

Aktivitāte „Pētījumi kvantu skaitļošanā” – 2010. gads

Aktivitāte pēta kvantu skaitļošanas teoriju. Notiek pētījumi šādos apakšvirzienos:

- Kvantu algoritmu konstruēšana (A. Ambainis, N. Nahimovs, A. Rivošs);
- Apakšējo novērtējumu pierādīšana kvantu algoritmiem (A. Ambainis);
- Kvantu stāvokļu konfigurācijas (A. Ambainis, J. Smotrovs);
- Kvantu spēles (A. Ambainis, D. Kravčenko, A. Škuškovniks, J. Smotrovs);
- Kvantu automāti (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 pirmā gada laikā iegūti vairāki rezultāti šajā virzienā:

- 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.)
- Parādīts, ka Grovera kvantu meklēšanas algoritmu iespējams paātrināt, ja tā darbību pārtrauc nedaudz ātrāk nekā Grovera algoritma standartvariantā.
- Veikti datoreksperimenti par kvantu klejošanas izmantošanu kvantu algoritmu konstruēšanā. Secināts, ka kvantu klejošanu plaknē var izmantot meklēšanā plaknē efektīvākā veidā nekā iepriekšējos kvantu algoritmos.

Nolasīts ielūgtais referāts par kvantu algoritmiem MFCS (Mathematical Foundations of Computer Science) – vienā no Eiropas vadošajām konferencēm par datorzinātņu teoriju.

Publikācijas:

1. Andris Ambainis, Andrew M. Childs, Francois Le Gall, and Seiichiro. Tani. The quantum query complexity of certification. *Quantum Information and Computation*, 10 (3-4):181-189, 2010.
2. Andris Ambainis. New Developments in Quantum Algorithms. *Proceedings of MFCS'2010*, Lecture Notes in Computer Science, vol. 6281, pp. 1-11.
3. Andris Ambainis: Quantum Search with Variable Times. *Theory of Computing Systems*, 47 (2010), 786-807
4. Andris Ambainis, Andrew M. Childs, Ben Reichardt, Robert Špalek, Shengyu Zhang: Any AND-OR Formula of Size N Can Be Evaluated in Time $N^{1/2+o(1)}$ on a Quantum Computer. *SIAM Journal on Computing*, 39(6): 2513-2530 (2010).
5. Andris Ambainis. Quantum Algorithms for Formula Evaluation, in R. Horodecki et al. (eds) *Quantum Cryptography: from Theory to Experiment*. Nato Science for Peace and Security Series, 26:115-124, IOS Press, 2010.
6. Nikolajs Nahimovs, Aleksandrs Rivošs. A note on the optimality of Grover's algorithm. In J. Bārzdiņš (ed.), *Scientific Papers University of Latvia*, Vol 756, Computer Science and Information Technologies, pp. 221-226.

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 projekta pirmajā gadā:

- Pabeigts darbs pie metodes, kā pierādīt kvantu apakšējos novērtējumus, izmantojot simetriju. (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.
- 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.

Publikācijas:

1. Andris Ambainis, A New Quantum Lower Bound Method, with an Application to a Strong Direct Product Theorem for Quantum Search. Žurnāls "Theory of Computing", 6:1-26, 2010.

Kvantu stāvokļu konfigurācijas. 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 visas aktivitātes lielāko sasniegumu projekta 1. gadā. 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 starpībām, nesen jaunaplūkotojām multistarpībām u. c.). Pētījuma ietvaros ir izdevies pierādīt dažu šādu izvietojumu neiespējamību, tomēr lielākajā daļā gadījumu jautājums joprojām paliek atklāts.

Publikācijas:

1. Andris Ambainis, Julia Kempe, Or Sattath. A quantum Lovász local lemma. *Proceedings of STOC 2010*, pp. 151-160.
2. Andris Ambainis. Limits on entropic uncertainty relations. *Quantum Information and Computation*, 10:848-858, 2010.

Kvantu spēles. Viena no interesantākajām kvantu mehānikas iezīmēm ir, ka ar kvantu efektiem var panākt būtiski lielāku statistisko korelāciju starp pusēm, kas nevar sazināties, nekā ar jebkādiem klasiskiem paņēmieniem. Šos efektus var pētīt caur kvantu spēlēm.

Kvantu spēles ir divu vai vairāk spēlētāju kooperatīvas spēles, kur spēlētāji nevar sazināties savā starpā. Tiesnesis aizsūta katram spēlētājam nejauši izvēlētu informāciju (ieejas datus) un saņem no katra spēlētāja atbildi (izejas datus). Spēlētāji uzvar, ja izejas dati apmierina noteiktu nosacījumu, kas var būt atkarīgs no ieejas datiem. Kvantu spēļu slavenākais piemērs ir CHSH (Clauser-Horne-Shimonyi-Holt) spēle, kurā spēlētāji, kas izmanto kvantu efektus var uzvarēt ar varbūtību 0.85..., bet spēlētāji, kas neizmanto kvantu efektus – tikai ar varbūtību 0.75. Šo spēli var izmantot kā eksperimentu, kas pārbauda kvantu mehānikas pareizību.

Projekta ietvaros tika pētītas kvantu spēles, īpašu uzmanību pievēršot XOR spēlēm – spēlēm, kurās uzvaras nosacījumam svarīgs tikai *izslēdzošais vai* no izejas datiem. Šī ir viena no svarīgākajām kvantu spēļu apakšklasēm un tā ietver vairākas plaši zināmas kvantu spēles, t.sk. CHSH spēli. Izstrādātas jaunas metodes XOR spēļu analīzei, ja ir vairāk kā 2 spēlētāji.

Publikācijas:

1. Andris Ambainis, Dmitry Kravchenko, Nikolajs Nahimovs, Alexander Rivosh: Nonlocal Quantum XOR Games for Large Number of Players. *Proceedings of TAMC'2010*, Lecture Notes in Computer Science, vol. 6108, pp. 72-83.

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.

2010. gadā izpildīts plāna 1. punkts. Katrai R1 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 arī 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.

Publikācijas:

1. Ruben Agadzanyan, Rūsiņš Freivalds. Finite state transducers with intuition. *Proceedings of UC'2010*, Lecture Notes in Computer Science, vol. 6079, p. 11-20, 2010.

2. Kaspars Balodis, Rūsiņš Freivalds, Lauma Pretkalniņa, Inga Rumkovska and Madars Virza. Language Recognition by Nonconstructive Finite Automata. *Proceedings of SOFSEM 2010*, vol. 2, pp. 14--21, 2010
3. Rūsiņš Freivalds. Amount of nonconstructivity in deterministic finite automata. *Theoretical Computer Science*, vol. 411 (38-39), pp. 3436-3443, 2010.
4. Rūsiņš Freivalds, Abuzer Yakaryılmaz, A.C. Cem Say. A new family of nonstochastic languages. *Information Processing Letters*, vol. 110 (10), pp. 420-423, 2010.
5. Oksana Scegunnaja-Dubrovskaja, Lelde Lāce, Rūsiņš Freivalds. Postselection finite quantum automata. *Proceedings of UC'2010*, Lecture Notes in Computer Science, vol. 6079, p. 115-126, 2010.
6. Abuzer Yakaryılmaz, Rūsiņš Freivalds, A.C. Cem Say, Ruben Agadzanyan. Quantum Computation with Devices Whose Contents Are Never Read. *Proceedings of UC'2010*, Lecture Notes in Computer Science, vol. 6079, p. 164--174, 2010.
7. Marats Golovkins, Jean-Eric Pin. Varieties Generated by Certain Models of Reversible Finite Automata. *Chicago Journal of Theoretical Computer Science*, Article 2, Volume 2010

Kvantu loģika. Gada pirmajā pusē veikta algebrisko struktūru, kas rodas zināšanu bāzu teorijā identifikācija un izpēte, sagatavojot ziņojumus 4 konferencēs un divas publikācijas. Gada otrajā pusē sākts risināt problēmu, kādās sistēmu klasēs katru zināšanu reprezentācijas sistēmu var simulēt ar informatīvi pilnu (jeb determinētu) sistēmu. Tika iesākts raksts par kopīgo starp zināšanu reprezentācijas sistēmām un kvantu sistēmām, bet izrādījās, ka materiāls ir pārāk plašs vienam pat lielumam rakstam un ir iespējami vairāki (dažādi) raksti gan fiziķu, gan datorīķu, gan matemātiķu auditorijai.

Publikācijas:

1. Jānis Cīrulis, Residuation subreducts of pocrigs, *Bull. Sect. Logic (Lodz)* 39 (2010), pp 11-16.
2. Jānis Cīrulis, Skew nearlattices: some structure and representation theorems. *Contrib. Gen. Algebra* 19 (2010), 33—41.
3. Jānis Cīrulis, Subtraction-like operations in nearsemilattices. *Demonstratio Math.*, 43 (2010), 725—738.
4. Jānis Cīrulis, Weak relative pseudocomplements in posets, *Bull. Sect. Logic (Lodz)* 40 (2010) 1--12.