



LATVIJAS
UNIVERSITĀTE
UNIVERSITY OF LATVIA



ĪEGULDĪJUMS TAVĀ NĀKOTNĒ

*Datorzinātnes pielietojumi un tās
saiknes ar kvantu fiziku*

Pārskats par pētījumiem kvantu skaitļošanā

Andris Ambainis
LU Datorikas fakultāte

Projekta noslēguma seminārs, 2012. gada 21. novembrī

Galvenie pētījumu virzieni

Kvantu algoritmi
(A. Ambainis,
N. Nahimovs,
A. Rivošs, J. Smotrovs)

Kvantu apakšējie
novērtējumi
(A. Ambainis)

Kvantu spēles
(A. Ambainis, D. Kravčenko,
A. Škuškovniks, J. Smotrovs)

Kvantu stāvokļu
konfigurācijas
(J. Smotrovs)

Kvantu galīgie automāti
(R. Freivalds,
M. Golovkins, M. Kravcevs)

Kvantu loģika un
zināšanu reprezentācija
(J. Cīrulis)

Kvantu algoritmi

Lineāras vienādojumu sistēmas

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1N}x_N = b_1$$

$$a_{21}x_1 + a_{22}x_2 + \dots + a_{2N}x_N = b_2$$

...

$$a_{N1}x_1 + a_{N2}x_2 + \dots + a_{NN}x_N = b_N$$

Zināms: $a_{11}, a_{12}, \dots, a_{NN}, b_1, b_2, \dots, b_N$.

Jāatrod: x_1, x_2, \dots, x_N .

Lineāras vienādojumu sistēmas

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1N}x_N = b_1$$

$$a_{21}x_1 + a_{22}x_2 + \dots + a_{2N}x_N = b_2$$

...

$$a_{N1}x_1 + a_{N2}x_2 + \dots + a_{NN}x_N = b_N$$

Klasiskais algoritms: $O(N^{2.38\dots})$.

Ieejas datu apjoms: N^2 .

Izejas datu apjoms: N .

[Harrow-Hassidim-Lloyd, 2008]

- Algoritma rezultāts – kvantu stāvoklis:

$$x_1|1\rangle + x_2|2\rangle + \dots + x_N|N\rangle$$

- N stāvokļi – $\log N$ kvantu biti.
- Stāvokli var radīt $O(\log N)$ laikā.

$$O(N^{2.38\dots}) \rightarrow O(\log N)$$

[Harrow-Hassidim-Lloyd, 2008]

- Algoritma rezultāts – kvantu stāvoklis:

$$x_1|1\rangle + x_2|2\rangle + \dots + x_N|N\rangle$$

- Trūkums: no kvantu stāvokļa nevar nolasīt visu atrisinājumu x_1, x_2, \dots, x_N .
- Var iegūt daļēju informāciju par atrisinājumu.

Scientific American



- **Warp-Speed Algebra: New Algorithm Does Algebra in a Snap**
New quantum algorithm can solve monster-size equations.

Algoritma ātrdarbība

- [Harrow, Hassidim, Lloyd, 08]: $O(k^2 \log N)$,
k – vienādojumu sistēmas kondīcijas
skaitlis.
- [A, 2012]: $O(k \log N)$.

Svarīgākās publikācijas

1. **A. Ambainis**, A. M. Childs, B. Reichardt, R. Spalek, S. 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)
2. **A. Ambainis**, A.M. Childs, F. Le Gall, and S. Tani. The quantum query complexity of certification. Quantum Information and Computation, 10 (3-4):181-189, 2010.
3. A. Ambainis, A. Bačkurs, N. Nahimovs, R. Ozols, A. Rivosh, Search by Quantum Walks on Two-Dimensional Grid without Amplitude Amplification. Lecture Notes in Computer Science, 7582:87-97, 2012.

Kopā: 9 publikācijas.

Kvantu apakšējie novērtējumi

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].

Melnās kastes modelis



Kvantiski:

A quantum version of the black box model. On the left, the expression $\sum_i a_i |i\rangle$ is connected by a horizontal line to a blue rectangular box. Inside the box, the text 'X₁, X₂, ..., X_N' is written. Another horizontal line connects the right side of the box to the expression $\sum_i a_i (-1)^{x_i} |i\rangle$ on the right.

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

Rezultāti



- [van Dam, 1998] Kvantu algoritms, kas iegūst visus bitus x_1, \dots, x_N , ar $N/2 + O(\sqrt{N})$ melnās kastes izsaukumiem.
- Var izrēķināt jebkuru $f(x_1, \dots, x_N)$.
- Vai tas ir optimāli?

Rezultāti



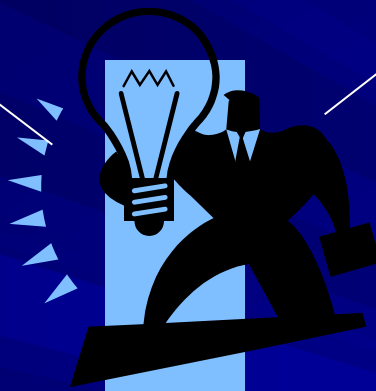
- [Beals et al., 1998] Lai izrēķinātu $x_1 \oplus x_2 \oplus \dots \oplus x_N$, vajag $N/2$ vaicājumus.
- [A, Bačkurs, Smotrovs, de Wolf, 2012] Gandrīz visām $f(x_1, \dots, x_N)$ vajag $N/2 - o(N)$ vaicājumus.

Svarīgākās publikācijas

1. S. Aaronson, **A. Ambainis**, "The need for structure in quantum speedups", Innovations in Computer Science - ICS 2011, Tsinghua University, Beijing, China, pp. 338-352.
2. **A. Ambainis**, L. Magnin, M. Roetteler, J. Roland. Symmetry-Assisted Adversaries for Quantum State Generation. Proceedings of IEEE Conference on Computational Complexity 2011, pp. 167-177.
3. A. Ambainis, A. Bačkurs, J. Smotrovs, R. de Wolf. Optimal quantum query bounds for almost all Boolean functions. Proceedings of STACS'2013, pieņemts publicēšanai.

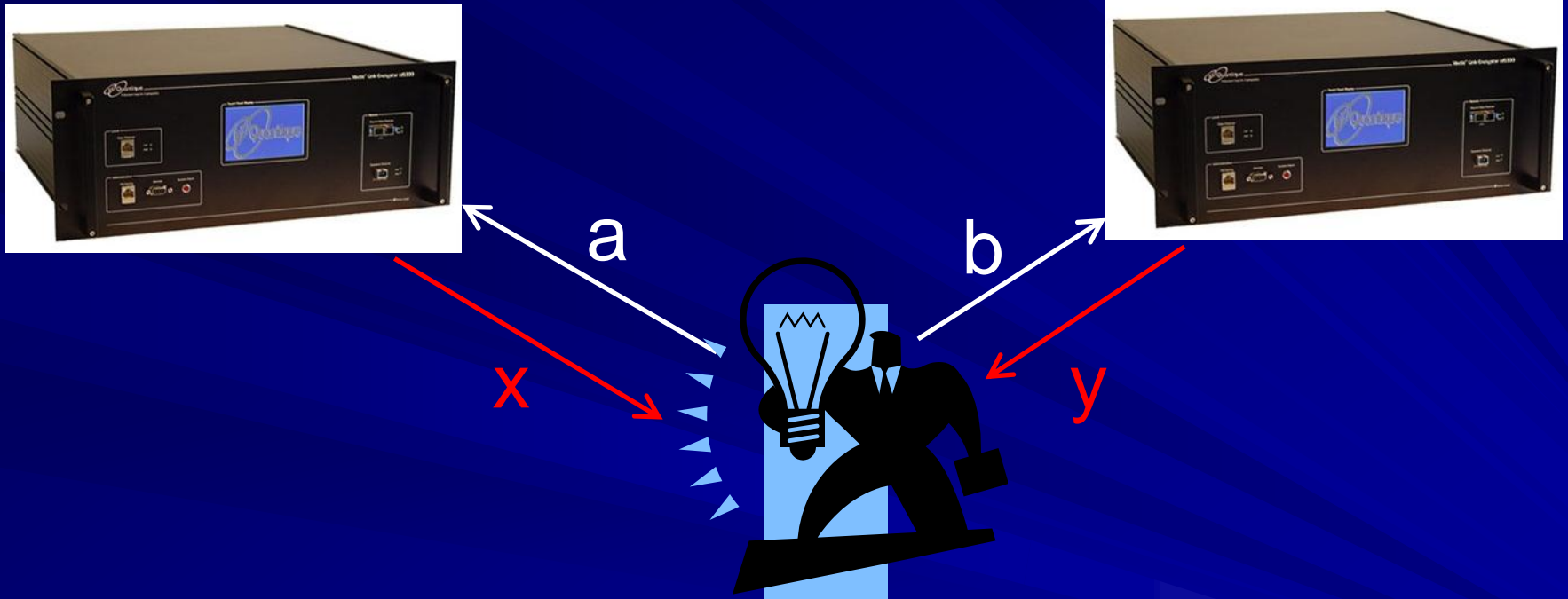
Kopā: 5 publikācijas.

Kvantu spēles



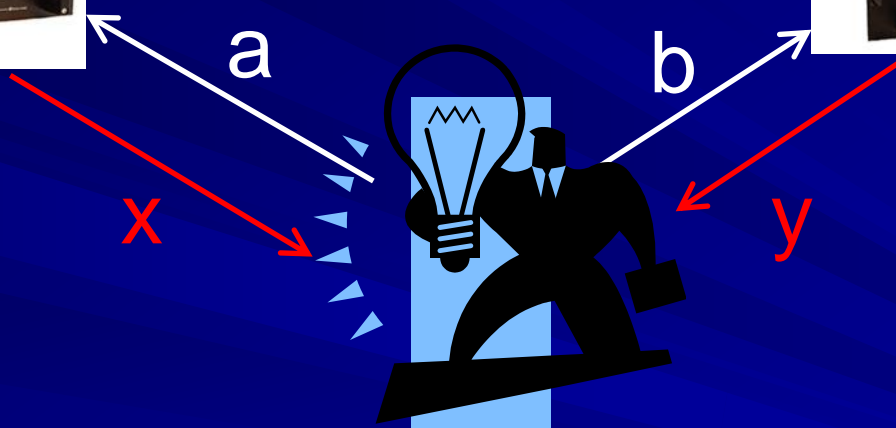
Ierīces nevar sazināties savā starpā

Clauser, Horne, Shimonyi, Holt, 69



- $a, b, x, y \in \{0, 1\}$;
- Ja $a = 0$ vai $b=0$, vēlams $x=y$;
- Ja $a=b=1$, vēlams $x \neq y$.

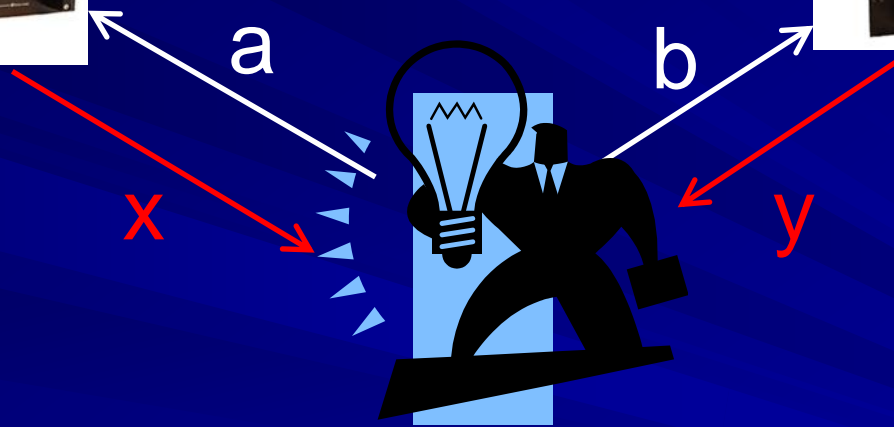
Klasiskas (ne-kvantu) ierīces



- 4 gadījumi: $ab = 00, 01, 10, 11$.
- Ierīces var izdot pareizu atbildi 3 no 4 gad.

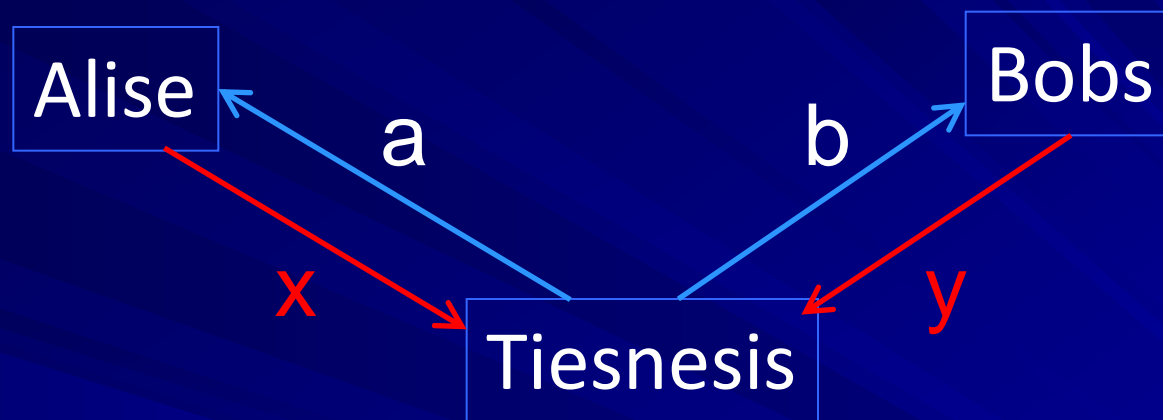
Varbūtība: 0.75

Kvantu ierīces



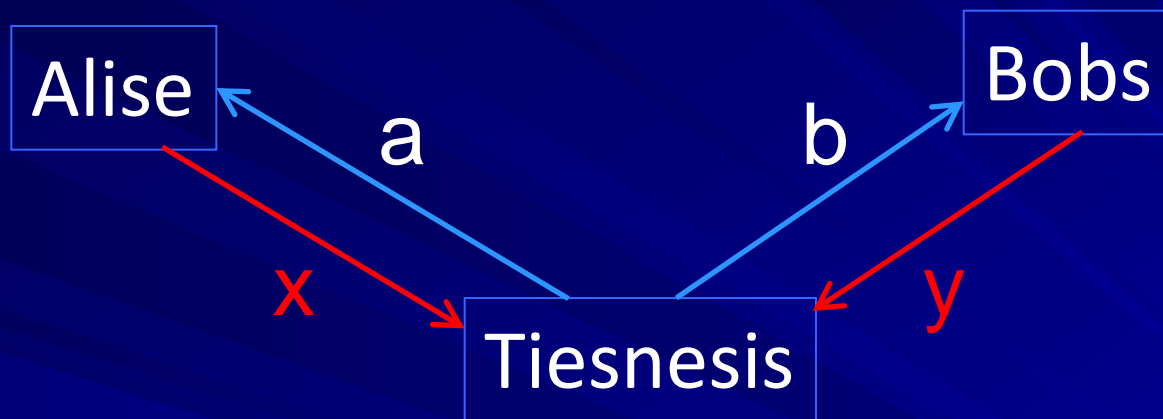
- Var izdot pareizo atbildi ar varbūtību 0.85...

Nelokālas spēles



- Tiesnesis uzdod jautājumus a , b Alisei un Bobam.
- Alise un Bobs atbild ar x , y ;
- Alise, Bob uzvar, ja izpildās nosacījums $P(a, b, x, y)$.

Nejaušas nelokālas spēles



- $a, b \in \{1, 2, \dots, N\}$;
- $x, y \in \{0, 1\}$;
- Nosacījums $P(a, b, x, y)$ – nejaušs;

Ar lielu varbūtību, kvantu uzvaras varbūtība ir lielāka par klasisko.

Svarīgākās publikācijas

1. **A. Ambainis, D. Kravchenko, N. Nahimovs, A. Rivosh:** Nonlocal Quantum XOR Games for Large Number of Players. Proceedings of TAMC'2010, Lecture Notes in Computer Science, 6108:72-83.
2. **A. Ambainis, A. Backurs, K. Balodis, D. Kravcenko, R. Ozols, J. Smotrovs, M. Virza:** Quantum Strategies Are Better Than Classical in Almost Any XOR Game. Proceedings of ICALP'2012, Lecture Notes in Computer Science, 7391:25-37.

Kopā: 4 publikācijas.

Nākošie projekti

- Quantum Computer Science (QCS) – ES 7. ietvara programma, 9/2010 - 8/2013.
- Quantum Algorithmics (QALGO) – ES 7. ietvara programma, 5/2013 - 4/2016.

Partneri

1. Latvijas Universitāte – koordinators;
2. Cambridge University (QCS, QALGO);
3. University of Paris Diderot (QCS, QALGO);
4. Centrum Wiskunde & Informatica (QCS, QALGO);
5. Universite Libre de Bruxelles (QCS, QALGO);
6. University of Bristol (QCS);
7. Institut de Ciencias Fotoniques (QCS);
8. Tel Aviv University (QCS);
9. RTWH Aachen (QALGO);
10. Hebrew University of Jerusalem (QALGO).