Datorzinātnes lietojumi un tās saiknes ar kvantu fiziku

Kvantu algoritmi un apakšējie novērtējumi

Andris Ambainis

LU Datorikas fakultāte

LU un LMT datorzinātņu dienas, 2011.g. 9. augusts

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].

Var tikt pielietots jebkuram meklēšanas uzdevumam.

Meklēšana

A. Bērziņš	22245678
I. Bērziņš	23456789
V. Bērziņš	22349029
...	....
A. Kalniņš	22390001
...	...

Kam pieder numurs 22332233?

Parasts dators: N soļi

Kvantu dators: √N soļi

1,000,000 vs. 1,000

Kā tas darbojas?

- Melnā kaste:

Vai šis ir meklētais objekts?

- Kvantu melnā kaste:

$$|i\rangle, \text{ ja } x_i=0$$
$$-|i\rangle, \text{ ja } x_i=1$$

Kvantu melnā kaste

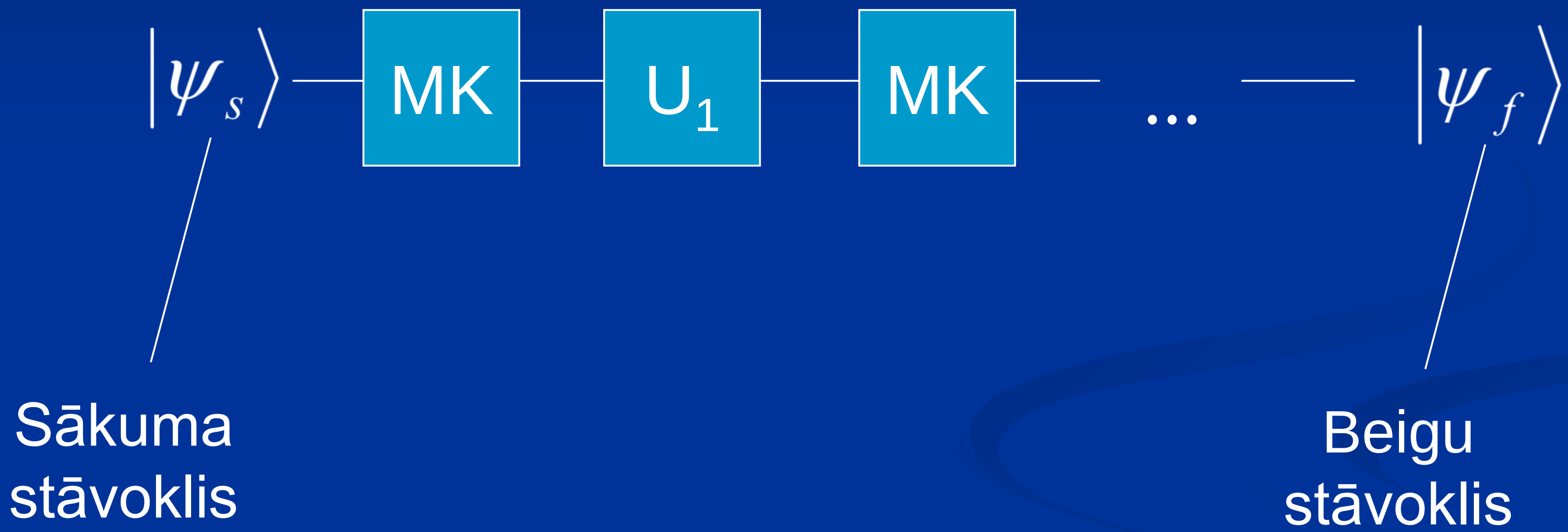
- $x_2=1,\ x_1=x_3=0$:

$$\frac{1}{\sqrt{2}}|1\rangle+\frac{1}{2}|2\rangle+\frac{1}{2}|3\rangle$$

MK

$$\frac{1}{\sqrt{2}}|1\rangle-\frac{1}{2}|2\rangle+\frac{1}{2}|3\rangle$$

Kvantu algoritms



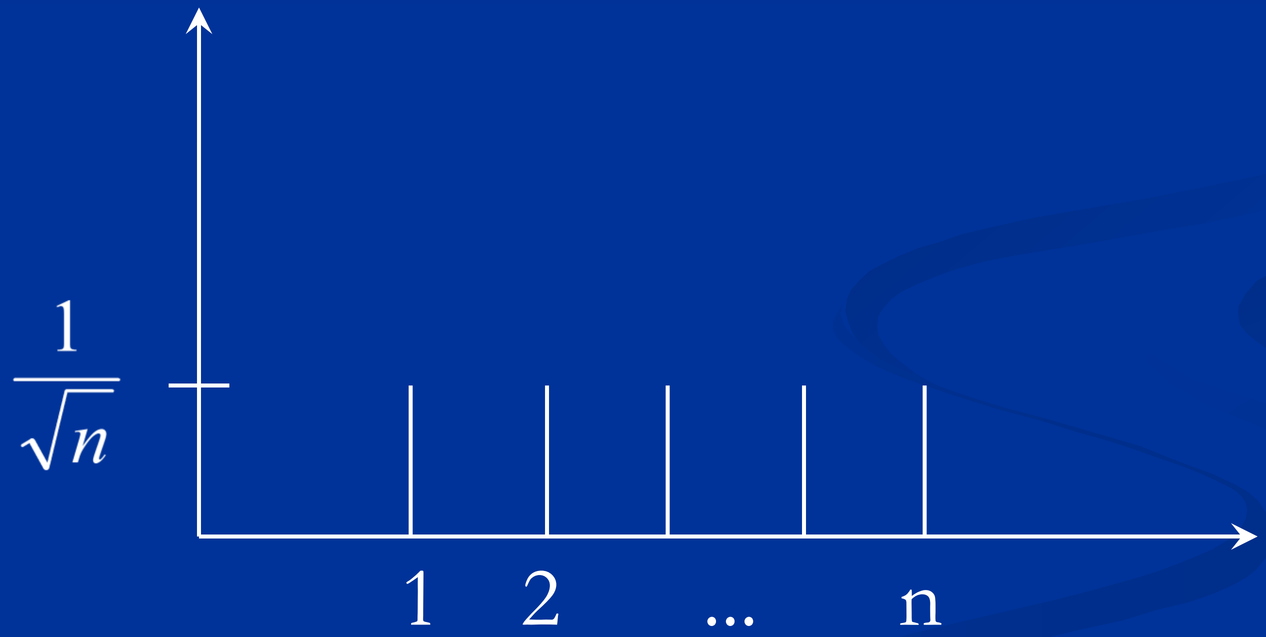
Meklēšana

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.

Sākuma stāvoklis

$$\frac{1}{\sqrt{n}}|1\rangle + \frac{1}{\sqrt{n}}|2\rangle + \ldots + \frac{1}{\sqrt{n}}|n\rangle$$

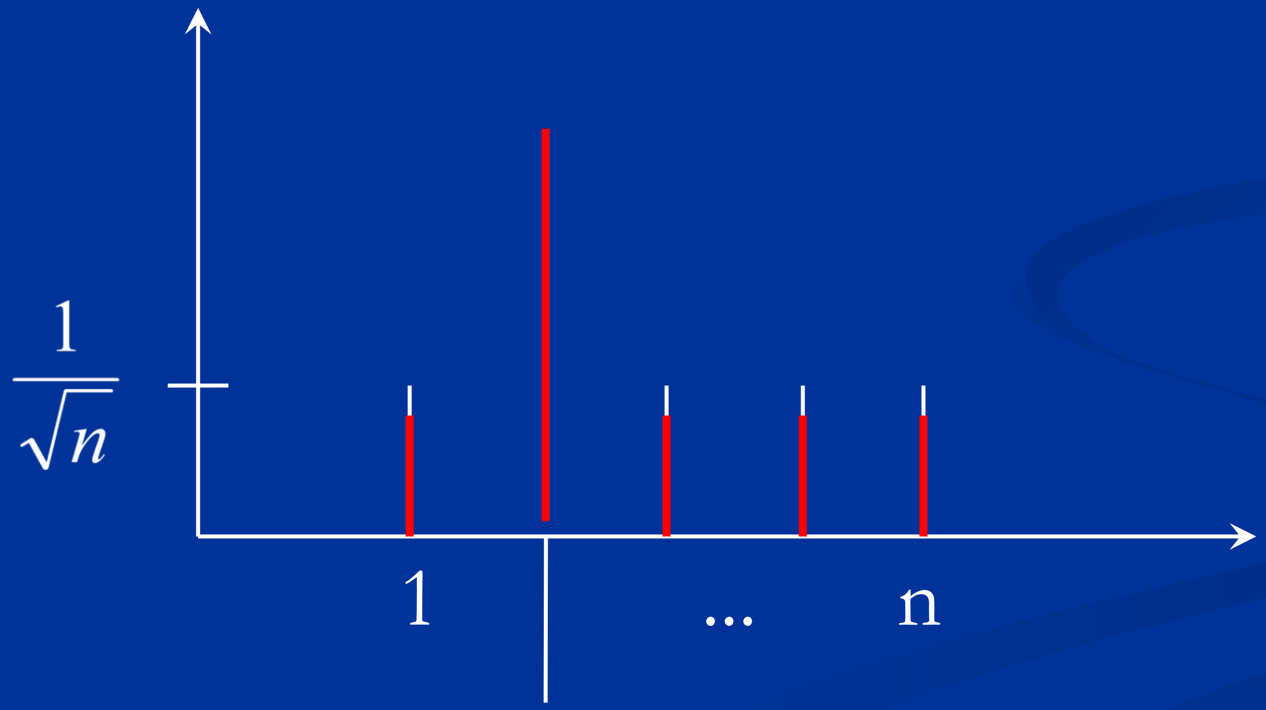


Melnā kaste

$$\frac{1}{\sqrt{n}}\left|1\right\rangle - \frac{1}{\sqrt{n}}\left|2\right\rangle + \ldots + \frac{1}{\sqrt{n}}\left|n\right\rangle$$

Difūzija (inversija pret vidējo)

Palielina mazās amplitūdas, samazina lielās.



Ko vēl var izdarīt ar kvantu datoru?

Sakritību meklēšana (A, 2004)

28	12	18	76	96	82	94	99	21	78	88	93	39	44	64
32	99	70	18	94	82	92	64	95	46	53	16	35	42	72
31	40	75	71	93	32	47	11	70	37	78	79	36	63	40
69	92	71	28	85	41	80	10	52	63	88	57	43	84	67
57	31	98	39	65	74	24	90	26	83	60	91	27	96	35
20	26	52	95	65	66	97	54	30	62	79	33	84	50	38
49	20	47	24	54	48	98	23	41	16	66	75	38	13	58
56	86	34	73	61	73	21	44	62	34	14	51	74	76	83
37	90										11	51	23	77
68	72										19	81	81	49
60	85										48	22	15	17
55	36	27	42	55	77	19	45	15	53	22	91	87	17	33

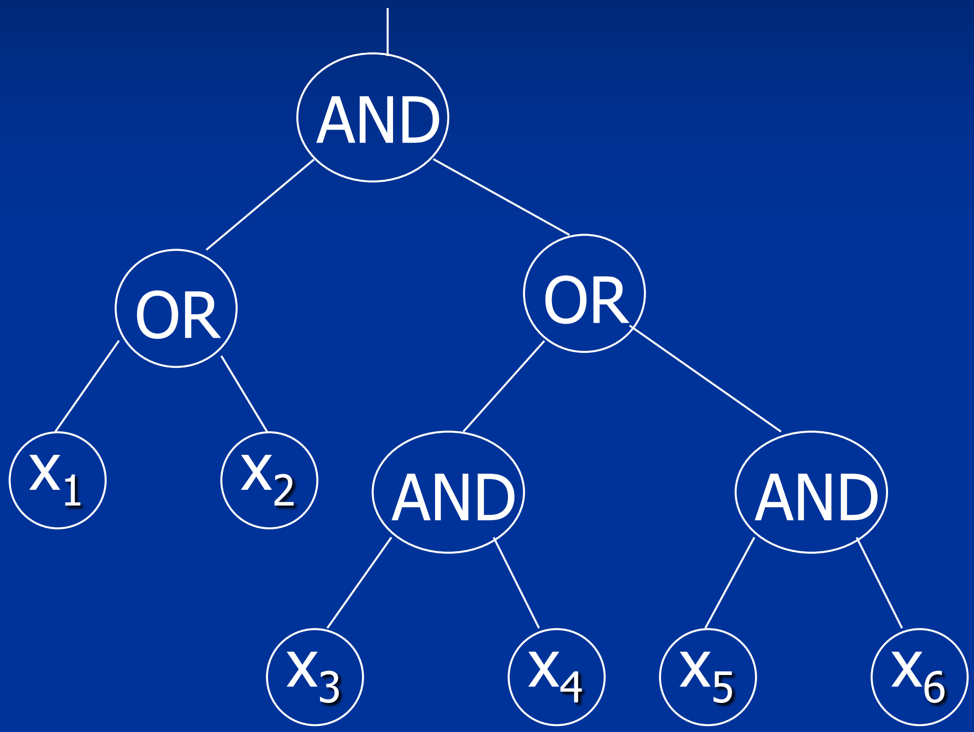
Uzdevums: atrast divus skaitļus, kas ir vienādi.

Sakritību meklēšana

31	40	75	71	93	32
47	11	70	37	78	79
36	63	40	48	98	23
41	16	66	75	38	27
42	55	77	19	45	15
53	22	91	37	90	58
13	10	25	29	25	56
68	12	11	51	23	77
15	17				

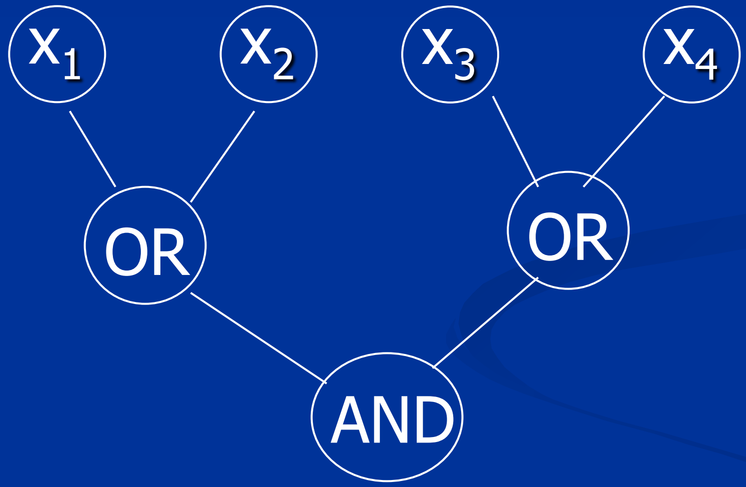
- Klasiskiem (ne-kvantu) algoritmiem vajadzīgi N soļi.
- Mūsu rezultāts: kvantu algoritmiem pietiek ar $\sim N^{2/3}$.

Loģikas formulas (A, 2007)

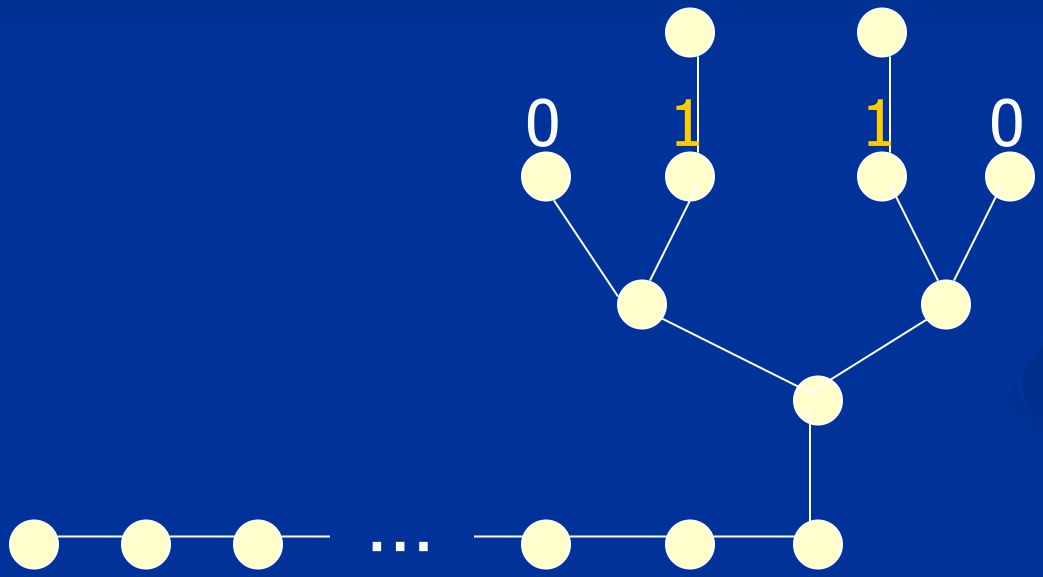


- Formulas izmērs: N.
- Laiks:
  - Parasts dators: N.
  - Kvantu dators: √N.

Formula

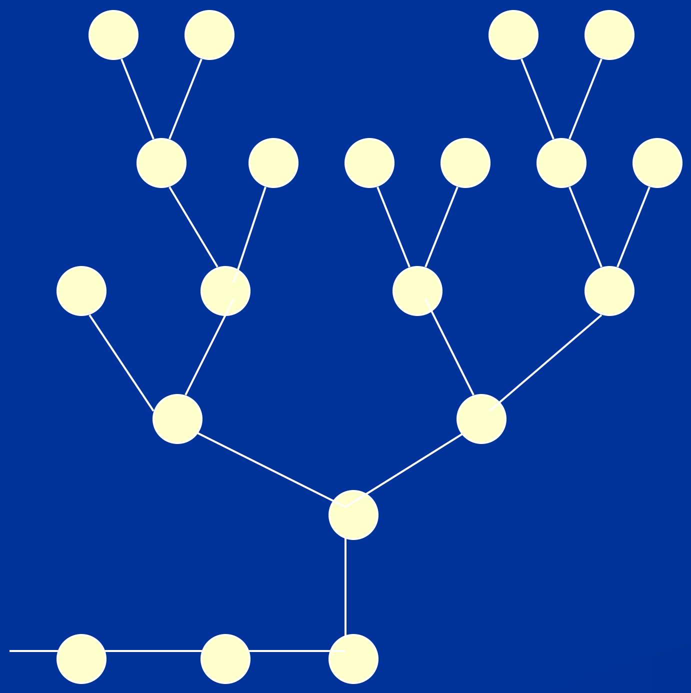


Kvantu algoritms



Kvantu klejošana:
daļiņa klejo pa koku, ar sākuma stāvokli "astē"

Rezultāts

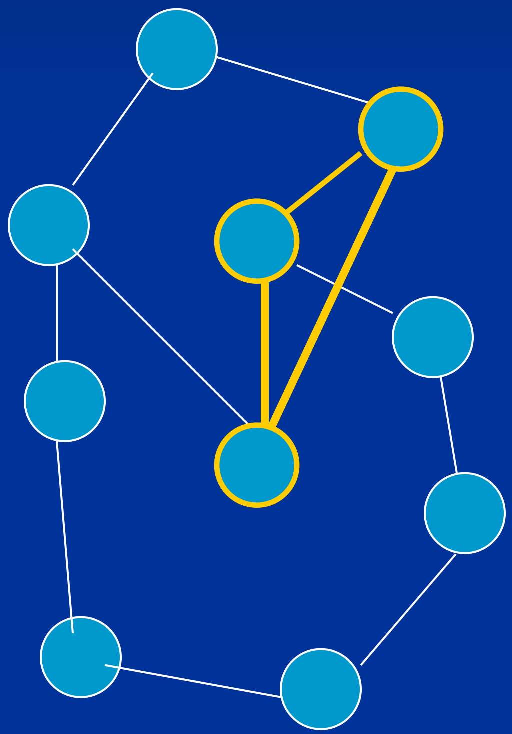


- Ja F = 0, tad daļiņa paliek "astē";
- Ja F=1, tad daļiņa pārvietojas uz formulas koka tām daļām, kas padara formulu patiesu.
- Tas notiek √N soļos.

Kopīgā iezīme

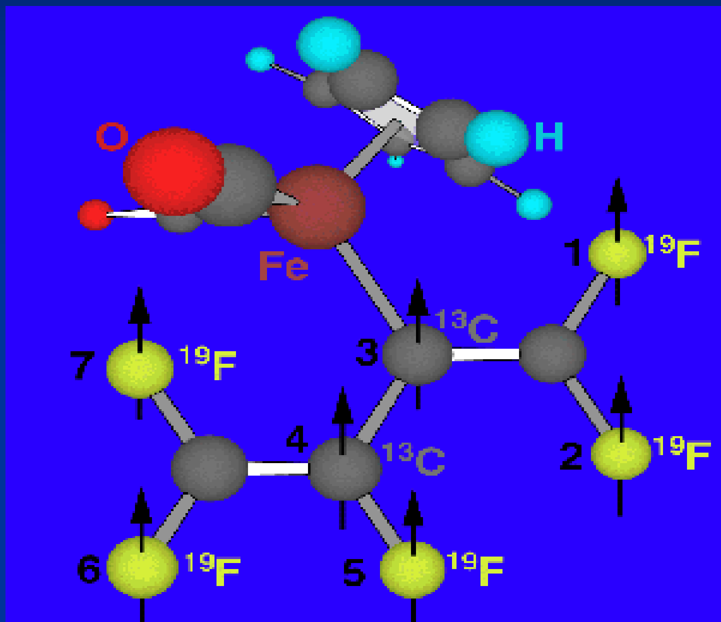
- Klasiskam datoram:
  - (Laiks) $\geq$ (Ievaddatu apjoms);
- Kvantu dators var rēķināt ātrāk, izmantojot kvantu paralēlismu.

Trijstūri grafos



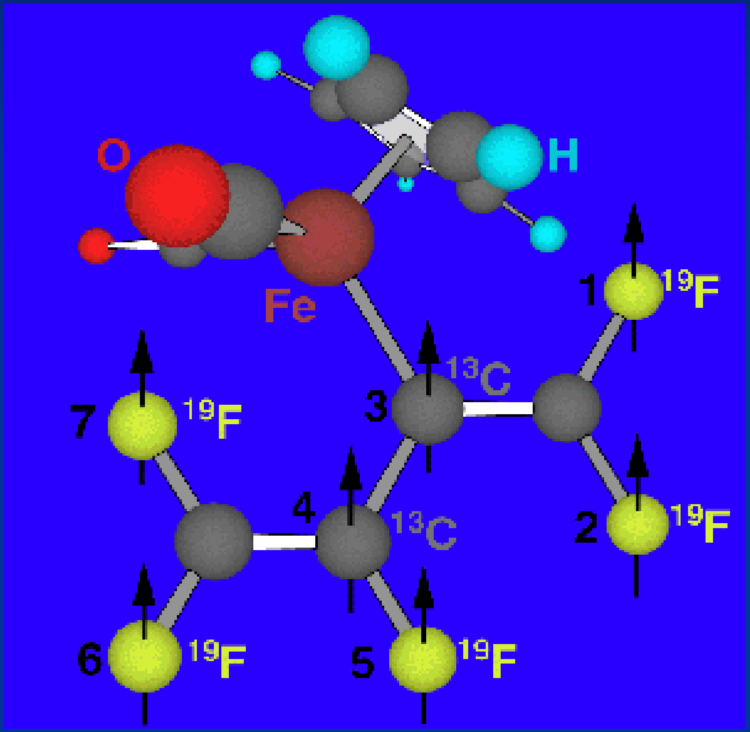
- Grafs G ar n virsotnēm.
- n^2 mainīgie x_{ij}; $x_{ij}=1$ ja ir mala (i, j).
- Vai G satur trijstūri?
- Klasiski: $O(n^2)$.
- Kvantu [Belovs, 2011]: $O(n^{1.29...})$.

13 bitu KMR kvantu dators (MIT/Waterloo, 2004)



Ir realizēta meklēšana starp 4 elementiem, skaitļa 15 sadalīšana pirmreizinātājos.

13 bitu KMR kvantu dators (MIT/Waterloo, 2004)



- Kvantu dators = molekula.
- Kvantu biti = atomu kodolu spini.
- Uz tiem iedarbojas ar magnētisko lauku.

Kādus uzdevumus* nevar *atrisināt kvantu dators?

Meklēšana

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.
- Kvantu algoritms: O(√n) soļi [Grover, 1996].

Labāka kvantu algoritma nav.

Kvantu stāvokļi = vektori

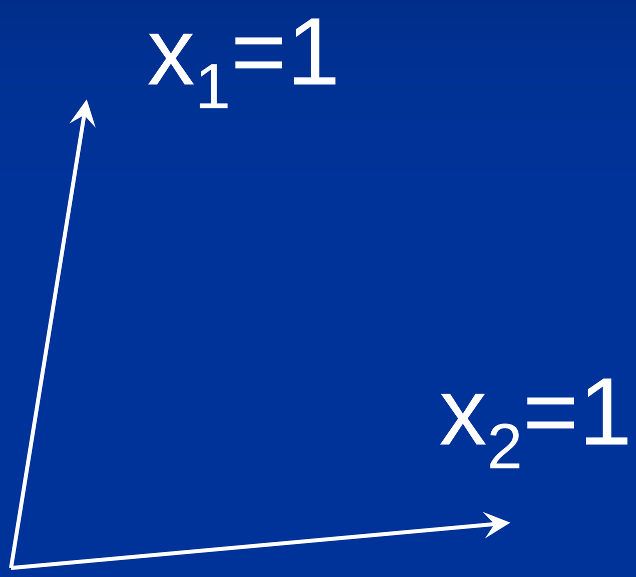
- Kvantu stāvoklis

$$a_1|1\rangle + a_2|2\rangle + \ldots + a_n|n\rangle$$

- Vektors

$$\begin{pmatrix} a_1 \\ a_2 \\ \ldots \\ a_n \end{pmatrix}$$

Algoritma analīze (A, 2000)



- Sākumā vektori sakrīt.
- Ja algoritms strādā pareizi, tad beigās vektori – perpendikulāri.

Algoritma analīze

- Ievieš lielumu S, kas parāda, cik perpendikulāri ir algoritma kvantu stāvokļi pie dažādiem meklējamajiem objektiem ($x_i=1$).
- Sākumā S = 0;
- Beigās S = n;
- Vienā solī S pieaug ne vairāk par $\sqrt{n}$.

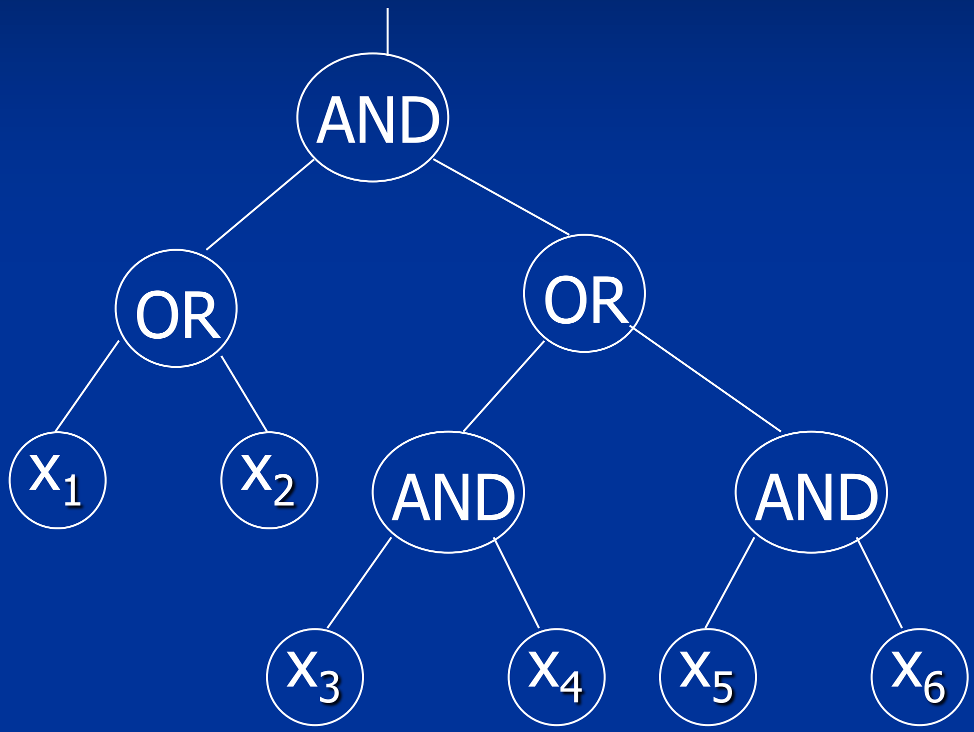
Vajag $\sqrt{n}$ soļus.

Sakritību meklēšana

31	40	75	71	93	32
47	11	70	37	78	79
36	63	40	48	98	23
41	16	66	75	38	27
42	55	77	19	45	15
53	22	91	37	90	58
13	10	25	29	25	56
68	12	11	51	23	77
15	17				

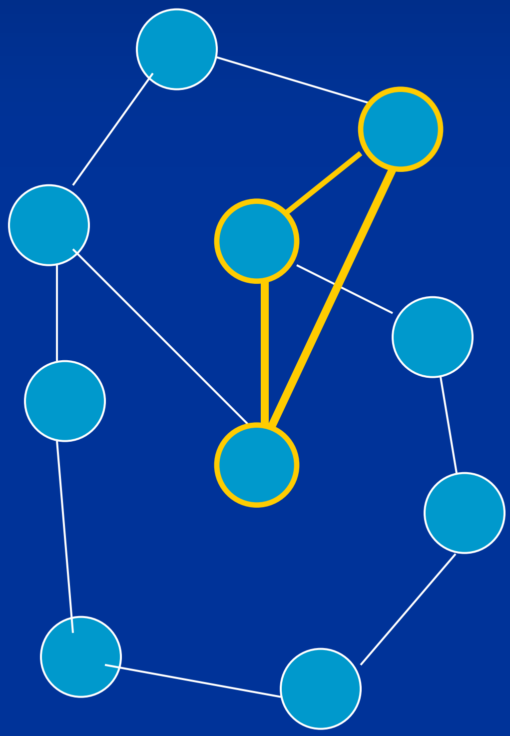
- [Aaronson, Shi, 2003] Kvantu algoritmiem vajag vismaz $N^{2/3}$ soļus.

Loģikas formulas



- [Barnum et al., 2003] Kvantu datoram vajag √N soļus.

Trijstūri grafos



- Vai G satur trijstūri?
- Kvantu algoritms [Belovs, 2011]: $O(n^{1.29...})$.
- Vajag vismaz n soļus.