Projekts "*Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku*"

- Tiek īstenots Latvijas universitātes Datorikas fakultātē
- Piesaista datorzinātnes, matemātikas un fizikas zinātniekus
- Projekta vadītājs – prof. Andris Ambainis
- Piecas pētnieku grupas jauno zinātnieku vadībā:
  - Pētījumi kvantu skaitļošanā (*Andris Ambainis*)
  - Pētījumi kvantu tehnoloģiju fizikālajos aspektos (*Vjačeslavs Kaščejevs*)
  - Modeļu bāzēto arhitektūru attīstība (*Guntis Arnicāns*)
  - Pētījumi par datu noliktavām (*Laila Niedrīte*)
  - Pētījumi programminženierijā (*Darja Šmite*)
- Īstenošanas termiņš: 2009.g. decembris- 2012.g. novembris
- ESF projekta Nr. 2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

LATVIJAS UNIVERSITĀTE
UNIVERSITY OF LATVIA

ESF
EIROPAS SOCIĀLAIS FONDS

Datorzinātnes lietojumi un tās saiknes ar kvantu fiziku

Kvantu skaitļošana: datoriķa skatījums

Andris Ambainis
LU Datorikas fakultāte

Viedo sensoru un kvantu skaitļošanas seminārs 2011. gada 27.maijā

Galvenie pētījumu virzieni

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

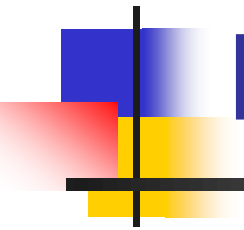
Kvantu apakšējie novērtējumi
(A. Ambainis)

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)



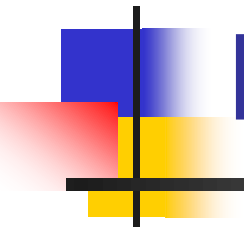
Kas ir kvantu skaitļošana?

Skaitļošanas būtība

- Fizikālās sistēmas (“**Datora**”) stāvoklis reprezentē informāciju
- Sistēmas attīstība laikā saskaņā ar fizikas likumiem (“**Datora darbība**”) maina stāvokli $\Rightarrow$ pārveido informāciju
- Dators darbojas vidē, kas nodrošina informācijas **ievadu**, **izvadu** un **komunikāciju**

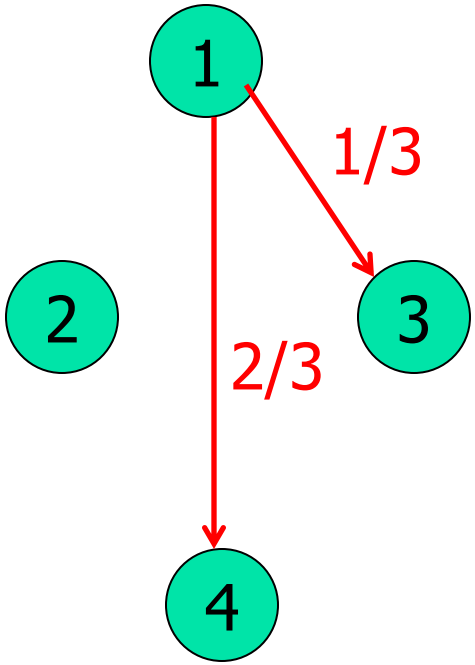
Kvantu skaitļošanas iezīmes

- **Sapinums** (*entanglement*)
  - atmiņas stāvoklis ir "bagātāks" par klasisko
- **Superpozīcija**
  - algoritmu izpildes "paralēlisms"
- **Nenoteiktība**
  - rezultāta nolasīšana ir varbūtiska



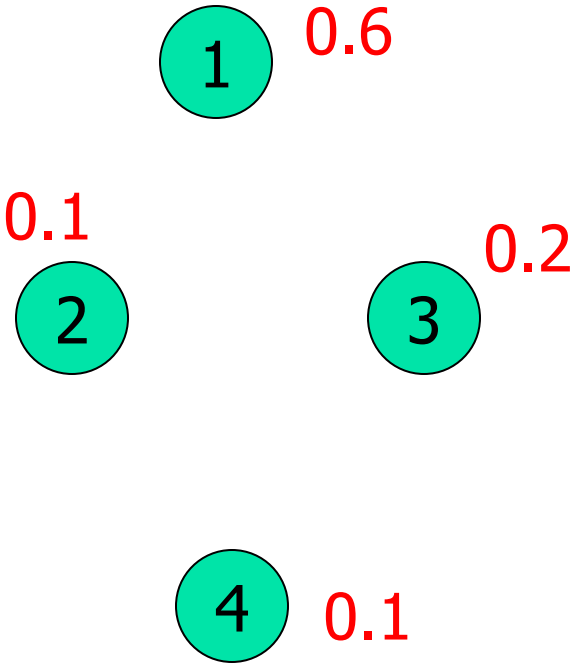
Kvantu skaitļošanas modelis

Varbūtiskā sistēma



- Galīgs skaits stāvokļu.
- Varbūtiski pārvietojamies no tekošā stāvokļa uz nākošā.

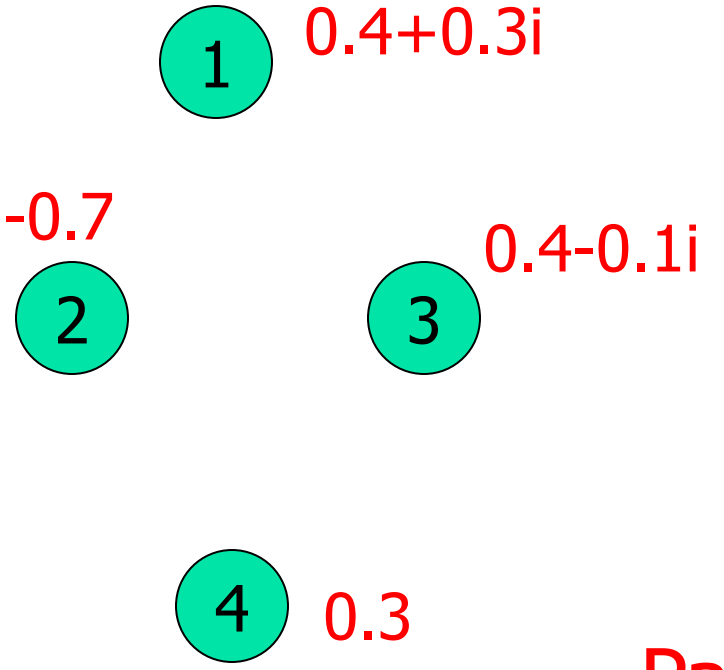
Varbūtiskā sistēma



- Tekošais stāvoklis: stāvoklis i ar varbūtību p_i.

$$\sum_i p_i = 1$$

Kvantu sistēma

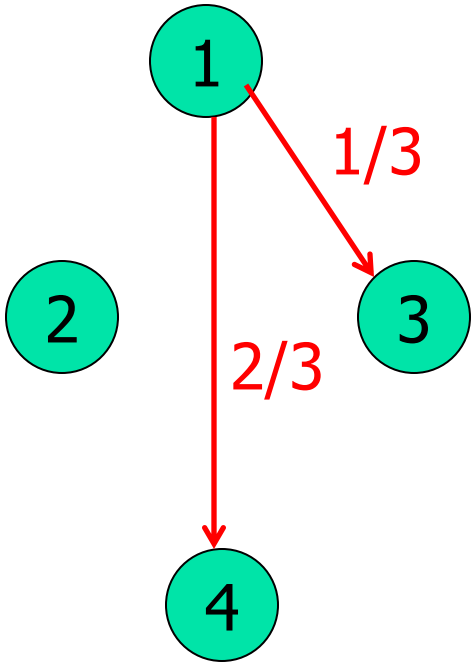


- Tekošais stāvoklis: stāvoklis i ar amplitūdu α_i.

$$\sum_i |\alpha_i|^2 = 1$$

Parasti, pietiek ar reālām amplitūdām (kas var būt negatīvas).

Varbūtiskā sistēma



- Pārejas: r_{ij} – varbūtība pāriet no i uz j.

$$p'_j = \sum_i p_i r_{ij}$$

Varbūtiska sistēma

- Varbūtību vektors $(p_1, \ldots, p_M)$.
- Pārejas:

$$\begin{pmatrix} p'_1 \\ \ldots \\ p'_M \end{pmatrix} = \begin{pmatrix} r_{11} & \ldots & r_{1M} \\ \ldots & \ldots & \ldots \\ r_{M1} & \ldots & r_{MM} \end{pmatrix} \begin{pmatrix} p_1 \\ \ldots \\ p_M \end{pmatrix}$$

pēc pārejas

pārejas varbūtības

pirms pārejas

Kvantu sistēma

- Amplitūdu vektors $(\alpha_1, \ldots, \alpha_M)$, $\sum_i |\alpha_i|^2 = 1$.
- Pārejas:

$$\begin{pmatrix} \alpha'_1 \\ \ldots \\ \alpha'_M \end{pmatrix} = \begin{pmatrix} u_{11} & \ldots & u_{1M} \\ \ldots & \ldots & \ldots \\ u_{M1} & \ldots & u_{MM} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \ldots \\ \alpha_M \end{pmatrix}$$

pēc pārejas

pārejas matrica

pirms pārejas

Atļautās operācijas

$$\begin{pmatrix} \alpha'_1 \\ \dots \\ \alpha'_M \end{pmatrix} = \begin{pmatrix} u_{11} & \dots & u_{1M} \\ \dots & \dots & \dots \\ u_{M1} & \dots & u_{MM} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_M \end{pmatrix}$$

- U – unitāra:
  - Ja $\sum_i |\alpha_i|^2 = 1$, tad $\sum_i |\alpha'_i|^2 = 1$.

Kopsavilkums

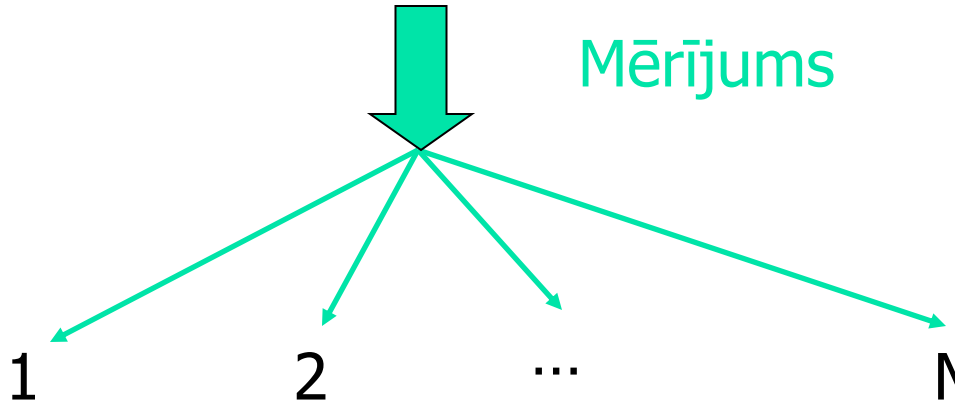
- Kvanti $\approx$ kompleksas varbūtības.
- $\Sigma_i p_i = 1$ vietā $\sum_i |\alpha_i|^2 = 1$.

Kā kvantu pasaule pārvēršas par tradicionālo pasauli?

Mērījums

Kvantu stāvoklis:

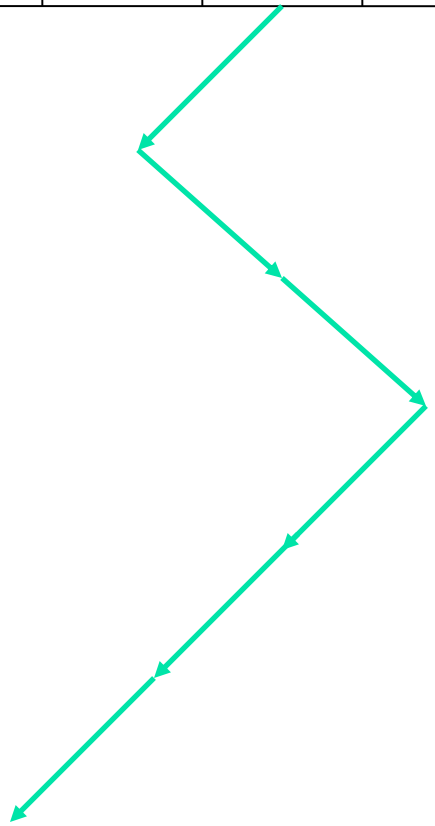
$$\alpha_1 1 + \alpha_2 2 + \ldots + \alpha_M M$$



varb. $|\alpha_1|^2$ $|\alpha_2|^2$ $|\alpha_M|^2$

Gadījuma klejošana

…	-2	-1	0	1	2	…



- Sāk pozīcijā 0.
- Katrā solī, pa kreisi ar varb. ½, pa labi ar varb. ½.

Gadījuma klejošana

…	-2	-1	0	1	2	…

- Stāvoklis (x, d), x – pozīcija, d-virziens.
- Katrā solī:
  - d=left ar varb. ½, d=right ar varb. ½.
  - (x, left) => (x-1, left);
  - (x, right) => (x+1, right).

Kvantu klejošana

…	-2	-1	0	1	2	…

- Stāvokļi $|x, d\rangle$, x – pozīcija, d-virziens.

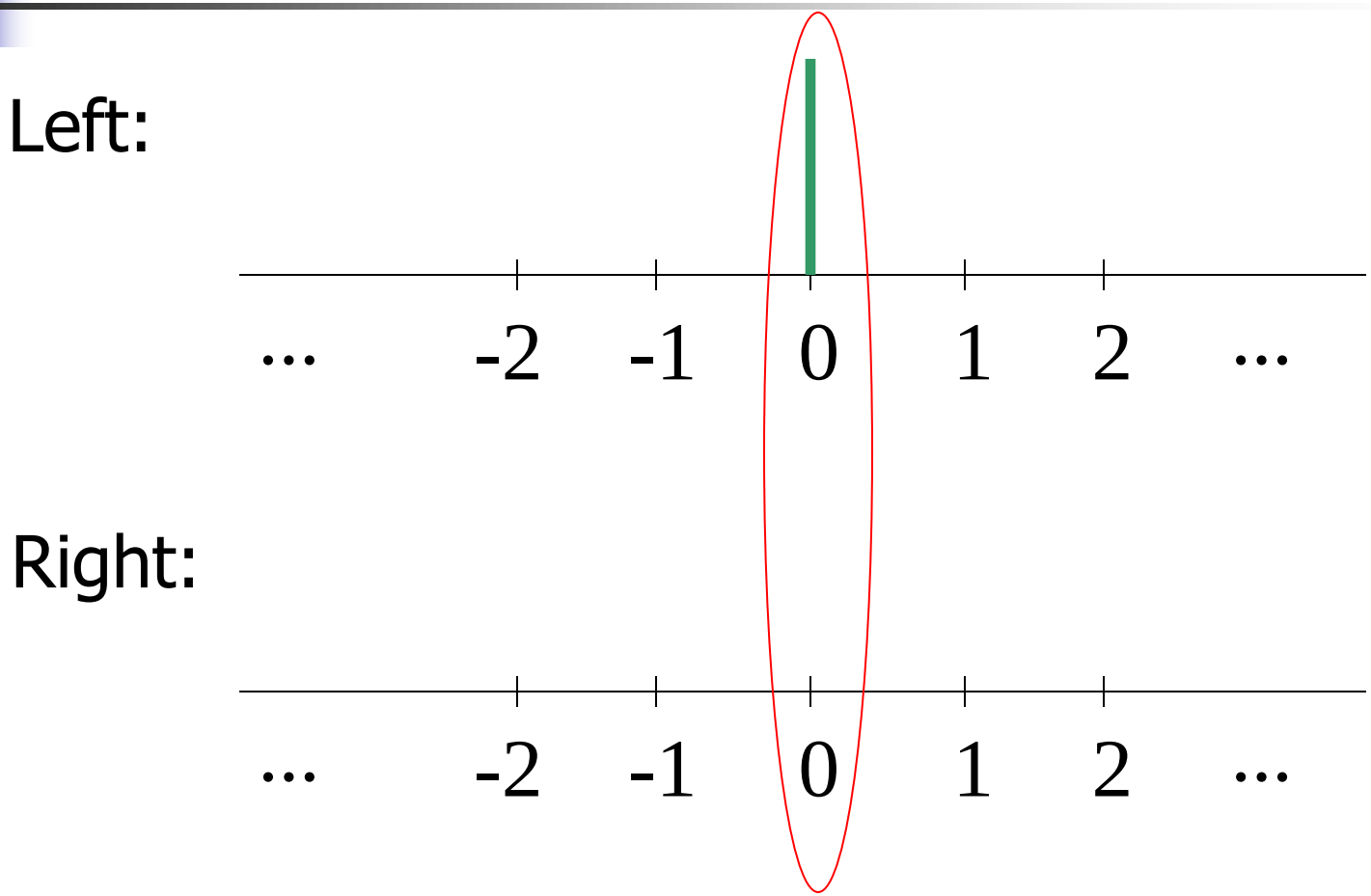
"Virziena izvēle":

$$\begin{cases} |x, left> \rightarrow \frac{1}{\sqrt{2}}|x, left> + \frac{1}{\sqrt{2}}|x, right> \\ |x, right> \rightarrow \frac{1}{\sqrt{2}}|x, left> - \frac{1}{\sqrt{2}}|x, right> \end{cases}$$

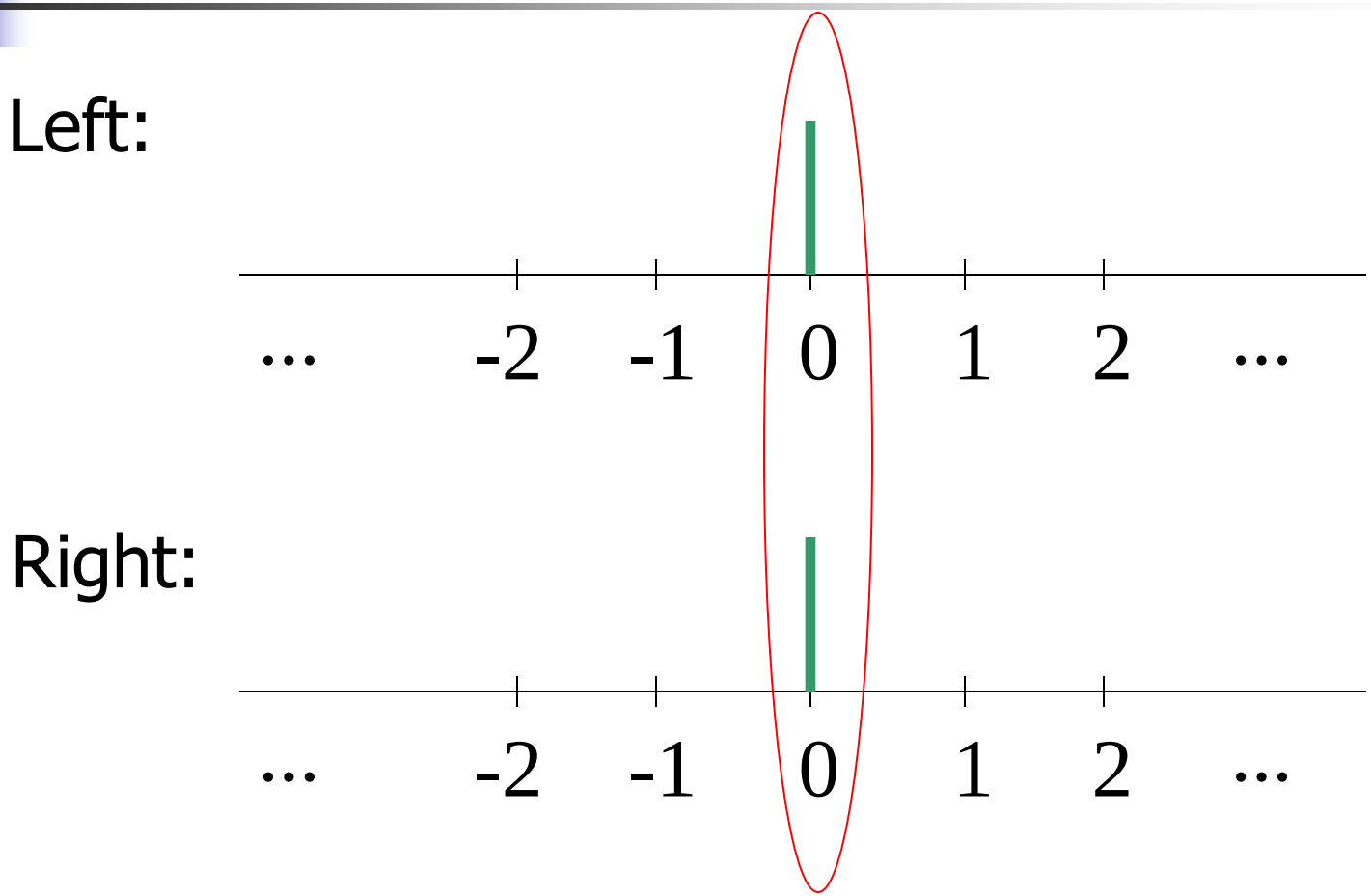
Solis:

$$\begin{cases} |x, left\rangle \rightarrow |x-1, left\rangle \\ |x, right\rangle \rightarrow |x+1, right\rangle \end{cases}$$

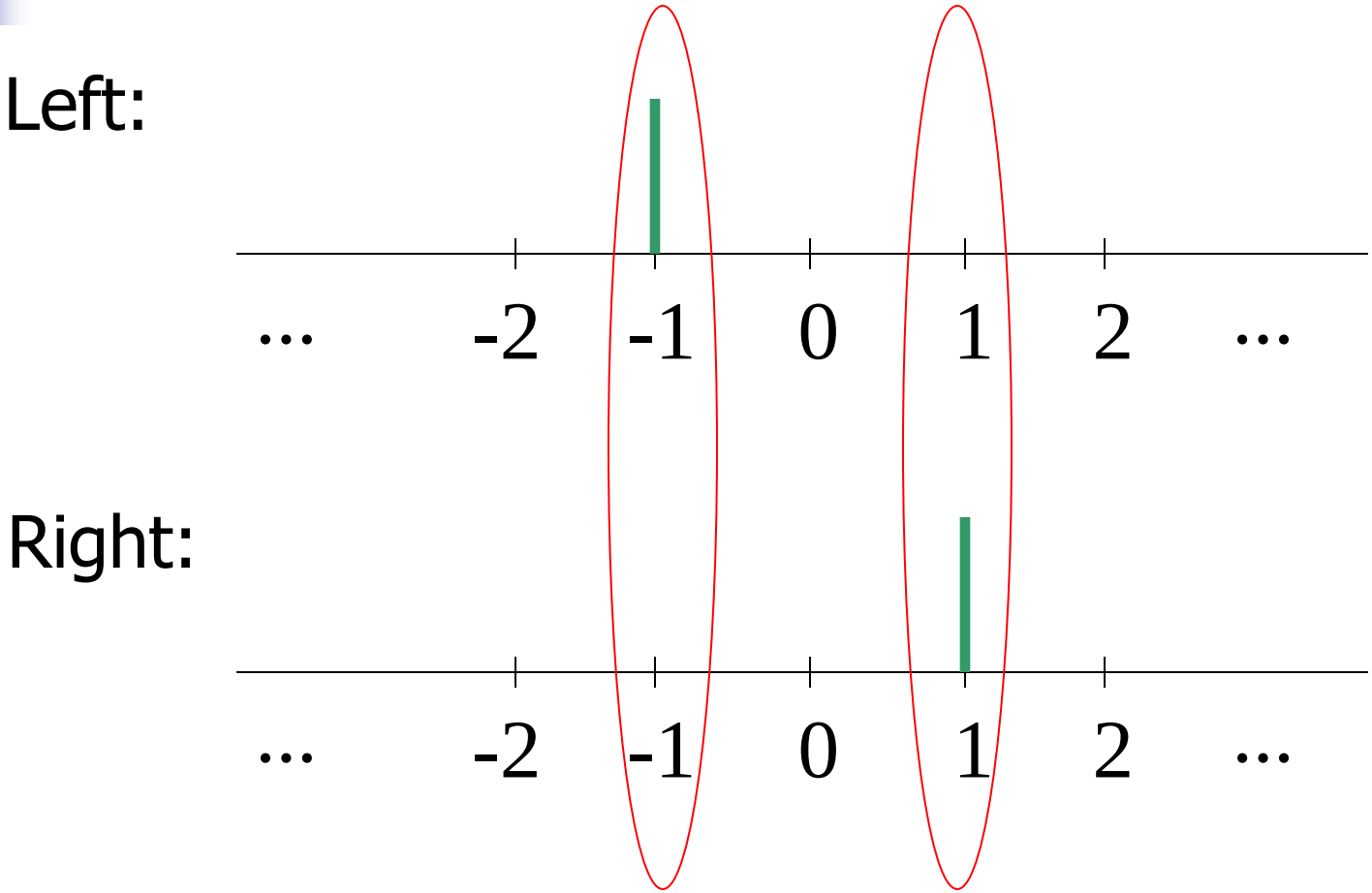
Kvantu klejošana



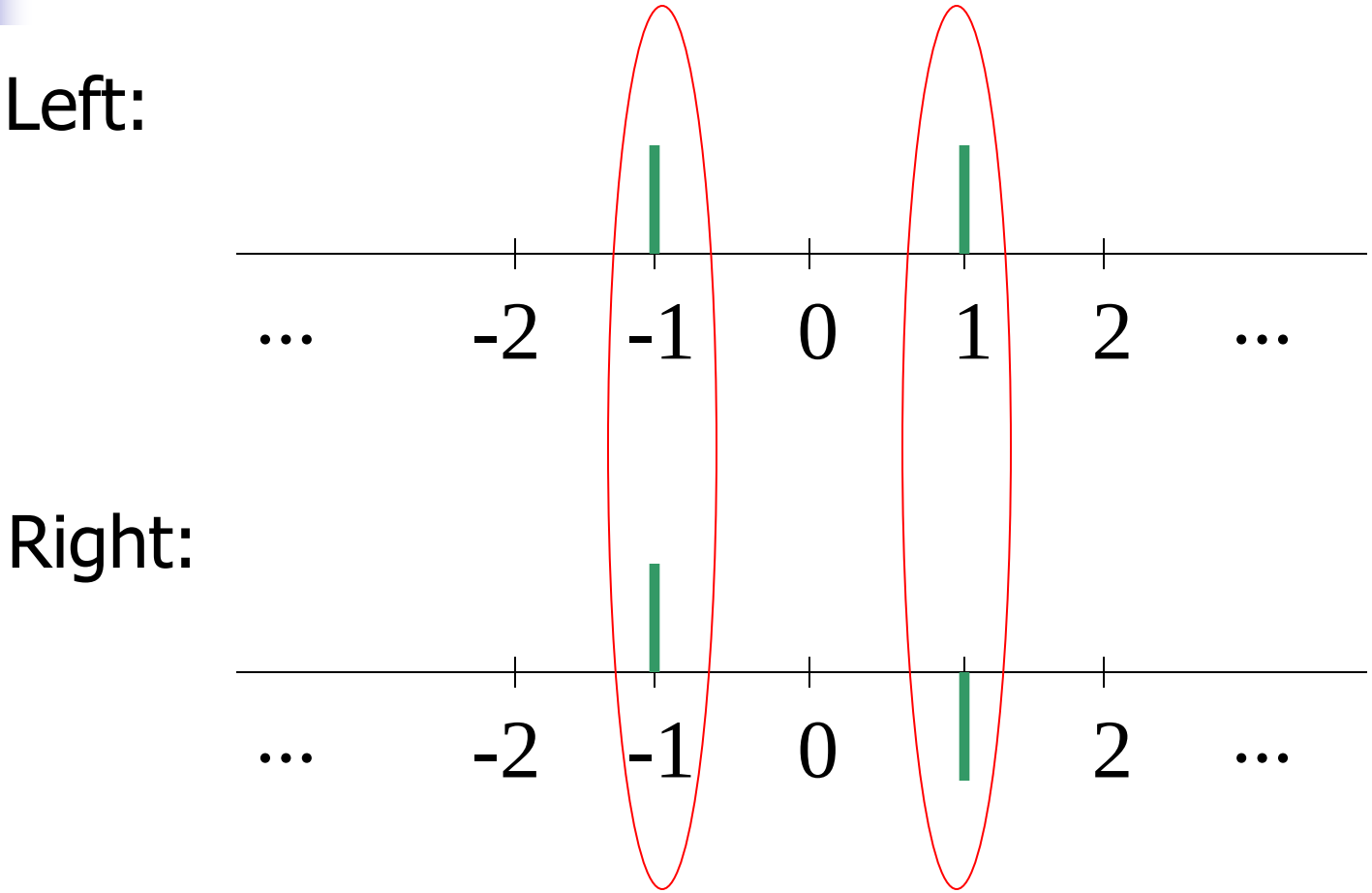
Kvantu klejošana



Kvantu klejošana

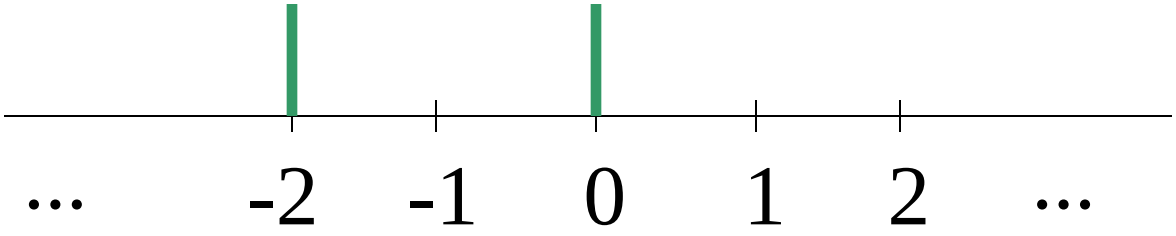


Kvantu klejošana

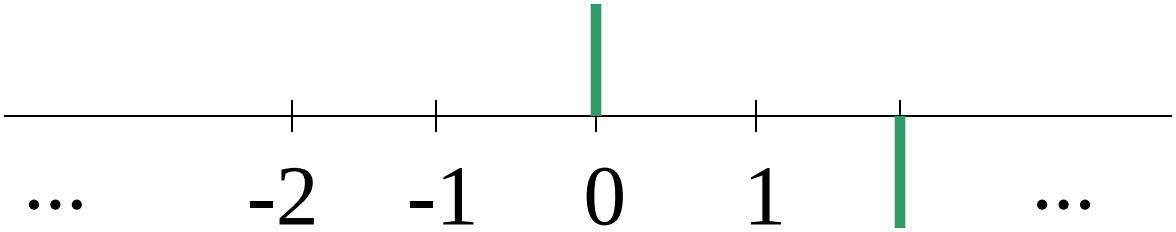


Kvantu klejošana

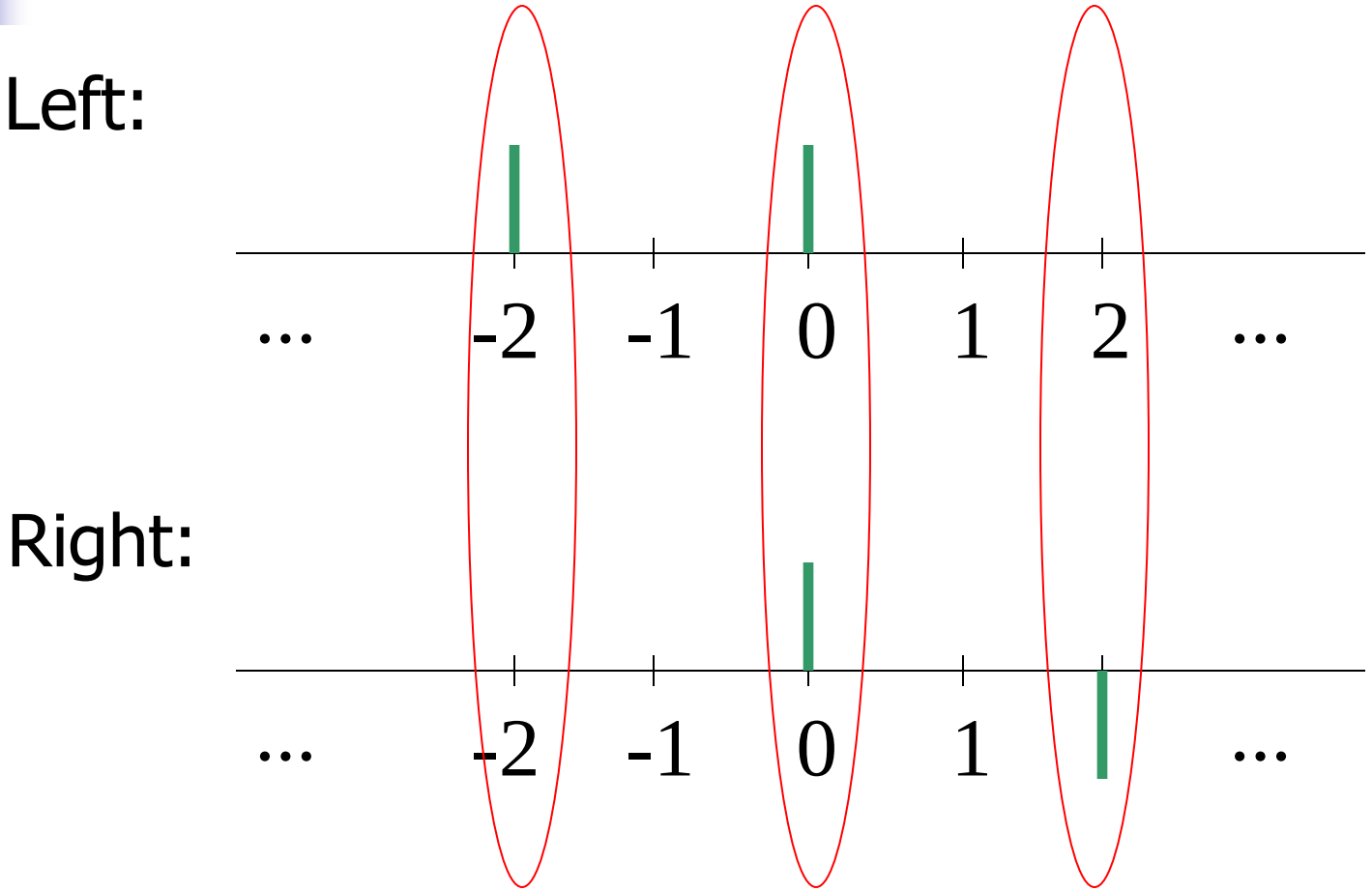
Left:



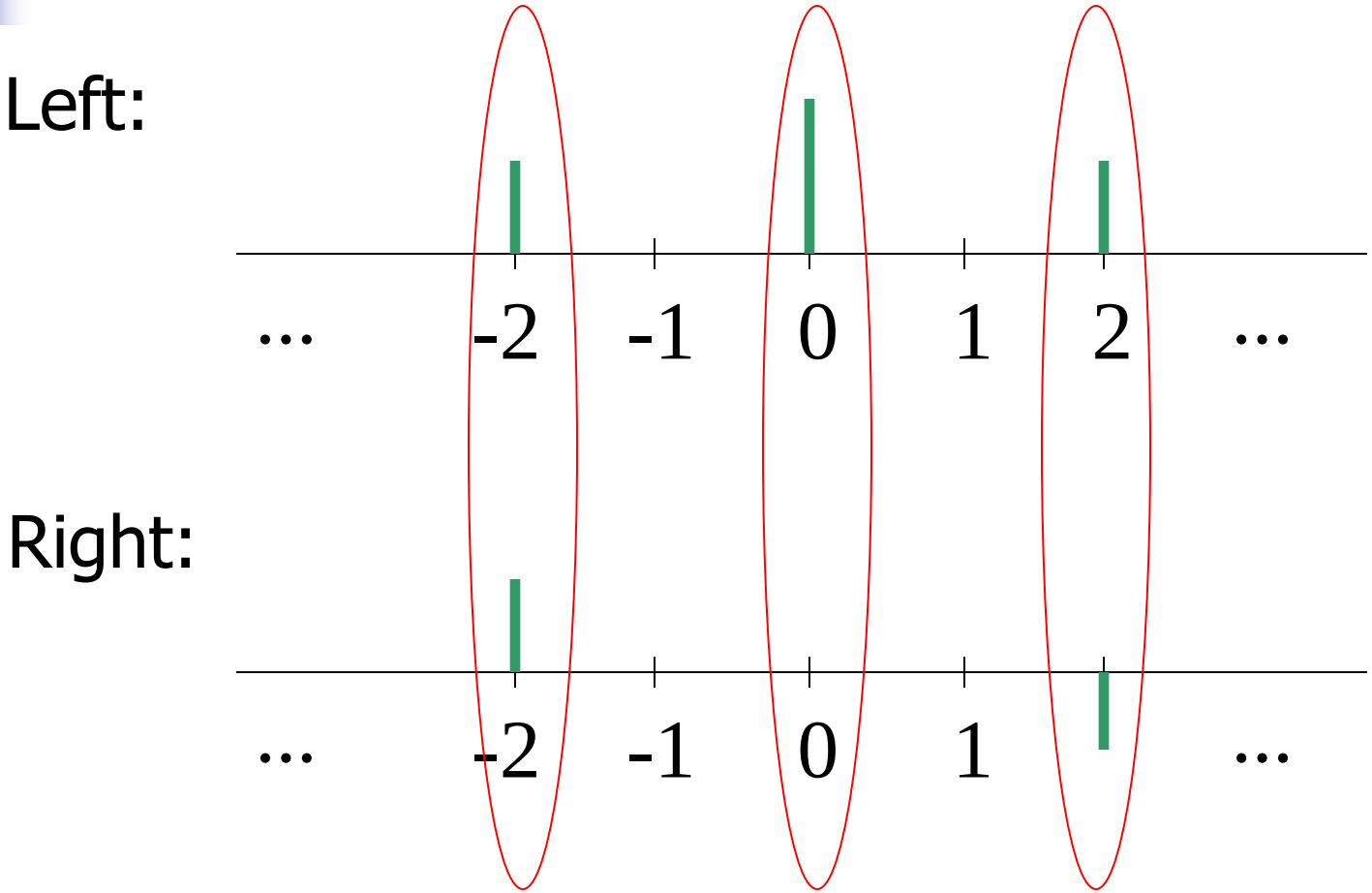
Right:



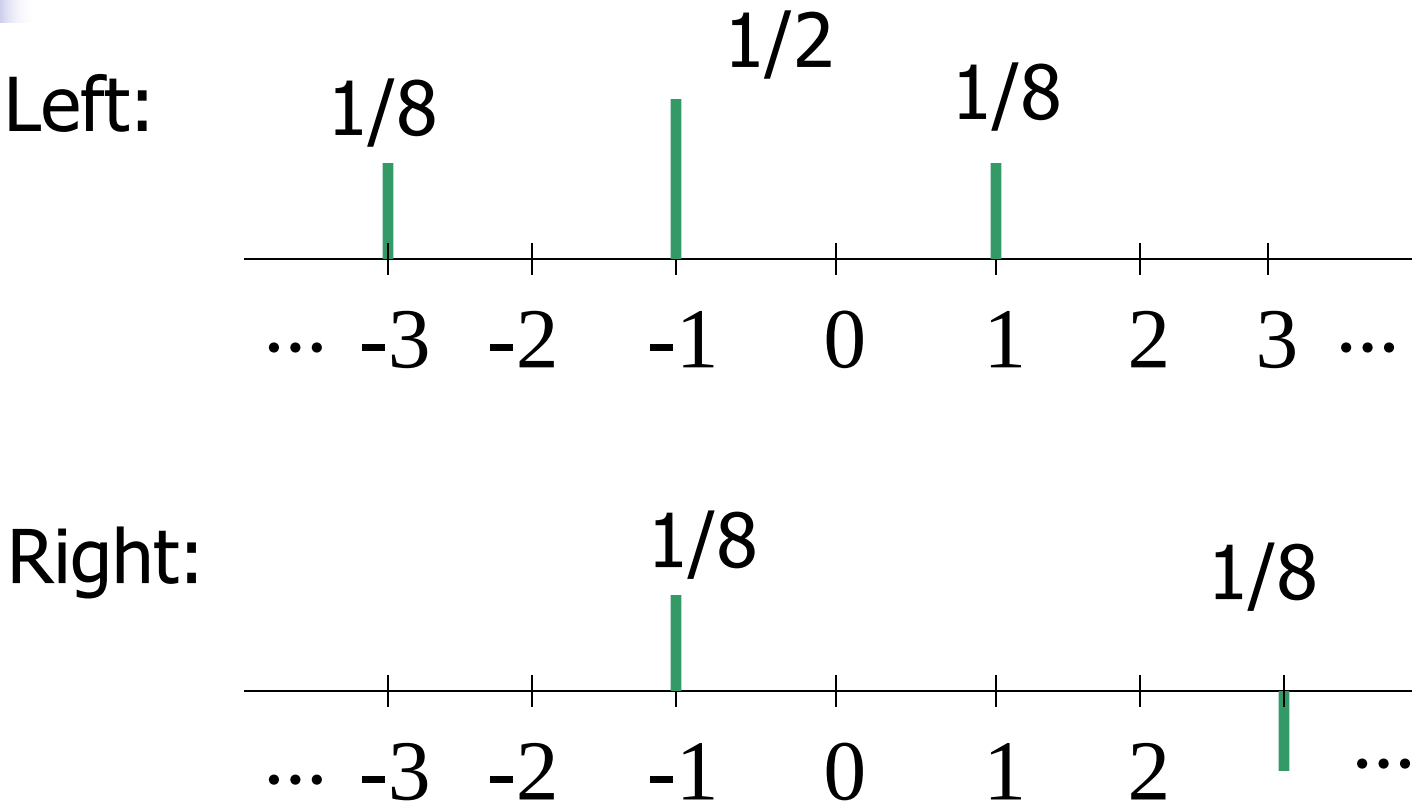
Kvantu klejošana



Kvantu klejošana

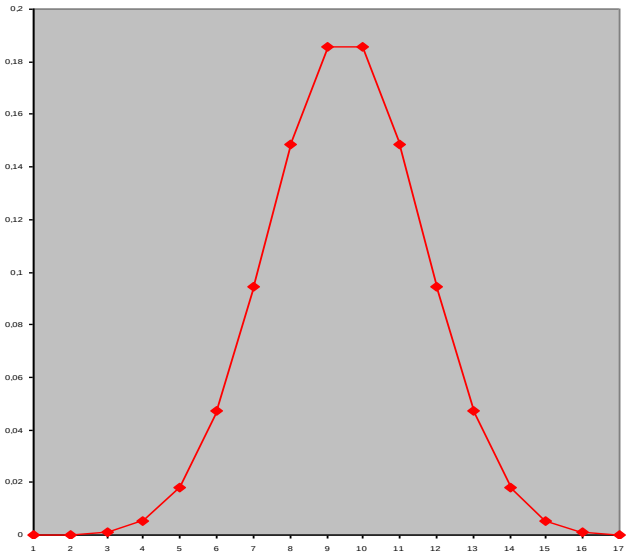


Kvantu klejošana

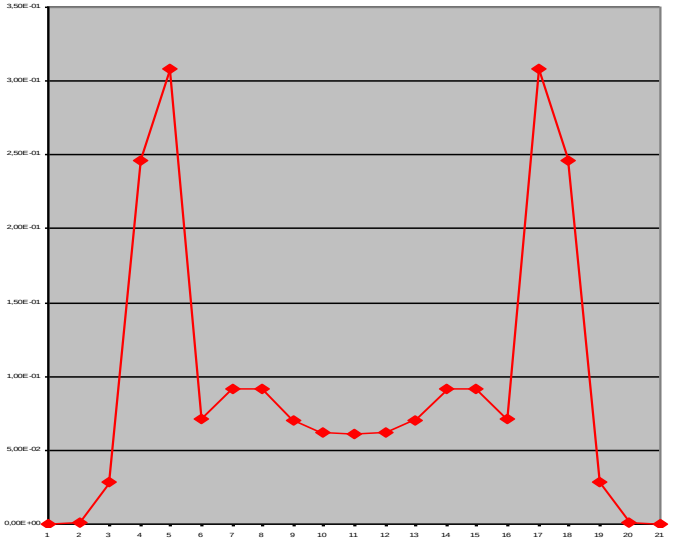


Varbūtiskā un kvantu klejošana

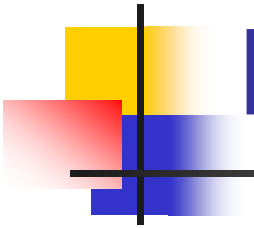
N soļi + mērījums.



Distance: $\Theta(\sqrt{N})$

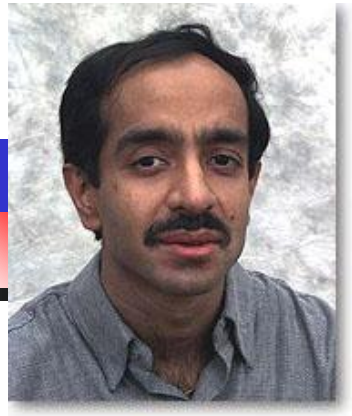


Distance: $\Theta(N)$



Kvantu algoritmu piemēri

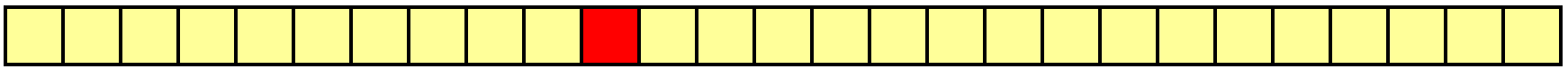
Meklēšana



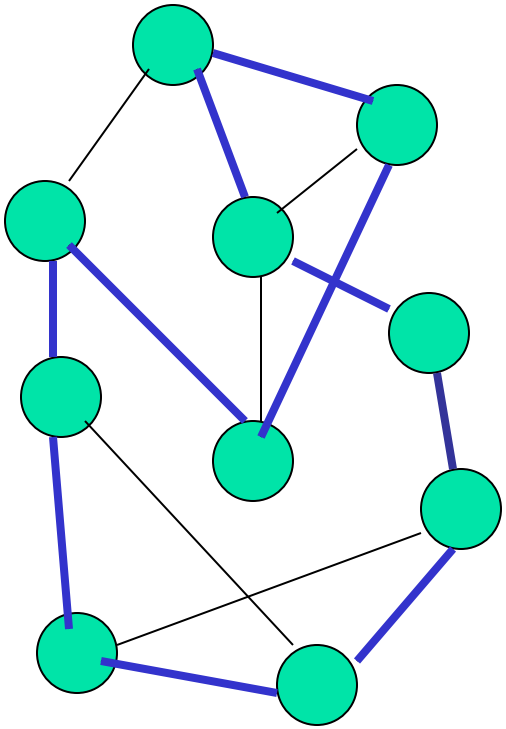
Algoritms, kas $\sim \sqrt{N}$ kvantu soļos atrod elementu ar noteiktu īpašību N elementu sarakstā. Klasiski, nepieciešami N soļi.

Lov Grover, 1996

Vajadzīgais elements



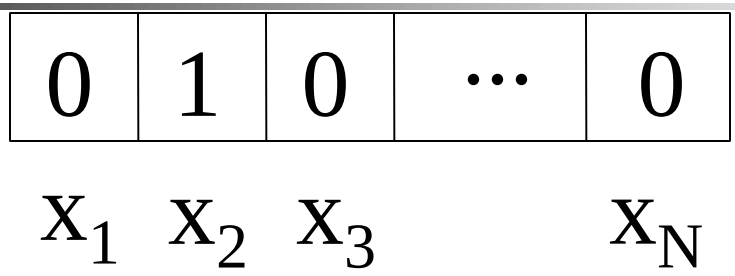
NP-pilnas problēmas



- Vai šajā grafā ir Hamiltona cikls?

- Hamiltona cikli ir:
  - Viegli pārbaudāmi;
  - Grūti atrodami (pārāk daudz iespēju).

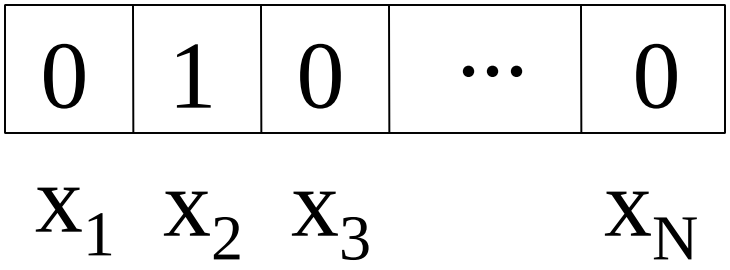
Kvantu algoritms



- N – *iespējamo* Hamiltona ciklu skaits.
- Melnā kaste = algoritms, kas pārbauda, vai itā iespēja patiešām ir Hamiltona cikls.
- Kvantu algoritms,
  kas darbojas O($\sqrt{N}$) laikā.

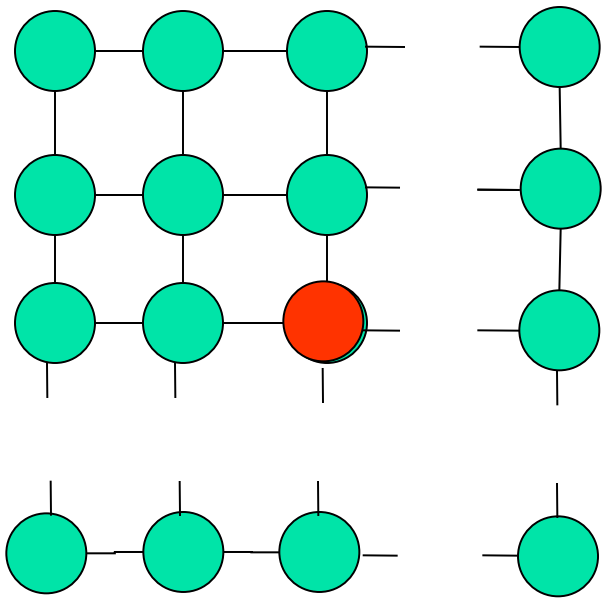
Der jebkurai pārlases problēmai

Grovera meklēšana



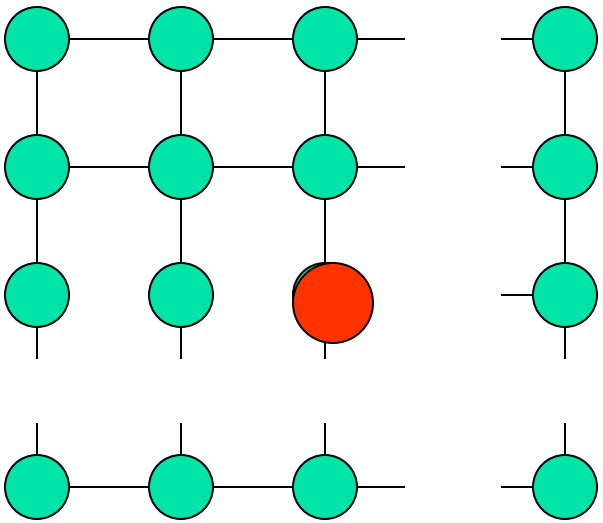
- Atrast i, kuram $x_i=1$.
- Melnā kaste: jautā i, atrod x_i.

Meklēšana uz režģa



- Režģis ar N elementiem.
- Jāatrod, kurā vietā ir noteikta vērtība.
- Vienā solī, var pārbaudīt tekošo atmiņas elementu vai pārvietoties 1 soli.

[Benioff, 2000]



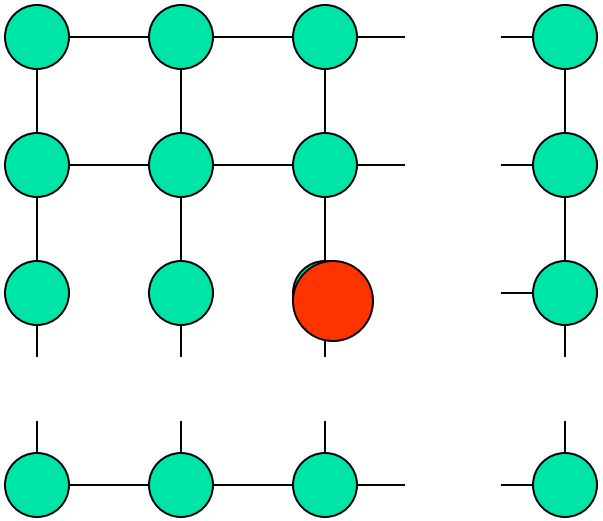
- √n* √n režģis.
- Attālums starp pretējiem stūriem = 2√n.
- Grovera algoritms:

$$\sqrt{\mathbf{n}} * \sqrt{\mathbf{n}} = \mathbf{n}$$

- Kvantu paātrinājums pazūd.

Kvantu klejošana!

[A, Kempe, Rivošs, 2005]



- Stāvokļi $|x,y,\leftarrow\rangle$, $|x,y,\rightarrow\rangle$, $|x,y,\uparrow\rangle$, $|x,y,\downarrow\rangle$.
- Virziena maiņa:

$$\begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

[Amabinis, Kempe, Rivošs, 2005]

- Nobīde:
  - $|x, y, \leftarrow\rangle \quad \Rightarrow \quad |x\text{-}1, y, \rightarrow\rangle$
  - $|x, y, \rightarrow\rangle \quad \Rightarrow \quad |x+1, y, \leftarrow\rangle$
  - $|x, y, \uparrow\rangle \quad \Rightarrow \quad |x, y\text{-}1, \downarrow\rangle$
  - $|x, y, \downarrow\rangle \quad \Rightarrow \quad |x, y+1, \uparrow\rangle$

[Amabinis, Kempe, Rivošs, 2005]

- Kvantu klejošana ar citu "virziena maiņu", ja pašreizējā pozīcijā atrodas meklējamais objekts.
- Pēc $O\left(\sqrt{N \log N}\right)$ soļiem, mēra stāvokli.
- Iegūst vajadzīgo (x, y) ar varb. 1/log N.
- Var atkārtot.

Sakritību meklēšana

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										51	74	76	83
37	90										11	51	23	77
68	72										19	81	81	49
60	85	80	50	61	59	89	67	89	29	86	48	22	15	17
55	36	27	42	55	77	19	45	15	53	22	91	87	17	33

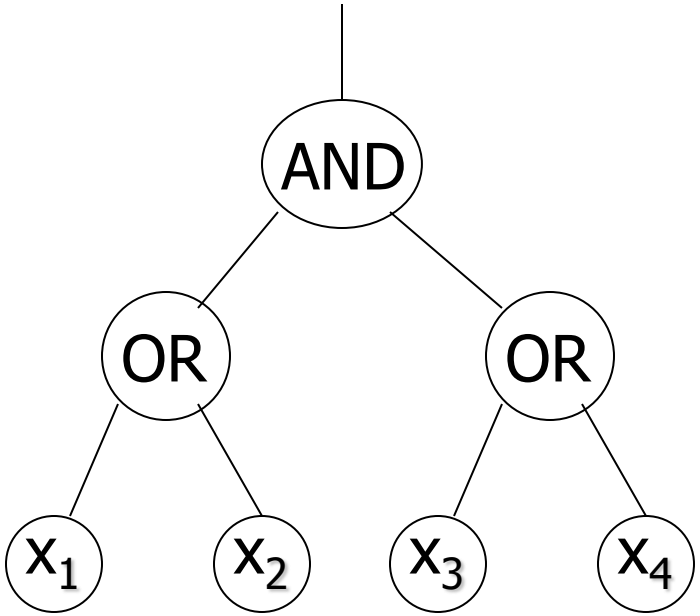
Uzdevums: atrast divus skaitļus, kas ir vienādi.

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

- Klasiskiem (ne-kvantu) algoritmiem vajadzīgi N soļi.
- [A, 2004] Kvantu algoritmiem pietiek ar $\sim N^{2/3}$.

[Ambainis, Childs, et al., 07]



- Formula ar M loģiskajām operācijām.
- Melnā kaste: jautājums i, atbilde x_i.
- Teorēma Jebkuru formulu var izrēķināt ar $O(M^{1/2+o(1)})$ vaicājumiem.

Kvantu algoritms jebkam, ko var izteikt ar loģikas formulām

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)