami n jautājumi.

Ievietojot zaros citas vērtības ir iespējams aprēķināt arī citas funkcijas, kas ir balstītas uz DifSum bāzes.

Teorēma 3-8. [5] *Ja H ir Bula funkcija no n mainīgajiem un*

- *H vērtība ir 1, ja DifSum($x_1,...x_n$)=0,*
- *H vērtība ir 0, ja DifSum($x_1,...x_n$)=2,*
- *Diviem dažādiem mainīgo ieejas vektoriem funkcijas H vērtība ir vienāda tad un tikai tad, ja šiem mainīgo vektoriem DifSum vērtība ir vienāda.*

Tad funkcijai H eksistē precīzs kvantu vaicājošais algoritms, kam ir nepieciešami n-1 jautājumi, bet determinētajam vaicājošajam algoritmam ir nepieciešami n jautājumi.

Pierādījums: Kvantu vaicājošais algoritms tiek veidots līdzīgi kā 3-7. teorēmā. Mums ir Bula funkcija, kuras vērtība ir atkarīga tikai no atbilstošas DifSum vērtības. Tā kā izveidotais kvantu vaicājošais algoritms sadala katru DifSum vērtību atsevišķā izejā, tad mēs varam iegūt nepieciešamo funkcijas vērtību. Tā kā funkcijas vērtība, ja visas x_i vērtības ir 0, ir 1, un funkcijas vērtība ir 0, ja viena no x_i vērtībām ir 1, tas funkcija atbilst 3-5. teorēmas prasībām. Tātad determinētajam algoritmam ir nepieciešami n jautājumi.

Starpība starp diviem mainīgajiem tika definēta starp diviem blakus esošajiem mainīgajiem, līdz ar to grafiski attēlojot starpības parādījās kā cikls. Ja mainīgos izvieto mazākos savstarpēji saistītos grafos, tad ar šīs metodes palīdzību ir iespējams izveidot algoritmus arī citām funkcijām.

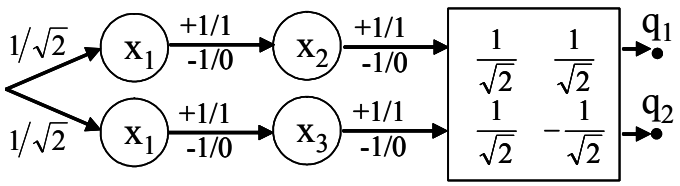
3.2.4. Precīzi kvantu vaicājošie algoritmi ar 2n/3 jautājumu

Aplūkosim Bula funkciju ar 3 mainīgajiem.

$$G(x_1,x_2,x_3)=\begin{cases}1, x_1=x_2=x_3\\ 0, citur\end{cases}$$

Teorēma 3-9. [5] *Funkcijai G eksistē precīzs kvantu vaicājošais algoritms ar 2 jautājumiem un šim algoritmam ir divas izejas.*

Pierādījums: 3.2.7. zīmējumā redzamais kvantu vaicājošais algoritms apmierina teorēmas prasības. Automāta izeja q_1 atbilst funkcijas vērtībai 1, bet izeja q_2 -0.



3.2.7. att. **Kvantu vaicājošais algoritms funkcijai G**

Šai funkcijai eksistē arī kvantu vaicājošais algoritms ar vienu jautājumu. Tas ir aprakstīts 3-3. teorēmā, bet šis algoritms nav precīzs, tam pareizās atbildes varbūtība bija 9/10.

Teorēma 3-10. [5] *Eksistē Bula funkciju kopa, kuru determinētā sarežģītība ir 3n, bet precīzu kvantu vaicājošo algoritmu sarežģītība ir 2n.*

Pierādījums: Pierādījumā tiks izmantotas teorēmas 3-5. un 2-8. Kvantu vaicājošais algoritms, kas tiek izveidots teorēmā 3-9., apmierina teorēmas 2-8. prasības, tas ir tam ir divas izejas un kvantu sarežģītība ir 2, bet determinētā -3. Ņemam patvaļīgu Bula funkciju D ar n mainīgajiem tādu, ka tā apmierina teorēmas 3-5. prasības, tas ir tai eksistē determinēts vaicājošais algoritms ar n jautājumiem. Tad, izmantojot 2-8. teorēmu ir iespējams izveidot precīzu kvantu vaicājošo algoritmu, kas rēķina funkciju $D(G(x_1,x_2,x_3),\ldots,G(x_{3n-2}, x_{3n-1}, x_{3n}))$ ar 2n jautājumiem. No teorēmas 3-5. seko, ka atbilstošajam determinētajam vaicājošajam algoritmam ir nepieciešami 3n jautājumi.

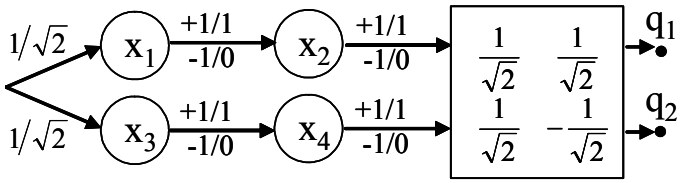
Par algoritma bāzi varētu ņemt arī jebkuru citu kvantu vaicājošo algoritmu, kas apmierinātu 2-8. teorēmas prasības.

3.2.5. Precīzi kvantu vaicājošie algoritmi ar n/2 jautājumu

Aplūkosim Bula funkciju ar 4 mainīgajiem.
$P(x_1,x_2,x_3,x_4)=PARITY(x_1,x_2,x_3,x_4)$

Teorēma 3-11. [5] *Funkcijai P eksistē precīzs kvantu vaicājošais algoritms ar diviem jautājumiem un divām izejām.*

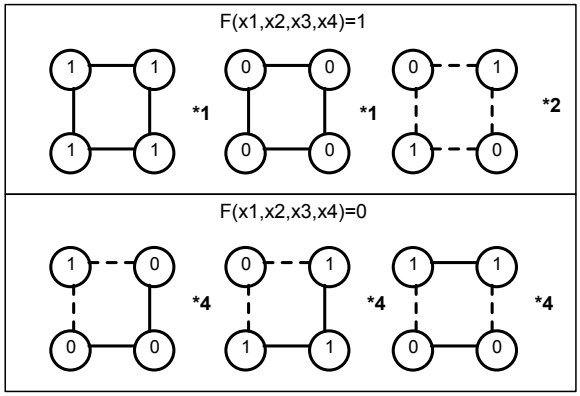
Pierādījums: 3.2.8. zīmējumā ir redzams atbilstošais kvantu vaicājošais algoritms. Izeja q_1 atbilst funkcijas vērtībai1, bet izeja q_2 -0.



3.2.8. att. **Kvantu vaicājošais algoritms funkcijai P**

Aplūkosim Bula funkciju ar 4 mainīgajiem.

$$F(x_1,x_2,x_3,x_4)=\begin{cases}1, DifSum(x_1,\ldots x_4)=0\\ 1, DifSum(x_1,\ldots x_4)=4\\ 0, DifSum(x_1,\ldots x_4)=2\end{cases}$$

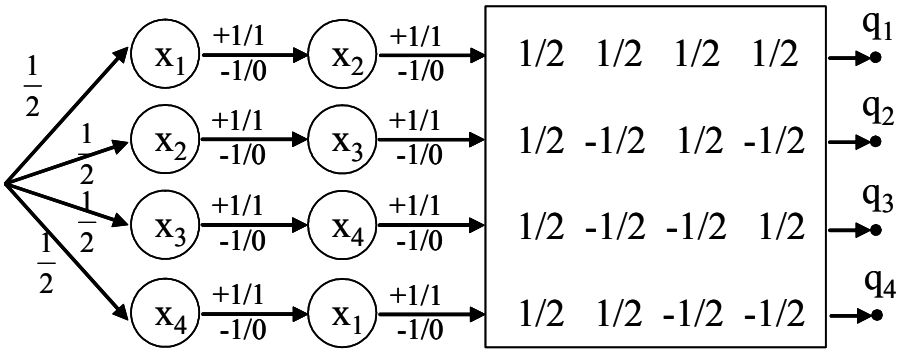


3.2.9. att. **Funkcijas F dažādas vērtības**

3.2.9. zīmējumā ir redzamas divas dažādās funkcijas F vērtības. Starpība starp diviem ieejas mainīgajiem tiek attēlota sekojoši. Ja starpība starp diviem blakus stāvošiem mainīgajiem ir 0 (mainīgie ir vienādi), tad tas tiek attēlots ar nepārtrauktu līniju. Ja starpība starp diviem blakus stāvošiem mainīgajiem ir 1 (mainīgie nav vienādi), tad tas tiek attēlots ar raustītu līniju. DifSum vērtība ir 0, ja visu ieejas mainīgo vērtības ir 0. DifSum vērtība ir 4, ja ieejas mainīgie ir {0,1,0,1} vai {1,0,1,0}. Ja ieejas mainīgo vērtību summa ir 1, tad DifSum vērtība ir 2. Četri dažādi ieejas vektoriem ir mainīgo summu 1 - {1,0,0,0}, {0,1,0,0}, {0,0,1,0}, {0,0,0,1}. Ja ieejas mainīgo summa ir 3, tad situācija ir tāda pati. Ir četri ieejas vektori ar mainīgo summu 2, kuru DifSum vērtība ir 2 - {1,1,0,0},{0,1,1,0}, {0,0,1,1}, {1,0,0,1}.

Teorēma 3-12. [6] *Eksistē precīzs kvantu vaicājošais algoritms funkcijai F ar diviem jautājumiem.*

Pierādījums: 3.2.10. zīmējumā ir attēlots precīzs kvantu vaicājošais algoritms, kurš rēķina funkciju F ar diviem jautājumiem. Izeja q_1 atbilst funkcijas F vērtībai 1, bet izejas q_2, q_3 un q_4 – funkcijas vērtībai 0.



3.2.10. att. **Kvantu vaicājošais algoritms funkcijai F**

Tabulā 3.2.7. ir redzamas funkcijas F un Paritātes funkcijas vērtības dažādiem ieejas vektoriem. Ir redzams, ka funkcijai F ir četras vērtības 1 un 12 vērtības 0, bet Paritātes funkcijai ir astoņas vērtības 1 un 8 vērtības 0. Tas nozīmē, ka šīs abas funkcijas nav vienādas. Ja tiek nomainīta stāvokļa q_2 vērtība no 0 uz 1, tad tiek iegūts algoritms, kas precīzi rēķina Paritātes funkciju ar diviem jautājumiem. Ja tiek nomainītas vērtības stāvokļiem q_3 vai q_4, tad tiek iegūti algoritmi, kas rēķina kādas citas funkcijas, bet šīm funkcijām determinētā sarežģītība nav 4.

x_1	x_2	x_3	x_4	Stāvoklis	PARITY	Funkcija F
0	0	0	0	q_1	1	1
0	0	0	1	q_4	0	0
0	0	1	0	q_3	0	0
0	1	0	0	q_4	0	0
1	0	0	0	q_3	0	0
1	1	0	0	q_2	1	0
0	1	1	0	q_2	1	0
0	0	1	1	q_2	1	0
1	0	0	1	q_2	1	0
1	0	1	0	q_1	1	1
0	1	0	1	q_1	1	1
1	1	1	0	q_4	0	0
1	1	0	1	q_3	0	0
1	0	1	1	q_4	0	0
0	1	1	1	q_3	0	0
1	1	1	1	q_1	1	1

Tabula 3.2.7.

Teorēma 3-13. [5] *Eksistē Bula funkciju kopa, bāzēta uz Paritātes funkciju, kuru determinētā sarežģītība ir 4n, bet precīzu kvantu vaicājošo algoritmu sarežģītība ir 2n.*

Pierādījums: Pierādījumā tiks izmantotas 3-5. un 2-8. teorēmas. Kvantu vaicājošais algoritms, kas tiek izveidots 3-11. teorēmā, apmierina 2-8. teorēmas prasības, tas ir tam ir divas izejas un kvantu sarežģītība ir 2, bet determinētā -4. Ņemam patvaļīgu Bula funkciju D ar n mainīgajiem tādu, ka tā apmierina 3-5. teorēmas prasības, tas ir tai eksistē determinēts vaicājošais algoritms ar n jautājumiem. Tad, izmantojot 2-8. teorēmu ir iespējams izveidot precīzu kvantu vaicājošo algoritmu, kas rēķina funkciju $D(P(x_1,x_2,x_3),\ldots,P(x_{4n-3}, \ldots x_{4n}))$ ar 2n jautājumiem. No 3-5. teorēmas seko, ka atbilstošajam determinētajam vaicājošajam algoritmam ir nepieciešami 4n jautājumi.

Teorēma 3-14. [6] *Eksistē Bula funkciju kopa G1, bāzēta uz funkciju F, kuru determinētā sarežģītība ir 4n, bet precīzu kvantu vaicājošo algoritmu sarežģītība ir 2n.*

Pierādījums: Pierādījumā tiks izmantotas 3-5. un 2-9. teorēmas. Kvantu vaicājošais algoritms, kas tiek izveidots teorēmā 3-12, apmierina teorēmas 2-9. prasības, tas ir tas ir precīzs un tā kvantu sarežģītība ir 2, bet determinētā - 4. Ņemam patvaļīgu Bula funkciju D ar n mainīgajiem tādu, ka tā apmierina 3-5. teorēmas prasības, tas ir tai eksistē determinēts vaicājošais algoritms ar n jautājumiem. Tad, izmantojot 2-9. teorēmu ir iespējams izveidot precīzu kvantu vaicājošo algoritmu, kas rēķina funkciju $D(F(x_1,x_2,x_3),\ldots,F(x_{4n-3}, \ldots x_{4n}))$ ar 2n jautājumiem. No 3-5. teorēmas seko, ka atbilstošajam determinētajam vaicājošajam algoritmam ir nepieciešami 4n jautājumi.

Teorēma 3-15. [6] *Ja Bula funkcija C apmierina sekojošus nosacījumus;*

- *C ir simetriska funkcija*
- *$\exists k$, $O(k)=O(n-k)=O(n)$ un katram mainīgo ieejas vektoram $\{x_1,\ldots x_n\}$*
  ja $sum(x_i) =k$ tad $C(x_1,\ldots x_n)=1$,
  ja $sum(x_i) =k+1$ tad $C(x_1,\ldots x_n)=0$,

tad kvantu vaicājošajam algoritmam ir nepieciešami $\Omega(n)$ jautājumi.

Pierādījums: Tiek izveidotas kopas A un B, atbilstoši Teorēmas A1, kas apraksta Ambaiņa metodi, prasībām:

Kopa A satur visus ieejas vektorus $\{x_1,\ldots x_n\}$ kuriem $sum(x_i)=k$. Kopa B satur visus ieejas vektorus $\{x_1,\ldots x_n\}$ kuriem $sum(x_i)=k+1$. No katra ieejas vektora $\{x_1,\ldots x_n\} \in A$, ir iespējams izveidot $\{x_1,\ldots x_n\}'$ izmainot vienu no $x_j=0$ uz 1. Tātad $m=n-k=O(n)$. No katras ieejas vektora $\{x_1,\ldots x_n\}' \in B$, ir iespējams izveidot $\{x_1,\ldots x_n\}$ izmainot vienu no $x_j=1$ uz 0. Tātad $m'=k+1=O(n)$. No teorēmas A1 seko, ka dotas funkcijas C kvantu vaicājošajam algoritmam $\Omega\sqrt{n \cdot n}$ =Ω(n) jautājumi.

Teorēma 3-16. [6] *Eksistē Bula funkciju kopa G2, kuru determinētā sarežģītība ir n, bet kvantu vaicājošajam algoritmam ir nepieciešami n/2 jautājumi. Pie tam kvantu vaicājošo algoritmu sarežģītības apakšējais novērtējums ir Ω(n).*

Pierādījums: Pierādījumā tiek izmantotas 3- 14. un 3-15. teorēmas. Funkciju kopa G2 tiek veidota tāpat kā funkciju kopa G1 teorēmā 3-14. Tikai šajā gadījumā tiek par ņemta nevis patvaļīga Bula funkcija, kam determinēta sarežģītība ir n, bet funkcija C no 3-15. teorēmas. Izveidoto funkciju kopa G2 ir funkciju kopas G1 apakškopa, no tā seko, ka eksistē kvantu vaicājošais algoritms ir n/2 jautājumiem. Tā kā Bula funkcijai $C(x_1,\ldots,x_n)$ ir nepieciešami $\Omega(n)$ jautājumi, tad funkcijai $C(F(x_1,x_2,x_3,x_4),\ldots,F(x_{4n-3},\ldots, x_{4n}))$ arī ir nepieciešami $\Omega(n)$ jautājumi.

4. KVANTU NEDETERMINĒTIE VAICĀJOŠIE ALGORITMI

4.1. Nedeterminēto kvantu vaicājošo algoritmu definīcija

R. de Wolf savā darbā [31] definē nedeterminētu kvantu vaicājošo algoritmu.

Definīcija: Nedeterminētais kvantu vaicājošais algoritms funkcijai f ir tāds algoritms, kas dod atbildi 1 ar pozitīvu varbūtību, ja funkcijas vērtība ir 1 un atbildi 0 ar varbūtību 1, ja funkcijas vērtība ir 0.

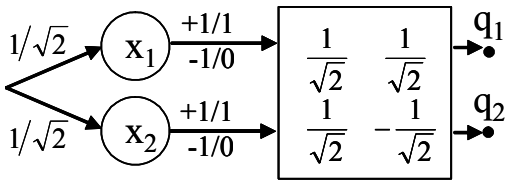
Šai pašā darbā tiek pierādīts, ka nedeterminētam kvantu vaicājošam algoritmam nepieciešamais jautājumu skaits ir vienāds ar atbilstošās funkcijas nedeterminētā polinoma pakāpi.

4.2. Izveidotie nedeterminētie kvantu vaicājošie algoritmi

Šajā nodaļā tiek aplūkoti nedeterminētie kvantu vaicājošie algoritmi. Uzsvars tiek likts uz algoritmiem ar mazu jautājumu skaitu, pamatā tiek aplūkoti algoritmi ar vienu jautājumu. Tiek apskatīti to veidošanas principi un atbilstošo funkciju aprakstošie polinomi.

4.2.1. Bula funkcijas ar diviem mainīgajiem

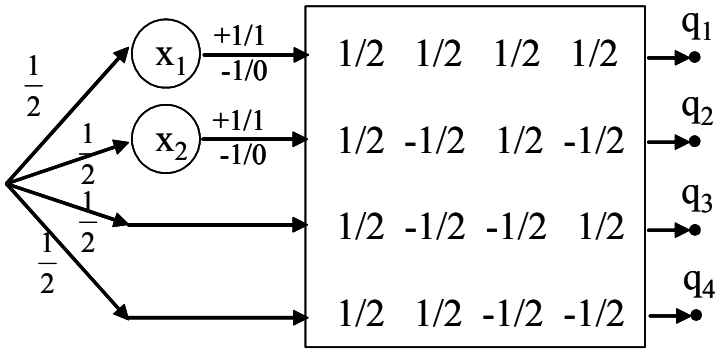
Ir tikai četras netriviālas četru mainīgo Bula funkcijas – OR, AND, Paritātes funkcija un Paritātes funkcijas pretējā funkcija. Ir zināms precīzs kvantu vaicājošais algoritms Paritātes funkcijai – 4.2.1. zīmējums. Katrs precīzs kvantu vaicājošais algoritms apmierina nedeterminētā kvantu vaicājoša algoritma nosacījumus. Tātad eksistē nedeterminēts kvantu vaicājošais algoritms, kas rēķina Paritātes funkciju ar vienu jautājumu. Nomainot dotā algoritmā funkcijas vērtības izejas stāvokļos, tiek iegūts algoritms, kas rēķina Paritātes funkcijas pretējo funkciju.



4.2.1. att. **Kvantu vaicājošais algoritms Paritātes funkcijai**

Ja aplūko funkciju OR, tad tai neeksistē precīzs kvantu vaicājošais algoritms ar vienu jautājumu. Bet mēs zinām, ka *NQ(f)=ndef(f)*. Piemēram, $p(x_1,x_2)=x_1-x_2$ ir nedeterminēts pirmās pakāpes polinoms Paritātes funkcijai no diviem mainīgajiem, tas pieņem vērtību 0,

ja mainīgo summa ir 0 vai divi, un vērtību +/-1, ja mainīgo summa ir 1. Bet $p(x_1,x_2)=x_1+x_2$ ir pirmās pakāpes nedeterminēts polinoms divu mainīgo funkcijai OR, tas pieņem vērtību 0, ja mainīgo summa ir 0 un vērtības 1 un 2, ja mainīgo summas ir 1 un 2. Eksistē nedeterminēts kvantu vaicājošais algoritms, kas rēķina funkciju OR. Šis algoritms ir attēlots 4.2.2. zīmējumā. Algoritma izeja q_1 atbilst funkcijas vērtībai 1, pārējās izejas atbilst funkcijas vērtībai 0.



4.2.2. att. **Nedeterminēts algoritms funkcijai OR**

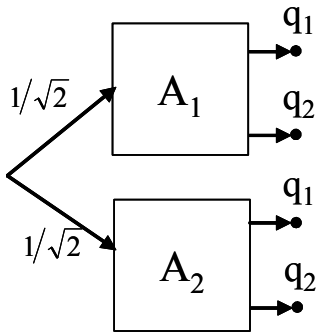
Ir viegli redzēt, ka nedeterminētie kvantu vaicājošie algoritmi nav simetriski. Ja funkcijas vērtība ir 0, tad algoritmam tiek uzstādīti stingrāki nosacījumi, nekā, ja funkcijas vērtība ir 1. Mēs pieņemam, ka jo funkcijai ir vairāk nulles vērtību, jo tas nedeterminētā sarežģītība ir lielāka. Piemēram, $p(x_1,x_2)=x_1*x_2$ ir otrās pakāpes nedeterminēts polinoms funkcijai AND. Šajā gadījumā neeksistē nedeterminēts polinoms ar pakāpi 1 un *ndeg(f)=def(f)*. Tas nozīme, ka funkcijai AND ar diviem mainīgajiem nav iespējams izveidot nedeterminētu kvantu vaicājošo algoritmu ar vienu jautājumu.

4.2.2. Bula funkcijas ar četriem mainīgajiem

Izmantojot iepriekš parādītos algoritmus divu argumentu funkcijām PARITY un ¬PARITY mēs varam izveidot vairākus četru argumentu algoritmus.

Teorēma 4-1. [9] *Ja funkcijām $F_1(x_1,...x_k)$ un $F_2(x_1,...x_l)$ eksistē nedeterminēti kvantu algoritmi ar jautājumu skaitu q_1 un q_2 , tad eksistē nedeterminēts kvantu automāts funkcijai $F(x_1,...x_{k+l})= F_1(x_1,...x_k) \vee F_2(x_{k+1},...x_{k+l})$ ar $q=max(q_1,q_2)$ jautājumiem.*

Pierādījums. 4.2.3. zīmējumā var redzēt kā tiek veidots nedeterminētais algoritms funkcijai F. Tas izdos funkcijas vērtību 0 tad un tikai tad ja $F_1(x_1,...x_k)$ un $F_2(x_1,...x_l)$ būs vērtība 0. Pārējos gadījumos tiek izdota funkcijas vērtība 1. Ja ir nepieciešams palielināt varbūtību funkcijas vērtībai 1, tad pirmajā pārejā vērtības ir jāņem atkarībā no algoritmu F_1 un F_2 minimālajām varbūtībām funkciju vērtībām 1. Piemēram, ja F_1 algoritma minimālā varbūtība ir 1/3 un F_2 – 2/3, tad lieto pārejas vērtības - $\sqrt{2/3}$ un $\sqrt{1/3}$. Abos algoritmos A1 un A2 izejām piekārtotās funkciju vērtības saglabājas.



4.2.3. att. **Nedeterminētu algoritmu apvienošana**

Izmantojot doto funkciju apvienošanas mehānismu un funkciju PARITY un ¬PARITY algoritmus mēs varam iegūt algoritmus 6 dažādām funkcijām. Funkciju 0 vērtības ir attēlotas tabulā 4-1.

D_1	D_2	D_3	D_4	D_5	D_6
$x_1\ x_2\ x_3\ x_4$	$x_1\ x_2\ x_3\ x_4$	$x_1\ x_2\ x_3\ x_4$	$x_1\ x_2\ x_3\ x_4$	$x_1\ x_2\ x_3\ x_4$	$x_1\ x_2\ x_3\ x_4$
0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 1	0 1 0 0	0 1 0 1
0 0 1 1	1 0 0 1	0 1 0 1	0 0 1 0	1 0 0 0	1 0 0 1
1 1 0 0	0 1 1 0	1 0 1 0	1 1 0 1	0 1 1 1	0 1 1 0
1 1 1 1	1 1 1 1	1 1 1 1	1 1 1 0	1 0 1 1	1 0 1 0

Tabula 4-1.

Atbilstošie funkciju nedeterminētie polinomi:

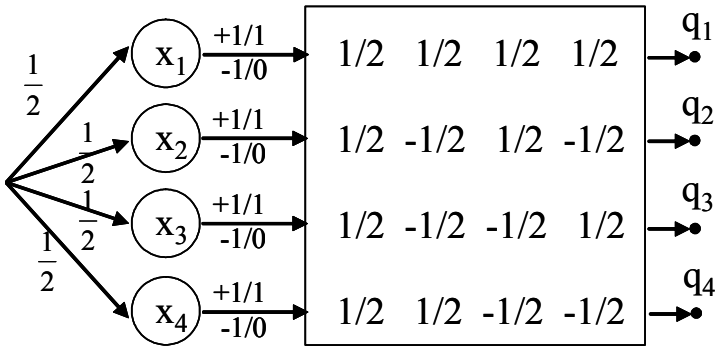
$$D_1 \quad x_1 - x_2 + 2x_3 - 2x_4$$
$$D_2 \quad x_1 + 2x_2 - 2x_3 - x_4$$
$$D_3 \quad x_1 + 2x_2 - x_3 - 2x_4$$
$$D_4 \quad 2x_1 - 2x_2 + x_3 + x_4 - 1$$
$$D_5 \quad x_1 + x_2 + 2x_3 - 2x_4 - 1$$
$$D_6 \quad x_1 + x_2 + 2x_3 + 2x_4 - 3$$

Ir viegli redzēt, ka polinomus funkcijām D_1,D_2 un D_3 var iegūt vienu no otra, mainot mainīgos vietām. Tas pats attiecās arī uz funkcijām D_4 un D_5. Funkcijai D_2 ir 0 vērtības, ja ieejas vektors ir simetrisks.

$$D_1(x_1,x_2,x_3,x_4) = D_2(x_2,x_3,x_4,x_1) = D_3(x_1,x_3,x_2,x_4)$$
$$D_4(x_1,x_2,x_3,x_4) = D_5(x_3,x_4,x_1,x_2)$$

Vēl var ievērot, ka visām funkcijām D_i izpildās nosacījums $D_i(x_1,x_2,x_3,x_4) = D_i(1-x_1,1-x_2,1-x_3,1-x_4)$. Šī īpašība seko no tā, ka funkcijas ir balstītas uz PARITY un ¬PARITY funkcijām.

4.2.4. zīmējumā ir redzams cits algoritms, kas varētu rēķināt kādu Bula funkciju. Dotās funkcijas vērtības būs atkarīgas no gala stāvokļiem piekārtotajām vērtībām.



4.2.4. att. **Nedeterminētu kvantu algoritms**

Katrs no šī algoritma izejas stāvokļiem var ar varbūtību 1 atpazīt divus ieejas vektorus (x_1 x_2 x_3 x_4) un (1-x_1 1-x_2 1-x_3 1-x_4).Piemēram, stāvoklis q_1 atpazīst (0 0 0 0) un (1 1 1 1), bet stāvoklis q_3 – (0 0 1 1) un (1 1 0 0). Stāvokļi q_2, q_3 un q_4 ir savstarpēji simetriski, tos var iegūt vienu no otra mainot mainīgos vietām. Ja izvēlas divus izejas stāvokļus, tad var atpazīt četrus ieejas vektorus. Maksimālais izejas stāvokļu skaits ar vienu vērtību netriviālai funkcijai ir 3. Ja visiem izejas stāvokļiem tiek piekārtota viena vērtība, tad tiek iegūta konstanta funkcija.

Tabulā 4-2.var redzēt funkciju E_1, ...E_6 nulles vērtības. Funkciju nedeterminētie kvantu vaicājošie algoritmi tiek iegūti piešķirot diviem izejas stāvokļiem vērtību 0.

E_1 (q_1,q_2)	E_2 (q_1,q_3)	E_3 (q_1,q_4)	E_4 (q_2,q_3)	E_5 (q_2,q_4)	E_6 (q_3,q_4)
x_1 x_2 x_3 x_4	x_1 x_2 x_3 x_4	x_1 x_2 x_3 x_4	x_1 x_2 x_3 x_4	x_1 x_2 x_3 x_4	x_1 x_2 x_3 x_4
1 1 1 1	1 1 1 1	1 1 1 1	0 1 0 1	0 1 0 1	0 0 1 1
0 0 0 0	0 0 0 0	0 0 0 0	1 0 1 0	1 0 1 0	1 1 0 0
0 1 0 1	0 0 1 1	0 1 1 0	0 0 1 1	0 1 1 0	0 1 1 0
1 0 1 0	1 1 0 0	1 0 0 1	1 1 0 0	1 0 0 1	1 0 0 1

Tabula 4-2.

Viegli pamanīt, ka $E_1=D_3$, $E_2=D_1$, $E_3=D_2$ un $E_5=D_6$, un $E_4(x_1,x_2,x_3,x_4) = E_5(x_1,x_4,x_2,x_3) = E_6(x_1,x_2,x_4,x_3)$.

Atbilstošie pirmās pakāpes nedeterminētie polinomi ir:

$$E_4 \quad x_1 + 2x_2 + 2x_3 + x_4 - 3$$
$$E_5 \quad x_1 + x_2 + 2x_3 + 2x_4 - 3$$
$$E_6 \quad x_1 + 2x_2 + x_3 + 2x_4 - 3$$

Tabulā 4-3. var redzēt funkciju F_1, ...F_4 nulles vērtības. Funkciju nedeterminētie kvantu vaicājošie algoritmi tiek iegūti piešķirot trijiem izejas stāvokļiem vērtību 0.

F_1 (I,II,III)	F_2 (I,II,IV)	F_3 (I,III,IV)	F_4 (II,III,IV)
x_1 x_2 x_3 x_4	x_1 x_2 x_3 x_4	x_1 x_2 x_3 x_4	x_1 x_2 x_3 x_4
1 1 1 1	1 1 1 1	1 1 1 1	0 1 0 1
0 0 0 0	0 0 0 0	0 0 0 0	1 0 1 0
0 1 0 1	0 1 0 1	0 0 1 1	0 0 1 1
1 0 1 0	1 0 1 0	1 1 0 0	1 1 0 0
0 0 1 1	0 1 1 0	0 1 1 0	0 1 1 0
1 1 0 0	1 0 0 1	1 0 0 1	1 0 0 1

Tabula 4-3.

$$F_1(x_1,x_2,x_3,x_4) = F_2(x_1,x_4,x_3,x_2) = F_3(x_1,x_2,x_4,x_3).$$

Atbilstošie pirmās pakāpes nedeterminētie polinomi ir:

F_1 $x_1 - x_2 - x_3 + x_4$

F_2 $x_1 + x_2 - x_3 - x_4$

F_3 $x_1 - x_2 + x_3 - x_4$

F_4 $x_1 + x_2 + x_3 + x_4 - 2$

Teorēma 4-2. [9] *Ar nedeterminēto viena jautājuma kvantu nedeterminēto algoritmu nevar atpazīt nekonstantu funkciju, kurai F(x)=F(y) =0 un ||x|-|y|| = 1.*

Pierādījums: Ja funkciju var atpazīt ar viena jautājuma nedeterminēto kvantu vaicājošo algoritmu tad tai eksistē pirmās pakāpes nedeterminēts polinoms. Pieņemsim, ka x =(0,0,0,0) un y= (1,0,0,0), (0,1,0,0), (0,0,1,0) un (0,0,0,1). Funkcijas polinomu var pierakstīt formā $c_0+c_1x_1+c_2x2+c_3x_3+c_4x_4$. Tā kā F(0,0,0,0)=0, tad c_0=0. No F(y)=0 seko c_1=1,c_2=0,c_3=0 un c_4=0. Mēs iegūstam konstantu funkciju.

Kā var redzēt no iepriekšējiem piemēriem maksimālais 0 vērtību skaits ir 6. Rodas jautājums, vai ar viena jautājuma nedeterminētu kvantu algoritmu var atpazīt funkcijas ar vairāk 0 vērtībām.

No Teorēmas 4-2. seko, ka vienīgie potenciālie 0 vērtības kandidāti ir :

I.{(0000) (1100) (1010) (1001) (0110) (0101) (0011) (1111)}

II. {(1000) (0100) (0010) (0001) (1110) (1101) (1011) (0111)}

Funkcijas polinomu izsaka kā $c_0+c_1x_1+c_2x_2+c_3x_3+c_4x_4$

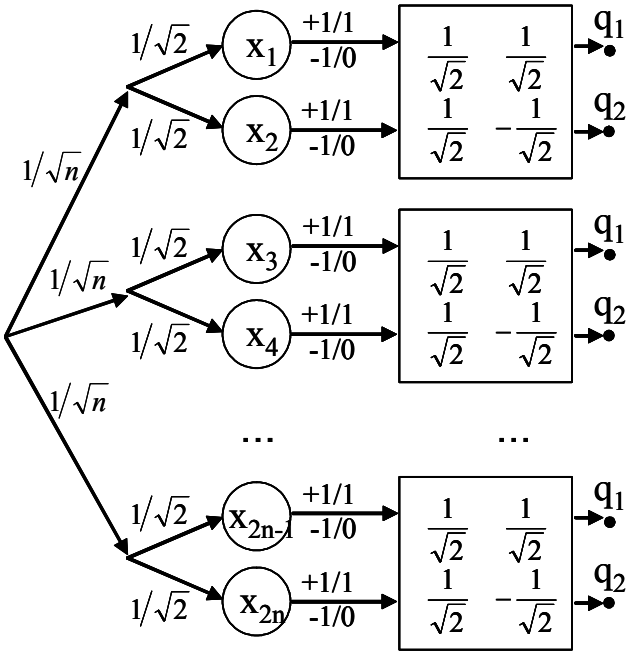
I. $c_0=0$ no pirmā ieejas vektora.
c1+c2=0 (2), $c_1+c_3=0$ (3), $c_1+c_4=0$ (4), $c_2+c_3=0$ (5), $c_2+c_4=0$ (6), $c_3+c_4=0$ (7),
$c_1+c_2+c_3+c_4=0$ (8)
No 2.,3.,4. seko $c_2=c_3=c_4=-c_1$
No 5. un 6. seko $c_2=c_3=c_4 = 0$ un arī $c_1=0$
Atkal tiek iegūta konstanta funkcija.

II. $c_0+c_1=0$ (1) $c_0+c_2=0$ (2) $c_0+c_3=0$ (3) $c_0+c_4=0$ (4)
$c_0+c_1+c_2+c_3=0$ (5) $c_0+c_1+c_2+c_4=0$ (6) $c_0+c_1+c_3+c_4=0$ (7) $c_0+c_2+c_3+c_4=0$ (8)
No 1.,2.,3., un 4. seko $c_1=c_2=c_3=c_4= -c_0$
Lai izpildītos 5. un 6. ir nepieciešams lai $c_0=c_1=c_2=c_3=c_4=0$.
Atkal tiek iegūta konstanta funkcija.

4.2.3. Bula funkcijas ar n mainīgajiem

Aplūkosim dažus vispārīgus piemērus, ka veidot nedeterminētus kvantu algoritmus ar vienu jautājumu. Ja izmanto PARITY un ¬PARITY funkciju algoritmus tad var iegūt 2^n dažādus nedeterminētus kvantu vaicājošos algoritmus. Katram šim algoritmam būs 2^{2n} dažādi ieejas vektori, bet tikai 2^n no tiem būs funkcijas vērtība 0.

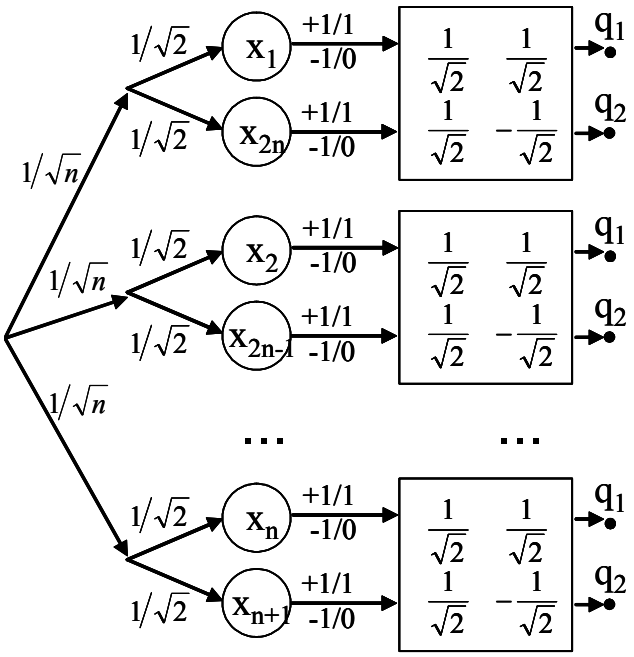
.



4.2.5. att. **Nedeterminēts kvantu algoritms balstīts uz Paritātes funkciju**

Viens no šiem algoritmiem dod funkcijas vērtības 0 uz ieejas vektoriem ((00)*(11)*)*. Šādu algoritmu var iegūt izmantojot 4.2.5. zīmējumā attēloto algoritmu, ja visām izejam q_1 tiek piekārtota funkcijas vērtība 0. Atbilstošais nedeterminētais polinoms ir $\sum_{i=1}^{n} i(x_{2i-1} - x_{2i})$.

Ir iespējams izveidot nedeterminētu kvantu vaicājošo algoritmu, kas dod funkcijas vērtību 0, ja ieejas vektors ir simetrisks. Dotais algoritms ir attēlots 4.2.6. zīmējumā. Funkcijas vērtība 0 tiek piekārtota izejām q_1. Šādas funkcijas nedeterminētais polinoms ir $\sum_{i=1}^{n} i(x_i - x_{2n-i+1})$.



4.2.6. att. **Nedeterminēts kvantu algoritms balstīts uz Paritātes funkciju**

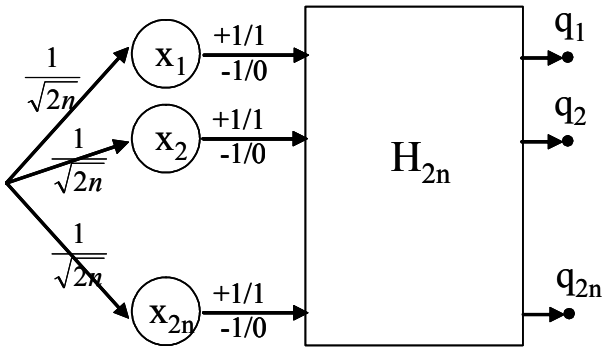
Ja eksistē nedeterminēti kvantu vaicājošie algoritmi ar $k_1,k_2<2n$ mainīgajiem un $k_1+k_2=2n$, tad ir iespējams izveidot nedeterminētu kvantu vaicājošo algoritmu ar 2n manīgajiem izmantojot 4-1. teorēmu. Ir iespējams apvienot ne tikai divus algoritmus, bet arī vairāk kā divus algoritmus.

Vienkāršākais pirmās pakāpes polinoms ir $x_1+x_2+x_3+...$. Ja $c_0=0$, tad funkcijai vērtība 0 ir tikai ieejas vektoram (00...0) un tā ir funkcija OR. Ir iespējams izveidot nedeterminētu kvantu vaicājošo algoritmu ar vienu jautājumu funkcijai OR 2n mainīgo gadījumam. Tas ir jāveido līdzīgi kā divu mainīgo gadījumā, kas attēlots 4.2.1. nodaļā.

Ja c_0=-n, tad polinoms ir $-n+\sum_{i=1}^{2n} x_i$, tad tiek iegūta funkcija P, kas dod 0 vērtības, ja ieejas vektorā ir n vieninieki un n nulles (|x|=n). Ir C_{2n}^{n} šādi ieejas vektori.

Teorēma 4-3. [9] *Eksistē nedeterminēts kvantu vaicājošais algoritms funkcijai P ar vienu jautājumu.*

Pierādījums: Atbilstošais nedeterminētais kvantu vaicājošais algoritms ir redzams 4.2.7. zīmējumā. Ja funkcijas vērtība ir 0, tad algoritmam pēc jautājuma uzdošanas ir n pozitīvas un n negatīvas amplitūdas, tātad algoritma izejā q_1 ir amplitūda 0. Tas nozīmē, ka izejai q_1 atbilst funkcijas vērtība 0, bet pārējam izejam ir piekārtota funkcijas vērtība 1. Algoritms dod atbildi 0 ar varbūtību 1, ja funkcijas vērtība ir 0. Ja funkcijas vērtība ir 1, tad pēc jautājuma uzdošanas algoritmam ir n+k pozitīvas un n-k negatīvas amplitūdas (k≠n).



4.2.7. att. **Nedeterminēts kvantu algoritms**

Teorēma 4-4. [9] *Eksistē nedeterminēts kvantu vaicājošais algoritms ar vienu jautājumu funkcijai ar 2n mainīgajiem, kura nedeterminētais polinoms ir* $-k+\sum_{i=0}^{2n} x_i$, *0≤k≤2n.*

Pierādījums: Ja c_0=-k, tad dotajai funkcijai ir vērtības 0, ja ieejas vektorā ir k vieninieki (|x|=k). Mēs pievienojam iepriekšējam algoritmam 2n stāvokļus un tad lietojam Adamāra matricu H_{4n}. Sākotnējais amplitūdu sadalījums tiek veidots tā, ka pievienotie stāvokļi simulē ieejas vektoru ar k nullēm un 2n-k vieniniekiem. Izveidotais algoritms dod funkcijas vērtību 0, ja |y|=2n un dota problēma reducējās uz funkciju P (teorēma 4-3.).

Teorēma 4-5. [9] *Eksistē nedeterminēts kvantu vaicājošais algoritms ar vienu jautājumu funkcija, kuras nedeterminētais polinoms ir* $\sum_{i=1}^{2n} x_{2i-1} - x_{2i}$.

Pierādījums: Algoritms tiek veidots līdzīgi kā 4-3. teorēmā, izņemot to, ka funkcijas vērtība 0 tiek piekārtota izejai q_2, bet pārējām izejam –1 . Funkcija dod vērtību 0, tikai tad, kad ieejas vektorā ir k vieninieki pāra pozīcijas un k vieninieki nepāra pozīcijās. Otrā rinda Adamāra matricā sastāv no viena pēc otra sekojošiem $1/\sqrt{2n}$ un $-1/\sqrt{2n}$. Ja funkcijas vērtība ir 0, tad algoritmam ir amplitūda 0 stāvoklī q_2. Citos gadījumos stāvoklī q_2 ir ne nulles amplitūda.

5. KVANTU VAICĀJOŠIE ALGORITMI AR PĒCATLASI

5.1. Pēcatlases vispārējie principi

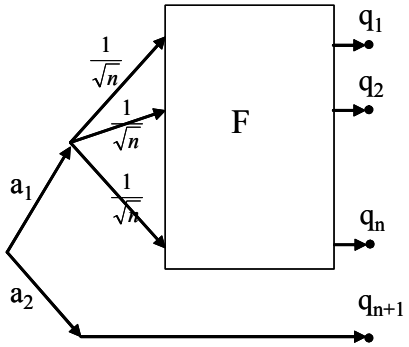
Vispārīgi kvantu algoritmi ar pēcatlasi tiek definēti Scott Aaronson darbā [33]. Kvantu algoritma beigu stāvokļu kopa, kas parasti sastāv no akceptējošiem un noraidošiem stāvokļiem, tiek papildināta ar parametru, kas norāda, vai dotais beigu stāvoklis ietilpst atlases kopā. Mērījumi tiek veikti tikai atlases kopas beigu stāvokļos.

5.2. Kvantu vaicājošo algoritmu ar pēcatlasi veidošana

Definīcija: Kvantu vaicājošais algoritms ar pēcatlasi ir kvantu vaicājošais algoritms ar speciālu stāvokļu kopu, kas ir atzīmēti, kā atlases kopa. Algoritma darba beigās, pirms mērījuma izdarīšanas, stāvokļos, kas atrodas ārpus atlases kopas, amplitūdas mehāniski tiek pielīdzinātas nullei. Atlases kopas stāvokļu amplitūdas tiek normalizētas, tas ir pareizinātas ar pozitīvu reālu skaitli tā, lai amplitūdu moduļu summa būtu 1.

Teorēma 5-1. *Ja eksistē nedeterminēts kvantu vaicājošais algoritms F ar q jautājumiem, kas rēķina funkciju f, tad eksistē kvantu vaicājošais algoritms ar pēcatlasi, kas rēķina funkciju f uzdodot q jautājumus ar varbūtību 2/3.*

Pierādījums: Ja F ir nedeterminēts kvantu vaicājošais algoritms, kas rēķina funkciju f un Q_1 ir akceptējošo beigu stāvokļu kopa (f(x)=1) un Q_0 ir noraidošo beigu stāvokļu kopa (f(x)=0), tad :Ja funkcijas vērtība ir 0, tad $\forall q_i \in Q_1$ $a_{qi}=0$ (a_{qi} –amplitūda stāvoklī q_i) un $\sum_{qi\in Q0}\left|a_{qi}\right|^2=1$. Ja funkcijas vērtība ir 1, tad $\exists\, q_j \in Q_1 \mid a_{qj} \mid >0$.
Apzīmējam ar $a_m= \min_{qi\in Q1}(a_{qi})$, minimālo funkcijas f vērtības 1 akceptēšanas amplitūdu.



5.2.1. att. Kvantu vaicājošais algoritms ar pēcatlasi

5.2.1. zīmējumā ir parādīti kvantu vaicājošā algoritma ar pēcatlasi veidošanas principi, izmantojot nedeterminētu kvantu vaicājošo algoritmu. Stāvoklis q_{n+1} atbilst funkcijas vērtībai 0. Pārējie beigu stāvokļi saglabājas iepriekšējie. Ir nepieciešams atrast manīgā a_1 vērtību.

$$\frac{a_1 a_m}{\sqrt{2}} = \sqrt{1-a_1^2} \Rightarrow a_1 = \sqrt{\frac{2}{a_m^2+2}},\ a_2 = \sqrt{\frac{a_m^2}{a_m^2+2}}$$

Ja $a_m = \frac{1}{\sqrt{n}}$ tad $a_1 = \sqrt{\frac{2n}{1+2n}}$ $a_2 = \sqrt{\frac{1}{1+2n}}$.

Atlases kopā tiek ievietoti visi stāvokļi no kopas Q_1 un stāvoklis q_{n+1}.

Ja funkcijas vērtība ir 0, tad $\forall q_i \in Q_1$ $a_{qi}=0$ un vienīgi stāvoklī q_{n+1} ir nenulles amplitūda. Tātad pēc normalizācijas tiek iegūta pareiza atbilde ar varbūtību 1.

Ja funkcijas vērtība ir 1 un atpazīšanas amplitūda ir minimālā - $a_m = 1/\sqrt{n}$, tad amplitūda stāvoklī q_{n+1} ir $\sqrt{1/(1+2n)}$ - šis stāvoklis atbilst funkcijas vērtībai 0. Kopējā amplitūda, kas atbilst funkcijas vērtībai 1 ir $\sqrt{2/(1+2n)}$. Pēc normalizācijas ($k = \sqrt{(1+2n)/3}$) tiek iegūtas amplitūdas $\sqrt{1/3}$ (f(x)=0) un $\sqrt{2/3}$ (f(x)=1), tātad pareizās atbildes varbūtība ir 2/3.

Teorēma 5-2. *Ja eksistē nedeterminēts kvantu vaicājošais algoritms F ar q jautājumiem, kas rēķina funkciju f, tad eksistē kvantu vaicājošais algoritms ar pēcatlasi, kas rēķina funkciju ¬f uzdodot q jautājumus ar varbūtību 2/3.*

Pierādījums: Kvantu vaicājošais algoritms ar pēcatlasi tiek veidots līdzīgi kā 5-1. teorēmā, tikai beigu stāvokļiem būs piekārtotas citas funkcijas vērtības. Stāvoklis q_{n+1} atbildīs funkcijas vērtībai 1, bet dotā algoritma beigu stāvoļiem tiks nomainītas atbilstošās funkcijas vērtības uz pretējām.

Tātad, ja funkcijas vērtība ir 0, tad $\exists\ q_j \in Q_0 \mid a_{qj} \mid > 0. \forall q_i \in Q_1$ $a_{qi}=0$. Bet ja funkcijas vērtība tad, $\forall q_i \in Q_0$ $a_{qi}=0$.

Atlases kopā tiek ievietoti visi stāvokļi no kopas Q_0 un stāvoklis q_{n+1} un pareizās atbildes varbūtība tiek iegūta vismaz 2/3.

NOBEIGUMS

Darba uzdevums bija veikt pētījumus kvantu vaicājošo algoritmu jomā. Darba gaitā ir sasniegti sekojoši rezultāti:

Iegūstot kvantu vaicājošo algoritmu apakšējos novērtējumus tika lietotas A. Ambaiņa pierādītās teorēmas apakšējo novērtējumu iegūšanai. Teorēmu lietojums balstās uz kopu A un B atrašanu. Darbā autore ir atradusi vairākus netriviālu un interesantu kopu piemērus ar kuru palīdzību tiek pierādīti vairāku problēmu apakšējie novērtējumi. Tomēr dotie uzdevumi, kuriem ir atrasti apakšējie novērtējumi nav visai pateicīgi konkrētu kvantu vaicājošo algoritmu veidošanā, jo tiem atbilstošās Bula funkcijas sanāk visai sarežģītas.

Otrajā darba nodaļā tiek aplūkoti dažādi kvantu algoritmu veidošanas un uzlabošanas varianti. Dažas no pierādītajām teorēmām tiek izmantotas konkrētu kvantu vaicājošo algoritmu veidošanā. Dažas no pierādītajām teorēmām nav tieši izmantojamas vienkāršo kvantu vaicājošo algoritmu veidošanā, bet šo teorēmu idejas ir iespējams izmantot nedeterminēto un kvantu vaicājošo algoritmu ar pēcatlasi gadījumos.

Konkrētu kvantu algoritmu veidošanā tiek izmantotas vairākas idejas. Veidojot precīzus kvantu vaicājošos algoritmus, viena no algoritmu kopām tiek veidota uz funkcijas XOR pamata. Vēl viens variants ir mēģināt atrast unitāras transformācijas un Bula funkcijas, kas atbilst šīm unitārajām transformācijām. Kvantu vaicājošo algoritmu ar kļūdas varbūtību veidošanā tiek izmantota Grovera amplitūdu palielināšanas metode.

Nedeterminēto kvantu vaicājošo algoritmu jomā tika pievērsta uzmanība algoritmiem ar vienu jautājumu. Tika uzkonstruēti vairāki konkrēti algoritmi ar vienu jautājumu, kā arī tika veikta analīze par iespējamiem funkciju kandidātiem.

Darba ietvaros tiek ieviests jauns kvantu vaicājošo algoritmu veids- kvantu vaicājošie algoritmi ar pēcatlasi. Tiek pierādīta šo algoritmu saistība ar nedeterminētiem kvantu vaicājošajiem algoritmiem un nodemonstrēta iespēja, kā šādus algoritmus izveidot.

Tālākajos pētījumos galveno uzmanību ir plānots pievērst nedeterminētajiem kvantu vaicājošajiem algoritmiem un kvantu vaicājošajiem algoritmiem ar pēcatlasi.

LITERATŪRAS SARAKSTS

Autora publikācijas recenzētos starptautisku konferenču materiālos

1. Lelde Lace - Some examples to show advantages of probabilistic and quantum decision trees. *Proceedings of the "Quantum Computation and Learning"*, Latvia, 2002, pp. 42-49.

2. Lelde Lace, Rusins Freivalds - Lower bounds for query complexity of some graph problems *Proceedings of International Conference on VLSI,* USA, 2003, pp. 309-313.

3. Aija Berzina, Andrej Dubrovsky, Rusins Freivalds, Lelde Lace, Oksana Scegulnaja - Quantum Query Complexity for Some Graph Problems. *Lecture Notes in Computer Science,* 2004, vol. 2932, pp. 140-150.

4. Lelde Lāce, Rūsiņš Freivalds - Lower Bounds for Query Complexity of Some Graph and Matrix Problems. *Proceedings of Baltic DB&IS 2004*, vol. 2, Riga, Latvia, pp.46-56

5. Lelde Lāce - Enlarging Gap between Quantum and Deterministic Query Complexities. *Proceedings of Baltic DB&IS 2004*, vol. 2, Riga, Latvia, pp.81-91.

6. Lelde Lace - "Enlarging gap between quantum and classical query complexities", *Proceedings of WCC 2004 Student forum*, Touluse, France, pp.275-283.

7. Lelde Lāce, Renāte Praude, Rūsiņš Freivalds - Some graph problems with equivalent lower bounds for query complexity. *FCS'05.* pp. 80-86.

8. Rūsiņš Freivalds, Lelde Lāce, Oksana Scegulnaja-Dubrovska - Two lower bounds for quantum query complexity. *QCMC'2006*, Tsukuba, Japan. pp. 101-104.

9. Lelde Lāce - Nondeterministic quantum query with minimal complexity. *Proceedings of the Satellite Workshops of DLT'2007*, Turku, Finland. pp. 55-64.

10. Lelde Lāce - Nondeterministic and postselection quantum query algorithms. *FCS'08*. (pieņemts publicēšani)

Citas autora publikācijas (tieši nesaistītas ar promocijas darba tēmu)

11. A.R.Silins, L.A.Lace.- Influence of stoichiometry on high temperature intrinsic defects in fused silica. - *J.Non-Crystalline Solids,* 1992, vol.149, pp.54-61.

12. A..Silins, L. Lace, A.Lukjanska. - Point Defect Equilibrium Concentrations at High Temerature in Fused Silica. - *Latv. J. of Phys. and Techn. Sci*., 1999, N5, pp. 3-15.

13. Raitis Ozols, Rusins Freivalds, Jevgenijs Ivanovs, Elina Kalnina, Lelde Lace, Masahiro Miyakawa, Hisayuki Tatsumi, Daina Taimina- Boolean Functions with a Low Polynomial Degree and Quantum Query Algorithms. *SOFSEM 2005.* pp. 408-412

14. Rūsiņš Freivalds, Lelde Lāce, Masahiro Miyakawa - Quantum Zero Error and Exact Algorithms That Can be Composed., *EQIS'05*. pp. 173-174.

15. Ramuns Usovs, Agnese Zalcmane, Oksana Scegulnaja-Dubrovska, Lelde Lace - Quantum cryptographic key distribution protocols., *FCS'06.*

16. Audris Kalnins, Janis Barzdins, Edgars Celms, Lelde Lace, Martins Opmanis, Karlis Podnieks, Andris Zarins - The First Step Towards Generic Modelling Tool. *Proceedings of Baltic DB&IS 2002*, Tallinn, 2002, v. 2, pp. 167-180.

17. Lace,L., Celms,E., Kalnins,A - Diagram definition facilities in a generic modeling tool. *Proceedings of the International Conference Modelling and Simulation of Business systems*, Vilnius, 2003, pp. 220-224.

18. Celms E., Kalnins A., Lace L. - Diagram definition facilities based on metamodel mappings. *Proceedings of the 18th International Conference, OOPSLA'2003*, Workshop on Domain-Specific Modeling, Anaheim, California, USA, October 2003, pp. 23-32.

19. Janis Barzdins, Andris Zarins, Karlis Cerans, Audris Kalnins, Edgars Rencis, Lelde Lace, Renars Liepins, Arturs Sprogis- GrTP: Transformation Based Graphical Tool Building Platform. *MDDAUI 2007.*

Citi darbā izmatotie avoti

20. David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society,* London, A400:97-117, (1985).

21. L. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th ACM symposium on Theory of Computing*, pp 212-219, 1996.

22. Charles H. Bennett, Ethan Bernstein, Gilles Brassard, Umesh V. Vazirani. Strengths and Weaknesses of Quantum Computing. *SIAM Journal on Computing, v. 26*, 1997, pp. 1510 –1523.

23. Richard Cleve, Arthur Ekert, Chiara Macchiavello, Michele Mosca. Quantum Algorithms Revisited. *Proceedings of the Royal Society London, A454* (1998) pp. 339-354.

24. J. Gruska. Quantum Computing. *McGraw-Hill*, 1999.

25. H.Burman, R.Cleve, R. de Wolf and Ch Zalka. Bounds for Small-Error and Zero-Error Quantum Algorithms. *40th IEEE Symposium on Foundations of Computer Science (FOCS'99)*, pp. 358-368.

26. M. Nielsen, I. Chuang. Quantum Computation and Quantum Information. *Cambridge University Press*, 2000.

27. R. de Wolf. Quantum Computing and Communication Complexity. *University of Amsterdam,* 2001.

28. H. Buhrman and R. de Wolf. Complexity Measures and Decision Tree Complexity : *A Survey. Theoretical Computer Science,* v. 288(1): 21-43 (2002)

29. A.Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences,* 64:750-767, 2002.

30. A.Ambainis. Quantum query algorithms and lower bounds(survey article). *Proceedings of FOTFS III.*

31. R.de Wolf. Nondeterministic Quantum Query and Quantum Communication Complexities. *SIAM Journal on Computing*, 32(3):681-699, 2003.

32. Gatis Midrijānis. Exact quantum query complexity for total Boolean functions. 2004. *pieejams internetā http://arxiv.org/abs/quant-ph/0403168*

33. Scott Aaronson. Quantum Computing, Postselection, and Probabilistic Polynomial-Time. *Proceedings of the Royal Society* A, 461(2063):3473-3482, 2005.