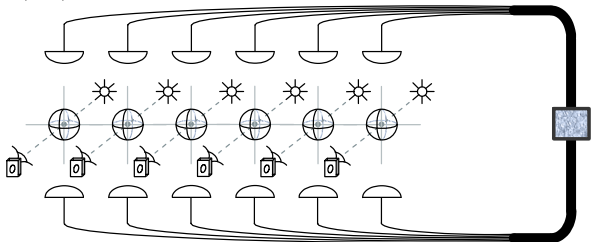


10 Квантови изчисления и квантови вериги. Дискретната Фурие трансформация. Начално понятие за квантов алгоритъм

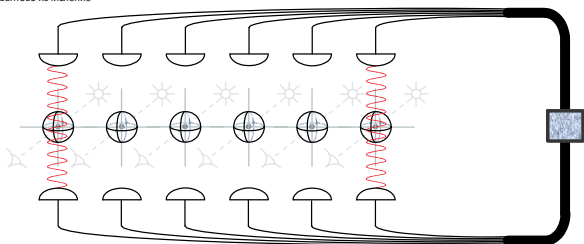
10.1 Квантови изчисления: начална постановка

Ще започнем с една схематична илюстрация на квантовите компютри дадена на фигурата по-долу. Тя изобразява един от основните модели на квантови изчисления: **квантовите вериги**, с който ще се запознаем в тази лекция.

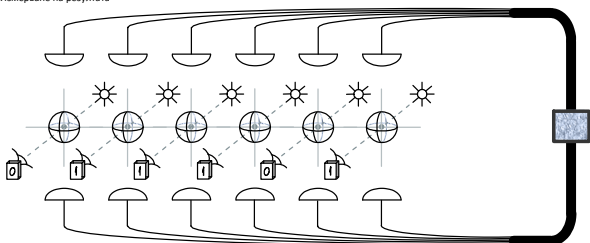
1) Инициализация



2) Квантово изчисление



3) Измерване на резултата



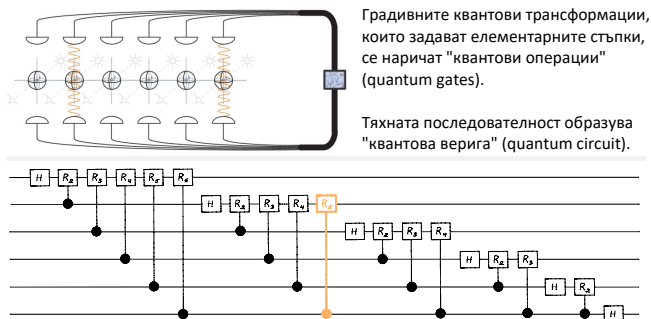
фиг. 64: Една опростена схема на действие на квантов компютър

Съгласно този модел на квантови изчисления, информацията е вложена и се обработва върху система от краен брой квантови битове. Една такава илюстрация вече разгледахме в лекцията за съставни системи. Тук ние сме “надградили” квантовите битове с допълнителни полета изобразени по вертикалните оси, които влияят върху състоянието на всеки квантов бит. Тези “вертикални” полета се коман-

дват от един център, който всъщност изпълнява квантовата програма. Преди това обаче, системата се **инициализира**, т.е., състоянията на квантовите битове, които също ще наричаме “квантови регистри” се привежда в някакво начално изчислително състояние. Това става, чрез хоризонтално изобразеното въздействие и измерване, което в края се използва и за разчитан на крайния резултат. В тази връзка нека си припомним от предната лекция, че измерването и регистрирането на елементарно събитие води до преход в чистото състояние, което съответства на това събитие и това може да се използва за формиране на чисти състояния, подобно на филтрация. След първата стъпка, инициализацията, следва самото изпълнение на квантовия алгоритъм, което се изразява в поредица от въздействия върху кубитите, изобразени по вертикалните оси. Накрая е третата стъпка, разчитането на резултата, чрез измерването на крайното състояние на кубитите.

Достигахме до важното понятие за **квантова верига**, което е поредицата от квантови гейтове изпълнявани в хода на квантовото

изчисление. Една такава квантова верига е изобразена на следната фигура:



фиг. 65: Моделът на квантовите вериги за квантовите изчисления

Тя изобразява т.нар. дискретна Фурие трансформация, с която подробно ще се запознаем след малко в тази лекция.

10.2 Система от няколко кубита: изчислителен базис

Припомняме – имаме две употреби на бра-кет означенията:

- За $\Psi = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_N \end{pmatrix} \in \mathbb{C}^N$ – вектор–стълб

пишем $|\Psi\rangle := \Psi$, като едноместна линейна операция върху $\mathbb{C}^n$, която е идентитета. Така, $|\alpha\Psi + \alpha'\Psi'\rangle = \alpha|\Psi\rangle + \alpha'|\Psi'\rangle$ и в частност, $|0\rangle \equiv 0$.

- Втората употреба на бра-кет означенията е за орто-нормиран базис $e_0, \dots, e_{N-1} \in \mathbb{C}^N$, когато означаваме

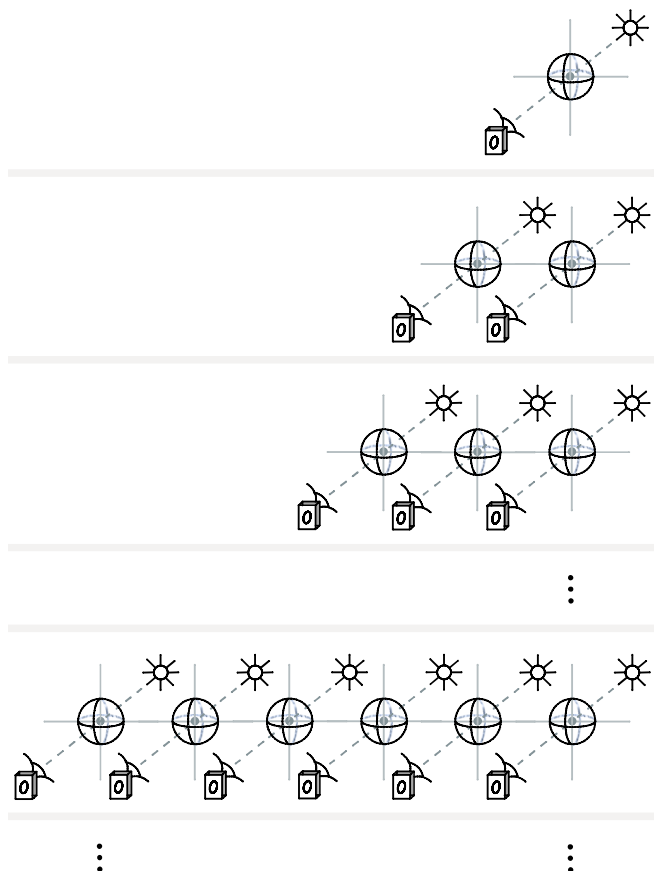
$$e_k \equiv |e_k\rangle =: |k\rangle ,$$

като така, вътре в скобите $|\dots\rangle$ стои не самия базисен вектор, а информацията за него, например, индекса му. Сега обаче имаме

$$|0\rangle \equiv e_0 \neq 0 ,$$

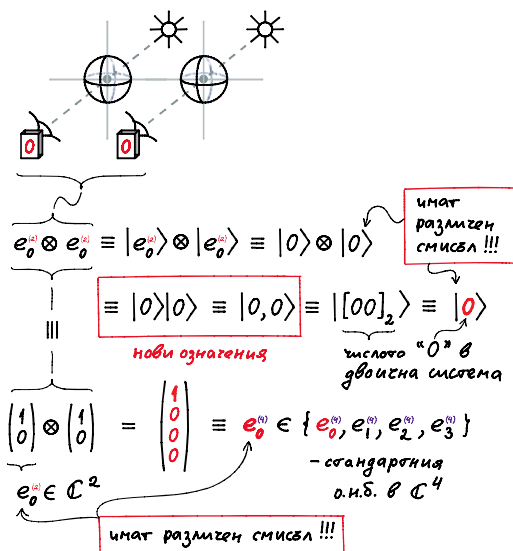
т.е., $|0\rangle$ не е нулевия вектор на $\mathbb{C}^N$ (!!!).

Преминаваме към описанието и построението на изчислителния базис в хода на надграждането на системата от кубити, както е изобразено на долната фигура:

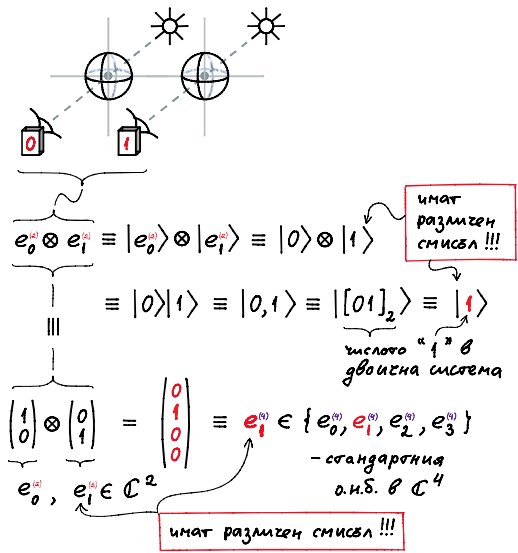


фиг. 66: Надграждане на броя на квантовите битове

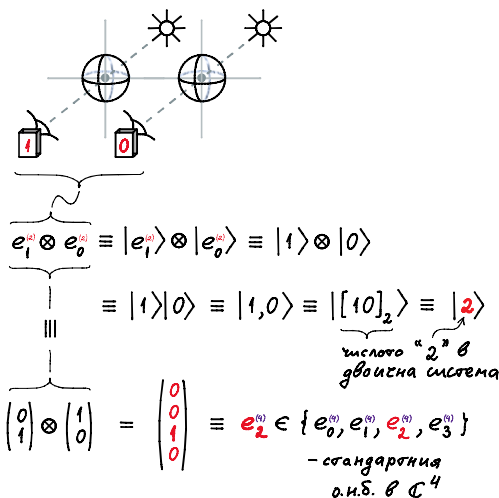
На следващите фигури е разгледан случая на дву-кубитна система:



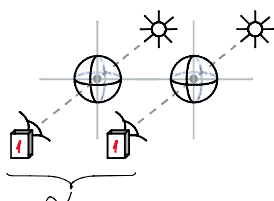
фиг. 67: Система от два кубита в изчислителен базис:
случай "00"



фиг. 68: Система от два кубита в изчислителен базис: случай “01”



фиг. 69: Система от два кубита в изчислителен базис:
случай "10"



$$\begin{aligned}
 \underbrace{e_i^{(z)} \otimes e_i^{(z)}} &\equiv |e_i^{(z)}\rangle \otimes |e_i^{(z)}\rangle \equiv |1\rangle \otimes |1\rangle \\
 &\equiv |1\rangle|1\rangle \equiv |1,1\rangle \equiv \underbrace{|[11]_2\rangle}_{\text{число "3" в двоична система}} \equiv |3\rangle \\
 \underbrace{\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)} &= \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \equiv e_3^{(4)} \in \{e_0^{(4)}, e_1^{(4)}, e_2^{(4)}, e_3^{(4)}\} \\
 &\quad \text{— стандартния о.н.б. в } \mathbb{C}^4
 \end{aligned}$$

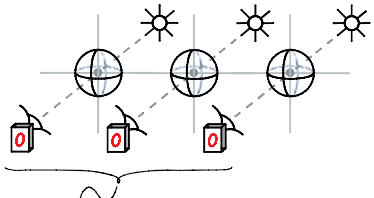
фиг. 70: Система от два кубита в изчислителен базис: случай “11”

По-нататък, при формиране на три и повече кубитни състояния използваме асоциативността на тензорното произведение.

$$\begin{array}{c}
 \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right) \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\
 \underbrace{\left(e_0^{(a)} \otimes e_0^{(a)} \otimes e_0^{(a)} \right)} = \longrightarrow \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\} \\
 \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right) \right) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right)
 \end{array}$$

фиг. 71: Тензорното произведение е асоциативно (т.е., скобите могат да се местят): пример

На базата на това, на следващите фигури е разгледан случая на три-кубитна система:



The diagram at the top shows three qubits, each represented by a sphere with a cross and a sun-like symbol above it. Below each sphere is a small box containing the number '0'. A bracket groups these three boxes.

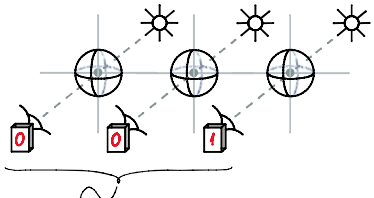
$$\begin{aligned}
 e_0^{(A)} \otimes (e_0^{(A)} \otimes e_0^{(A)}) &\equiv |e_0\rangle \otimes |e_0\rangle \otimes |e_0\rangle \\
 &\equiv |0\rangle \otimes |0\rangle \otimes |0\rangle \equiv |0\rangle|0\rangle|0\rangle \\
 &\equiv |0,0,0\rangle \equiv |[000]_2\rangle \equiv |0\rangle
 \end{aligned}$$

|||

$$\begin{aligned}
 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_0^{(8)} \in \{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\} \\
 &\quad \text{— стандартния о.и.б. в } \mathbb{C}^8
 \end{aligned}$$

число "0" в двоична система

фиг. 72: Система от три кубита в изчислителен базис:
случай "000"



The diagram at the top shows three qubits, each represented by a sphere with a cross and a sun-like symbol above it. Below each sphere is a small box containing a binary digit: the first two contain '0' and the third contains '1'. A bracket groups these three boxes.

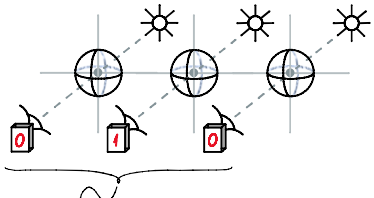
$$\begin{aligned}
 e_0^{(2)} \otimes (e_0^{(2)} \otimes e_1^{(2)}) &\equiv |e_0\rangle \otimes |e_0\rangle \otimes |e_1\rangle \\
 &\equiv |0\rangle \otimes |0\rangle \otimes |1\rangle \equiv |0\rangle|0\rangle|1\rangle \\
 &\equiv |0,0,1\rangle \equiv |[001]_2\rangle \equiv |1\rangle
 \end{aligned}$$

|||

$$\begin{aligned}
 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_1^{(8)} \in \{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\} \\
 &\quad \text{— стандартния о.и.б. в } \mathbb{C}^8
 \end{aligned}$$

число "1" в двоична система

фиг. 73: Система от три кубита в изчислителен базис:
случай "001"



The diagram at the top shows three qubits, each represented by a sphere with a cross and a sun-like symbol above it. Below each sphere is a small box containing a binary digit: 0, 1, and 0 respectively. A bracket groups these three boxes.

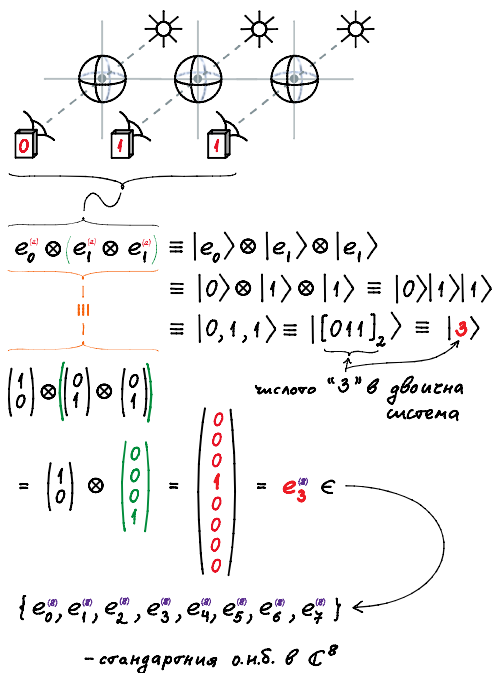
$$\begin{aligned}
 e_0^{(2)} \otimes (e_1^{(2)} \otimes e_0^{(2)}) &\equiv |e_0\rangle \otimes |e_1\rangle \otimes |e_0\rangle \\
 &\equiv |0\rangle \otimes |1\rangle \otimes |0\rangle \equiv |0\rangle|1\rangle|0\rangle \\
 &\equiv |0,1,0\rangle \equiv |[010]_2\rangle \equiv |2\rangle
 \end{aligned}$$

|||

$$\begin{aligned}
 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_2^{(8)} \in \{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\} \\
 &\quad \text{— стандартния о.и.б. в } \mathbb{C}^8
 \end{aligned}$$

число "2" в двоична система

фиг. 74: Система от три кубита в изчислителен базис:
случай "010"



The diagram illustrates the calculation of the tensor product of three qubit basis states. At the top, three qubits are shown as spheres with axes, each with a measurement outcome box below it: the first shows '0', the second and third show '1'. Dashed lines connect the spheres to the mathematical expressions below. The calculation proceeds as follows:

$$\begin{aligned}
 e_0^{(2)} \otimes (e_1^{(2)} \otimes e_1^{(2)}) &\equiv |e_0\rangle \otimes |e_1\rangle \otimes |e_1\rangle \\
 &\equiv |0\rangle \otimes |1\rangle \otimes |1\rangle \equiv |0\rangle|1\rangle|1\rangle \\
 &\equiv |0,1,1\rangle \equiv |[011]_2\rangle \equiv |3\rangle
 \end{aligned}$$

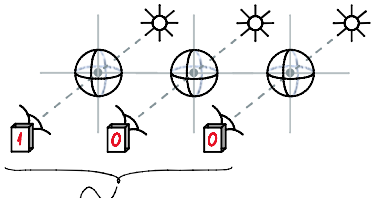
Below this, the calculation is shown using column vectors:

$$\begin{aligned}
 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) \\
 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_3^{(8)} \in \{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\}
 \end{aligned}$$

A handwritten note with an arrow points to the state $|3\rangle$ and the vector $e_3^{(8)}$: "число '3' в двоична система".

At the bottom, the set of basis vectors is identified: $\{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\}$ - стандартния о.и.б. в $\mathbb{C}^8$.

фиг. 75: Система от три кубита в изчислителен базис: случай "011"



The diagram at the top shows three qubits, each represented by a sphere with a cross and a sun-like symbol above it. Below each sphere is a small box containing a binary value: 1, 0, and 0 respectively. A bracket groups these three boxes.

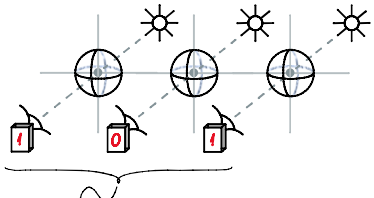
$$\begin{aligned}
 e_1^{(2)} \otimes (e_0^{(2)} \otimes e_0^{(2)}) &\equiv |e_1\rangle \otimes |e_0\rangle \otimes |e_0\rangle \\
 &\equiv |1\rangle \otimes |0\rangle \otimes |0\rangle \equiv |1\rangle|0\rangle|0\rangle \\
 &\equiv |1, 0, 0\rangle \equiv |[100]_2\rangle \equiv |4\rangle
 \end{aligned}$$

|||

$$\begin{aligned}
 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = e_4^{(8)} \in \{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\} \\
 &\quad \text{— стандартния о.и.б. в } \mathbb{C}^8
 \end{aligned}$$

число "4" в двоична система

фиг. 76: Система от три кубита в изчислителен базис:
случай "100"



The diagram at the top shows three qubits, each represented by a sphere with a cross and a sun-like symbol above it. Below each sphere is a small box containing a binary digit: 1, 0, and 1 respectively. A bracket groups these three boxes.

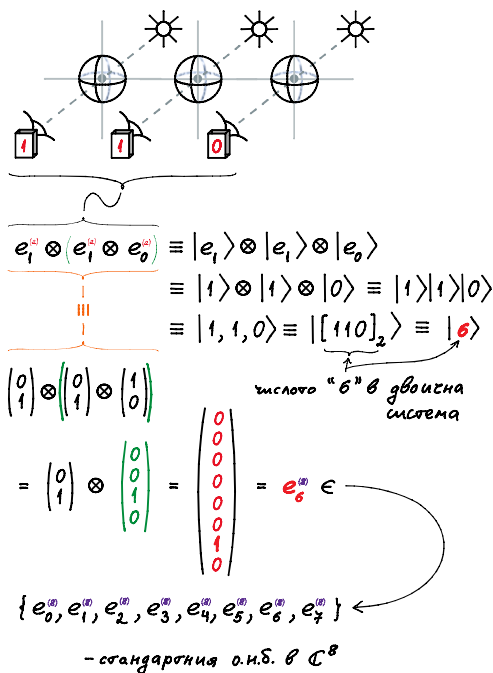
$$\begin{aligned}
 e_1^{(2)} \otimes (e_0^{(2)} \otimes e_1^{(2)}) &\equiv |e_1\rangle \otimes |e_0\rangle \otimes |e_1\rangle \\
 &\equiv |1\rangle \otimes |0\rangle \otimes |1\rangle \equiv |1\rangle|0\rangle|1\rangle \\
 &\equiv |1, 0, 1\rangle \equiv |[101]_2\rangle \equiv |5\rangle
 \end{aligned}$$

|||

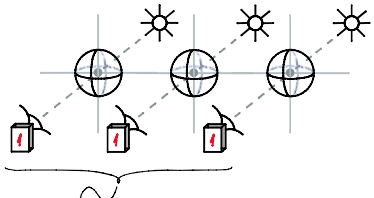
$$\begin{aligned}
 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = e_5^{(8)} \in \{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\} \\
 &\quad \text{— стандартния о.и.б. в } \mathbb{C}^8
 \end{aligned}$$

число "5" в двоична система

фиг. 77: Система от три кубита в изчислителен базис:
случай "101"



фиг. 78: Система от три кубита в изчислителен базис:
случай "110"



The diagram at the top shows three qubits, each represented by a sphere with a cross and a sun-like symbol above it. Below each sphere is a small box with a red arrow pointing upwards, representing a qubit in the state $|1\rangle$. A bracket groups these three qubits, leading to the following mathematical expressions:

$$\begin{aligned}
 e_1^{(2)} \otimes (e_1^{(2)} \otimes e_1^{(2)}) &\equiv |e_1\rangle \otimes |e_1\rangle \otimes |e_1\rangle \\
 &\equiv |1\rangle \otimes |1\rangle \otimes |1\rangle \equiv |1\rangle|1\rangle|1\rangle \\
 &\equiv |1, 1, 1\rangle \equiv |[111]_2\rangle \equiv |\textcolor{red}{7}\rangle
 \end{aligned}$$

Below this, the tensor product is calculated using column vectors:

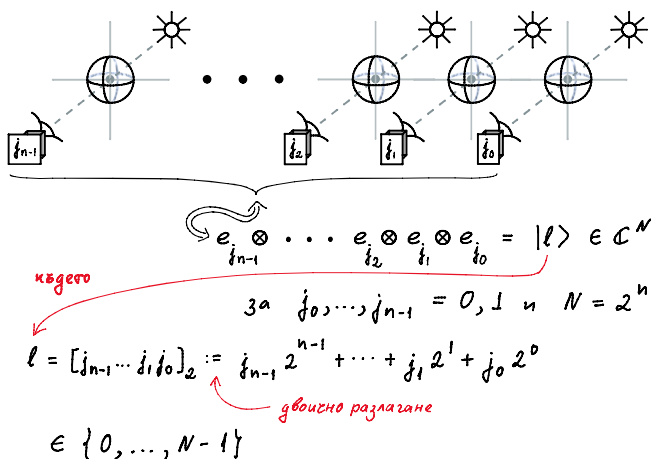
$$\begin{aligned}
 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \textcolor{red}{1} \end{pmatrix} = \textcolor{red}{e}_7^{(8)} \in \{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\}
 \end{aligned}$$

A note with an arrow pointing to the $|\textcolor{red}{7}\rangle$ state says: "число '7' в двоична система".

At the bottom, the set of basis vectors is listed: $\{e_0^{(8)}, e_1^{(8)}, e_2^{(8)}, e_3^{(8)}, e_4^{(8)}, e_5^{(8)}, e_6^{(8)}, e_7^{(8)}\}$, with a note below it: "- стандартния о.и.б. в $\mathbb{C}^8$ ".

фиг. 79: Система от три кубита в изчислителен базис:
случай "111"

Така достигаме до най-общия случай:



фиг. 80: Общ случай на система от няколко кубита в изчислителен базис.

Изводи: хилбертовото пространство на състоянията на система от n кубита е:

$$\underbrace{\mathbb{C}^N}_{n \text{ пъти}}, \quad N \text{ мерно, за } N = 2^n$$

$$\underbrace{\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n \text{ пъти}} = \mathbb{C}^{2 \cdots 2} = \mathbb{C}^{2^n}.$$

Стандартният базис $e_0 \equiv |0\rangle$ и $e_1 \equiv |1\rangle$ в $\mathbb{C}^2$ поражда стандартния базис в така построеното хилбертово пространство $\mathbb{C}^N$: $|[j_1 \dots j_n]_2\rangle \equiv e_{j_1} \otimes \dots \otimes e_{j_n}$. Тези базиси се наричат също **изчислителни базиси**.

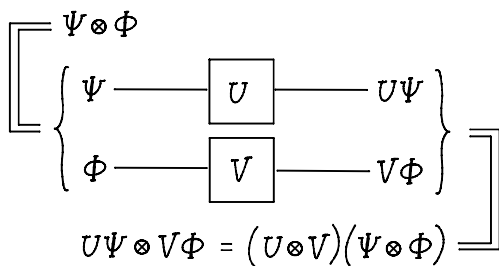
10.3 Система от няколко кубита: квантови трансформации. Квантови мрежи

10.3.1 Комбиниране на квантови трансформации

Нека $U : \mathbb{C}^N \rightarrow \mathbb{C}^N$ и $V : \mathbb{C}^M \rightarrow \mathbb{C}^M$ са унитарни оператори на квантови трансформации. Векторите на несплетените състояния $\Psi \otimes \Phi$ на съставната система $\mathbb{C}^N \otimes \mathbb{C}^M$ отново във вектори на несплетени състояния, при което Ψ и Φ се трансформират независимо. Това ни води до понятието за **тензорно произведение** на линейни изображения,

$$\begin{aligned} U \otimes V : \mathbb{C}^N \otimes \mathbb{C}^M &\rightarrow \mathbb{C}^N \otimes \mathbb{C}^M \\ \Psi \otimes \Phi &\mapsto U\Psi \otimes V\Phi, \end{aligned}$$

което допълнително се разпространява по линейност и за сплетени състояния. Схематично това е изобразено на долната фигура:



фиг. 81: Тензорното произведение на две квантови трансформации – основна стъпка при строене на квантови мрежи

Следователно, съставната квантова трансформация се представя от матрицата $U \otimes V$, която $NM \times NM$ –матрица и е също унитарна, понеже

$$(U \otimes V)^*(U \otimes V) = U^*U \otimes V^*V = \hat{1}.$$

10.3.2 Примери

Да разгледаме, като първи пример паралелното прилагане на n гейта на Адамар върху

базисния вектор $|0, 0, \dots, 0\rangle$:

$$\begin{array}{ccccc}
 |0\rangle & \text{---} & \boxed{\text{H}} & \text{---} & \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
 |0\rangle & \text{---} & \boxed{\text{H}} & \text{---} & \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
 \vdots & & \vdots & & \vdots \\
 |0\rangle & \text{---} & \boxed{\text{H}} & \text{---} & \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)
 \end{array}$$

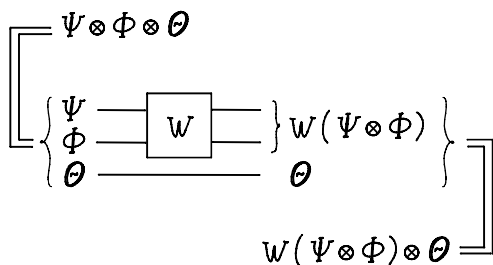
В резултат получаваме тензорното произведение:

$$\begin{aligned}
 & \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \overset{\otimes}{\vee} (|0\rangle + |1\rangle) \overset{\otimes}{\vee} \dots \overset{\otimes}{\vee} (|0\rangle + |1\rangle) \\
 &= \frac{1}{\sqrt{2^n}} \left(\underbrace{|0\rangle|0\rangle\dots|0\rangle}_{|[00\dots0]_2\rangle} + \underbrace{|0\rangle|0\rangle\dots|1\rangle}_{|[00\dots1]_2\rangle} + \dots \right. \\
 & \left. + \underbrace{|1\rangle|1\rangle\dots|1\rangle}_{|[11\dots1]_2\rangle} \right) = \frac{1}{\sqrt{N}} \sum_{\ell=0}^{N-1} |\ell\rangle .
 \end{aligned}$$

Друг пример: ако $W : \mathbb{C}^N \otimes \mathbb{C}^M \rightarrow \mathbb{C}^N \otimes \mathbb{C}^M$, то трансформацията

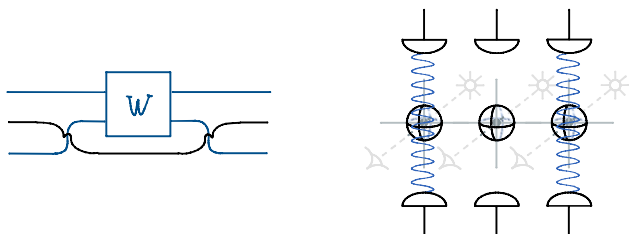
$$W \otimes \hat{1} : (\mathbb{C}^N \otimes \mathbb{C}^M) \otimes \mathbb{C}^L \rightarrow (\mathbb{C}^N \otimes \mathbb{C}^M) \otimes \mathbb{C}^L$$

е изобразена на долната фигура



фиг. 82: Специален случай на квантова трансформация, при която на една от линиите не се действа

Възможно е и с допълнително пренареждане, както е показано на долната фигура, като в този случай казваме, че W действа върху първия и третия кубити.



фиг. 83: В случая на фиг. 82 може свободната линия да е между тези на които се действа: математически това се описва с допълнителна операция на разместване на линиите

10.3.3 Операциите на пренареждане

Да разгледаме най-общо квантовите операции на пренареждане: за всяка пермутация $\sigma \in \mathcal{S}_n$ съществува единствено линейно изображение

$$\begin{aligned} \Gamma_\sigma : \underbrace{\mathbb{C}^M \otimes \cdots \otimes \mathbb{C}^M}_{n \text{ пъти}} &\rightarrow \underbrace{\mathbb{C}^M \otimes \cdots \otimes \mathbb{C}^M}_{n \text{ пъти}} \\ \Psi_1 \otimes \cdots \otimes \Psi_n &\rightarrow \Psi_{\sigma(1)} \otimes \cdots \otimes \Psi_{\sigma(n)}. \end{aligned} \quad (10.1)$$

В частност, $\Gamma_\sigma(e_{j_1} \otimes \cdots \otimes e_{j_n}) = e_{j_{\sigma(1)}} \otimes \cdots \otimes e_{j_{\sigma(n)}}$, което определя Γ_σ напълно и показва, че е унитарна (понеже изобразява ортонормиран базис в ортонормиран).

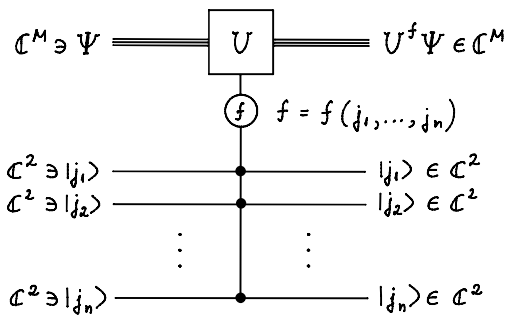
Забележка: $\Gamma_\eta \circ \Gamma_\sigma = \Gamma_{\sigma\eta}$ и за да се коригира запазването на реда понякога избират σ^{-1} по-горе в определението на Γ_σ вместо σ .

10.3.4 Условни операции: “IF $f = 1$ THEN U ELSE $\hat{1}$ ”

Нека $f : \{0, 1\}^{\times n} \rightarrow \{0, 1\} : (j_1, \dots, j_n) \mapsto f(j_1, \dots, j_n)$ ($= 0$ или 1) и нека $U : \mathbb{C}^M \rightarrow \mathbb{C}^M$ е унитарна. Тогава определяме

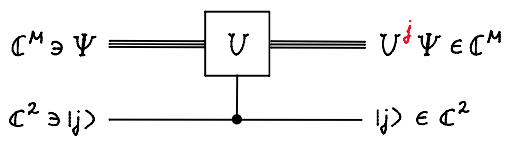
$$\tilde{U} : \mathbb{C}^N \otimes \mathbb{C}^M \rightarrow \mathbb{C}^N \otimes \mathbb{C}^M,$$

$N = 2^n$, според както е показано на долната фигура:



фиг. 84: Условните квантни трансформации: “ако $f = 1$ тогава изпълни U , в противен случай - нищо не изпълнявай” (“if $f = 1$ then do U , else - do nothing”)

В частност, когато $n = 1$ и $f : \{0, 1\} \rightarrow \{0, 1\}$ е идентитета, то имаме важния частен случай:



фиг. 85: Специалния случай на условните квантова трансформация с едно-кубитов контролен гейт: ако контролният гейт е $j = 1$, тогава U се изпълнява, $U^j \equiv U^1 = U$, в противен случай, когато $j = 0$, тогава U не се изпълнява, $U^j \equiv U^0 = \hat{1}$

което е унитарна трансформация:

$$\tilde{U} : \mathbb{C}^2 \otimes \mathbb{C}^M \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^M .$$

10.4 Дискретна Фурие трансформация

10.4.1 Определение и свойства

По определение, дискретната Фурие трансформация е линейна трансформация

$$F : \mathbb{C}^N \rightarrow \mathbb{C}^N,$$

която е определена от $N \times N$ -матрицата: $F := (f_{j,k})_{j,k=0}^{N-1} :=$

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \xi & \xi^2 & \dots & \xi^{N-1} \\ 1 & \xi^2 & \xi^4 & \dots & \xi^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi^{N-1} & \xi^{(N-1)^2} & \dots & \xi^{(N-1)^2} \end{pmatrix} \quad (10.2)$$

където $\xi := e^{\frac{2\pi i}{N}}$ е примитивен N -ти корен на единицата, $\xi^N = 1$.

Така,

$$\begin{aligned} f_{j,k} &= N^{-\frac{1}{2}} \xi^{jk} \equiv N^{-\frac{1}{2}} e^{\frac{2\pi i}{N} jk} \\ &= N^{-\frac{1}{2}} \left(\cos \frac{2\pi jk}{N} + i \sin \frac{2\pi jk}{N} \right). \end{aligned}$$

Въведената матрица е унитарна, наистина, $(c_{j,k})_{j,k=0}^{N-1} := F^* F \stackrel{?}{=} \hat{1}$, понеже $F^* = (\overline{f_{k,j}})_{j,k=0}^{N-1}$

и $\overline{f_{k,j}} = \overline{f_{j,k}} = N^{-\frac{1}{2}} \bar{\xi}^{jk} = N^{-\frac{1}{2}} \xi^{-jk}$ и оттук:

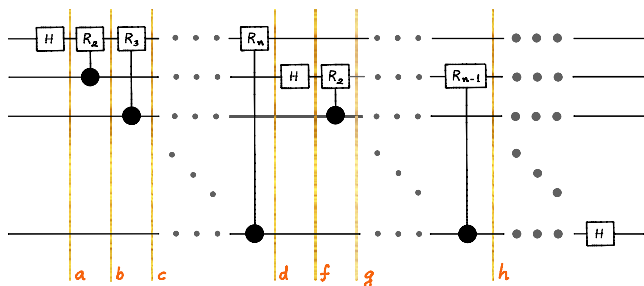
$$\begin{aligned} c_{j,k} &= \sum_{\ell=0}^{N-1} \overline{f_{\ell,j}} f_{\ell,k} = \frac{1}{N} \sum_{\ell=0}^{N-1} \xi^{(k-j)\ell} \\ &= \begin{cases} \frac{1}{N} N = 1 & \text{за } j = k \\ \frac{\xi^{(j-k)N} - 1}{\xi - 1} = 0 & \text{за } j \neq k. \end{cases} \end{aligned}$$

Действието може да се разпише и така:

$$\begin{aligned} F |j\rangle &= \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i}{N} j \cdot 1} |1\rangle \right. \\ &\quad \left. + e^{\frac{2\pi i}{N} j \cdot 2} |2\rangle + e^{\frac{2\pi i}{N} j \cdot 3} |3\rangle + \dots \right). \end{aligned}$$

10.4.2 Реализация с квантова мрежа

Ние вече дадохме квантовата мрежа за дискретната Фурие трансформация в началото на тази лекция, като илюстрация на квантовите изчисления. В общия случай, тази мрежа е дадена на долната фигура:



фиг. 86: Мрежа за дискретната фурие трансформация в n кубитовия случай

За да се убедим, че указаната мрежа дава наистина за дискретната Фурие трансформация, нека определим състоянието на n -те квантови бита, на указаните на фигурата разрези, при условие, че стартираме от състояние

$$|j_1, j_2, j_3, \dots, j_n\rangle \equiv |j_1\rangle |j_2\rangle |j_3\rangle \dots |j_n\rangle$$

В хода на действието на мрежата състоянието на n -те бита ще остане несплетено, т.е., тензорно произведение на n -те еднокубитни състояния и ние ще определим какви са те. Това е така, защото действаме с условни квантови гейтове, които в изчислителен базис имат това свойство. Освен това, контролните бите са винаги под бита на който се действа

и те не се променят при действие. И накрая, виждаме, че по всяка линия имаме една и съща последователност на гейтове, започваща от гейт на Адамар, $\boxed{\text{H}}$ и последвана от условни гейтове на ротации $\boxed{\text{R}_2}$, $\dots$, $\boxed{\text{R}_k}$. Затова, достатъчно е да проследим как се изменя състоянието на първия бит по разрезите до края, а за следващите битове пресмятането е аналогично:

$$\begin{aligned} \text{a. } |j_1\rangle &\xrightarrow{\boxed{\text{H}}} \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{j_1} |1\rangle) \\ &= \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{2\pi i \cdot [0.j_1]_2} |1\rangle, \end{aligned}$$

където сме използвали, че $(-1)^{j_1} = (e^{2\pi i \frac{1}{2}})^{j_1} = e^{2\pi i \frac{j_1}{2}}$ и $\frac{j_1}{2} = [0.j_1]_2$ в двоичен запис.

$$\begin{aligned} \text{b. } &\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{2\pi i \cdot [0.j_1]_2} \\ &\xrightarrow{\boxed{\text{R}_2}} \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{2\pi i \cdot [0.j_1 j_2]_2}. \end{aligned}$$

Това е така, защото условния гейт $\boxed{\text{R}_2}$, при стойност j_2 на контролния бит действа, като матрицата

$$\begin{pmatrix} 1 & 0 \\ 0 & (e^{2\pi i \frac{1}{4}})^{j_2} \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i \cdot [0.0 j_2]_2} \end{pmatrix}.$$

$$\text{c. } \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{2\pi i \cdot [0.j_1 j_2]_2}$$

$$\boxed{R_2} \xrightarrow{\quad} \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{2\pi i \cdot [0.j_1 j_2 j_3]_2} |1\rangle,$$

което е аналогично на предходното действие.

- d. На този етап приключваме с действието върху първия кубит. Крайният резултат от действието на останалите условни гейтове $\boxed{R_4}, \dots, \boxed{R_n}$ е:

$$\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{2\pi i \cdot [0.j_1 j_2 j_3 \dots j_n]_2} |1\rangle.$$

- f. – h. На тези разрези състоянието на първия кубит не се променя повече.

И така, крайното състояние се дава от тензорното произведение:

$$\begin{aligned} & 2^{-\frac{n}{2}} \left(|0\rangle + e^{2\pi i \cdot [0.j_1 j_2 j_3 \dots j_n]_2} |1\rangle \right) \\ & \quad \times \left(|0\rangle + e^{2\pi i \cdot [0.j_2 j_3 \dots j_n]_2} |1\rangle \right) \\ & \quad \times \left(|0\rangle + e^{2\pi i \cdot [0.j_3 \dots j_n]_2} |1\rangle \right) \\ & \quad \vdots \\ & \quad \times \left(|0\rangle + e^{2\pi i \cdot [0.j_n]_2} |1\rangle \right). \end{aligned}$$

Отчитайки, че

$$e^{2\pi i \cdot [0.j_k \dots j_n]_2} = e^{2\pi i \cdot [j_1 \dots j_n]_2 \cdot 2^{-(n-k+1)}},$$

получаваме израза на дискретната Фурие трансформация.

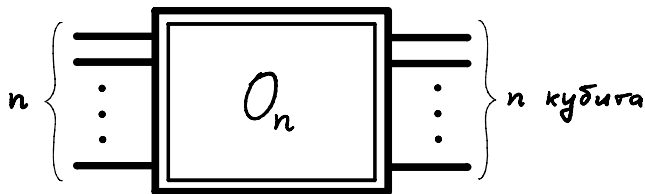
10.5 Първо понятие за квантов алгоритъм

И така, съвсем естествено достигнахме до следното понятие за квантов алгоритъм. Това е редица от квантови мрежи

$$\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_n, \dots$$

такива, че:

- $\mathcal{O}_n$ оперира върху n кубита;
- при $m < n$, ако ограничим действието на $\mathcal{O}_n$ върху последните m бита, занулявайки първите, то ще получим действието на $\mathcal{O}_m$;
- редицата от мрежи $\mathcal{O}_1, \mathcal{O}_2, \dots, \mathcal{O}_n, \dots$ се поражда от класически алгоритъм.
- В края на изпълнението на мрежата върху изчислителен базис, при измерване отново в изчислителния базис резултата се получава с вероятност близка до 1. Това сме илюстрирали схематично на долната фигура:



фиг. 87: Първоначалното ни понятие за квантов алгоритъм е “алгоритмично породена”, съгласувана редица от квантови мрежи $\{\mathcal{O}_n\}_{n=1}^{\infty}$

По такъв начин, квантовите изчисления са винаги обратими. Растежа на дължината на мрежата $\mathcal{O}_n$ в зависимост от n (което е $\log_2 N$) определя понятието за ефективност на алгоритъма. От особен интерес са тези алгоритми, за които този растеж е полиномиален.