

Aktivitāte „Pētījumi kvantu skaitļošanā” – 2011. gads

Aktivitāte pēta kvantu skaitļošanas teoriju. 2011. gadā notika pētījumi šādos apakšvirzienos:

- Kvantu algoritmu konstruēšana (A. Ambainis, N. Nahimovs, A. Rivošs);
- Apakšējo novērtējumu pierādīšana kvantu algoritmiem (A. Ambainis);
- Būla funkciju vaicājumsarežģītība (A. Ambainis, J. Smotrovs);
- Kvantu spēles (A. Ambainis, D. Kravčenko, A. Škuškovniks, J. Smotrovs);
- Kvantu automāti (A. Ambainis, R. M. Freivalds, M. Golovkins, M. Kravcevs);
- Kvantu loģika (J. Cīrulis).

Kvantu algoritmu konstruēšana. Viens no kvantu skaitļošanas teorijas galvenajiem uzdevumiem ir atrast uzdevumus, kurus kvantu dators spētu atrisināt ātrāk nekā tradicionālie datori. Projekta otrajā gadā iegūti sekojoši rezultāti:

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

Publikācijas:

Andris Ambainis, Andrew M. Childs, Yi-Kai Liu: Quantum Property Testing for Bounded-Degree Graphs. APPROX-RANDOM 2011: 365–376.

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. Rezultāti projekta otrajā gadā:

- 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.
- publicēts pierādījums, 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.

Publikācijas:

1. Andris Ambainis, Loïck Magnin, Martin Roetteler, Jérémie Roland: Symmetry-Assisted Adversaries for Quantum State Generation. IEEE Conference on Computational Complexity 2011: 167–177.

2. Scott Aaronson, Andris Ambainis: The Need for Structure in Quantum Speedups. ICS 2011: 338–352.

Būla funkciju vaicājumsarežģītība. Būla funkciju vaicājumsarežģītības modelis ir viens no pētītākajiem kvantu skaitļošanā: tajā var aprakstīt daudzas svarīgas skaitļošanas problēmas. Šajā modelī ir dota zināma Būla funkcija ar N argumentiem un melnā kaste, kurā ir šīs funkcijas argumentu vērtības. Algoritms drīkst ar vaicājumu palīdzību prasīt melnajai kastei argumentu vērtības un, kad zina par argumentiem pietiekami daudz, izdot funkcijas vērtību. Sarežģītības mērs ir vaicājumu skaits. Skaidrs, ka ar N vaicājumiem pietiek, jo, ja zināmi visi argumenti, tad skaidra arī funkcijas vērtība.

Viena no ilgi neatrisinātām problēmām šajā jomā ir noskaidrot, kāda ir kvantu vaicājumsarežģītība nejaušai Būla funkcijai jeb, kas ir būtībā ekvivalenti, gandrīz visām

Būla funkcijām ar doto argumentu skaitu. A. Ambainis 1998. gadā pierādīja, ka vajag vismaz $N/4 - o(N)$ vaicājumus. No otras puses, pielietojot Grovera algoritmu, viegli secināt, ka pietiek ar $N/2 + o(N)$ vaicājumiem. Kopš 1998. gada būtisku uzlabojumu šiem novērtējumiem līdz šim nebija izdevies gūt.

2011. gadā ar dažādiem paņēmieniem pētīta Būla funkciju izsakāmība ar polinomiem un polinomu kvadrātu summām, ir izdevies iegūt novērtējumu, ka, N tiecoties uz bezgalību, gandrīz visām Būla funkcijām kvantu vaicājumsarežģītība ir $N/2 - o(N)$. Tā kā tas ar precizitāti līdz $o(N)$ sakrīt ar augšējo novērtējumu, tad ar to problēma būtībā ir atrisināta.

Papildus tam, ir piedāvāta alternatīva nedeterminētā vaicājošā algoritma definīcija un pētīta šāda modeļa sarežģītība, izmantojot Fano plaknes Būla funkciju, kā arī pētīta vaicājošo algoritmu sarežģītība attiecībā uz permutācijām.

Publikācijas:

1. Alina Vasilieva, Taisia Miscenko-Slatenkova, Rūsiņš Freivalds, Ruslans Tarasovs. Quantum vs. Deterministic Queries on Permutations. Proceedings of the 3rd Workshop on Reversible Computation (RC), Gent, Belgium, July 4th–5th, 2011, pp.187–194.
2. Alina Vasilieva, Rusins Freivalds: Nondeterministic Query Algorithms. J. UCS 17(6): 859-873 (2011).

Kvantu spēles. Nelokālās (nevietējās) spēles ir spēles, kurās spēlētāji (piemēram, atrodoties tālu cits no cita) 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.

Nelokālās spēles cita starpā ir ērts paņemiens, kas parāda klasiskās fizikas nepietiekamību kvantu parādību izskaidrošanā jeb, datorikas terminos, kvantu skaitļošanas pārkāpumu pār klasisko.

2011. gadā ir pabeigti konkrēto spēļu gadījumu pētījumi, iegūtie rezultāti apkopoti zinātniskā rakstā. Raksts būtībā parāda, ka dažādu spēļu gadījumā notiek stipri atšķirīgas lietas. Ir spēles, kur pie sliktākā sadalījuma spēlētāji tik un tā var sasniegt to pašu spēles vērtību kā pie vienmērīgā sadalījuma, gan klasiskajā, gan kvantu gadījumā; ir spēles, kurās sliktākajā gadījumā sasniedzamā vērtība ir daudz zemāka nekā pie vienmērīgā sadalījuma. Ir spēles, kur kvantu gadījumā spēlētāji var sasniegt maksimālo iespējamo spēles vērtības pārsvaru pār klasisko gadījumu; ir spēles, kur kvantu gadījumā spēlētāji būtībā nevar sasniegt neko vairāk par klasisko gadījumu.

2011. gadā ir pētīts arī cits ar nelokālām spēlēm saistīts uzdevums: cik daudz spēlētāji var sasniegt nejaušā XOR spēlē (šoreiz ar vienmērīgo ieejas datu sadalījumu) jeb vidēji pa visām XOR spēlēm ar dotajiem parametriem. Par XOR spēli sauc tādu nelokālu spēli, kur spēlētāju veiksmes kritērijs ir atkarīgs tikai no 1) viņu saņemtajiem ieejas datiem un 2) viņu izdoto izejas datu-bitu izslēdzošā vai vērtības. Ar nejaušu XOR spēli saprotam tādu, kur pie katriem ieejas datiem tas, kura no divām iespējamām izejas bitu XOR vērtībām – 0 vai 1 – ir uzvarošā, tiek noteikts nejauši (mēs aplūkojam: ar varbūtību $\frac{1}{2}$ nulle, ar varbūtību $\frac{1}{2}$ viens).

Ar dažādiem, arvien sarežģītākiem paņēmieniem pamazām izdevās iegūt gan augšējos, gan apakšējos novērtējumus sasniedzamajai spēles vērtībai gan klasiskajā, gan kvantu gadījumā.

Galvenais rezultāts: gandrīz visām XOR spēlēm kvantiski var sasniegt vismaz 1,2 reizes labāku vērtību nekā klasiski. Precizējot novērtējumus, var izdoties šo koeficientu vēl uzlabot.

Publikācijas:

1. A. Ambainis, A. Bačkurs, K. Balodis, A. Škuškovniks, J. Smotrovs, M. Virza. Worst case analysis of non-local games. <http://arxiv.org/abs/1112.2856>.
2. A. Ambainis, A. Bačkurs, K. Balodis, D. Kravcenko, R. Ozols, J. Smotrovs, M. Virza. Quantum strategies are better than classical in almost any XOR game. <http://arxiv.org/abs/1112.3330>.

Kvantu automāti. Tiek pētīts, kādas regulāras valodas galīgie kvantu automāti pazīst ar izolētu šķēluma punktu. Šī mērķa realizācijai ir uzstādīts plāns raksturot valodas, kādas pazīst kvantu galīgie automāti šādās valodu klasēs (katra nākošā klase ir plašāka par iepriekšējo):

1. R-triviālās idempotentās valodas (R1 valodas);
2. Visas R-triviālās valodas (R valodas);
3. ER1 valodas;
4. ER valodas.

2011. gadā turpināti pētījumi par valodām, kuras pazīst kvantu automāti. Ņemot vērā iegūtos rezultātus attiecībā uz R1 valodām, ir 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.

Publikācijas:

1. Andris Ambainis: Quantum Finite Automata. NCMA 2011: 9–13.
2. Marats Golovkins, Maksim Kravtsev, Vasilij Kravcevs. Quantum Finite Automata and Probabilistic Reversible Automata: R-trivial Idempotent Languages. MFCS 2011, Lecture Notes in Computer Science; Vol. 6907, p. 351–363, 2011.

Kvantu loģika. 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.

Publikācijas:

Jānis Cīrulis, Weak relative pseudocomplements in semilattices. Demonstratio Mathematica (44) (2011), 651–672.