LATVIJAS UNIVERSITĀTE
UNIVERSITY OF LATVIA

ESF
EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA
IEGULDĪJUMS TAVĀ NĀKOTNĒ

Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku

ESF projekts,
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044
01.12.2009-30.11.2012.

Projekts

- Realizē LU Datorikas fakultāte;
- 5 aktivitātes, 28 pētnieki.

1. Kvantu skaitļošana (A. Ambainis);
2. Kvantu tehnoloģiju fizikālie aspekti (V. Kaščejevs).
3. Modeļu bāzētās arhitektūras (G. Arnicāns);
4. Datu noliktavas (L. Niedrīte);
5. Programminženierija (D. Šmite).

Aktivitāte “Kvantu skaitļošana”

- Kvantu dators – dators, kas darbojas saskaņā ar kvantu mehānikas likumiem.
- Ko varēs izdarīt ar kvantu datoru?

- Kādi ir kvantu datoru fundamentālie ierobežojumi?
- Kvantu stāvokļi kā matemātisks objekts.

Galvenie pētījumu virzieni

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

Kvantu apakšējie novērtējumi
(A. Ambainis)

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

Kvantu stāvokļu konfigurācijas
(J. Smotrovs, A. Belovs)

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

Kvantu loģika un zināšanu reprezentācija
(J. Cīrulis)

LATVIJAS UNIVERSITĀTE
UNIVERSITY OF LATVIA

ESF
EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA
IEGULDĪJUMS TAVĀ NĀKOTNĒ

Kvantu algoritmi algebriskām problēmām

Andris Ambainis
LU Datorikas fakultāte

DF-CFI seminārs, 2012.g. 10. maijs

Skaitļa sadalīšana reizinātājos

- 6231540623 = 93599 * 66577.
  - Cik ātri mēs varam atrast reizinātājus, ja mums dots tikai 6231540623?
  - Lieliem (300 cipari) skaitļiem tradicionālie datori ir par lēnu.

Kāpēc tas ir svarīgi?

amazon.com

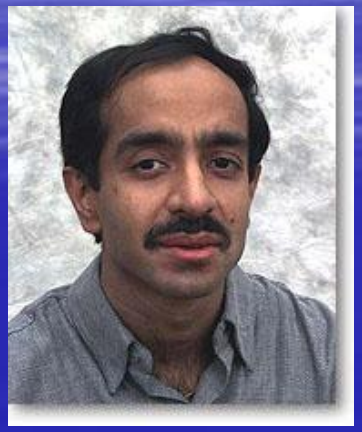
4252 1890 6767 1345

4252 1890 6767 1345

qwerasd8902jkl → qwerasd8902jkl

Drošība balstās uz to, ka ir sarežģīti lielus skaitļus sadalīt reizinātājos

Meklēšana



Lov Grover, 1996

Algoritms, kas $\sim\sqrt{N}$ kvantu soļos atrod elementu ar noteiktu īpašību N elementu sarakstā. Klasiski, nepieciešami N soļi.

Lineāras vienādojumu sistēmas

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

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

$$\ldots$$

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

Zināms: a_{11}, a_{12}, ..., a_{NN}, b_1, b_2, ..., b_N.
Jāatrod: x_1, x_2, ..., x_N.

Lineāras vienādojumu sistēmas

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

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

$$\ldots$$

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

Klasiskais algoritms: $O(N^{2.38\ldots})$.
Ieejas datu apjoms: N^2.
Izejas datu apjoms: N.

Scientific American

- **Warp-Speed Algebra: New Algorithm Does Algebra in a Snap**

  New quantum algorithm can solve monster-size equations.

[Harrow-Hassidim-Lloyd, 2008]

- Algoritma rezultāts – kvantu stāvoklis:

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

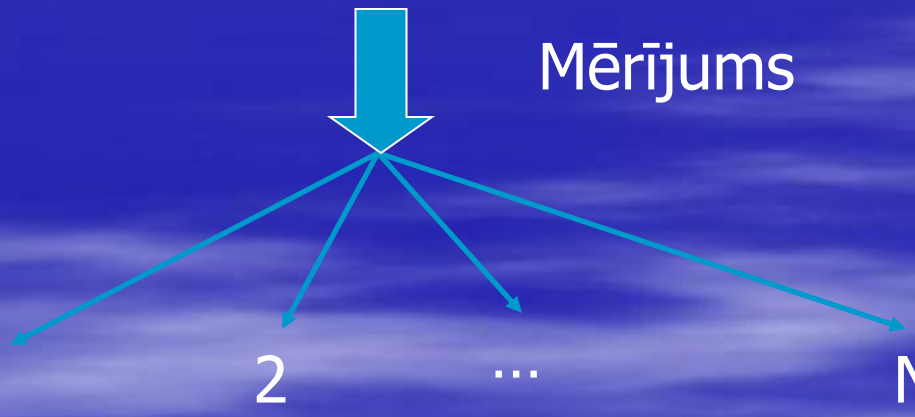
- N stāvokļi – log N kvantu biti.
- Stāvokli var radīt O(log N) laikā.

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

[Harrow-Hassidim-Lloyd, 2008]

- Algoritma rezultāts – kvantu stāvoklis:

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



varb. $|x_1|^2$ $|x_2|^2$ $|x_N|^2$

[Harrow-Hassidim-Lloyd, 2008]

- Trūkums: no stāvokļa

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

nevar nolasīt visu atrisinājumu x_1, x_2, ..., x_N.

- Var iegūt daļēju informāciju par atrisinājumu.

Pamatideja

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

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

$$\ldots$$

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

$$\sum_{i=1}^{N} b_i |i\rangle \longrightarrow \sum_{i=1}^{N} x_i |i\rangle$$

Zināms Risinājums

Pamatidejas

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1N} \\ a_{21} & a_{22} & \dots & a_{2N} \\ \dots & \dots & \dots & \dots \\ a_{N1} & a_{N2} & \dots & a_{NN} \end{pmatrix} \qquad x=\begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_N \end{pmatrix} \qquad b=\begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_N \end{pmatrix} \qquad Ax=b$$

$$\sum_{i=1}^{N} b_i \left| i \right\rangle \longrightarrow \sum_{i=1}^{N} x_i \left| i \right\rangle$$

$$x=A^{-1}b$$

Īpašvērtību novērtēšana [Cleve, 1998]

- Input: stāvoklis $|\psi\rangle$: $A|\psi\rangle=\lambda|\psi\rangle$.
- Output: novērtējums λ', $|\lambda'-\lambda|\leq\varepsilon$.

Nepieciešams pielietot: $A^{-1}|\psi\rangle=\lambda^{-1}|\psi\rangle$.

Algoritma darbības laiks

1. Atkarība no vienādojumu/nezināmo skaita:

   O(log N).

2. Kondīcijas skaitlis k.

$$k = \frac{\lambda_{\max}}{\lambda_{\min}}$$

λ_{min}, λ_{max} – singulārās vērtības

Kondīcijas skaitlis

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

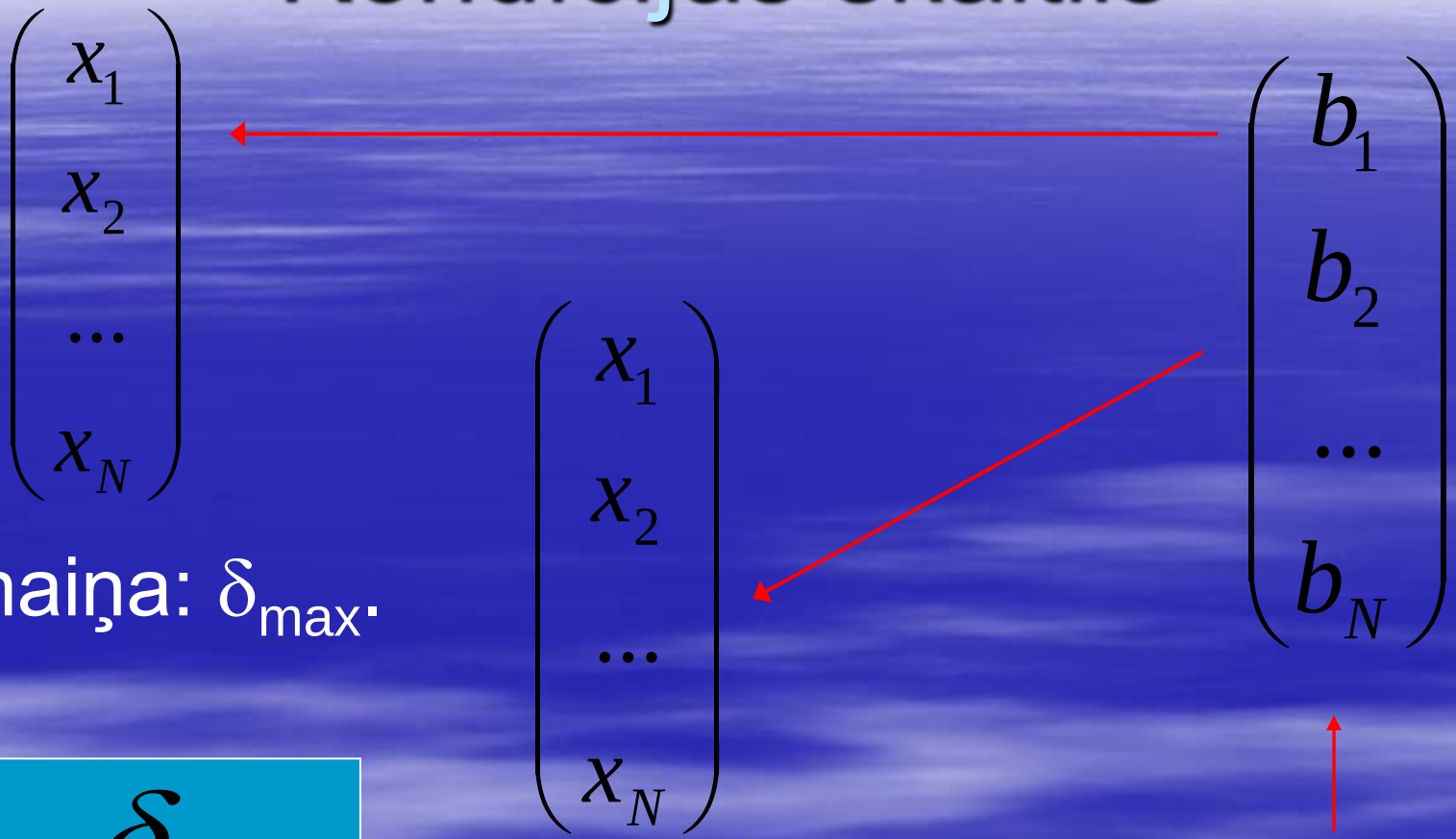
$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2N}x_N = b_2$$

$$\ldots$$

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

Cik daudz mainās atrisinājums, nedaudz izmainot b_1, b_2, ..., b_N?

Kondīcijas skaitlis



$$k = \frac{\delta_{\max}}{\delta_{\min}}$$

Algoritma ātrdarbība

- [Harrow, Hassidim, Lloyd, 08]: $O(k^2 \log N)$.
- [A, 2010]: $O(k \log N)$.

Algoritma pielietojumi

- Kā var izmantot atrisinājumu – kvantu stāvokli?

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

- [Rivošs, 2010]: piemēri, kur no šāda atrisinājuma var iegūt lietderīgu informāciju.

Singularitātes pārbaude

- Matrica A;
- Dots: A – singulāra (det(A) = 0) vai tālu no singulāras (visas A singulārās vērtības $\geq \lambda_{min}$).
- Uzdevums: atšķirt šos 2 gadījumus.

Efektīvs kvantu algoritms šai problēmai.

Pielietojumi

- Skaitļošanas problēmas $\rightarrow$ matricas A.
- Kādas problēmas var reducēt uz pārbaudi, vai det(A)=0?