КВАНТОВА ИНФОРМАТИКА

Николай М. Николов

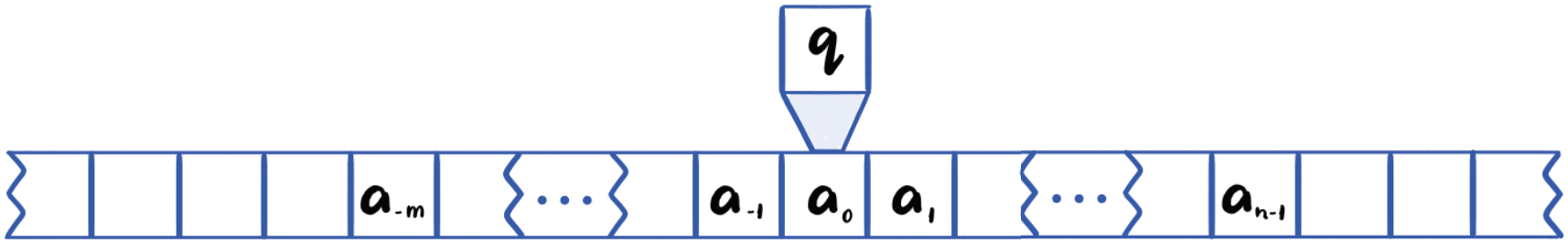
Лекция 12 / 08.01.2024, версия 0


Теоретична
квантова
физика
Експериментална
и инженерна
квантова
физика
Алгебра
Квантова
информатика
Компютърни
науки
Вероятности
и статистика
Математическа логика
и теория на алгоритмите

Понятие за алгоритъм

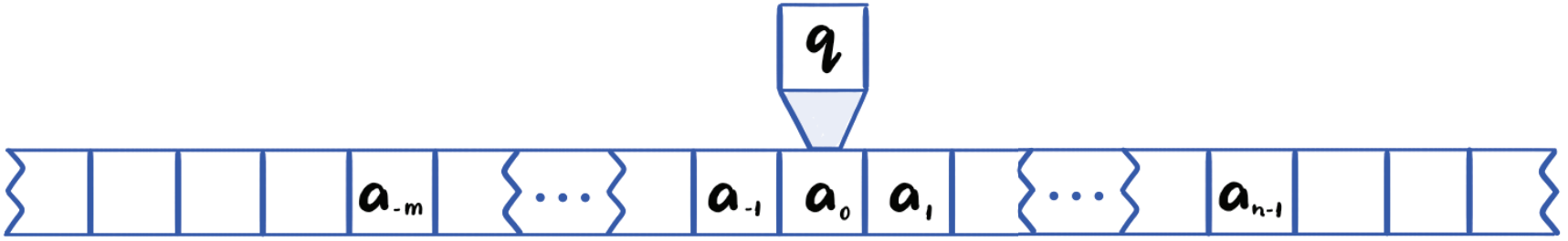
класическо	квантов аналог

Машина на Тюринг



Машина на Тюринг

- класическа, детерминистична

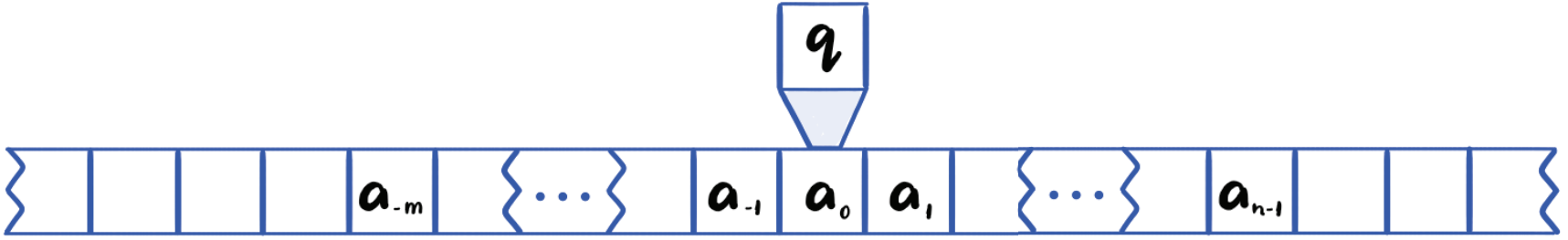


функцията на преход

$$\tau : \Sigma' \times Q \to \Sigma' \times Q \times \{\leftarrow, \downarrow, \rightarrow\}$$

Машина на Тюринг

- класическа, детерминистична



(a, q)

$\downarrow \tau$

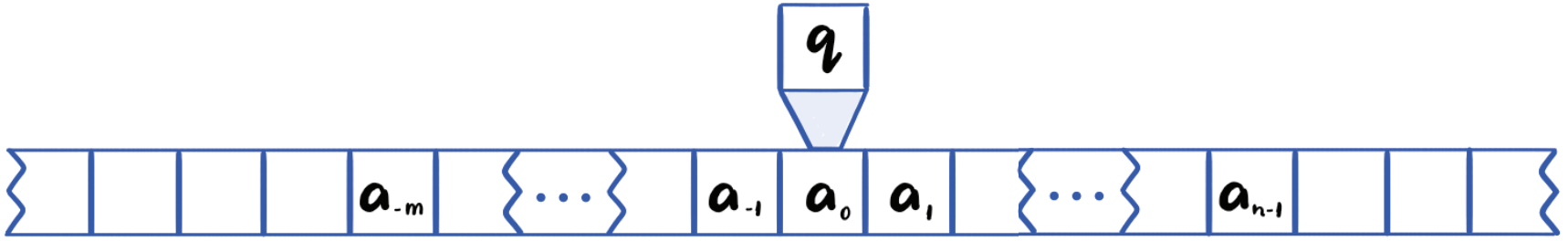
$(a', q', \leftarrow / \downarrow / \rightarrow)$

функцията на преход

$$\tau : \Sigma' \times Q \to \Sigma' \times Q \times \{\leftarrow, \downarrow, \rightarrow\}$$

Машина на Тюринг

- квантова



(a, q)

$\downarrow \tau$

амплитуда $(a', q', \leftarrow, \downarrow, \rightarrow)$

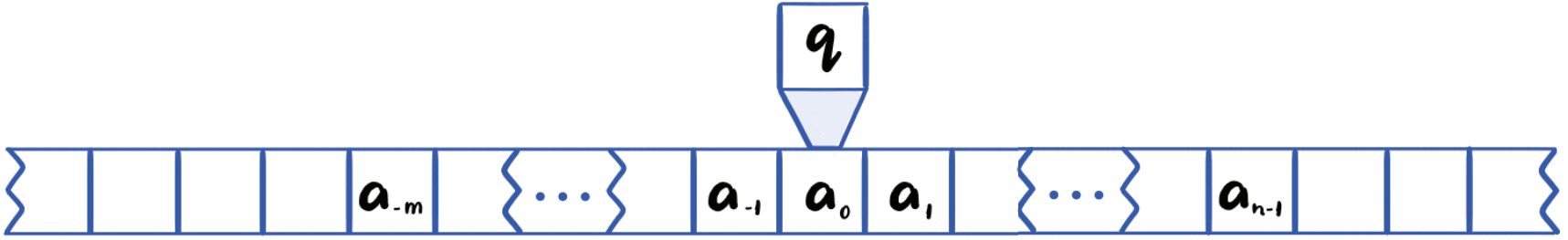
с условие: това да са координати на ортонормирана система

функцията на преход

$\tau : \Sigma' \times Q \rightarrow$ Вероятностни амплитуди над $\Sigma' \times Q \times \{\leftarrow, \downarrow, \rightarrow\}$

Машина на Тюринг

- класическа, детерминистична



(a, q)

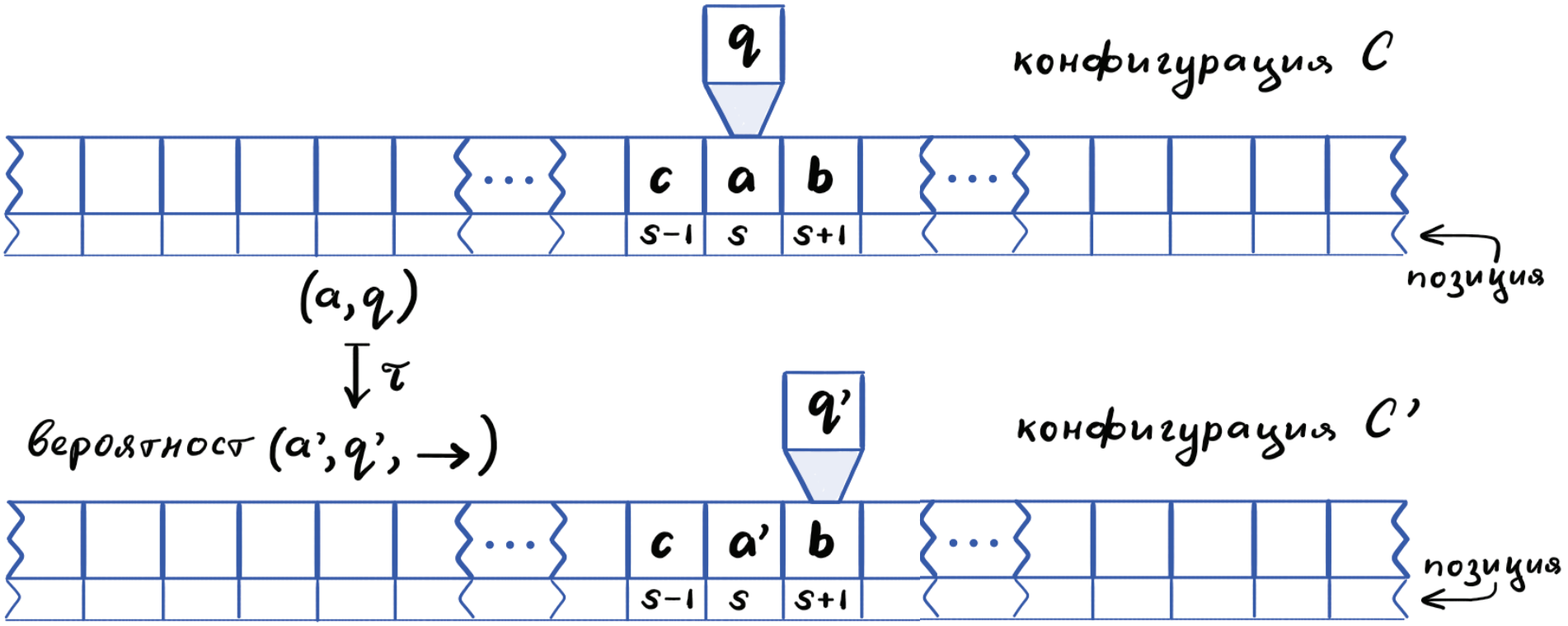
$\downarrow \tau$

$(a', q', \leftarrow / \downarrow / \rightarrow)$

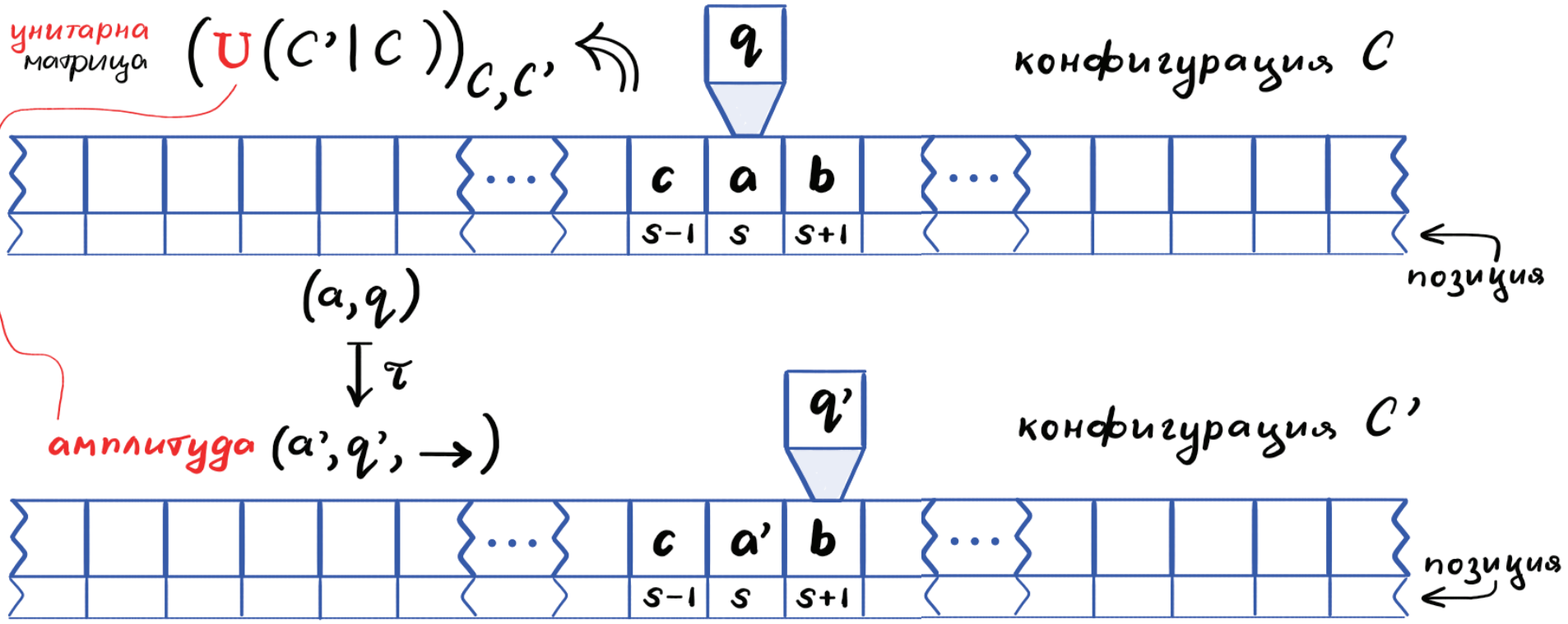
функцията на преход

$$\tau : \Sigma' \times Q \to \Sigma' \times Q \times \{\leftarrow, \downarrow, \rightarrow\}$$

Машина на Тюринг | ДИНАМИКА | - класическа, вероятностна

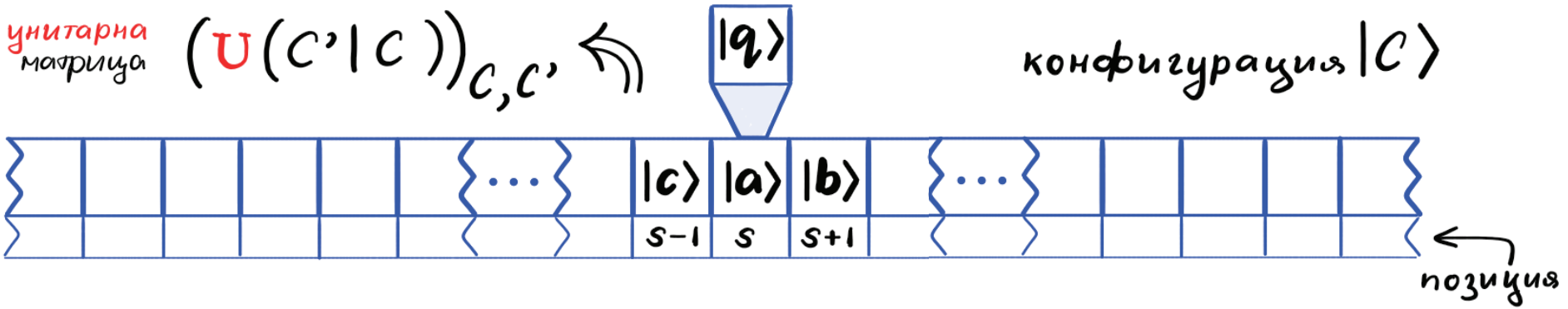


Машина на Тюринг | ДИНАМИКА | -квантова

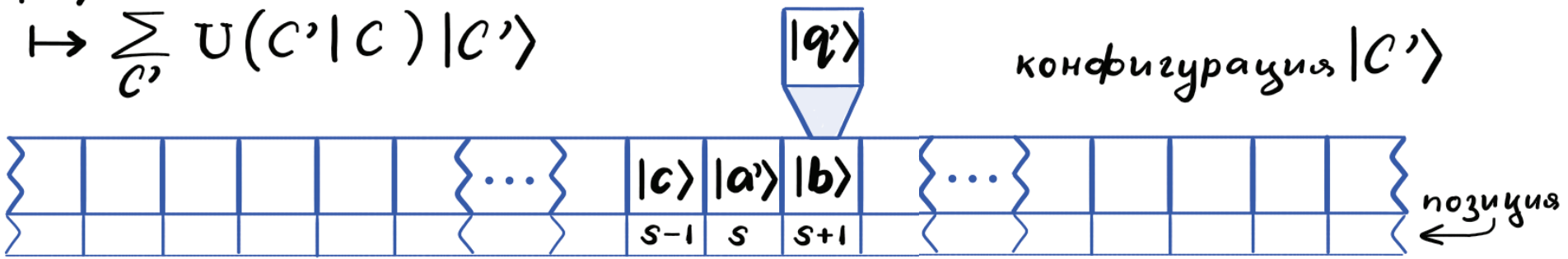


Машина на Тюринг | ДИНАМИКА | -квантова

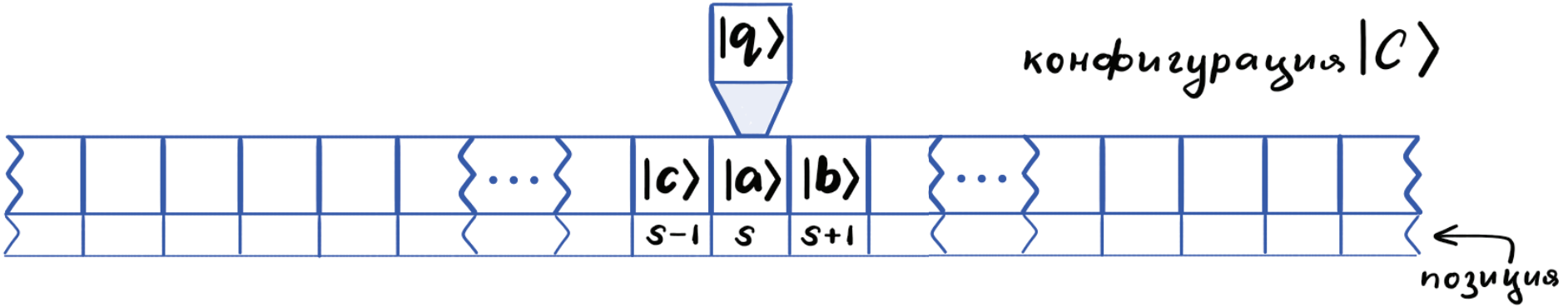
унитарна матрица $(U(C'|C))_{C,C'}$



$$|C\rangle \mapsto \sum_{C'} U(C'|C)\,|C'\rangle$$

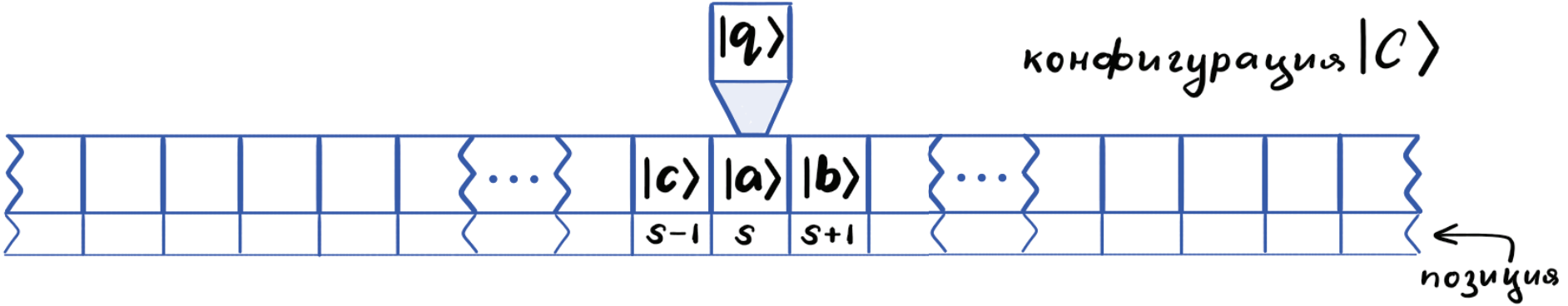


Машина на Тюринг	ДИНАМИКА	-квантова



$$|C\rangle := |q\rangle \otimes |s\rangle \otimes (\cdots \otimes |c\rangle \otimes |a\rangle \otimes |b\rangle \otimes \cdots)$$

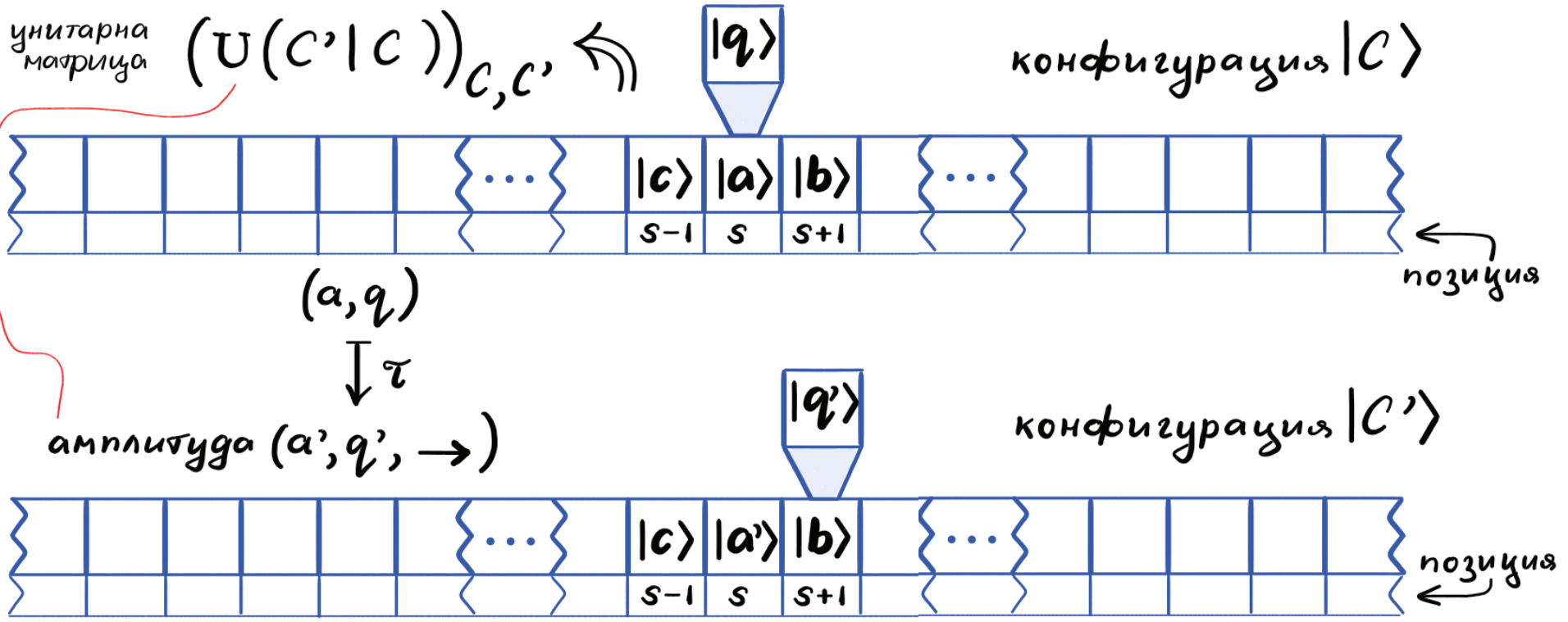
Машина на Тюринг	ДИНАМИКА	-квантова



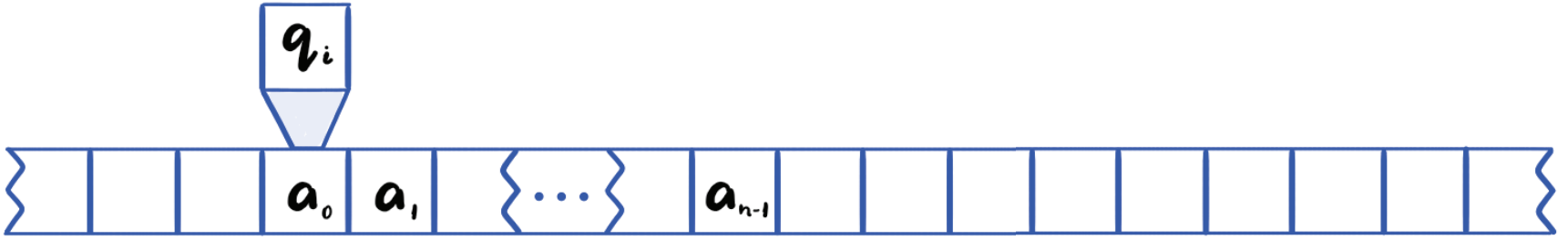
$$|C\rangle := |q\rangle \otimes |s\rangle \otimes (\cdots \otimes |c\rangle \otimes |a\rangle \otimes |b\rangle \otimes \cdots)$$

На всеки параметър в конфигурацията се съпоставя базисен вектор от изчислителния базис

Машина на Тюринг | ДИНАМИКА | -квантова

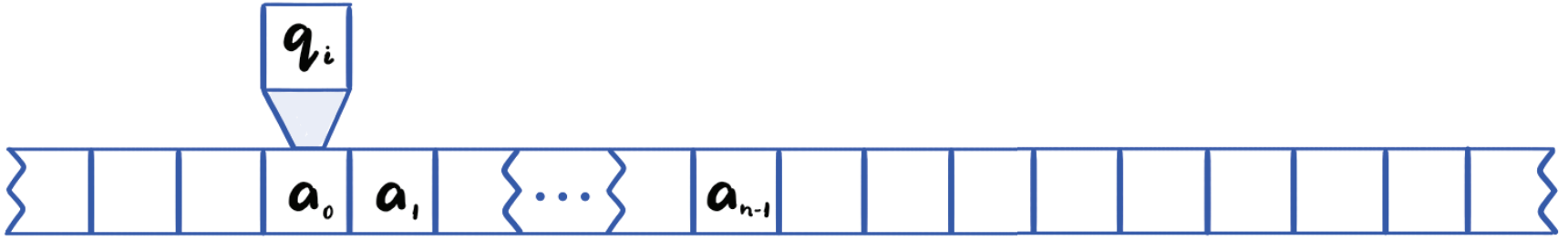


Машина на Тюринг | ИЗЧИСЛЕНИЕ | - класическа, детерминистична



i

Машина на Тюринг	ИЗЧИСЛЕНИЕ	- класическа, детерминистична

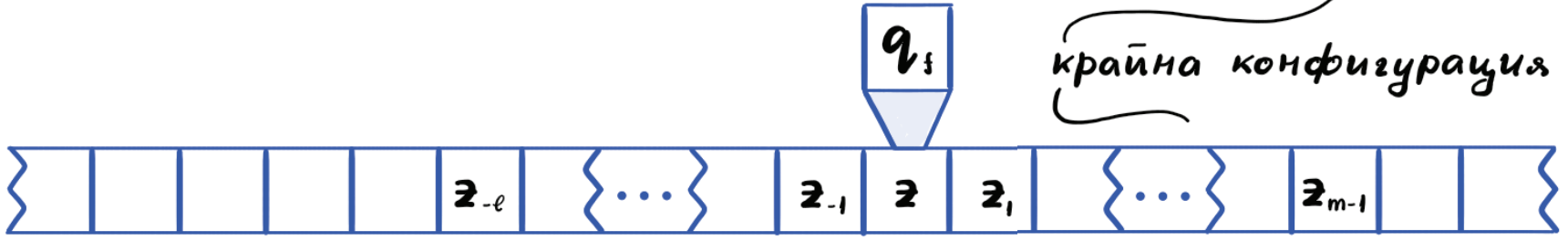


начална конфигурация

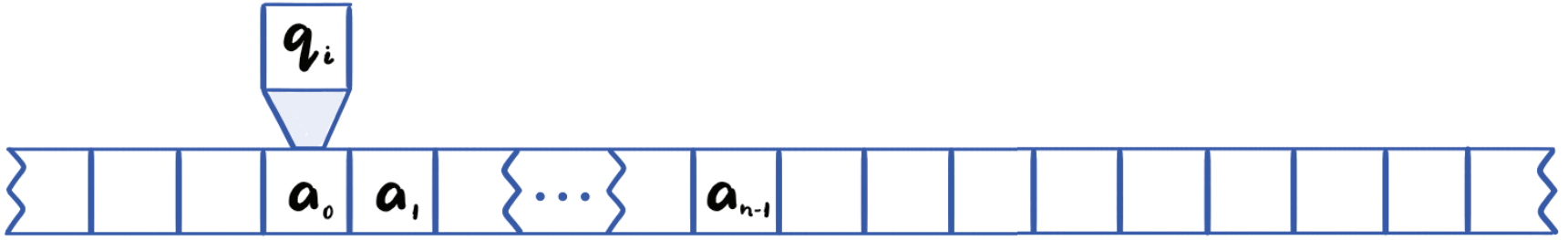
C_i

C_f

крайна конфигурация



Машина на Тюринг | ИЗЧИСЛЕНИЕ | - класическа, детерминистична



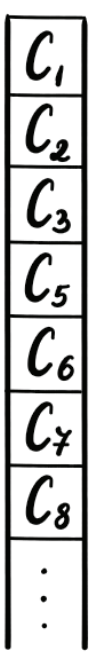
начална конфигурация

$C_i =: C_0 \rightarrow C_1 \rightarrow C_2 \rightarrow C_3 \rightarrow \cdots \rightarrow C_t := C_f$

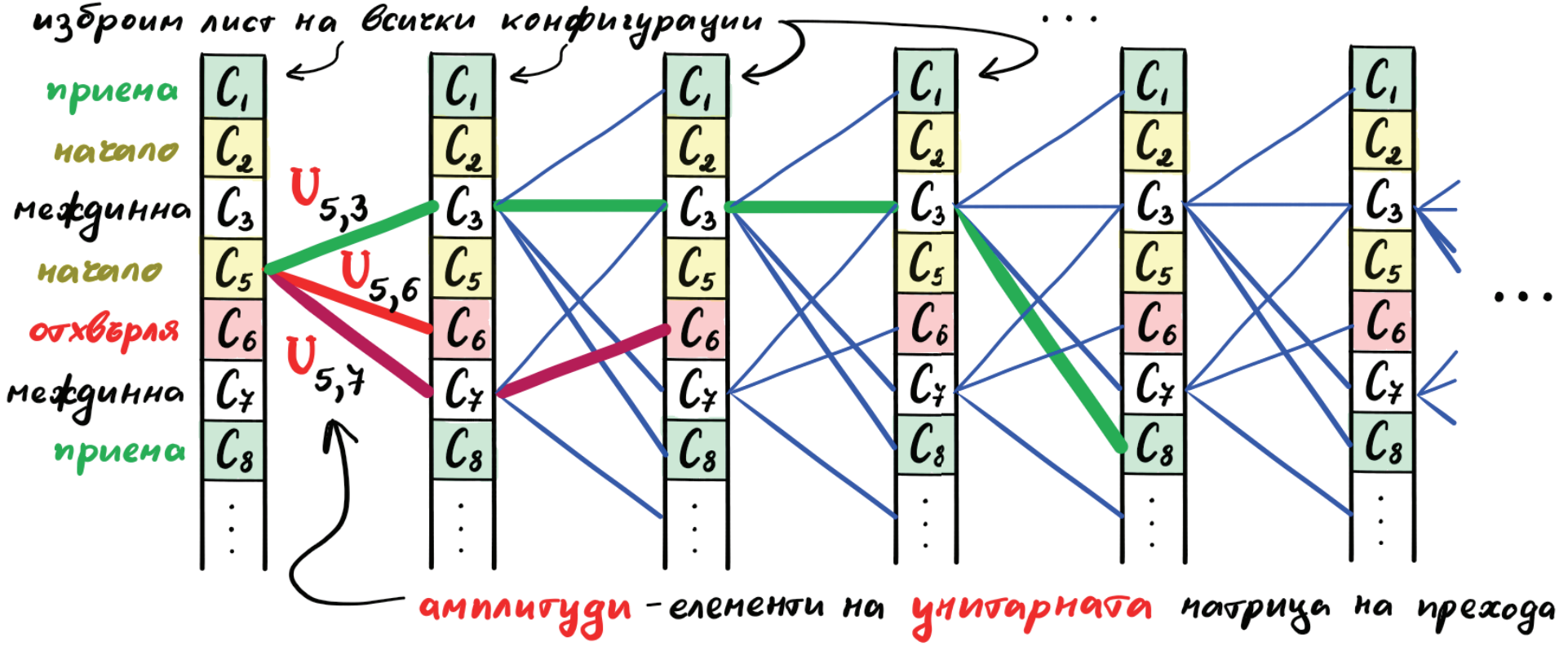
верига на изчислението

Машина на Тюринг	ИЗЧИСЛЕНИЕ	- класическа, вероятностна

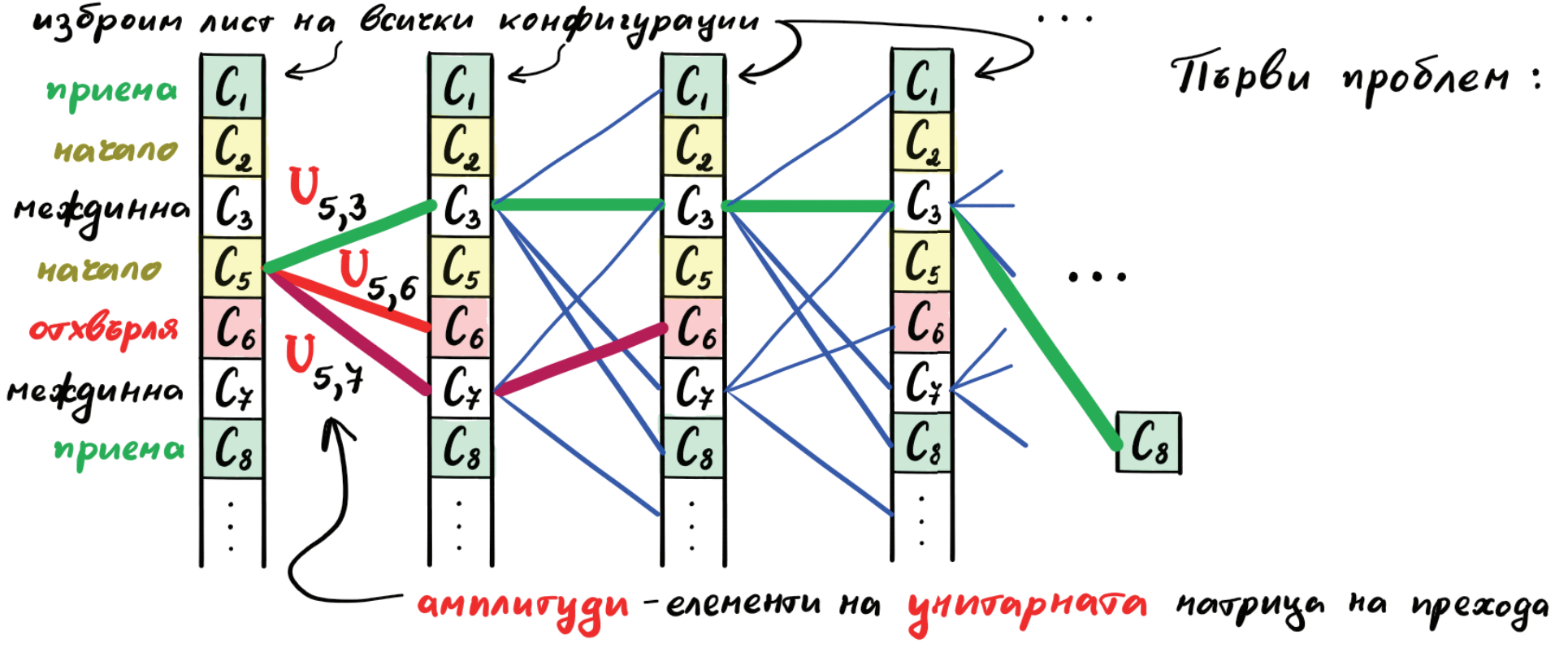
изброим лист на всички конфигурации



Машина на Тюринг | ИЗЧИСЛЕНИЕ | -квантова



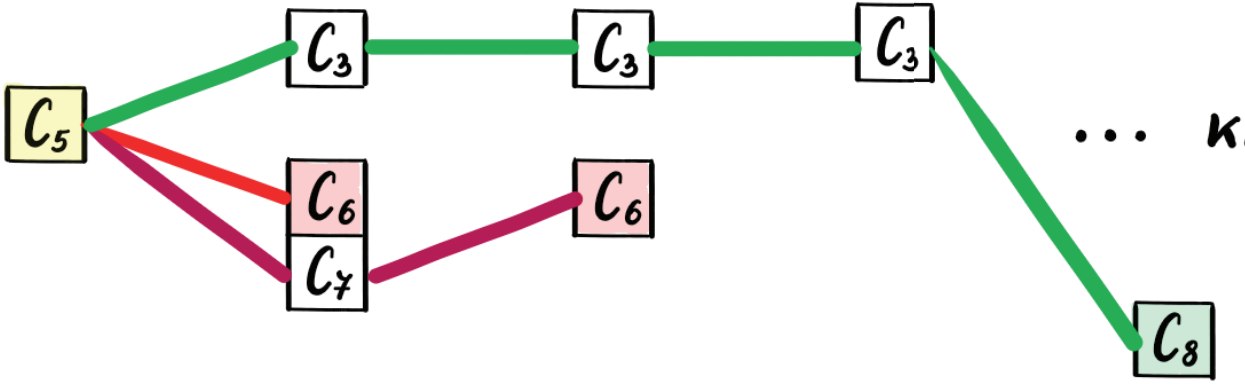
Машина на Тюринг | изчисление | -квантова



Машина на Тюринг	ИЗЧИСЛЕНИЕ	-квантова

Част от проблема идва от това, че изчислителните пътища са с различна дължина.

Първи проблем:



... как се спира?

"halting problem"

Квантовата машина на Тюринг: исторически бележки и литература

Квантовата машина на Тюринг: исторически бележки и литература

Първи работи:

[1985-D] D. Deutsch

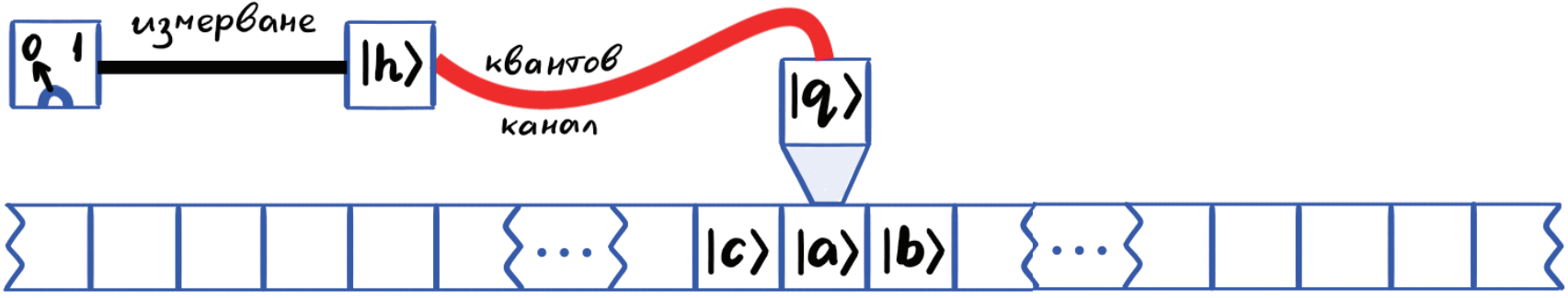
Осъзнава проблема със спирането: в края се извършва измерване, но ако резултата още не е получен, то измерването разрушава извършеното до момента изчисление.

Квантовата машина на Тюринг: исторически бележки и литература

Първи работи:

[1985-D] D. Deutsch

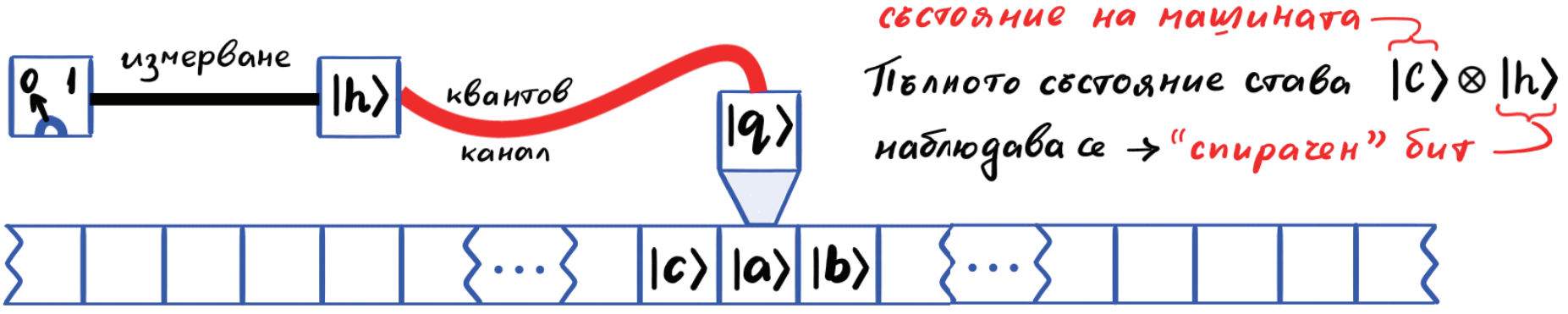
Схематично:



Квантовата машина на Тюринг: исторически бележки и литература

Първо оспорване:

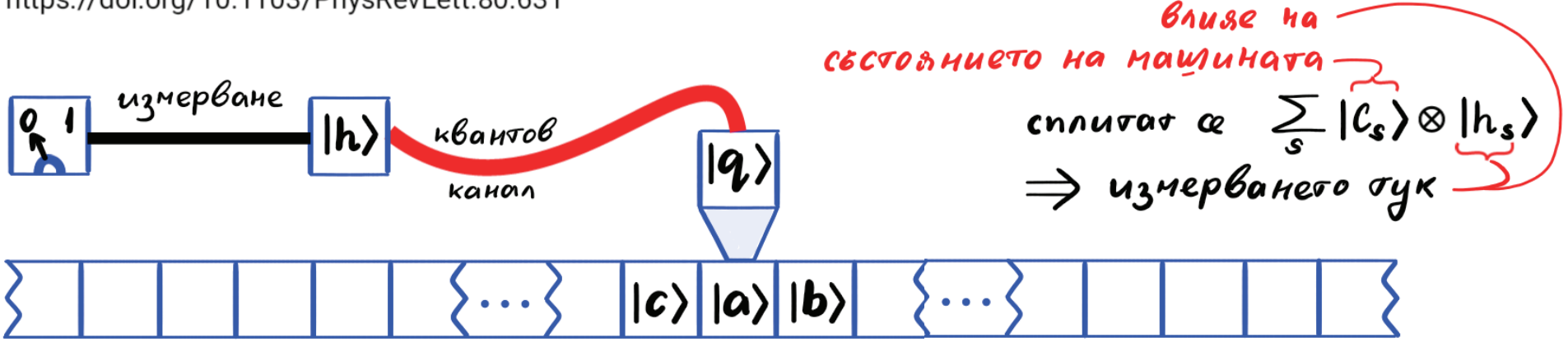
[1997-M] John M. Myers, *Can a Universal Quantum Computer Be Fully Quantum?* Phys. Rev. Lett. 78, 1823 (1997).
https://doi.org/10.1103/PhysRevLett.78.1823



Квантовата машина на Тюринг: исторически бележки и литература

Първа реабилитация:

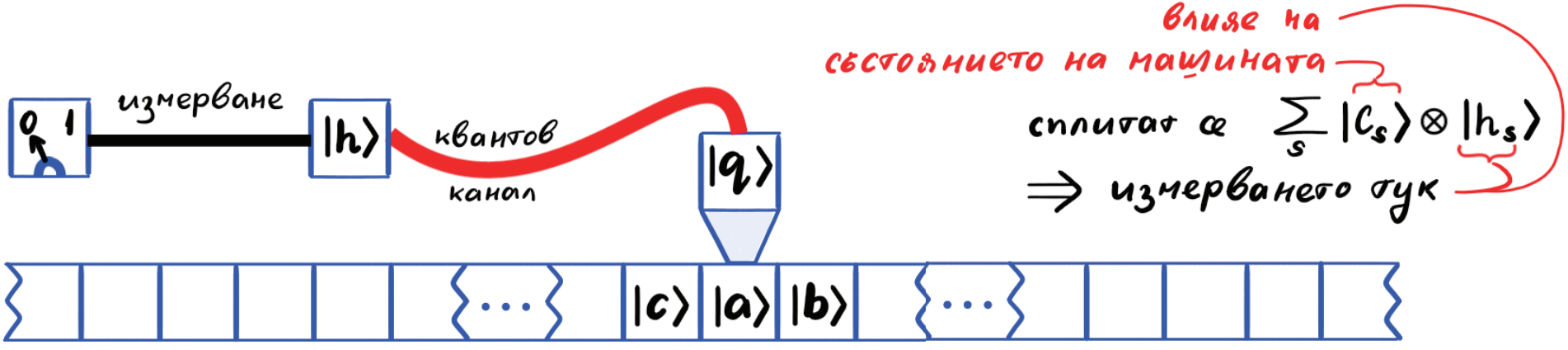
[1998-O] Masanao Ozawa, *Quantum Nondemolition Monitoring of Universal Quantum Computers,* Phys. Rev. Lett. 80, 631 (1998).
https://doi.org/10.1103/PhysRevLett.80.631



Квантовата машина на Тюринг: исторически бележки и литература

Първа реабилитация:

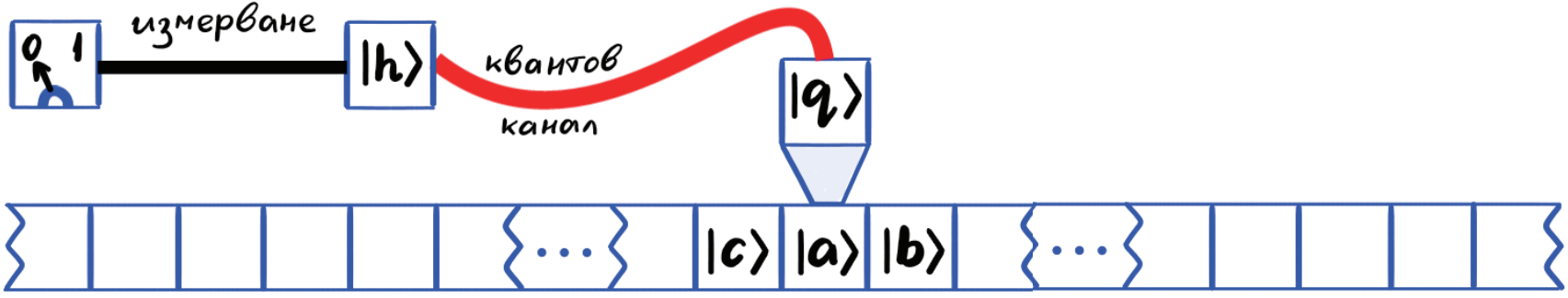
[1998-O] M. Ozawa,
Quantum Nondemolition Monitoring ...



Квантовата машина на Тюринг: исторически бележки и литература

Ново оспорване:

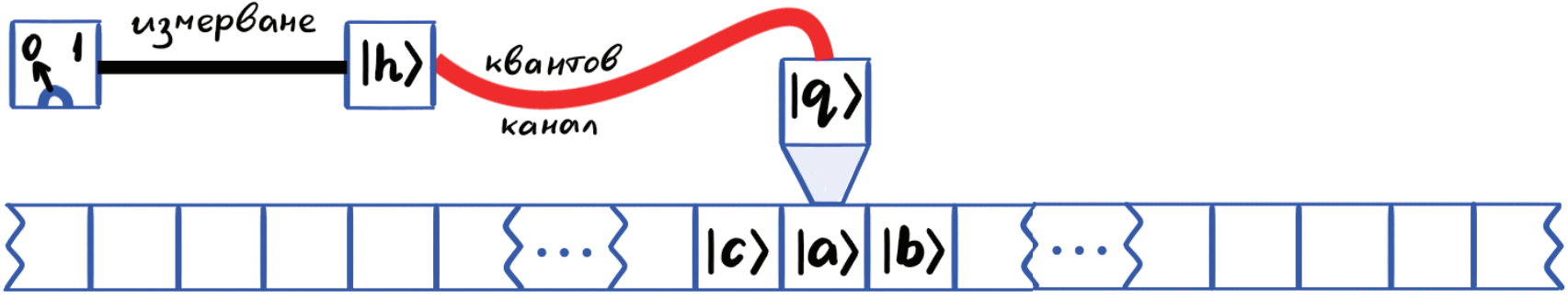
[1998-LP] Noah Linden, Sandu Popescu, *The Halting Problem for Quantum Computers,* LANL Eprint: quant-ph/9806054.
https://doi.org/10.48550/arXiv.quant-ph/9806054



Квантовата машина на Тюринг: исторически бележки и литература

Ново оспорване:

[1998-LP] N. Linden, S. Popescu



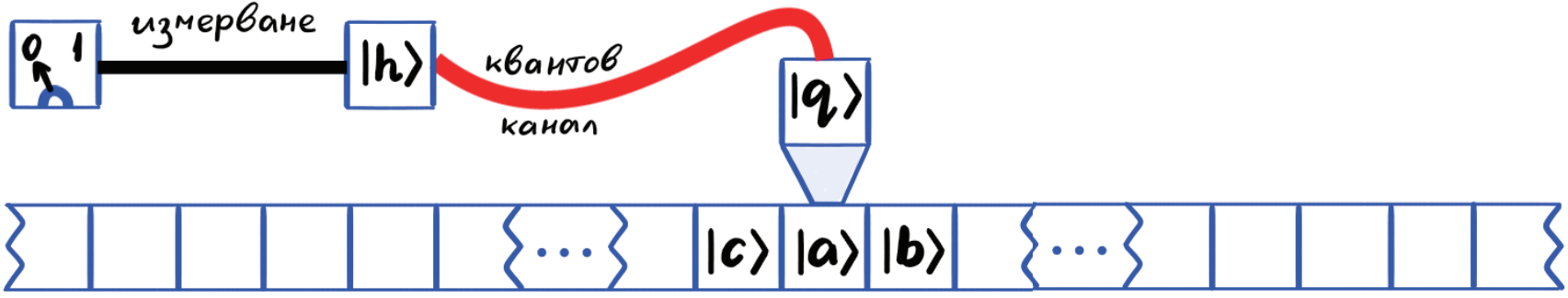
Квантовата машина на Тюринг: исторически бележки и литература

Ново оспорване:

От унитарността на динамиката ⇒ ако едно състояние се променя, то това ще продължи "вечно":

[1998-LP] N. Linden, S. Popescu

Изход: ако искаме конфигурацията C на машината да спре да се променя след като $h = 1$ и $q = q_S$



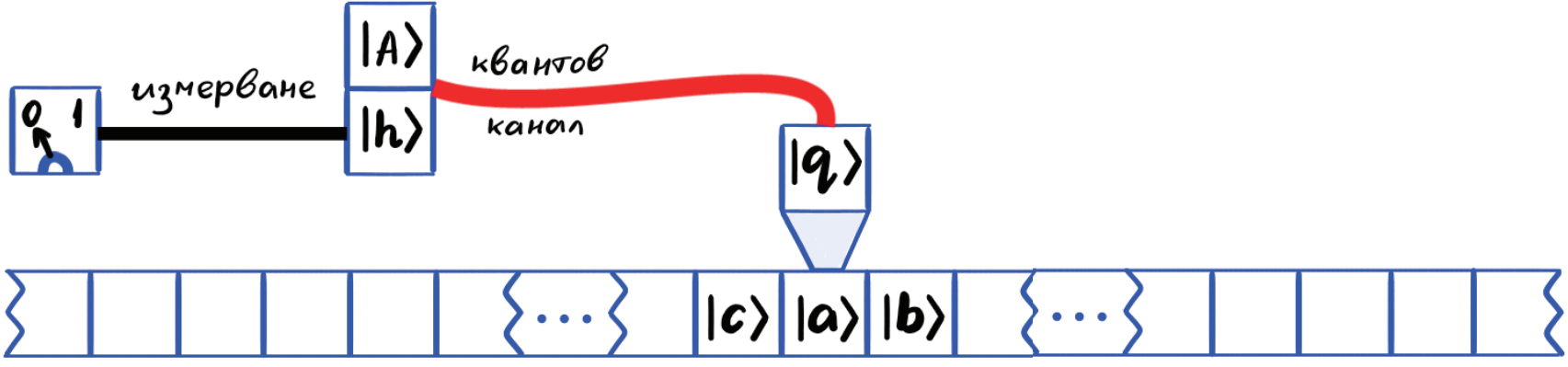
Квантовата машина на Тюринг: исторически бележки и литература

Ново оспорване:

От унитарността на динамиката ⇒ ако едно състояние се променя, то това ще продължи "вечно":

[1998-LP] N. Linden, S. Popescu

Изход: ако искаме конфигурацията C на помощни (Ancilla) регистри, които да "поемат" изменението



Квантовата машина на Тюринг: исторически бележки и литература

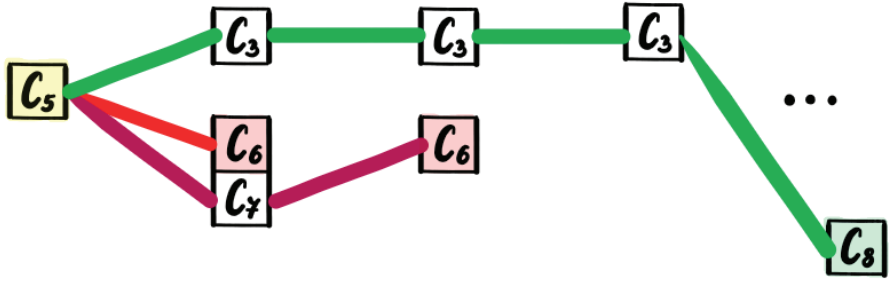
Ново оспорване:

От унитарността на динамиката ⇒ ако едно състояние се променя, то това ще продължи "вечно":

[1998-LP] N. Linden, S. Popescu

Изход: ако искаме конфигурацията C на помощни (Ancilla) регистри, които да "поемат" изменението

Виж по-горе:

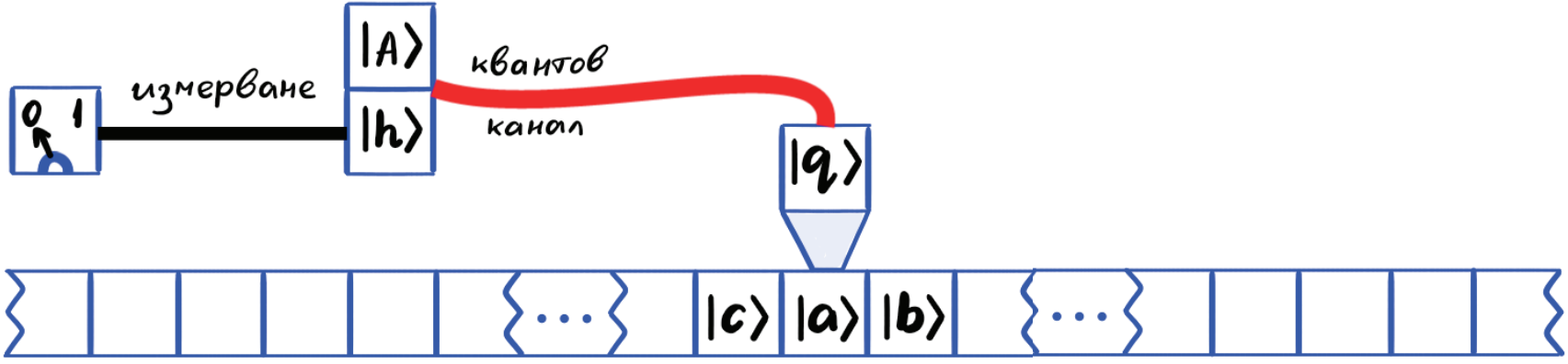


Но: We argue that the halting problem for quantum computers which was first raised by Myers, is by no means solved, as has been claimed recently. We explicitly demonstrate the difficulties that arise in a quantum computer when different branches of the computation halt at different, unknown, times.

Квантовата машина на Тюринг: исторически бележки и литература

Нова реабилитация:

[1998-2002-O] M. Ozawa



Квантовата машина на Тюринг: исторически бележки и литература

До тук разгледахме
следния цикъл:

[1985-D] Deutsch
[1997-M] Myers
[1998-O] Ozawa
[1998-LP] Linden, Popescu
[1998-2002-O] Ozawa

[1989-D] David Deutsch, *Quantum computational networks,* Proc. R. Soc. Lond. A 425, 73 (1989). https://doi.org/10.1098/rspa.1989.0099

[1997-BV] Ethan Bernstein and Umesh Vazirani, *Quantum Complexity Theory*, SIAM J. Comput. 26, 1411 (1997), https://doi.org/10.1137/S0097539796300921

[1993-Y] Andrew Yao, *Quantum circuit complexity*, in Proceedings of the 34th Annual Symposium on Foundations of Computer Science, S. Goldwasser (ed.), p.352 (1993). https://doi.org/10.1109/SFCS.1993.366852

[2002-NO] Harumichi Nishimura and Masanao Ozawa, *Computational complexity of uniform quantum circuit families and quantum Turing machines*, Theoret. Computer Sci., **276**, pp.147-181 (2002). https://doi.org/10.1016/S0304-3975(01)00111-6

[2019-MW] Abel Molina and John Watrous, *Revisiting the simulation of quantum Turing machines by quantum circuits*, Proc. R. Soc. A**475**: 20180767. http://dx.doi.org/10.1098/rspa.2018.0767

Квантовата машина на Тюринг: исторически бележки и литература

Квантовата машина на Тюринг: исторически бележки и литература

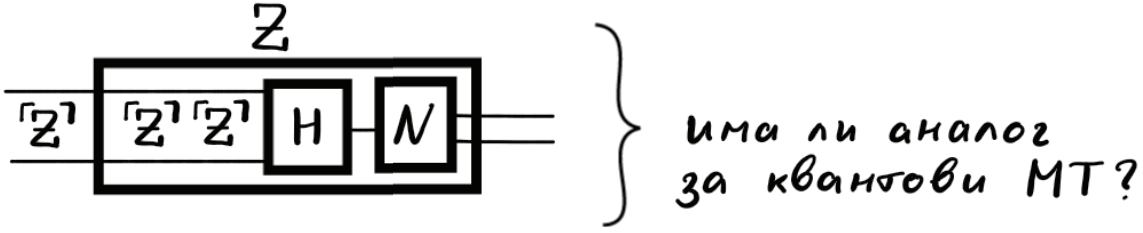
Преди да преминем по-нататък, ще се още малко на проблема за спирането в квантовите изчисления, а също и отражението на класическия проблем за спирането.

Проблемът за спирането: класически и квантов

Проблемът за спирането: класически и квантов

Да припомним класическия проблем за спиране и неговата алгоритмична нерешимост (схематично):

Проблемът за спирането: класически и квантов



Проблемът за спирането: класически и квантов

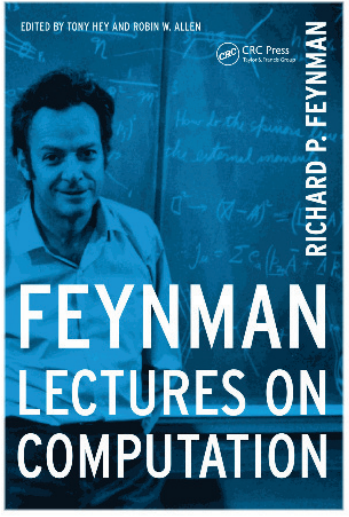
[2021-JNVWY] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen
MIP = RE*, Communications of the ACM, Volume 64 Issue 11pp 131–138 (2021).
https://doi.org/10.1145/3485628

още една перспектива за квантови физични "оракули".

Изчислителен модел на логическите вериги / схеми (circuits) { класически / и квантов

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Източник на фигурите:

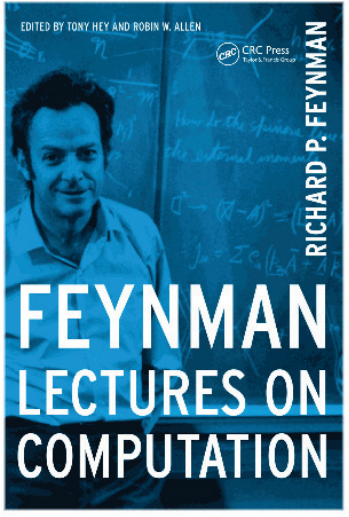


Издания:
1996 - 2018

Някои означения от курсовете по "цифрова електроника" ("digital electronics")

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Източник на фигурите:



Издания:
1996 - 2018

Някои означения от курсовете по "цифрова електроника" ("digital electronics")

изключващо или = събиране mod 2 (=: ⊕)

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

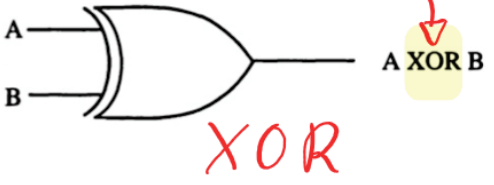
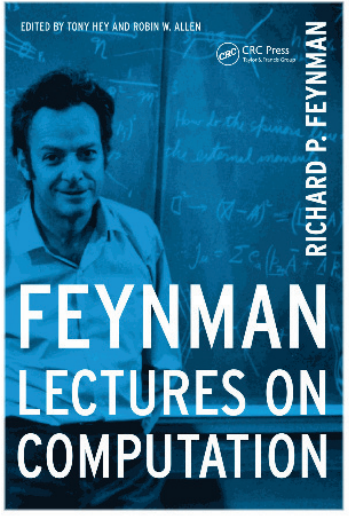


Fig. 2.4 The XOR Gate

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

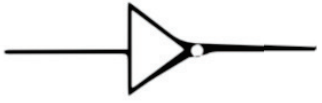
Източник на фигурите:



Издания:
1996 - 2018

Някои означения от курсовете по "цифрова електроника" ("digital electronics")

A	NOT A
0	1
1	0



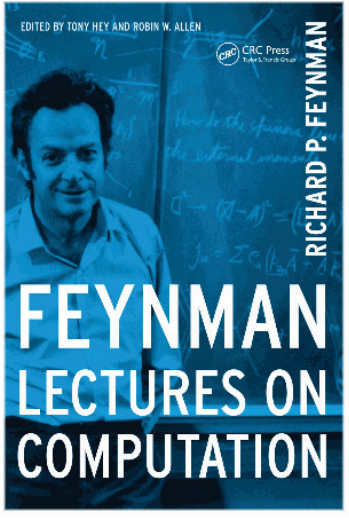
NOT

Fig. 2.7 The NOT Gate

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Физическа (инженерна) реализация:

Източник на фигурите:



Издания:
1996 - 2018

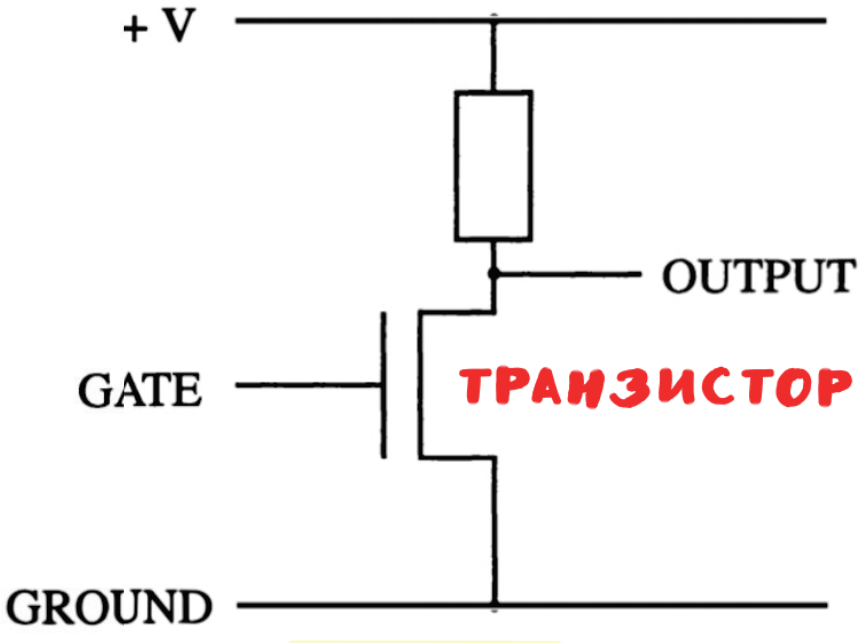


Fig. 2.12 The Transistor Inverter, or NOT Gate

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

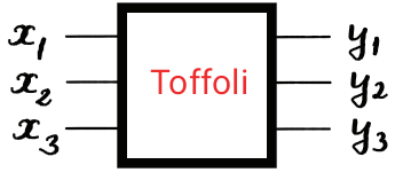
Обратимостта (и борбата с глобалното затопляне)

Изчислителен модел на логическите вериги / схеми (circuits) { класически / и квантов

Обратимостта (и борбата с глобалното затопляне): целим да използваме само обратими логически вериги, в които се използват само обратими гейтове.

↳ Обратими изчисления (Reversible computing)

Пример за обратим гейт – гейт на Тофоли / Toffoli



вз. еднозн. и обр.

$$\begin{aligned} y_1 &= x_1 + x_2 x_3 \pmod 2 \\ y_2 &= x_2 \\ y_3 &= x_3 \end{aligned}$$

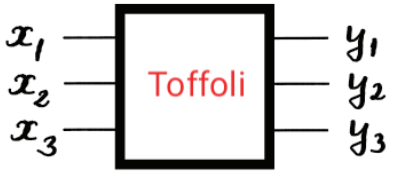
← остатъци при делене на 2

$$\begin{aligned} x_1 &= y_1 + y_2 y_3 \pmod 2 \\ x_2 &= y_2 \\ x_3 &= y_3 \end{aligned}$$

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Обратимост

Гейт на Тофоли / Toffoli



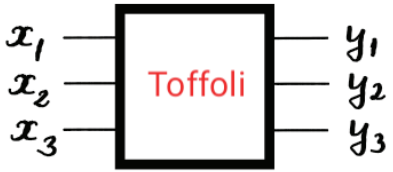
$$y_1 = x_1 + x_2 x_3 \pmod 2$$
$$y_2 = x_2$$
$$y_3 = x_3$$

↳ вз. еднозн. и обр. $(\mathbb{Z}/2\mathbb{Z})^{\times 3}$ ↺ $\{0,1\}$

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Обратимостта

Гейт на Тофоли / Toffoli



$$y_1 = x_1 + x_2 x_3 \pmod 2$$
$$y_2 = x_2$$
$$y_3 = x_3$$

↳ вз. еднозн. и обр. $(\mathbb{Z}/2\mathbb{Z})^{\times 3}$ $\{0,1\}$

Теорема на Тофоли

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Обратими изчисления (Revesible computing) : литература

https://en.wikipedia.org/wiki/Reversible_computing

[2017-Mo] *Theory of reversible computing*, by Juraj Morita

[2010-dV] *Reversible Computing Fundamentals, Quantum Computing,and Applications*, by Alexis De Vos

[20..-2023-Pr] *Reversible Computation* (RC) International Conference

12th: RC 2020, Oslo, Norway, July 9-10
11th: RC 2019, Lausanne, Switzerland, June 24–25
10th: RC 2018, Leicester, UK, September 12-14
9th: International Conference, RC 2017, Kolkata, India, July 6-7
8th: RC 2016, Bologna, Italy, July 7-8
7th: RC 2015, Grenoble, France, July 16-17
6th: RC 2014, Kyoto, Japan, July 10-11
5th: RC 2013, Victoria, BC, Canada, July 4-5
4th: RC 2012, Copenhagen, Denmark, July 2-3
3d: RC 2011, Gent, Belgium, July 4-5

2023-LPU] *An Axiomatic Theory for Reversible Computation*, by Ivan Lanese, Iain Phillips, Irek Ulidowski, arXiv:2307.13360 (cs)

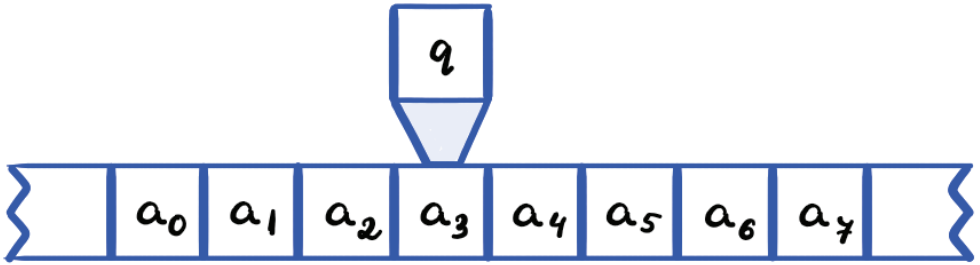
Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

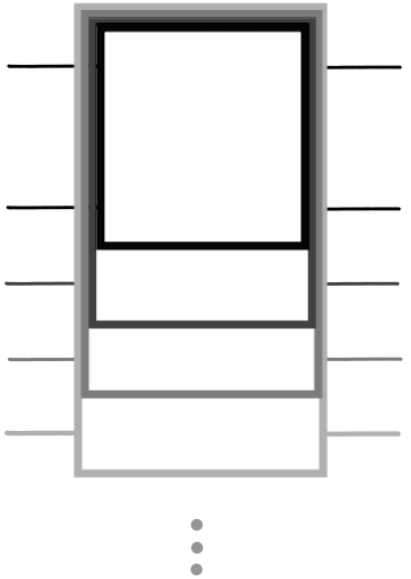
Равномерни фамили от схеми (Uniform Circuit Families)

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

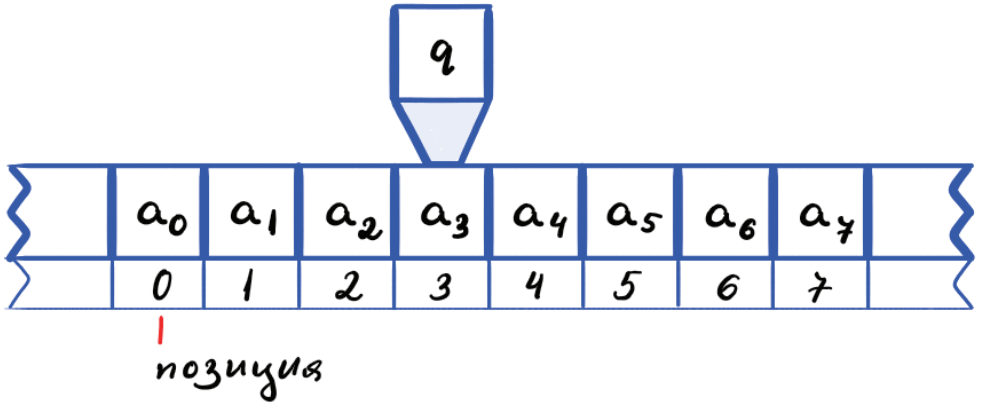
Равномерни фамили от схеми (Uniform Circuit Families)

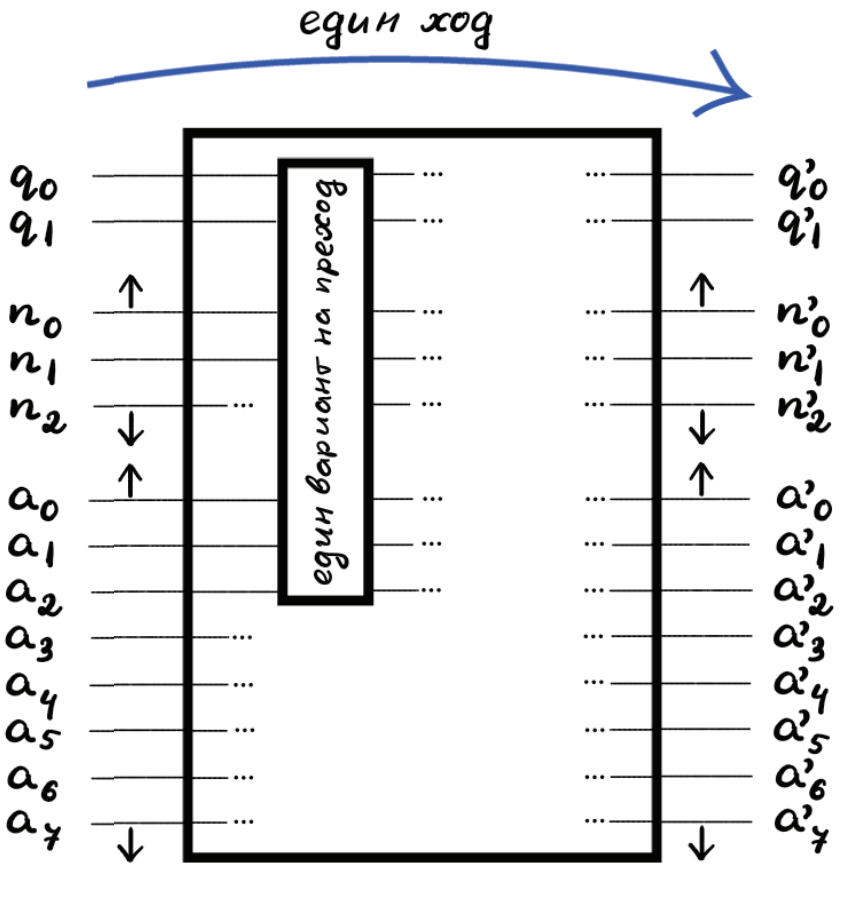
Машини на Тюринг



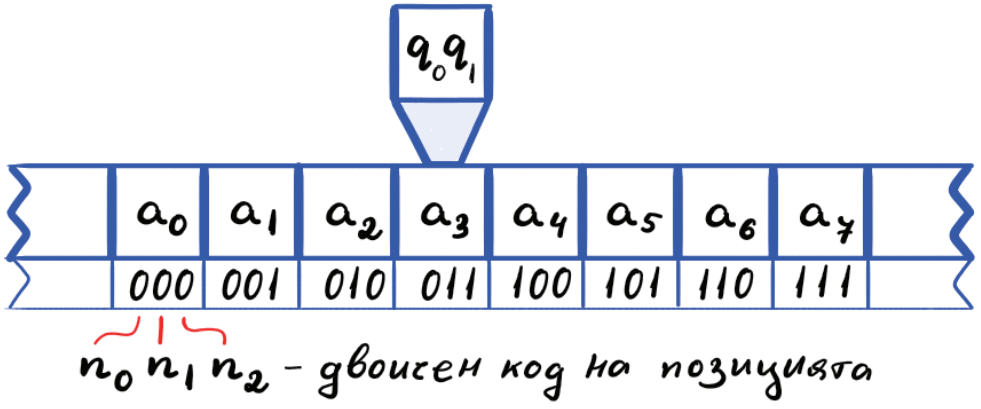


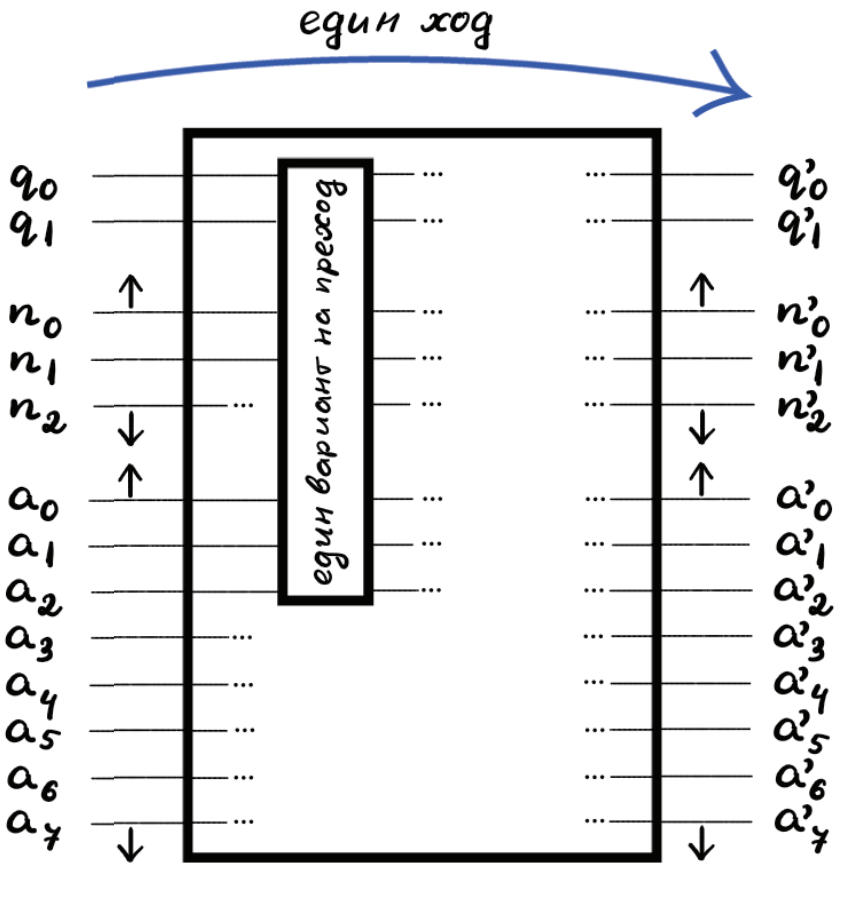
Един път за построяване на съответствие машина на Тюринг → булева верига:





Един път за построяване на съответствие машина на Тюринг → булева верига:





Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Равномерни фамили от схеми (Uniform Circuit Families)

⇕ Установено е и в квантовия случай

Машини на Тюринг

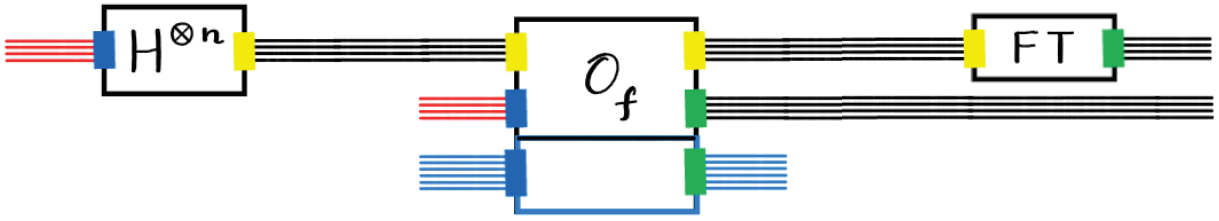
Литература (от по-горе):

...

2019-MW] Abel Molina and John Watrous, *Revisiting the simulation of quantum Turing machines by quantum circuits*, Proc. R. Soc. A**475**: 20180767. http://dx.doi.org/10.1098/rspa.2018.0767

Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

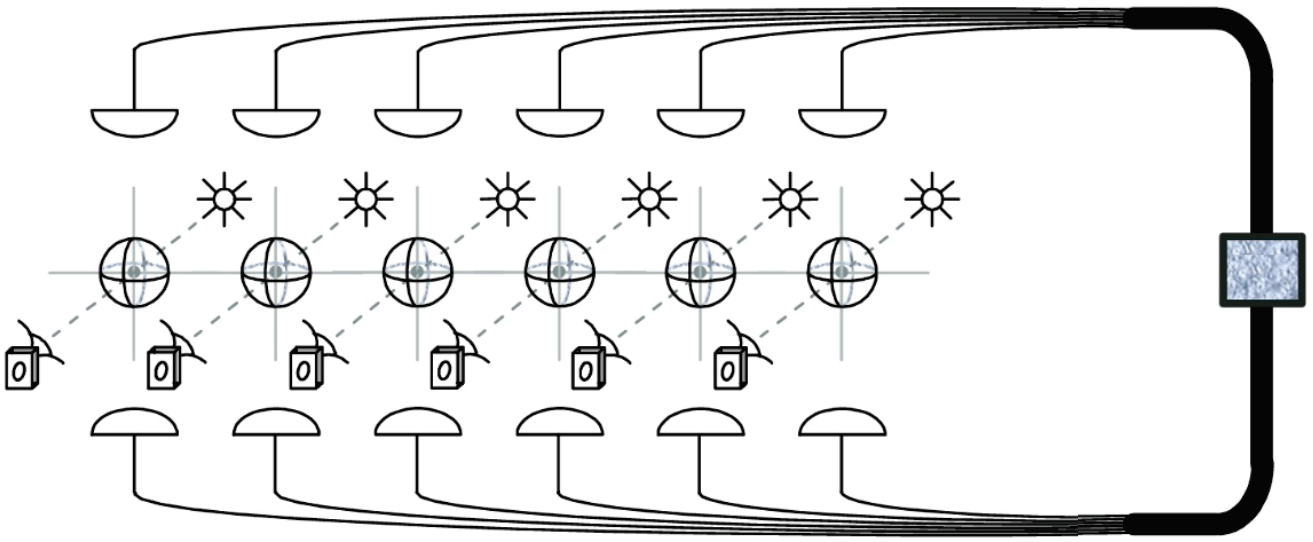
В миналата лекция изследвахме следния пример на квантова схема:



Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Примерно изпълнение на квантов алгоритъм по квантова схема:

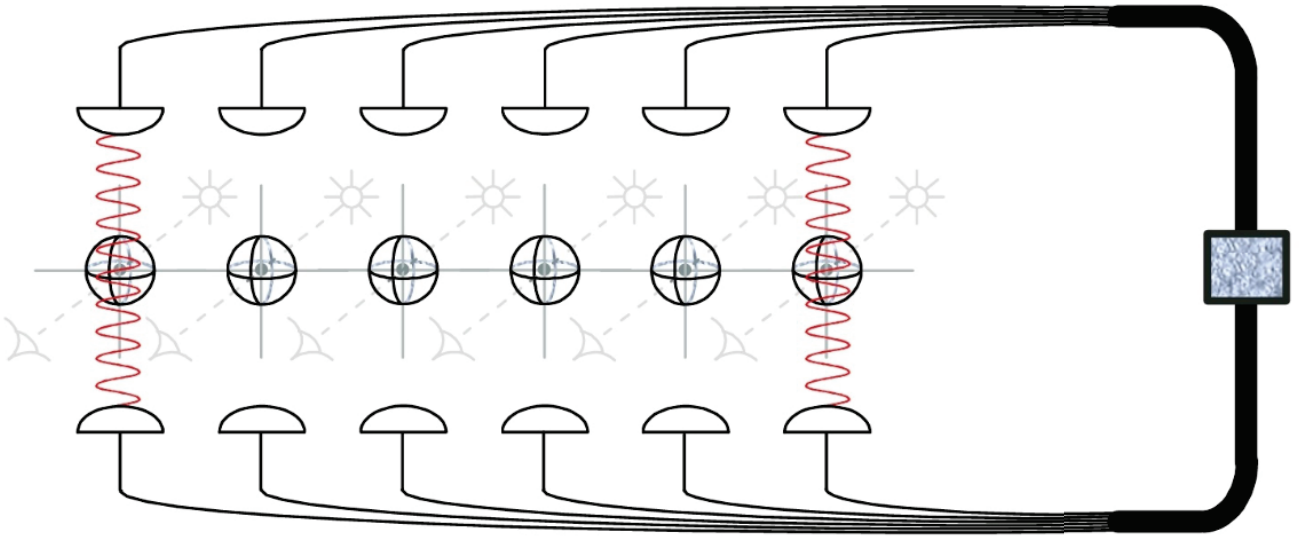
1) Инициализация



Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Примерно изпълнение на квантов алгоритъм по квантова схема:

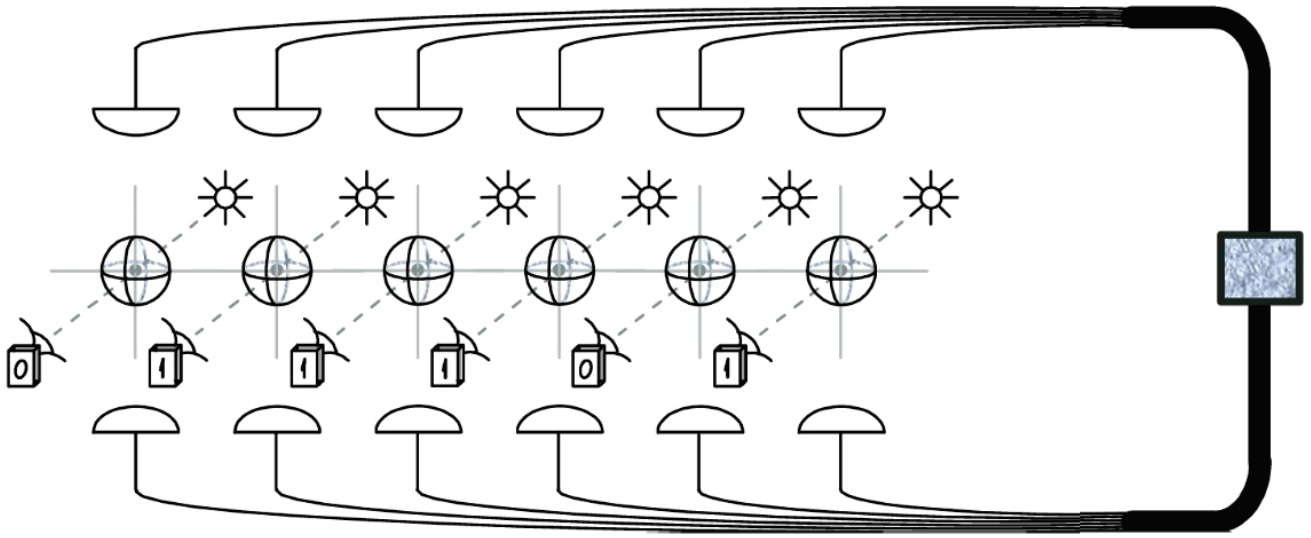
2) Квантово изчисление



Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

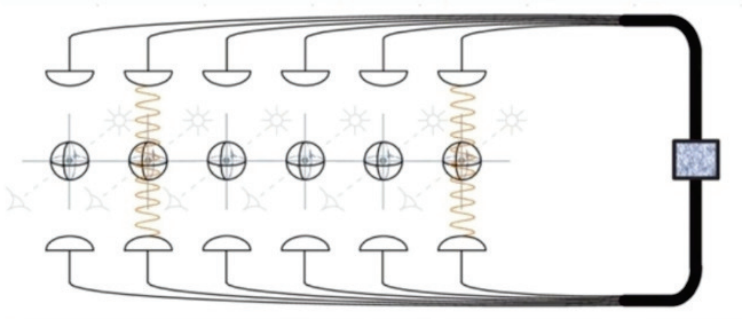
Примерно изпълнение на квантов алгоритъм по квантова схема:

3) Измерване на резултата



Изчислителен модел на логическите вериги / схеми (circuits) { класически и квантов

Примерно изпълнение на квантов алгоритъм по квантова схема:



Градивните квантови трансформации, които задават елементарните стъпки, се наричат "квантови операции" (quantum gates).

Тяхната последователност образува "квантова верига" (quantum circuit).