



LATVIJAS
UNIVERSITĀTE
UNIVERSITY OF LATVIA



*Datorzinātnes lietojumi un tās
saiknes ar kvantu fiziku*

Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Kvantu skaitļošana: datorika skatījums

Andris Ambainis
LU Datorikas fakultāte

LU 68. konference, 2010. gada 5. februārī

Kvantu mehānika

Datorzinātnes

Kvantu skaitļošana

```
graph TD; A[Kvantu mehānika] --> C[Kvantu skaitļošana]; B[Datorzinātnes] --> C;
```

The diagram illustrates the interdisciplinary field of Quantum Computing. It features three rectangular boxes with white borders on a dark blue background. At the top left, a box contains the text 'Kvantu mehānika'. At the top right, a box contains the text 'Datorzinātnes'. Arrows from the bottom-right corner of the 'Kvantu mehānika' box and the bottom-left corner of the 'Datorzinātnes' box point towards a central box at the bottom. This central box contains the text 'Kvantu skaitļošana'.

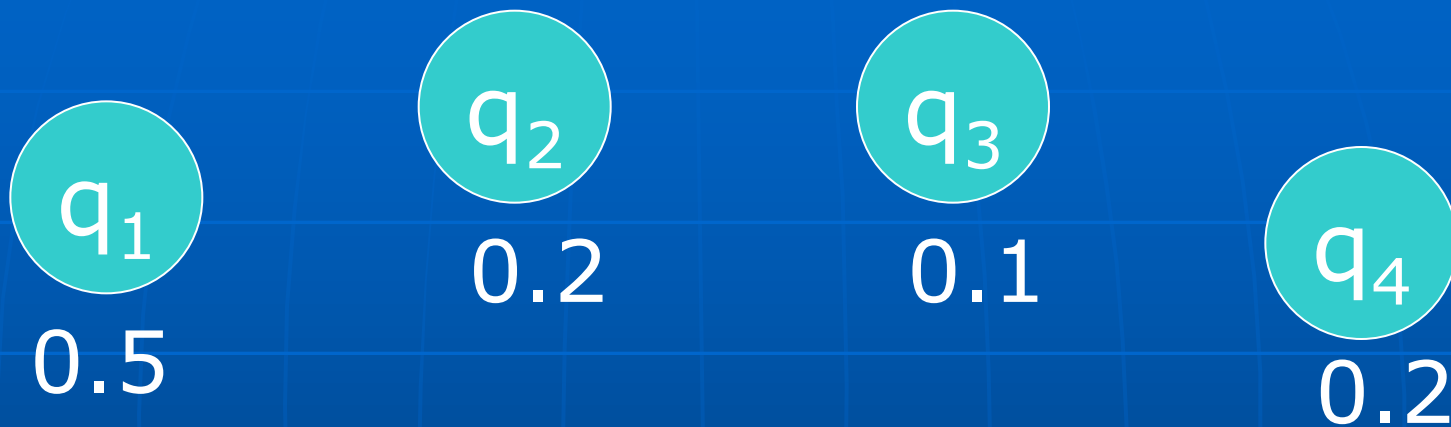
Kvantu mehānika – fizikas
nozare, kas apraksta dabas
likumus atomu līmenī.

Kvantu mehāniskās sistēmas

- Fotoni (gaisma);
- Atomu kodoli, elektroni;
- Molekulas;
- Strāva supravadītājā;
- Kvantu punkti ("mākslīgie atomi");

Vienots matemātiskais aparāts, kas apraksta visas šīs sistēmas.

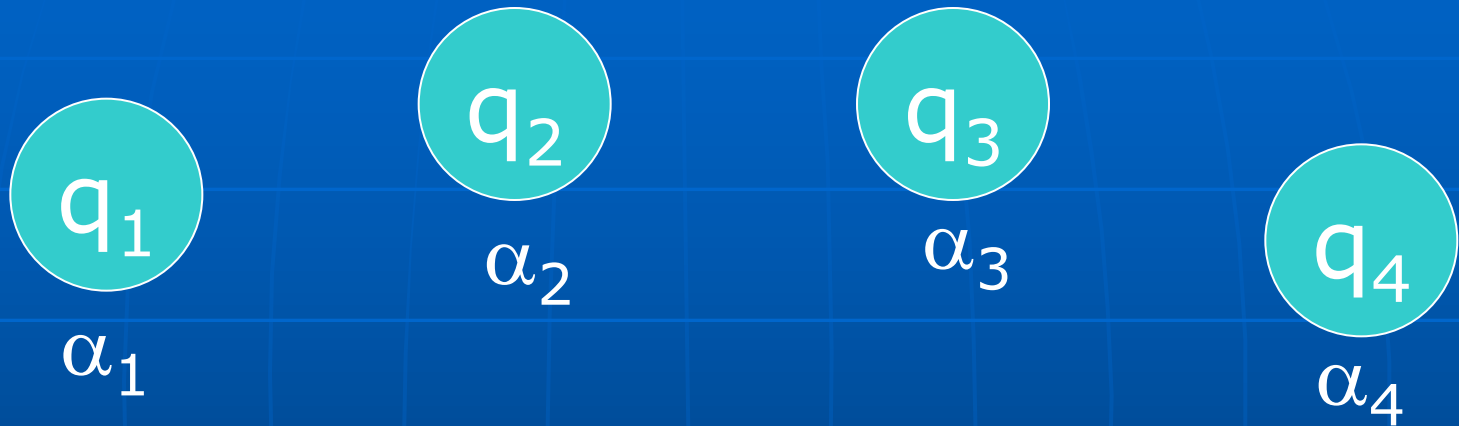
Varbūtiska sistēma



$$p_i \geq 0$$

$$\sum_i p_i = 1$$

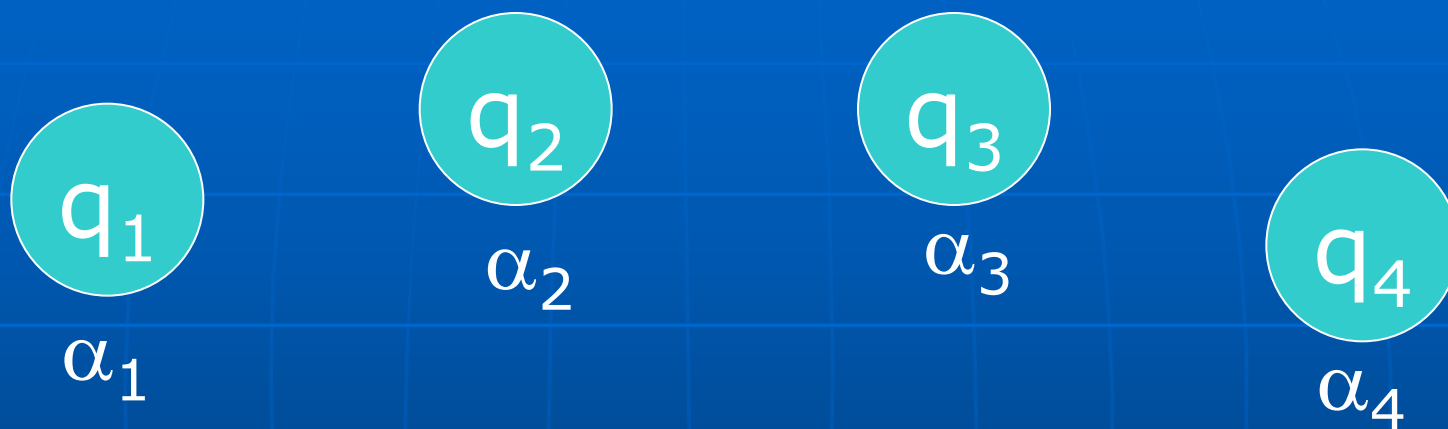
Kvantu sistēma



α_i – kompleksi skaitļi

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

Kvantu sistēma



Mērot iegūstam q_i
ar varbūtību $|\alpha_i|^2$.

Transformācijas

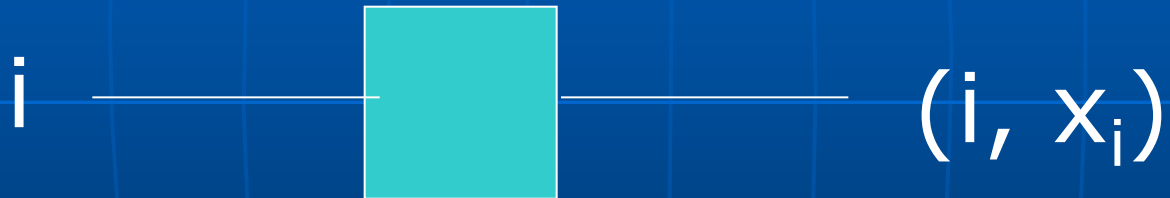


- β_i ir α_i lineāras kombinācijas.
- Ja $\sum_i |\alpha_i|^2 = 1$, tad $\sum_i |\beta_i|^2 = 1$

Perioda meklēšana

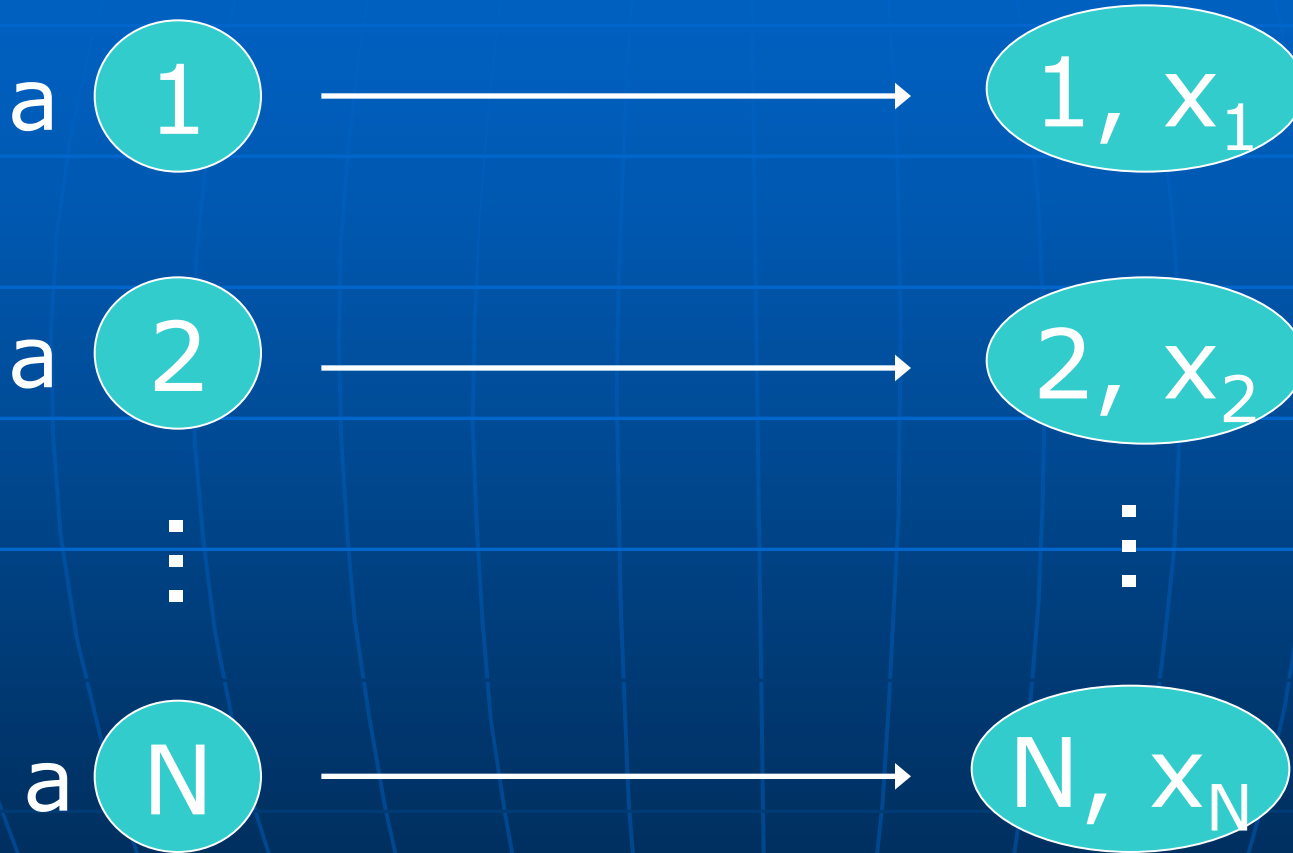
$x_0, x_1, x_2, x_3, \dots$

periodiska ar periodu r .



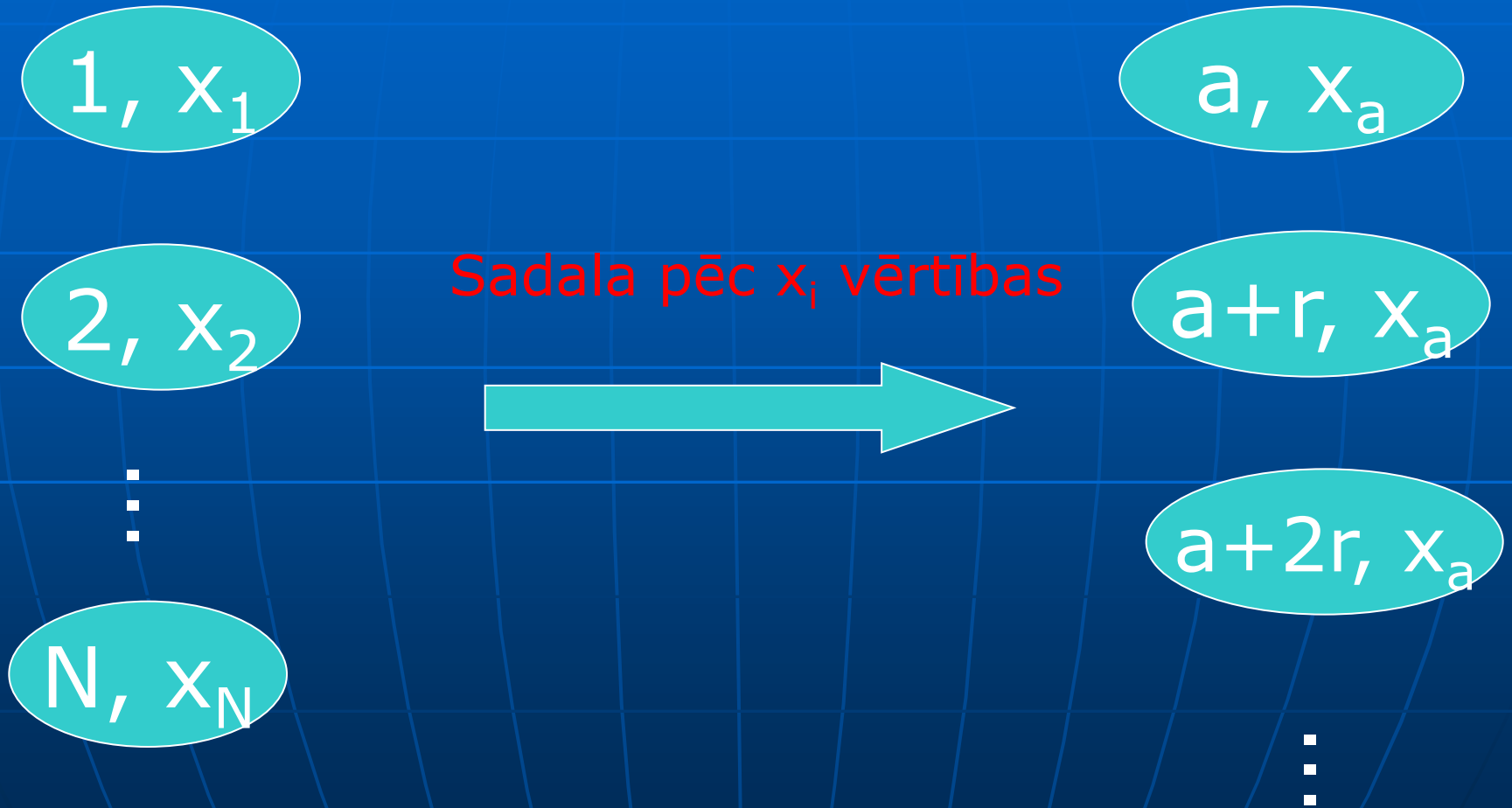
Atrast r .

Algoritms (1)



$$N \quad |a|^2 = 1$$

Algoritms (2)



Algoritms (3)

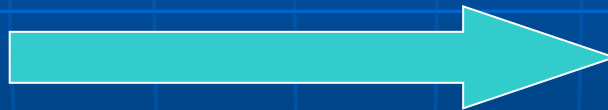
a

$a+r$

$a+2r$

$\vdots$

Kvantu Furjē
transformācija



N/r

Lietojumi

Perioda atrašana



Skaitļa sadalīšana
pirmreizinātājos



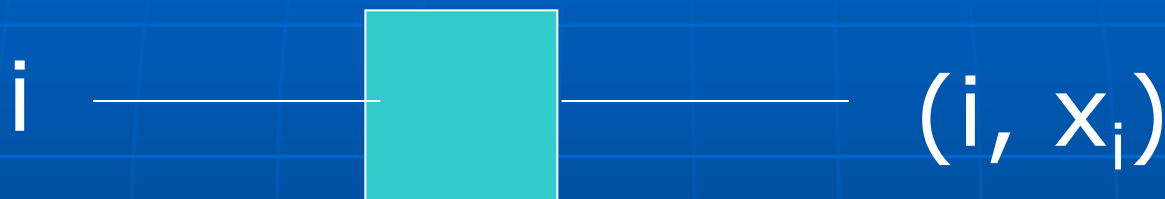
RSA kriptosistēmas
uzlaušana



[Shor, 1994]

Melnās kastes modelis

$x_1, x_2, x_3, \dots, x_N$



- Kvantiski: 1 melnās kastes izsaukums.
- Klasiski: $\Omega\left(\sqrt[4]{N}\right)$

Mūsu rezultāts

- Teorēma Ja virknes $x_1, \dots, x_N$ īpašību var noteikt kvantiski ar 1 melnās kastes lietojumu, tad to var noteikt klasiski ar $O(\sqrt{N})$ melnās kastes lietojumiem.

Hipotēze

- 2 melnās kastes izsaukumi kvantiski
 - $O(N^{2/3})$ klasiski.
- k melnās kastes izsaukumi kvantiski
 - $O(N^{k/k+1})$ klasiski.