EIROPAS SOCIĀLAIS FONDS

IEGULDĪJUMS TAVĀ NĀKOTNĒ

EIROPAS SAVIENĪBA

„Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku”
Nr. 2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

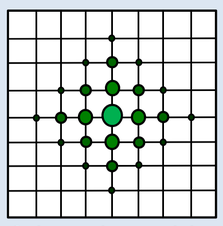
Pētījumi kvantu skaitļošanā

Kvantu algoritmi

A. Ambainis, N. Nahimovs, A. Rivošs, J. Smotrovs

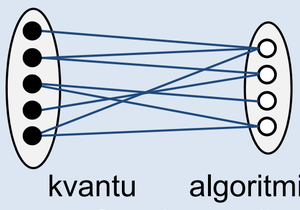
Kvantu klejošana plaknē

Veikti datoreksperimenti par kvantu klejošanas izmantošanu kvantu algoritmu konstruēšanā. Analītiski pierādīts, ka kvantu klejošanu plaknē var izmantot meklēšanā plaknē efektīvākā veidā nekā iepriekšējos kvantu algoritmos.



Kvantu algoritmi grafu problēmām

- Atrasti efektīvāki kvantu algoritmi divdaļu (bipartite) grafu noteikšanai.
- Atrasti efektīvāki kvantu algoritmi ierobežotas pakāpes grafu ekspansijas noteikšanai.



Apakšējo novērtējumu pierādīšana kvantu algoritmiem

Apakšējie novērtējumi ir rezultāti, kas pierāda, ka noteiktu problēmu nevar atrisināt ātrāk par noteiktu laiku. Ja apakšējais novērtējums sakrīt ar labākā algoritma darbības laiku, tad mēs zinām, ka algoritms ir optimāls un to nav iespējams tālāk uzlabot.

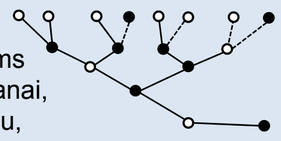
Galvenie rezultāti:

- Pabeigts darbs pie metodes, kā pierādīt kvantu apakšējos novērtējumus, izmantojot simetrijas. (Izmantotais matemātiskais aparāts: grupu reprezentāciju teorija.) Metode izmantota, lai pierādītu, ka risinot vairākus meklēšanas uzdevumus vienlaikus, labākais iespējamais kvantu algoritms ir katra meklēšanas uzdevuma risināšana neatkarīgi no pārējiem meklēšanas uzdevumiem.
- Atrastas jaunas metodes, lai pierādītu apakšējos novērtējumus kvantu stāvokļu ģenerēšanas problēmai. Ar šo metodi pierādīts, ka indeksu dzēšanas (*Index erasure*) problēmas apakšējais novērtējums sakrīt augšējo novērtējumu.
- Pierādīts, ka simetriskām funkcijām kvantu vaicājošo algoritmu modelī kvantu paātrinājums ir ne vairāk kā polinomiāls: ja funkciju var izrēķināt ar kvantu algoritmu, kas izmanto Q vaicājumus, to var izrēķināt arī ar klasisku algoritmu, kas izmanto $O(Q^9)$ vaicājumus.

AND-OR formulu rēķināšanas algoritms

Jebkura AND-OR formula ar garumu N kvantu datorā var būt aprēķināta laikā $N^{1/2+o(1)}$.

Vispārināts iepriekš zināmais kvantu algoritms loģikas formulu rēķināšanai, iegūstot kvantu algoritmu, kas ne tikai izrēķina formulas vērtību, bet arī atrod sertifikātu šai vērtībai. (Sertifikāts ir mainīgo, kuru vērtības nosaka formulas vērtību, kopa.)



Grovera algoritms ar kļūdām

Grovera algoritms:

0	1	0	…	0
x_1	x_2	x_3	…	x_n

Atrast i, kuram $x_i = 1$.

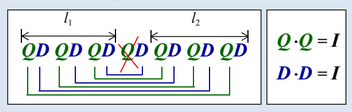
Melnā kaste, saņem i, izdod x_i.

Klasiski, n soļi.

Kvantu algoritms: $O(\sqrt{n})$ soļi [Grover, 1996].

Atklāti gadījumi, kad algoritms pārstās darboties, kaut arī tā darbības laikā ir notikusi tikai viena kļūda. Tika dots vispārinājums patvaļīgam kļūdu skaitam.

Secinājums: Grovera algoritms ir pietiekoši sensitīvs pret noteiktiem kļūdu veidiem



Kvantu eksaktie algoritmi

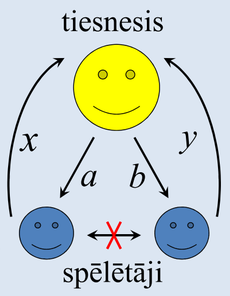
Pētīti kvantu algoritmi, kas vienmēr izdod pareizo atbildi. Šādus kvantu algoritmus sauc par eksaktiem kvantu algoritmiem un konstruēt šādus kvantu algoritmus ir daudz grūtāk nekā parastos kvantu algoritmus, kuri var izdod nepareizo atbildi ar nelielu varbūtību.

Rezultāts: atrasts pirmais piemērs vaicājošo algoritmu modelī, kur eksakti kvantu algoritmi ir vairāk nekā 2 reizes efektīvāki par klasiskajiem algoritmiem.

Kvantu nelokalitāte un kvantu spēles

A. Ambainis, D. Kravčenko, A. Škuškovniks, J. Smotrovs

Nelokālās spēles ir spēles, kurās spēlētāji spēles laikā nevar sazināties, tomēr cenšas risināt kādu uzdevumu, kura atrisinājums atkarīgs no visu viņu ieejas datiem, lai arī katrs spēlētājs redz tikai savus ieejas datus (ieejas datus spēlētāji saņem no tiesneša, kas tos izsūta atbilstoši kādam varbūtību sadalījumam). Uzdevuma risināšanā spēlētāji parasti drīkst izmantot kopīgu nejaušību. Klasiskajā gadījumā tā ir nejaušu bitu virkne, ar kuru pirms spēles spēlētāji dalās savā starpā. Kvantu gadījumā tas ir kvantu sapīts stāvoklis, kura daļas pirms spēles spēlētāji izdala savā starpā. Spēlētāju sasniegumi tiek mērīti ar spēles vērtību, kas ir starpība starp varbūtību, ka spēlētāji uzdevumu atrisina un varbūtību, ka tie to neatrisina.



Galvenie rezultāti:

- Izstrādātas jaunas metodes XOR spēļu analīzei, ja ir vairāk kā 2 spēlētāji.
- Atklāts, ka gandrīz visām XOR spēlēm kvantiski var sasniegt vismaz 1,2 reizes labāku vērtību nekā klasiski.
- Nejaušām nelokālām spēlēm ar N spēlētājiem (XOR spēļu modelī) kvantu stratēģijas sasniedz reizes lielāku $\Theta\left(\sqrt{\log N}\right)$ vērtību nekā labākā klasiskā stratēģija.

Kvantu galīgie automāti

R. Freivalds, M. Golovkins, M. Kravcevs, A. Škuškovniks

Katrai R1 valodai (R-triviālai idempotentai valodai) tika definēta noteikta veida lineāru nevienādību sistēma. Noskaidrots, ka R1 valodu var pazīt ar kvantu galīgo automātu tad un tikai tad, ja valodai atbilstošā lineāru nevienādību sistēma ir savietojama. Turklāt, ja nevienādību sistēma ir savietojama, tad ar tās atrisinājuma palīdzību var uzkonstruēt kvantu automātu, kas pazīst atbilstošo R1 valodu. Tika noskaidrots, ka vesela virkne kvantu automātu modeļu (kvantu galīgie automāti, varbūtiskie apgriežamie automāti, Najaka kvantu automāti un bistohastiskie kvantu automāti) pazīst vienas un tās pašas R1 valodas. Pierādīta virkne rezultātu par kvantu galīgiem automātiem ar izeju (transdjūseriem).

Tā kā kvantu automātiem, kuriem bez kvantu informācijas eksistē arī makroskopiska informācija (izdrukas uz lentes, galviņu novietojums uz lentes, u.c.), amplitūdu saskaitīšanai ir savas īpatnības, iespējams iegūt rezultātus, kas ir atšķirīgi gan no determinētiem, gan arī no tradicionālajiem kvantu automātiem.

Pierādīts, ka līdz šim zināmās aizliegtās konstrukcijas neaptver visu to regulāro valodu klasi, kuras nevar pazīt ar kvantu automātiem. Vienlaicīgi ir pētīta arī kvantu operāciju dinamika, kvantu operāciju izpildot vairākas reizes pēc kārtas.

Veikti pētījumi par R1 valodām varbūtiskiem apgriežamiem automātiem bez sākuma marķieriem. Pierādīts, ka apstādināmie varbūtiskie apgriežamie automāti bez sākuma marķiera pazīst tikai apakškopu no tām valodām, ko apstādināmie varbūtiskie apgriežamie automāti ar sākuma marķieri..

Kvantu loģika un zināšanu reprezentācija

J. Cīrulis

Veikti pētījumi par sekojošiem jautājumiem:

- Kvantu loģikas, daudzvērtīgās loģikas un informāciju sistēmas algebriskie modeļi.
- Algebriskās struktūras, kurām ir tiešs sakars ar (algebrisko) kvantu loģiku, kā arī ar t.s. aproksimācijas operatoriem raupjo kopu (*rough sets*) teorijā.
- Kvantu loģikas un noteikta tipa informācijas sistēmu algebrisko modeļu kopīgās un atšķirīgās īpašības.

Kvantu stāvokļu konfigurācijas

A. Ambainis, J.Smotrovs

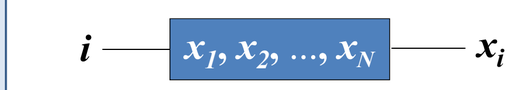
Veikti pētījumi vairākos jautājumos, kas saistīti ar kvantu stāvokļiem kā ģeometriskiem objektiem un to konfigurācijām.

- Svarīgākais rezultāts ir kvantu Lovaša (*Lovasz*) lemma – ungāru matemātiķa L. Lovaša 1975. gadā pierādītās lokālās lemmas vispārinājums kvantu stāvokļiem. Kvantu Lovaša lemma apskata nosacījumus attiecībā uz kvantu stāvokļiem. Ja katru nosacījumu apmierinošie stāvokļi veido apakštelpu ar lielu dimensiju skaitu un nosacījumi ir gandrīz neatkarīgi, tad kvantu Lovaša lemma garantē, ka eksistē kvantu stāvoklis, kas apmierina visus nosacījumus. Kvantu Lovaša lemma iegūta sadarbībā ar zinātniekiem no Telavivas universitātes (J. Kempe un O. Sattath) un uzskatāma par nozīmīgu projekta aktivitātes sasniegumu. Raksts par šo lemmu publicēts pasaules vadošajā konferencē datorzinātņu teorijā – *ACM Symposium on Theory of Computing*.
- Otrs pētījumu virziens ir savstarpēji nenosliektas bāzes (SNB; angliski „*Mutually unbiased bases*”, MUB). SNB ir noteikti vienmērīgi vektoru (ortonormētu bāžu) izvietojumi daudzdimensiju telpā, kas ir nozīmīgi kvantu mehānikā un informācijas teorijā. Tiek pētīts jautājums, vai n dimensiju telpā ir iespējams izvietot n+1 savstarpēji nenosliektu bāzi. Pētījumā tiek izmantotas sakarības starp SNB vektoru izvietojumus un noteiktiem kombinatoriskiem skaitļu izvietojumiem (relatīvām starpībkopām, nesen jaunaplūkotajām multistarpībkopām u.c.). Pētījuma ietvaros ir izdevies pierādīt dažu šādu izvietojumu neiespējamību, tomēr lielākajā daļā gadījumu jautājums joprojām paliek atklāts.

Būla funkciju vaicājumsarežģītība

A. Ambainis, J.Smotrovs

Melnās kastes modelis



Kvantu skaitļošanā:

$$\sum_i a_i |i\rangle \longrightarrow \boxed{x_1, x_2, \ldots, x_N} \longrightarrow \sum_i a_i (-1)^{x_i} |i\rangle$$

Cik melnās kastes izsaukumu (vaicājumu) nepieciešams, lai izrēķinātu $f(x_1, ..., x_N)$?

Iepriekšējie rezultāti:

- [van Dam, 1998] kvantu algoritms, kas iegūst visus bitus $x_1, ..., x_N$, ar $N/2+O(\sqrt{N})$ melnās kastes izsaukumiem.
- Var izrēķināt jebkuru $f(x_1, ..., x_N)$.
- Vai tas ir optimāli?
- [Beals et al., 1998] Lai izrēķinātu $x_1 \oplus x_2 \oplus \ldots x_N$, vajag $N/2$ vaicājumus.

Jaunie rezultāti:

[Ambainis, Bačkurs, Smotrovs, de Wolf, 2012] Gandrīz visām $f(x_1, ..., x_N)$ vajag $N/2$-$o(N)$ vaicājumus.