

КВАНТОВА ИНФОРМАТИКА

Николай М. Николов

Лекция 11 / 18.12.2023, версия 0

В тази лекция ще представим квантов алгоритъм.

Това ще бъде първо въвеждане на това [↑] понятие
върху пример.

В следващата лекция ще дадем общи определения:
варианти и дискусия.

В тази лекция ще представим квантов алгоритъм
за следната задача:

В тази лекция ще представим квантов алгоритъм за следната задача:

Нека $f: \{0, 1, 2, \dots\} \rightarrow \{0, 1, 2, \dots\}$ е такава, че

В тази лекция ще представим квантов алгоритъм за следната задача:

Нека $f: \{0, 1, 2, \dots\} \rightarrow \{0, 1, 2, \dots\}$ е такава, че съществува $P \in \{1, 2, \dots, N\}$, $N := 2^n$, така че

В тази лекция ще представим квантов алгоритъм за следната задача:

Нека $f: \{0, 1, 2, \dots\} \rightarrow \{0, 1, 2, \dots\}$ е такава, че съществува $P \in \{1, 2, \dots, N\}$, $N := 2^n$, така че

- $f(X + P) = f(X)$ - периодичност с период P

В тази лекция ще представим квантов алгоритъм за следната задача:

Нека $f: \{0, 1, 2, \dots\} \rightarrow \{0, 1, 2, \dots\}$ е такава, че съществува $P \in \{1, 2, \dots, N\}$, $N := 2^n$, така че

- $f(X + P) = f(X)$ - периодичност с период P
- $f: \{0, 1, 2, \dots, P-1\} \xrightarrow{\sim} \{0, 1, 2, \dots, P-1\}$ е биекция.

Квантов алгоритъм за следната задача:

Нека $f: \{0, 1, 2, \dots\} \rightarrow \{0, 1, 2, \dots\}$ е такава, че съществува $P \in \{1, 2, \dots, N_0\}$, $N_0 := 2^{n_0}$, така че

- $f(X + P) = f(X)$ - периодичност с период P
- $f: \{0, 1, 2, \dots, P-1\} \xrightarrow{\sim} \{0, 1, 2, \dots, P-1\}$ е биекция.

Квантов алгоритъм за следната задача:

Нека $f: \{0, 1, 2, \dots\} \rightarrow \{0, 1, 2, \dots\}$ е такава, че съществува $P \in \{1, 2, \dots, N_0\}$, $N_0 := 2^{n_0}$, така че

- $f(X + P) = f(X)$ - периодичност с период P
- $f: \{0, 1, 2, \dots, P-1\} \xrightarrow{\sim} \{0, 1, 2, \dots, P-1\}$ е биекция.

Търси се P .

Считаме, че f ни е зададена като "черна кутия",

$$\overline{X} \boxed{f} \overline{X'} = f(X)$$

Считаме, че f ни е зададена като "черна кутия",

$$n_0 \text{ дига } \left\{ \overline{X} \boxed{f} \overline{X'} = f(X) \right.$$

Считаме, че f ни е зададена като "черна кутия",

$$n_0 \text{ бита } \left\{ \overline{X} \boxed{f} \overline{X'} = f(X) \right.$$

която "бързо" изчислява $f(X)$ (т.е., за време $\sim$ полином на n_0)

Считаме, че f ни е зададена като "черна кутия",

$$n_0 \text{ бита } \{ \overline{X} \boxed{f} \overline{X'} = f(X) \}$$

която "бързо" изчислява $f(X)$ (т.е., за време $\sim$ полином на n_0)

Бихме могли да започнем да смятаме:

$$F := f(0), f(1), \dots, F = f(P) \text{ до първото повторение}$$

$$\underbrace{\hspace{10em}} = \underbrace{\hspace{10em}}$$

Считаме, че f ни е зададена като "черна кутия",

$$n_0 \text{ бита } \left\{ \overline{X} \boxed{f} \overline{X'} = f(X) \right.$$

$\Rightarrow$ търсенето ще продължи за време $\sim P \sim 2^{n_0}$

Считаме, че f ни е зададена като "черна кутия",

$$n_0 \text{ бита } \left\{ \overline{X} \boxed{f} \overline{X'} = f(X) \right.$$

$\Rightarrow$ търсенето ще продължи за време $\sim P \sim 2^{n_0}$

-експоненциално време спрямо броя битовете n_0 на резултата

Считаме, че f ни е зададена като "черна кутия",

$$n_0 \text{ бита } \left\{ \overline{X} \boxed{f} \overline{X'} = f(X) \right.$$

$\Rightarrow$ търсенето ще продължи за време $\sim P \sim 2^{n_0}$

-експоненциално време спрямо броя битовете n_0 на резултата

За сравнение:  един електрон би направил $\sim 2^{150}$ обиколки във водородния атом за предполагаемото време на фивот на вселената

Считаме, че f ни е зададена като "черна кутия",

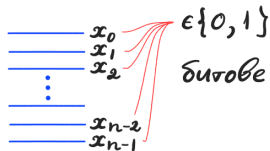
$$n_0 \text{ бита } \left\{ \overline{X} \boxed{f} \overline{X'} = f(X) \right.$$

$\Rightarrow$ търсенето ще продължи за време $\sim P \sim 2^{n_0}$

-експоненциално време спрямо броя битовете n_0 на резултата

Квантовият алгоритъм ще даде време $\sim$ полином от n_0 ,
(това ще дойде от вградената в алгоритъма Фурие-трансформация)

Данните
се задават
и четат във
формата на



Данните
се задават
и четат във
формата на

x_0
 x_1
 x_2
 $\vdots$
 x_{n-2}
 x_{n-1}

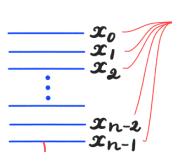
$\in \{0, 1\}$

битове

→ задаващи двоично число

$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

Данните
се задават
и четат във
формата на



$\in \{0, 1\}$

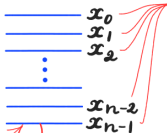
битове

→ задаващи двоично число

$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

→ всяка линия ще означава бит

Данните се задават и четат във формата на



$\in \{0, 1\}$

битове ↗ задаващи двоично число

$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

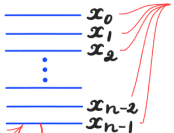
всяка линия ще означава бит

Ако това са класически битове, то състоянието им е

→ $(x_0, x_1, \dots, x_{n-1})$

→ X

Данните се задават и четат във формата на



x_0
 x_1
 x_2
 $\vdots$
 x_{n-2}
 x_{n-1}

$\in \{0, 1\}$
 битове $\rightarrow$ задаващи двоично число

$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

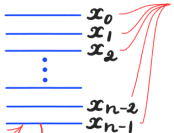
всяка линия ще означава бит

Ако това са класически битове, то състоянието им е

$\rightarrow (x_0, x_1, \dots, x_{n-1}) \in \{0, 1\}^{x_n}$ - n -та декартова степен

$\rightarrow X$

Данните се задават и четат във формата на



$\in \{0, 1\}$
битове $\rightarrow$ задаващи двоично число

$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

всяка линия ще означава бит

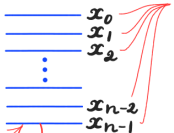
Ако това са класически битове, то състоянието им е

$\rightarrow (x_0, x_1, \dots, x_{n-1}) \in \{0, 1\}^{x_n}$ - n -та декартова степен

$\rightarrow X$

$\{0, 1\} \times \{0, 1\} \times \dots \times \{0, 1\}$

Данните се задават и четат във формата на



$\in \{0, 1\}$

битове ↗ задаващи двоично число

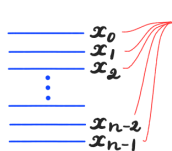
$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

↘ всяка линия ще означава бит

Ако това са **квантови** битове, то състоянието им е вектор $\Psi \in (\mathbb{C}^2)^{\otimes n}$ - n -та тензорна степен

$$\underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n \text{ times}} = \mathbb{C}^{2^n}$$

Данните
се задават
и четат във
формата на



$\in \{0, 1\}$

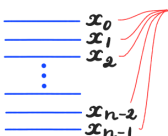
битове

→ задаващи двоично число

$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

Съответствие между класически и квантови данни ползваме
в изчислителния базис

Данните x задават и четат във формата на



$\in \{0, 1\}$

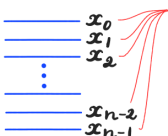
битове ↗ задаващи двоично число

$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

Съответствие между класически и квантови данни ползваваме в изчислителния базис

$$\begin{aligned}
 |x_0\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_{n-1}\rangle &\equiv: |x_0\rangle |x_1\rangle \dots |x_{n-1}\rangle \equiv: |x_0 x_1 \dots x_{n-1}\rangle \\
 &\equiv |X\rangle
 \end{aligned}$$

Данните се задават и четат във формата на



$\in \{0, 1\}$

битове ↗ задаващи двоично число

$$X := x_0 + x_1 2^1 + \dots + x_{n-1} 2^{n-1}$$

Съответствие между класически и квантови данни ползваваме в изчислителния базис

$$|x_0\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_{n-1}\rangle \equiv: |x_0\rangle |x_1\rangle \dots |x_{n-1}\rangle \equiv: |x_0 x_1 \dots x_{n-1}\rangle$$

↪ виж. Лекция 8: "Описание на паметта на квантов компютър"

$$\equiv |X\rangle$$

квантови
регистри { 

$$|x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{n-1}\rangle \equiv: |x_0\rangle |x_1\rangle \cdots |x_{n-1}\rangle \equiv: |x_0 x_1 \cdots x_{n-1}\rangle$$

$$\hookrightarrow \text{виз. Лекция 8: "Описание на паметта на квантов компютър"} \equiv |X\rangle$$

квантови регистри $\left\{ \begin{array}{c} \text{---} \\ \text{---} \\ \vdots \\ \text{---} \\ \text{---} \end{array} \right\}$ В междинни етапи на изчисление състоянието на регистрите е линейна комбинация

$$\Psi = \sum_{X=0}^{N-1} \psi_X |X\rangle$$

$$|x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{n-1}\rangle \equiv: |x_0\rangle |x_1\rangle \cdots |x_{n-1}\rangle \equiv: |x_0 x_1 \cdots x_{n-1}\rangle$$

$\hookrightarrow$ виж. Лекция 8: "Описание на паметта на квантов компютър" $\equiv |X\rangle$

квантови регистри $\left\{ \begin{array}{c} \text{---} \\ \text{---} \\ \vdots \\ \text{---} \\ \text{---} \end{array} \right\}$ В междинни етапи на изчисление състоянието на регистрите е линейна комбинация

$$\Psi = \sum_{X=0}^{N-1} \psi_X |X\rangle$$

$$\equiv \sum_{x_0, x_1, \dots, x_{n-1}=0}^1 \psi_{x_0 x_1 \dots x_{n-1}} |x_0 x_1 \dots x_{n-1}\rangle$$

$$|x_0\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_{n-1}\rangle \equiv: |x_0\rangle |x_1\rangle \dots |x_{n-1}\rangle \equiv: |x_0 x_1 \dots x_{n-1}\rangle$$

$$\hookrightarrow \text{виз. Лекция 8: "Описание на паметта на квантов компютър"} \equiv |X\rangle$$

квантови регистри $\left\{ \begin{array}{c} \text{---} \\ \text{---} \\ \vdots \\ \text{---} \\ \text{---} \end{array} \right\}$ В междинни етапи на изчисление състоянието на регистрите е линейна комбинация

$$\Psi = \sum_{X=0}^{N-1} \psi_X |X\rangle \quad (N = 2^n)$$

$$\equiv \sum_{x_0, x_1, \dots, x_{n-1}=0}^1 \psi_{x_0 x_1 \dots x_{n-1}} |x_0 x_1 \dots x_{n-1}\rangle$$

$$|x_0\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_{n-1}\rangle \equiv: |x_0\rangle |x_1\rangle \dots |x_{n-1}\rangle \equiv: |x_0 x_1 \dots x_{n-1}\rangle$$

$$\hookrightarrow \text{виз. Лекция 8: "Описание на паметта на квантов компютър"} \equiv |X\rangle$$

квантови
регистри $\left\{ \begin{array}{c} \text{---} \\ \text{---} \\ \vdots \\ \text{---} \\ \text{---} \end{array} \right\}$

В междинни етапи на изчисление състоянието на регистрите е линейна комбинация

$$\Psi = \sum_{X=0}^{N-1} \psi_X |X\rangle$$

$$(N = 2^n)$$

$$\equiv \sum_{x_0, x_1, \dots, x_{n-1}=0}^1 \psi_{x_0 x_1 \dots x_{n-1}} |x_0 x_1 \dots x_{n-1}\rangle$$

квантови
регистри



В междинни етапи на изчисление състоянието на регистрите е линейна комбинация

$$\Psi = \sum_{X=0}^{N-1} \psi_X |X\rangle$$

$$(N = 2^n)$$



Ако направим
измерване в

изчислителен базис, то резултата ще е

$$\equiv \sum_{x_0, x_1, \dots, x_{n-1}=0}^1 \psi_{x_0 x_1 \dots x_{n-1}} |x_0 x_1 \dots x_{n-1}\rangle$$

$$\rightarrow \left\{ \begin{array}{l} \text{---} x_0 \\ \text{---} x_1 \\ \text{---} x_2 \\ \vdots \\ \text{---} x_{n-2} \\ \text{---} x_{n-1} \end{array} \right.$$

квантови регистри $\left\{ \begin{array}{c} \text{---} \\ \text{---} \\ \vdots \\ \text{---} \\ \text{---} \end{array} \right\}$ В междинни етапи на изчисление състоянието на регистрите е линейна комбинация

$$\Psi = \sum_{X=0}^{N-1} \psi_X |X\rangle$$

$$(N = 2^n)$$

↓
Ако направим измерване в изчислителен базис, то резултата ще е $\rightarrow$

$$\sum_{x_0, x_1, \dots, x_{n-1}=0}^1 \psi_{x_0 x_1 \dots x_{n-1}} |x_0 x_1 \dots x_{n-1}\rangle$$

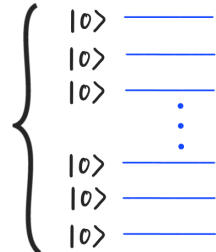
с вероятност $|\psi_{x_0 x_1 \dots x_{n-1}}|^2$

$$\left\{ \begin{array}{c} \text{---} x_0 \\ \text{---} x_1 \\ \text{---} x_2 \\ \vdots \\ \text{---} x_{n-2} \\ \text{---} x_{n-1} \end{array} \right\}$$

Например:

при входе

$\left\{ \begin{array}{l} |0\rangle \\ |0\rangle \\ |0\rangle \\ \vdots \\ |0\rangle \\ |0\rangle \\ |0\rangle \end{array} \right.$



Например:

при вход

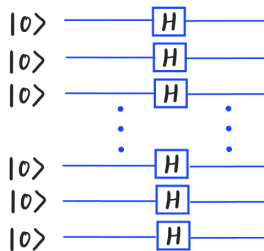
$|0\rangle$ _____
 $|0\rangle$ _____
 $|0\rangle$ _____
⋮
 $|0\rangle$ _____
 $|0\rangle$ _____
 $|0\rangle$ _____

означава:

$|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle$

Например:

при вход



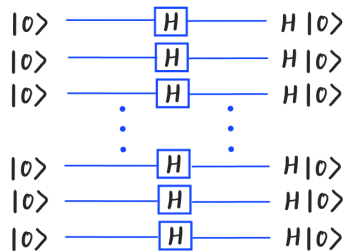
означава:

$$|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle$$

Гейт на Адамар: виж Лекция 9 в точката
"квантови трансформации: примери и дискусия".

Например:

при вход



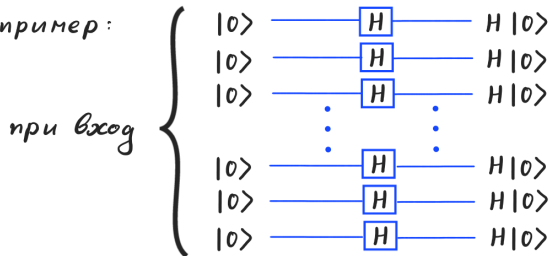
означава:

$$|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle$$

→ означава: $H|0\rangle \otimes H|0\rangle \otimes \dots \otimes H|0\rangle$

Гейт на Адамар: виж Лекция 9 в точката
"квантови трансформации: примери и дискусия".

Например:

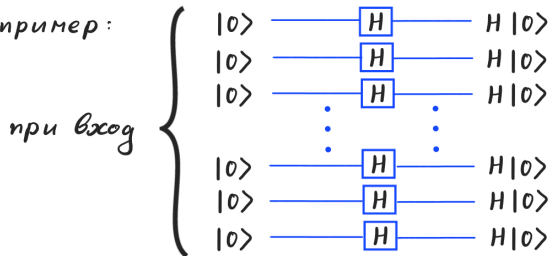


Припомниме:

→ означава: $H|0\rangle \otimes H|0\rangle \otimes \dots \otimes H|0\rangle$

$$H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

Например:

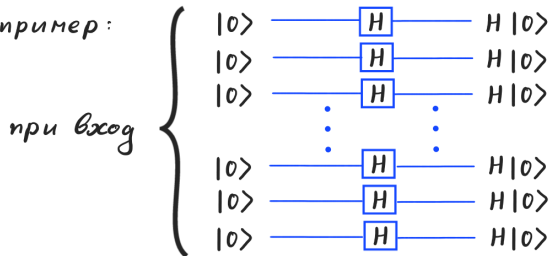


Припомниме:

→ означава: $H|0\rangle \otimes H|0\rangle \otimes \dots \otimes H|0\rangle$

$$H|0\rangle = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Например:

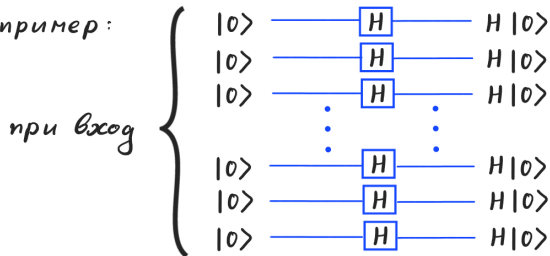


Припомним:

→ означава: $H|0\rangle \otimes H|0\rangle \otimes \dots \otimes H|0\rangle$

$$H|0\rangle = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

Например:

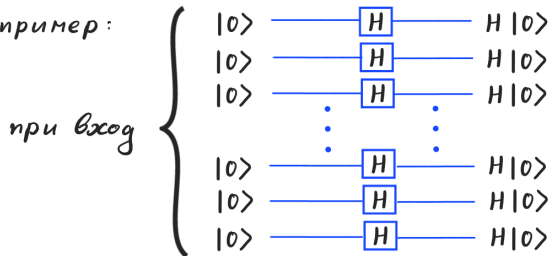


Припомним:

→ означава: $H|0\rangle \otimes H|0\rangle \otimes \dots \otimes H|0\rangle$

$$H|0\rangle = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Например:



Припомним:

→ означава: $H|0\rangle \otimes H|0\rangle \otimes \dots \otimes H|0\rangle$

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

Например:

при входе

$$\left\{ \begin{array}{lll} |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ & \vdots & \vdots \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right.$$

Припомним:

→ означава: $H|0\rangle \otimes H|0\rangle \otimes \dots \otimes H|0\rangle$

$$H|0\rangle = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

Например:

при входе

$$\left\{ \begin{array}{l} |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2}(|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2}(|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2}(|0\rangle + |1\rangle) \\ \vdots \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2}(|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2}(|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2}(|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

Припомним:

→ означава: $H|0\rangle \otimes H|0\rangle \otimes \dots \otimes H|0\rangle$

$$H|0\rangle = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

Например:

при входе

$$\left\{ \begin{array}{l} |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ \vdots \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

$$2^{-n/2} (|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |0\rangle +$$

Например:

при вход

$$\left\{ \begin{array}{lcl} |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ & \vdots & \vdots \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

$2^{-n/2} (|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |0\rangle +$

Например:

при входе

$$\left\{ \begin{array}{lcl} |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ & \vdots & \vdots \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

$$2^{-n/2} (|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |0\rangle + |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |1\rangle + \dots)$$

Например:

при входе

$$\left\{ \begin{array}{lcl} |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ & \vdots & \vdots \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

$\downarrow$

$$2^{-n/2} (|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |0\rangle + |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |1\rangle + \dots)$$

Например:

при входе

$$\left\{ \begin{array}{l} |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ \vdots \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

$$2^{-n/2} (|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |0\rangle + |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |1\rangle + \dots)$$

$$= 2^{-n/2} \sum_{x_0, x_1, \dots, x_{n-1} = 0}^1 |x_0\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_{n-1}\rangle$$

сумма по всем возможным

Например:

при входе

$$\left\{ \begin{array}{l} |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ \vdots \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

$$2^{-n/2} (|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |0\rangle + |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |1\rangle + \dots)$$

сумма по всем возможным

$$= 2^{-n/2} \sum_{x_0, x_1, \dots, x_{n-1} = 0}^1 |x_0\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_{n-1}\rangle = 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle$$

Например:

при входе

$$\left\{ \begin{array}{lcl}
 |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\
 |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\
 |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\
 & \vdots & \vdots \\
 |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\
 |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\
 |0\rangle & \text{---} \boxed{H} \text{---} & H|0\rangle = 2^{-1/2} (\textcolor{brown}{|0\rangle} + \textcolor{green}{|1\rangle})
 \end{array} \right\} \otimes$$

$$2^{-n/2} \sum_{X=0}^{N-1} |X\rangle$$

Например:

при вход

$$\left\{ \begin{array}{lcl} |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ & \vdots & \vdots \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle & \text{---} \boxed{H} & H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

Ако в този момент ние направим измерване в изчислителен базис, то с равна вероятност ще получим всички възможности $X \leftrightarrow (x_0, \dots, x_{n-1})$

$$\Leftarrow 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle$$

Например:

при вход

$$\left\{ \begin{array}{l} |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ \vdots \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \\ |0\rangle \text{ --- } \boxed{H} \text{ --- } H|0\rangle = 2^{-1/2} (|0\rangle + |1\rangle) \end{array} \right\} \otimes$$

Ако в този момент ние направим измерване в изчислителен базис, то с равна вероятност ще получим всички възможности $X \leftrightarrow (x_0, \dots, x_{n-1})$

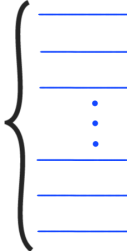
$$\Leftarrow 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle$$

но ние не спираме тук!

Анонс:

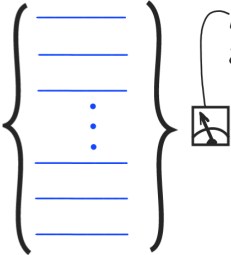


Анонс: В края
на алгоритъма
ще има група
регистри



Анонс: в края
на алгоритъма
ще има група
регистри

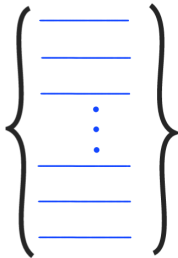
такива че



ако направим измерване в изчислителен
базис

The diagram consists of a large right-facing curly bracket on the left. Inside the bracket are seven horizontal blue lines representing registers. The third line from the top has three blue dots centered between it and the fourth line, indicating a continuation of the list. To the right of the bracket is a square box containing a circle with a diagonal arrow pointing from the bottom-left to the top-right, which is a standard symbol for a quantum measurement operation. A curved line connects the text 'ако направим измерване в изчислителен базис' to this measurement box.

Анонс: в края
на алгоритъма
ще има група
регистри



такива че

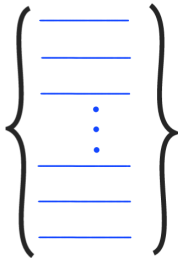


ако направим измерване в изчислителен
базис, то с **вероятност близка до 1 ***)
ще получим резултат

$$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$$

таков, че

Анонс: в края
на алгоритъма
ще има група
регистри



такива че



ако направим измерване в изчислителен
базис, то с **вероятност близка до 1 ***
ще получим резултат

$$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$$

таков, че Q дели P , където ******

$Q :=$ най-близкото цяло число

до $2^n / Y$

Анонс: в края на алгоритъма ще има група регистри

такива че

ако направим измерване в изчислителен базис, то с **вероятност близка до 1 *** ще получим резултат

$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$

таков, че Q дели P , където ******

$Q :=$ най-близкото цяло число до $2^n / Y$

→ Преминваме към $f_1(X) := f(QX)$ и т.н.

Забележки :

*) "вероятност близка до 1"

ако направим измерване в изчислителен базис, то с вероятност близка до 1 *)
ще получим резултат



$$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$$

таков, че Q дели P , където **)

$Q :=$ най-близкото цяло число
до $2^n / Y$

Забележки :

*) "вероятност близка до 1"

означава, че за $\forall \varepsilon > 0$
съществува $n = n(\varepsilon)$,
така че при този брой
използвани битове
вероятността е $1 - \varepsilon (\rightarrow 1)$

ако направим измерване в изчислителен
базис, то с вероятност близка до 1 *)
ще получим резултат



$$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$$

таков, че Q дели P , където **)

$Q :=$ най-близкото цяло число
до $2^n / Y$

Забележки :

*) "вероятност близка до 1"

означава, че за $\forall \epsilon > 0$
существува $n = n(\epsilon)$,
така че при този брой
използвани битове
вероятността е $1 - \epsilon (\rightarrow 1)$
Времето е $\text{Time}(n)$

ако направим измерване в изчислителен
базис, то с вероятност близка до 1 *)
ще получим резултат



$$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$$

таков, че Q дели P , където **)

$Q :=$ най-близкото цяло число
до $2^n / Y$

Забележки :

**) " Q дели P "



ако направим измерване в изчислителен базис, то с **вероятност близка до 1** **) ще получим резултат

$$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$$

таков, че Q дели P , където **)

$Q :=$ най-близкото цяло число
до $2^n / Y$

Забележки :

**) "Q дели P"

резултата от първото
изпълнение на алгоритъма
е делител на периода P,
а не кратно !!!



ако направим измерване в изчислителен
базис, то с **вероятност близка до 1** *)
ще получим резултат

$$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$$

таков, че Q дели P, където **)

$Q :=$ най-близкото цяло число
до $2^n / Y$

Забележки :

**) "Q дели P"

резултата от първото изпълнение на алгоритъма е делител на периода P, **а не кратно !!!**

(корекция към написаното на дъската - в записките няма корекция)

ако направим измерване в изчислителен базис, то с **вероятност близка до 1** *)
ще получим резултат



$$(y_0, y_1, \dots, y_{n-1}) \leftrightarrow Y$$

таков, че Q дели P, където **)

Q := най-близкото цяло число
до $2^n / Y$

Забележки :

Допълнително пояснение :

**) " Q дели P "

резултата от първото
изпълнение на алгоритъма
е делител на периода P ,
а не кратно !!!

(корекция към написаното
на дъската - в записките
няма корекция)

Забележки :

****) "Q дели P"**

резултата от първото изпълнение на алгоритъма е делител на периода P ,
а не кратко !!!

(корекция към написаното на дъската - в записките няма корекция)

Допълнително пояснение :

ако търсим връзка с "кратно", а не "делител", то това не е спрямо периода, а спрямо честота

$$K \approx \frac{N}{P}$$

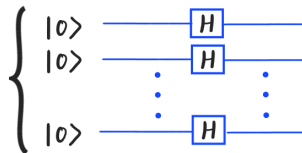
-виж точка 7 на Лекция 10.

(Преди периода беше означен с T а честотата с S .)

Алгоритъмът

go succ:

n q -бита

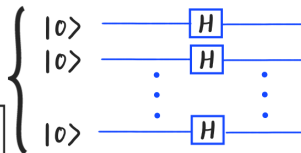


Алгоритъмът

до сук:

↙ n q -бита

$n > n_0$ е избрано
за да се осигури
добра вероятност
 $1 - \varepsilon \approx 1$ за успех

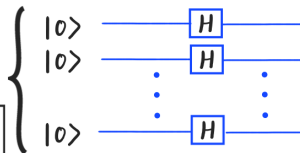


Алгоритъмът

до сук:

↙ n q -бита

$n > n_0$ е избрано
за да се осигури
добра вероятност
 $1 - \varepsilon \approx 1$ за успех



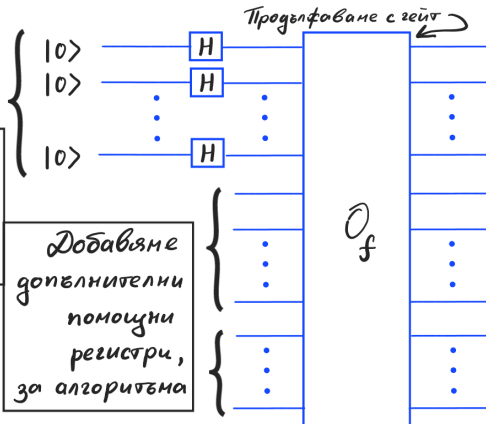
Добавяме
допълнителни
помощни
регистри,
за алгоритъма



Алгоритъмът
до тук:

↖ n q -бита

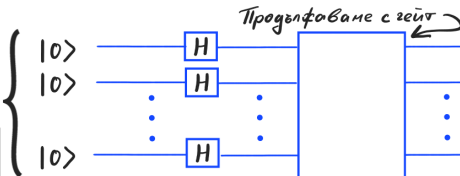
$n > n_0$ е избрано
за да се осигури
добра вероятност
 $1 - \varepsilon \approx 1$ за успех



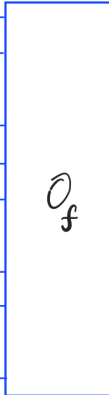
Алгоритъмът
до сук:

↖ n q -бита

$n > n_0$ е избрано
за да се осигури
добра вероятност
 $1 - \varepsilon \approx 1$ за успех

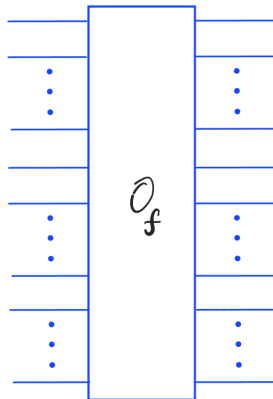


Добавяме
допълнителни
помощни
регистри,
за алгоритъма

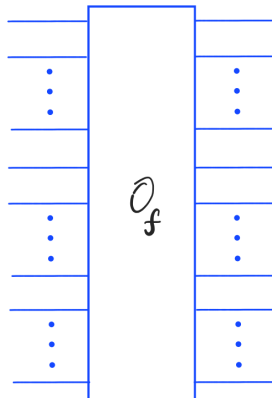


Квантовите
гейтове са
винаги
обратими:
затова
брой на
влизащи и
излизащи
регистри е
равен

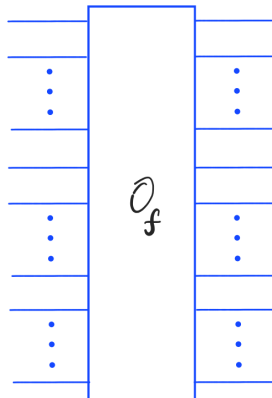
Продължаваме с гейт O_f



Продължаваме с гейт O_f ,
който "имплементира"
("внедрява") f
в алгоритъма

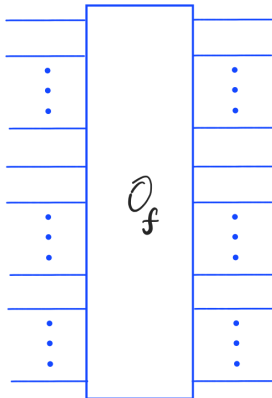


Продължаваме с гейт O_f ,
който "имплементира"
("внедрява") f
в алгоритма и има
смисъл на "входни
данни" ("input") за
алгоритма.

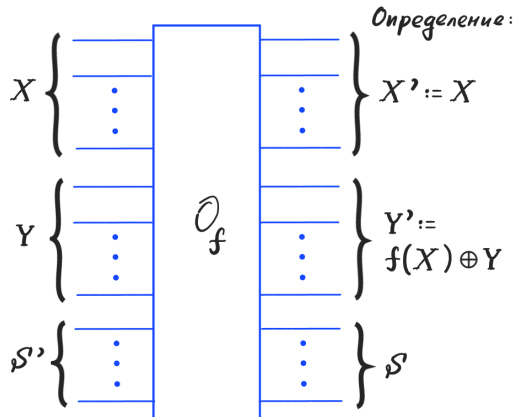


Продължаваме с гейт O_f ,
който "имплементира"
("внедрява") f
в алгоритма и има
смисъл на "входни
данни" ("input") за
алгоритма.

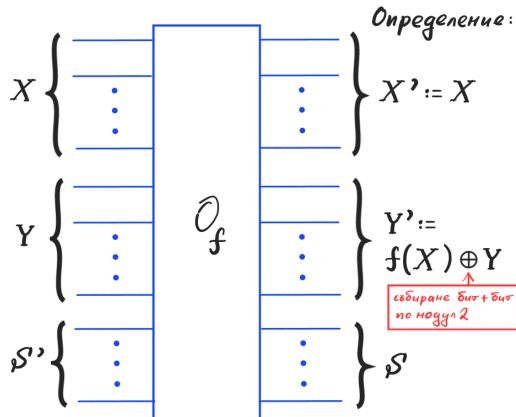
O_f - от оракул на f
- "черна кутия".



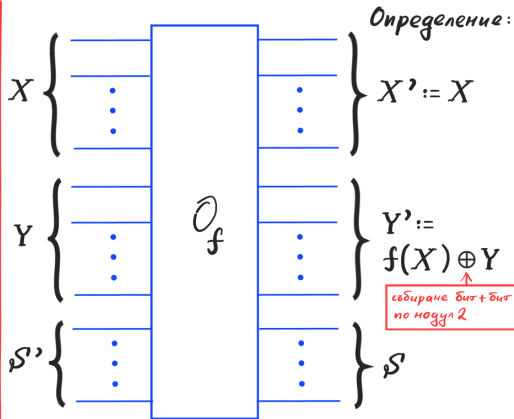
Продължаваме с гейт $\mathcal{O}_f$,
който "имплементира"
("внедрява") f
в алгоритъма и има
смисъл на "входни
данни" ("input") за
алгоритъма.
 $\mathcal{O}_f$ - от оракул на f
- "черна кутия".



Продължаваме с гейт O_f ,
който "имплементира"
("внедрява") f
в алгоритма и има
смисъл на "входни
данни" ("input") за
алгоритма.
 O_f - от оракул на f
- "черна кутия".



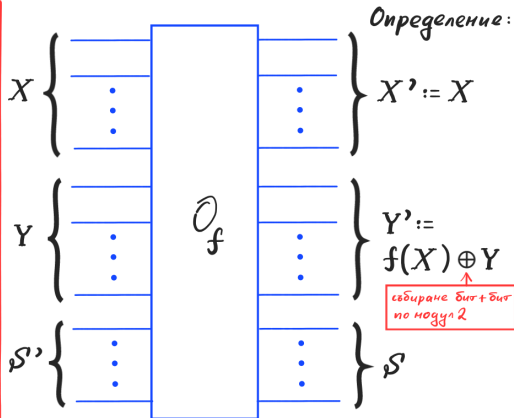
Забележете, че O_f е определен като класически гейт.



Забележете, че O_f е определен като класически гейт.

Той се пренася като квантов гейт в изчислителен базис

$$O_f(|X\rangle \otimes |Y\rangle \otimes |S'\rangle) \\ := |X'\rangle \otimes |Y'\rangle \otimes |S\rangle$$

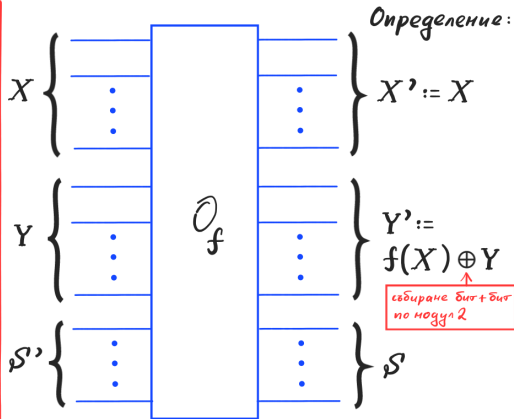


Забележете, че O_f е определен като класически гейт.

Той се пренася като квантов гейт в изчислителен базис

$$O_f(|X\rangle \otimes |Y\rangle \otimes |S'\rangle) \\ := |X'\rangle \otimes |Y'\rangle \otimes |S\rangle$$

Ангажирани са допълнително ако има нужда



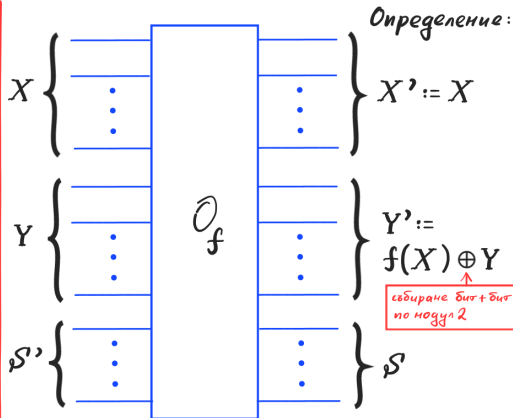
Забележете, че O_f е определен като класически гейт.

Той се пренася като квантов гейт в изчислителен базис

$$O_f(|X\rangle \otimes |Y\rangle \otimes |S'\rangle) \\ := |X'\rangle \otimes |Y'\rangle \otimes |S\rangle$$

За тях е нужно
едно условие
(S') – по-късно

Ангажирани са
← допълнително
ако има нужда



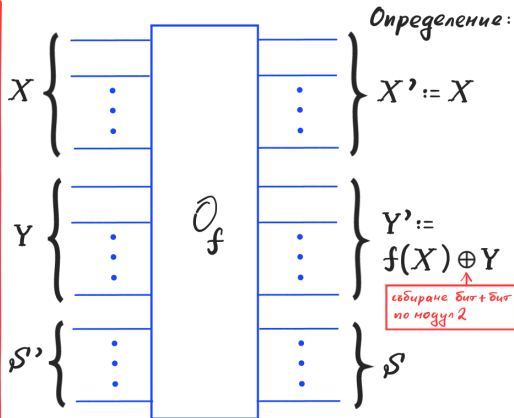
Забележете, че O_f е определен като класически гейт.

Той се пренася като квантов гейт в изчислителен базис

$$O_f(|X\rangle \otimes |Y\rangle \otimes |S'\rangle) \\ := |X'\rangle \otimes |Y'\rangle \otimes |S\rangle$$



главното условие за да е квантов гейт е унитарността: в случая означава да е биекция на базиса (орто-нормиран).

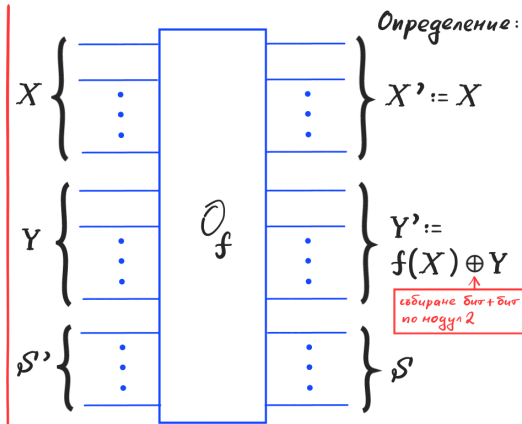


$$O_f(|X\rangle \otimes |Y\rangle \otimes |S'\rangle)$$

$$:= |X'\rangle \otimes |Y'\rangle \otimes |S\rangle$$



главното условие за да е квантов гейт
е унитарността: в случая означава да е
биекция на базиса (орто-нормиран).



$$O_f(|X\rangle \otimes |Y\rangle \otimes |S'\rangle)$$

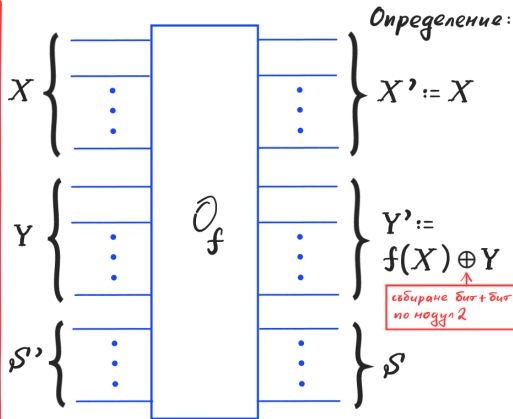
$$:= |X'\rangle \otimes |Y'\rangle \otimes |S\rangle$$



главното условие за да е квантов гейт
е унитарността: в случая означава да е
биекция на базиса (орто-нормиран).

→ изпълнено е, защото:

$$\begin{array}{l|l} X' = X & X = X' \\ Y' = f(X) \oplus Y & Y = f(X') \oplus Y' \end{array}$$



$$O_f(|X\rangle \otimes |Y\rangle \otimes |S'\rangle)$$

$$:= |X'\rangle \otimes |Y'\rangle \otimes |S\rangle$$

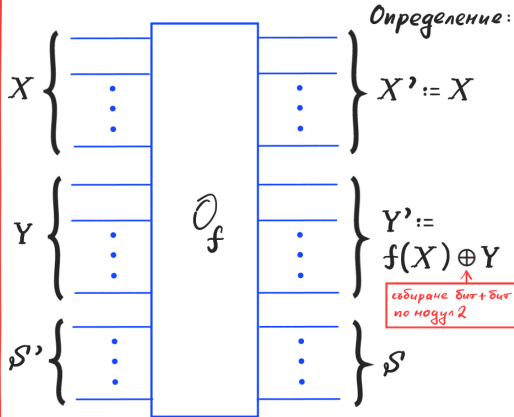


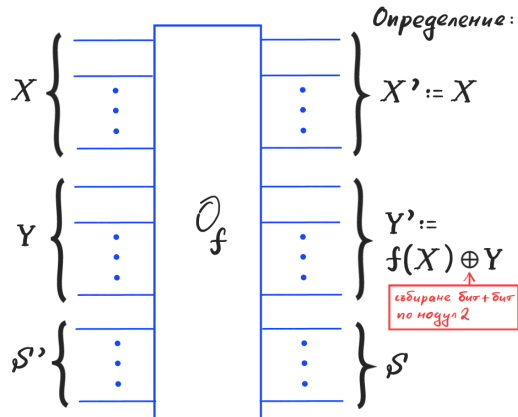
главното условие за да е квантов гейт е унитарността: в случая означава да е биекция на базиса (орто-нормиран).

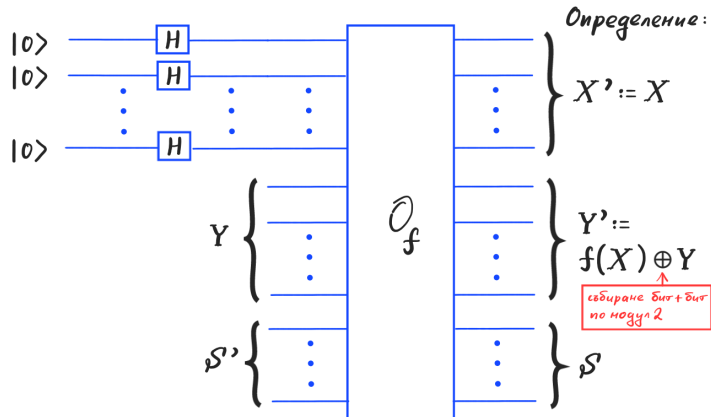
→ изпълнено е, защото:

$$\begin{array}{l|l} X' = X & X = X' \\ Y' = f(X) \oplus Y & Y = f(X') \oplus Y' \end{array}$$

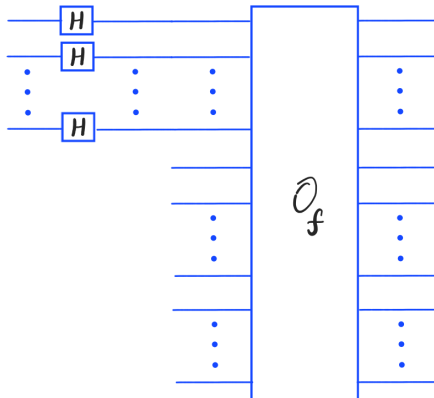
сбирането по модул 2 е и изваждане





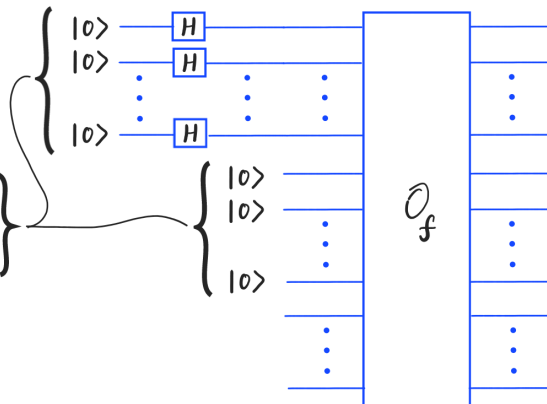


До тук
изпълнихме
две стъпки в
алгоритъма.



До тук
изпълнихме
две стъпки в
алгоритъма.

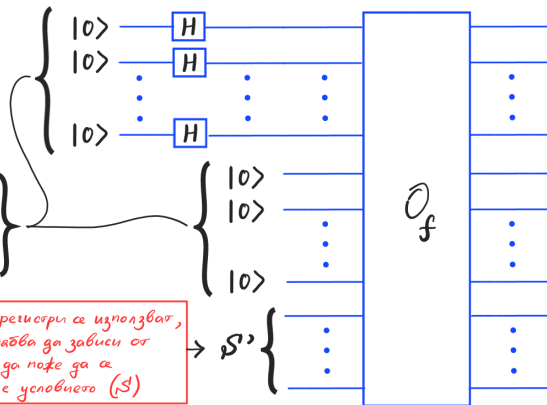
В началото се
зачуват и
двете групи



До тук
изпълнихме
две стъпки в
в алгоритма.

В началото се
зачуват и
двете групи

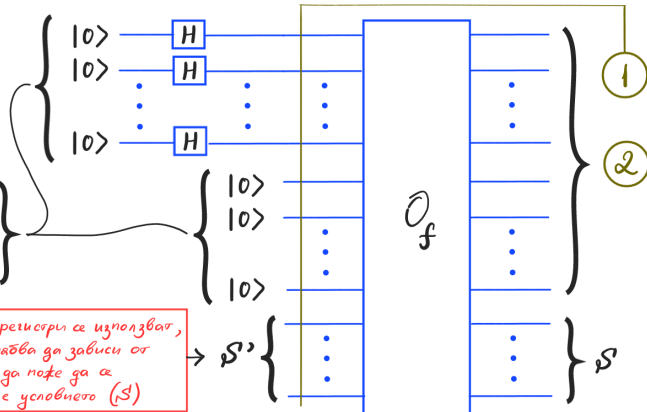
Ако такива помощни регистри се използват,
то резултата S не трябва да зависи от
първата група X за да може да се
факторизира - това е условието (S)



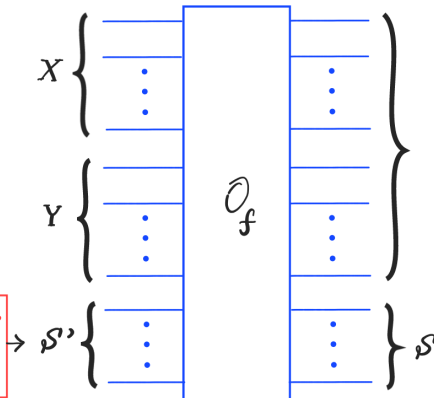
До тук
изпълнихме
две стъпки в
в алгоритма.

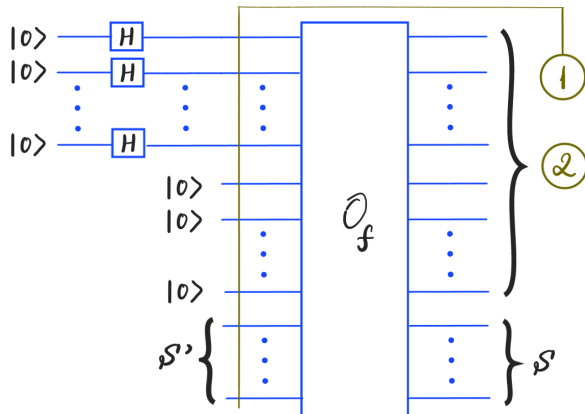
В началото се
зачуват и
двете групи

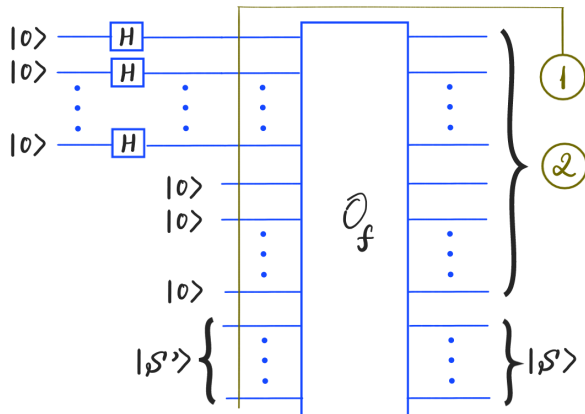
Ако такива помощни регистри се използват,
то резултата S не трябва да зависи от
първата група X за да може да се
факторизира - това е условието (S)

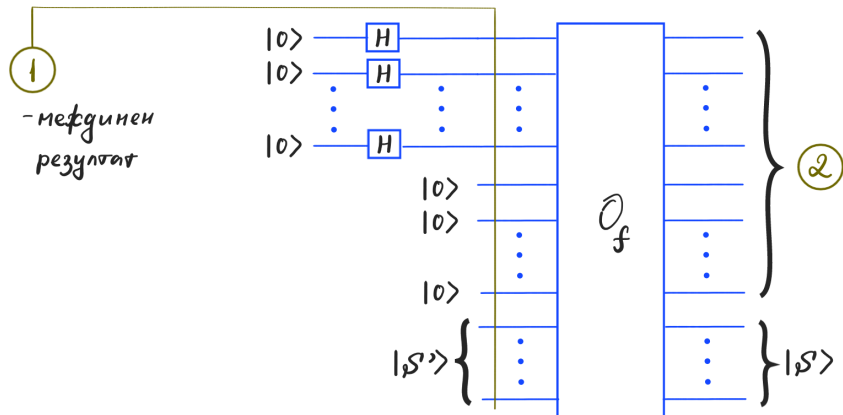


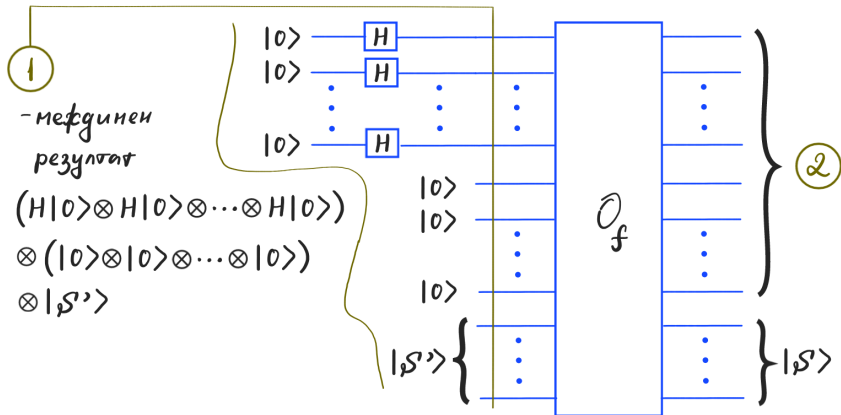
Ако такива помощни регистри се използват, то резултата S не трябва да зависи от първата група X за да може да се факторизира - това е условието (S)

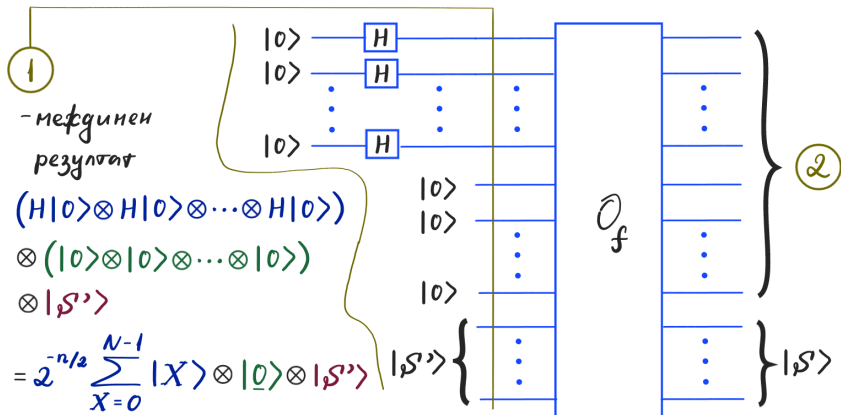


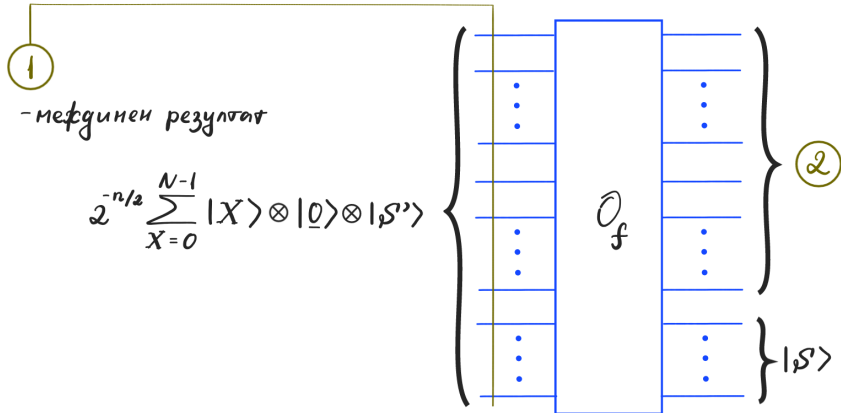


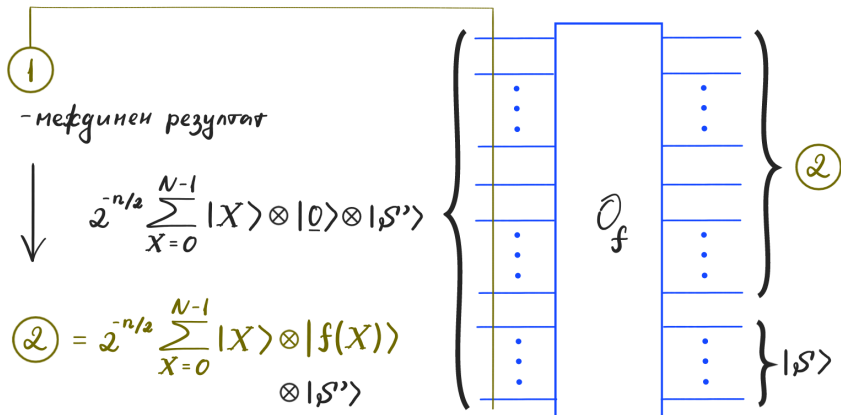












Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle \otimes |f(X)\rangle$$

Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle \otimes |f(X)\rangle$$

$$= 2^{-n/2} \left(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle + \dots + |P-1\rangle \otimes |f(P-1)\rangle \right. \\ \left. + \dots \right)$$

Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle \otimes |f(X)\rangle$$

използване
периодичността



$$\begin{aligned} = 2^{-n/2} & \left(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle + \dots + |P-1\rangle \otimes |f(P-1)\rangle \right. \\ & + |P\rangle \otimes |f(P)\rangle \quad + \dots + \quad |2P-1\rangle \otimes |f(P-1)\rangle \\ & \vdots \end{aligned}$$

Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle \otimes |f(X)\rangle$$

използване
периодичността



$$\begin{aligned}
 &= 2^{-n/2} \left(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle + \dots + |P-1\rangle \otimes |f(P-1)\rangle \right. \\
 &\quad + |P\rangle \otimes |f(P)\rangle \quad + \dots + \quad |2P-1\rangle \otimes |f(P-1)\rangle \\
 &\quad \vdots \\
 &\quad + |KP\rangle \otimes |f(P)\rangle \quad + \dots + \quad |KP-1\rangle \otimes |f(P-1)\rangle \left. \right) \\
 &+
 \end{aligned}$$

Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle \otimes |f(X)\rangle$$

използване
периодичността



$$= 2^{-n/2} \left(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle + \dots + |P-1\rangle \otimes |f(P-1)\rangle \right. \\ \left. + |P\rangle \otimes |f(P)\rangle + \dots + |2P-1\rangle \otimes |f(P-1)\rangle \right. \\ \left. \vdots \right. \\ \left. + |KP\rangle \otimes |f(P)\rangle + \dots + |KP-1\rangle \otimes |f(P-1)\rangle \right)$$

+ remainder $\leftarrow R = N - KP$ на брой остатъчни членове

Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle \otimes |f(X)\rangle$$

$$= 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} |X_C + LP\rangle \otimes |C\rangle + \text{remainder}$$

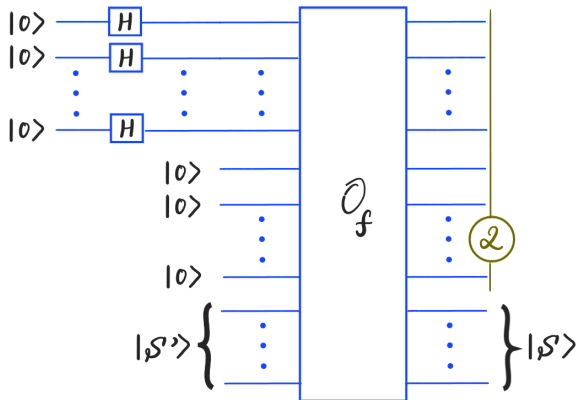
Преработваме :

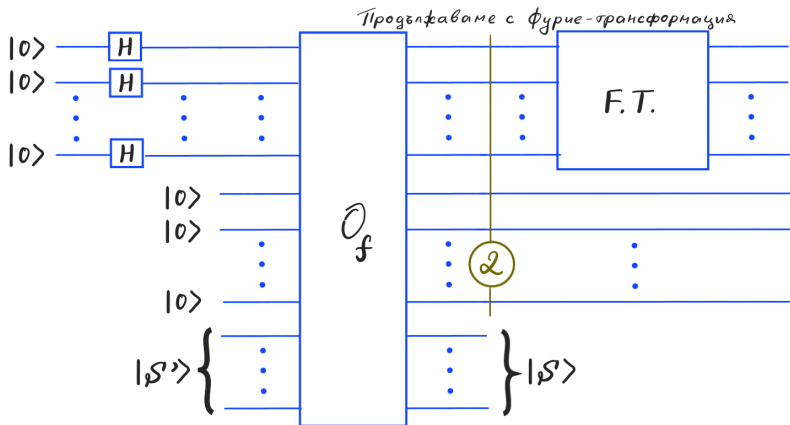
$$\textcircled{2} = 2^{-n/2} \sum_{X=0}^{N-1} |X\rangle \otimes |f(X)\rangle$$

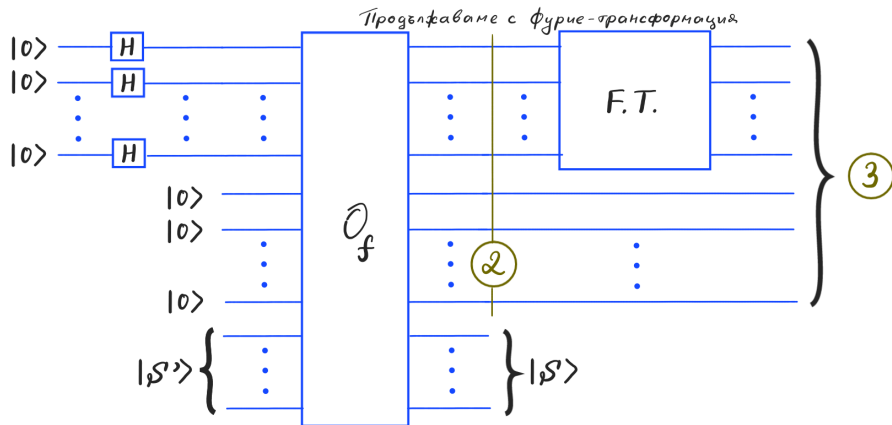
понеже f е биекция върху периода си

$$= 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} |X_C + LP\rangle \otimes |C\rangle + \text{remainder}$$

това е най-малкото неотрицателно решение на
 $f(X) = C$







Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} |X_C + LP\rangle \otimes |C\rangle + \text{remainder}$$

Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} |X_C + LP\rangle \otimes |C\rangle + \text{remainder}$$

↓ F.T.

$$\textcircled{3} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \text{F.T.}(|X_C + LP\rangle) \otimes |C\rangle + \text{remainder}'$$

Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} |X_C + LP\rangle \otimes |C\rangle + \text{remainder}$$

↓ F.T.

$$\textcircled{3} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \text{F.T.}(|X_C + LP\rangle) \otimes |C\rangle + \text{remainder}'$$

По определение : $\text{F.T.}(|X\rangle) = 2^{-N/2} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X \bar{Y}\right) |Y\rangle$

Преработваме :

$$\textcircled{2} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} |X_C + LP\rangle \otimes |C\rangle + \text{remainder}$$

↓ F.T.

$$\textcircled{3} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \text{F.T.}(|X_C + LP\rangle) \otimes |C\rangle + \text{remainder}'$$

тук ще я определим
с обратно разчитане
на битовете на Y

По определение : $\text{F.T.}(|X\rangle) = 2^{-n/2} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X \bar{Y}\right) |Y\rangle$

Преработваме :

$$\textcircled{3} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \text{F.T.}(|X_C + LP\rangle) \otimes |C\rangle + \text{remainder},$$

По определение : $\text{F.T.}(|X\rangle) = 2^{-n/2} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X \bar{Y}\right) |Y\rangle$

Преработваме :

$$\textcircled{3} = 2^{-n/2} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \text{F.T.}(|X_C + LP\rangle) \otimes |C\rangle + \text{remainder'}$$

По определение : $\text{F.T.}(|X\rangle) = 2^{-N/2} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X \bar{Y}\right) |Y\rangle$

Преработваме :

$$\textcircled{3} \approx 2^{-n} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} (X_C + LP) \bar{Y}\right) |Y\rangle \otimes |C\rangle$$

Преработваме :

$$\begin{aligned}
 \textcircled{3} &\approx 2^{-n} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} (X_C + LP) \bar{Y}\right) |Y\rangle \otimes |C\rangle \\
 &= 2^{-n} \sum_{C=0}^{P-1} \sum_{Y=0}^{N-1} \sum_{L=0}^{K-1}
 \end{aligned}$$

Преработваме :

$$\begin{aligned}
 \textcircled{3} &\approx 2^{-n} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} (X_C + LP) \bar{Y}\right) |Y\rangle \otimes |C\rangle \\
 &= 2^{-n} \sum_{C=0}^{P-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X_C \bar{Y}\right) \sum_{L=0}^{K-1} \exp\left(\frac{2\pi i}{N} P \bar{Y}\right)^L |Y\rangle \otimes |C\rangle
 \end{aligned}$$

Преработваме :

$$\begin{aligned}
 \textcircled{3} &\approx 2^{-n} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} (X_C + LP) \bar{Y}\right) |Y\rangle \otimes |C\rangle \\
 &= 2^{-n} \sum_{C=0}^{P-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X_C \bar{Y}\right) \underbrace{\sum_{L=0}^{K-1} \exp\left(\frac{2\pi i}{N} P \bar{Y}\right)^L}_{\frac{e^{\frac{2\pi i}{N} P \bar{Y} K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1}} |Y\rangle \otimes |C\rangle
 \end{aligned}$$

Преработваме :

$$\begin{aligned}
 \textcircled{3} &\approx 2^{-n} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} (X_C + LP) \bar{Y}\right) |Y\rangle \otimes |C\rangle \\
 &= 2^{-n} \sum_{C=0}^{P-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X_C \bar{Y}\right) \underbrace{\sum_{L=0}^{K-1} \exp\left(\frac{2\pi i}{N} P \bar{Y}\right)^L}_{\frac{e^{\frac{2\pi i}{N} P \bar{Y} K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1}} |Y\rangle \otimes |C\rangle
 \end{aligned}$$

Преработваме :

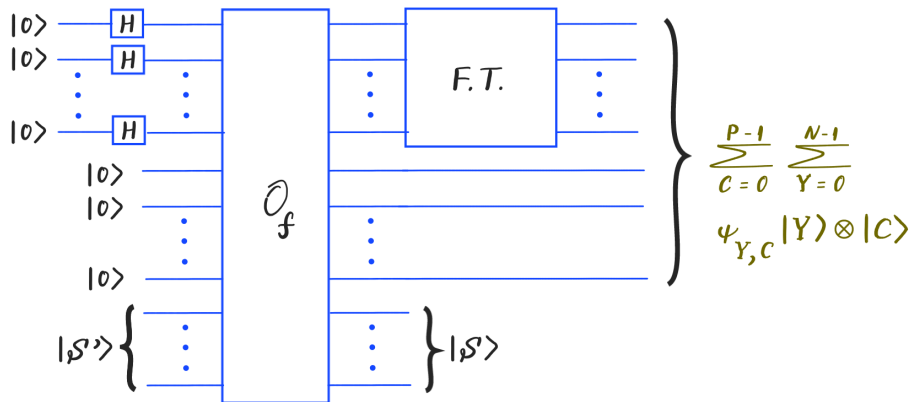
$$\begin{aligned}
 \textcircled{3} &\approx 2^{-n} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} (X_C + LP) \bar{Y}\right) |Y\rangle \otimes |C\rangle \\
 &= 2^{-n} \sum_{C=0}^{P-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X_C \bar{Y}\right) \frac{e^{\frac{2\pi i}{N} P \bar{Y} K - 1}}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1} |Y\rangle \otimes |C\rangle
 \end{aligned}$$

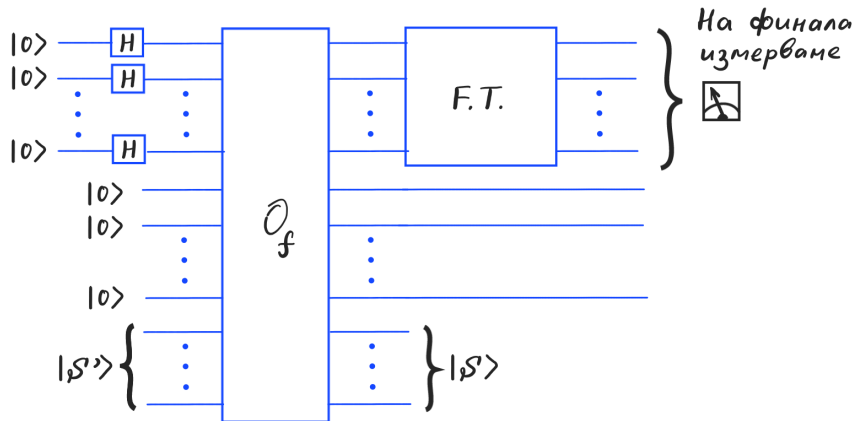
Преработваме :

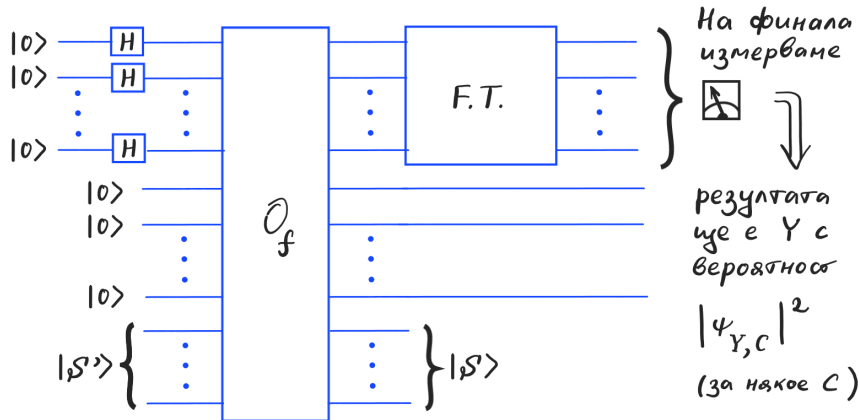
$$\begin{aligned}
 \textcircled{3} &\approx 2^{-n} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} (X_C + LP) \bar{Y}\right) |Y\rangle \otimes |C\rangle \\
 &= 2^{-n} \sum_{C=0}^{P-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X_C \bar{Y}\right) \underbrace{\frac{e^{\frac{2\pi i}{N} P \bar{Y} K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1}}_{=: \psi_{Y,C} \text{ } 2^n} |Y\rangle \otimes |C\rangle
 \end{aligned}$$

Преработваме :

$$\begin{aligned}
 \textcircled{3} &\approx 2^{-n} \sum_{C=0}^{P-1} \sum_{L=0}^{K-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} (X_C + LP) \bar{Y}\right) |Y\rangle \otimes |C\rangle \\
 &= 2^{-n} \sum_{C=0}^{P-1} \sum_{Y=0}^{N-1} \exp\left(\frac{2\pi i}{N} X_C \bar{Y}\right) \underbrace{\frac{e^{\frac{2\pi i}{N} P \bar{Y} K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1}}_{=: \psi_{Y,C} 2^n} |Y\rangle \otimes |C\rangle \\
 &= \sum_{C=0}^{P-1} \sum_{Y=0}^{N-1} \psi_{Y,C} |Y\rangle \otimes |C\rangle
 \end{aligned}$$







Анализ кога е максимална вероятността

при предположение, че
остатък

$$R = N - PK \ll N (= 2^n)$$

Анализ кога е максимална вероятността

$$|\psi_{Y,C}|^2 = \left| \frac{e^{\frac{2\pi i}{N} P \bar{Y}_K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1} \right|^2$$

при предположение, че
остатък

$$R = N - PK \ll N (= 2^n)$$

Анализ кога е максимална вероятността

$$|\psi_{Y,C}|^2 = \left| \frac{e^{\frac{2\pi i}{N} P \bar{Y}_K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1} \right|^2$$

↙ не зависи
от C

при предположение, че
остатък

$$R = N - PK \ll N (= 2^n)$$

Анализ кога е максимална вероятността

$$|\psi_{Y,C}|^2 = \left| \frac{e^{\frac{2\pi i}{N} P \bar{Y} K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1} \right|^2 = \frac{\sin^2\left(\pi \frac{P \bar{Y} K}{N}\right)}{\sin^2\left(\pi \frac{P \bar{Y}}{N}\right)}$$

не зависи
от C

при предположение, че
остатък

$$R = N - PK \ll N (= 2^n)$$

Анализ кога е максимална вероятността

при предположение, че
остатък

$$|\psi_{Y,C}|^2 = \left| \frac{e^{\frac{2\pi i}{N} P \bar{Y} K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1} \right|^2 = \frac{\sin^2\left(\pi \frac{P \bar{Y} K}{N}\right)}{\sin^2\left(\pi \frac{P \bar{Y}}{N}\right)}$$

↙ не зависи
от C

Условието е приблизително анулиране на знаменателя

$$R = N - PK \ll N (= 2^n)$$

Анализ кога е максимална вероятността

при предположение, че
остатък

$$|\psi_{Y,C}|^2 = \left| \frac{e^{\frac{2\pi i}{N} P \bar{Y} K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1} \right|^2 = \frac{\sin^2\left(\pi \frac{P \bar{Y} K}{N}\right)}{\sin^2\left(\pi \frac{P \bar{Y}}{N}\right)}$$

$$R = N - PK \ll N (= 2^n)$$

↙ не зависи
от C

Условието е приблизително анулиране на знаменателя

за което е нужно $\frac{P}{N/\bar{Y}}$ да е $\approx$ цяло число $Q (\Rightarrow \text{делител на } P)$.

Анализ кога е максимална вероятността

при предположение, че
остатъка

$$|\psi_{Y,C}|^2 = \left| \frac{e^{\frac{2\pi i}{N} P \bar{Y} K} - 1}{e^{\frac{2\pi i}{N} P \bar{Y}} - 1} \right|^2 = \frac{\sin^2\left(\pi \frac{P \bar{Y} K}{N}\right)}{\sin^2\left(\pi \frac{P \bar{Y}}{N}\right)}$$

$$R = N - PK \ll N (= 2^n)$$

↙ не зависи
от C

Условието е приблизително анулиране на знаменателя

за което е нужно $\frac{P}{N/\bar{Y}}$ да е $\approx$ цяло число $Q (\Rightarrow \text{делител на } P)$.

(Аналогичен анализ има и в точка 9 на Лекция 10).

Квантова префа на Фурие-трансформацията



Квантова префа на Фурие-трансформацията



Основният изчислителен елемент на представения квантов алгоритъм е дискретната Фурие трансформация.

Квантова мрежа на Фурие-трансформацията



Основният изчислителен елемент на представения квантов алгоритъм е дискретната Фурие трансформация.

От нейната реализация като квантова мрежа (quantum circuit) се определя и изчислителното време: то е пропорционално на броя на използваните елементарни квантови гейтове.

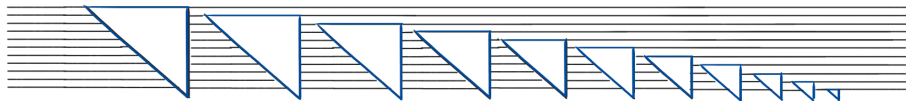
Квантова префа на Фурие-трансформацията



Квантова префа на Фурие-трансформацията



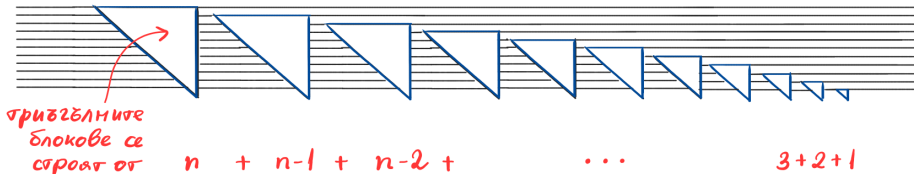
Схематично :



Квантова префа на Фурие-трансформацията



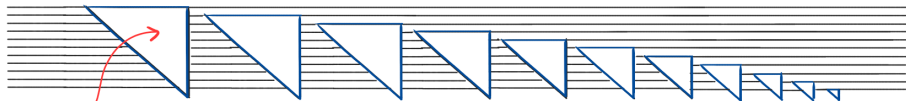
Схематично :



Квантова префа на Фурие-трансформацията



Схематично :



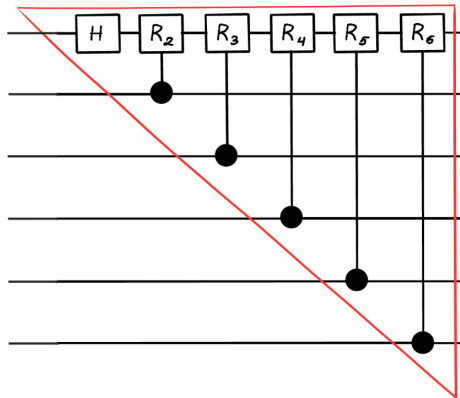
триъгълните
блокове се
сроят от

$$n + n-1 + n-2 + \dots$$

$$3+2+1$$

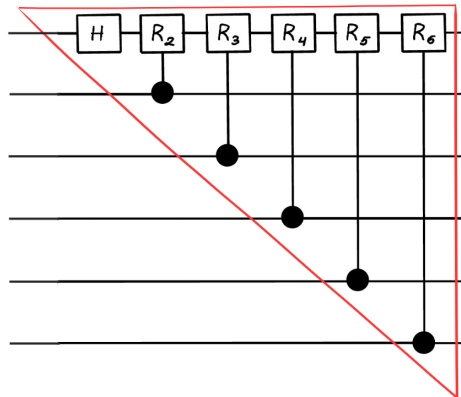
$$= \frac{n(n+1)}{2} \text{ базисни квантови гейта}$$

Всеки триъгълен блок
се строи така :



Всеки триъгълен блок
се строи така :

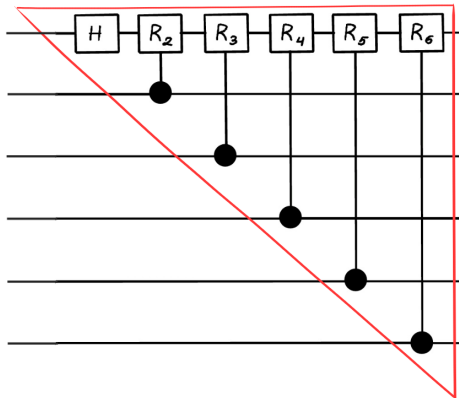
(пример за триъгълния
блок с 6 линии)

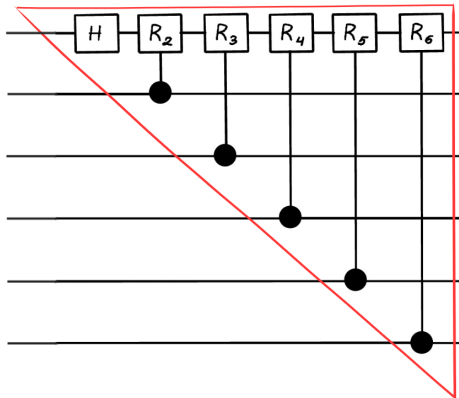


Всеки триъгълен блок
се строи така :

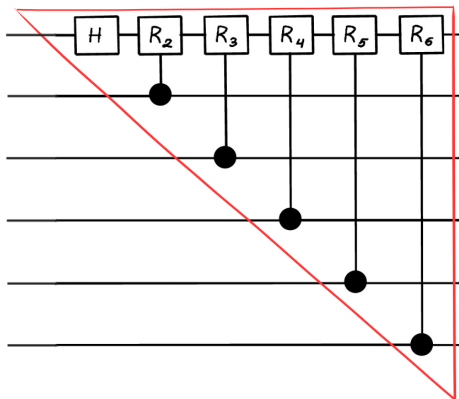
(пример за триъгълния
блок с 6 линии)

където ↘





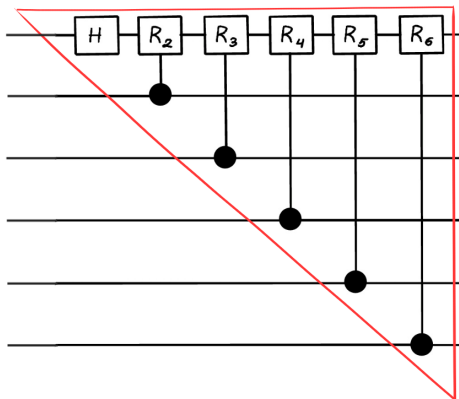
където използваните базисни
гейтове са :



където използваните базисни
гейтове са :

• гейта на Адамар



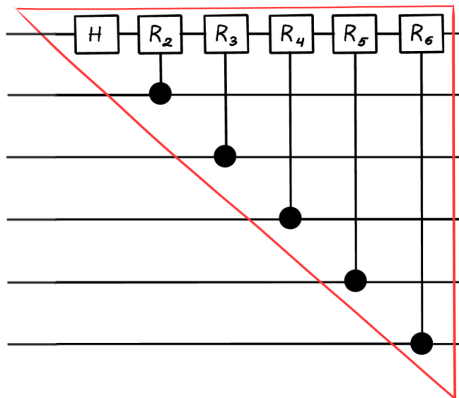


където използваните базисни
гейтове са :

• гейта на Адамар 

Отговаря на
матрицата

$$2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



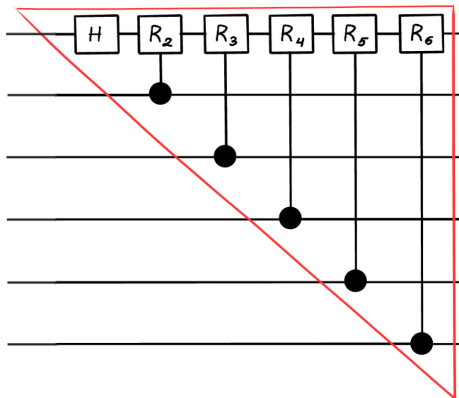
където използваните базисни
гейтове са :

• гейта на Адамар 

Отговаря на
матрицата

$$2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|x\rangle = 2^{-1/2} (|0\rangle + (-1)^x |1\rangle)$$



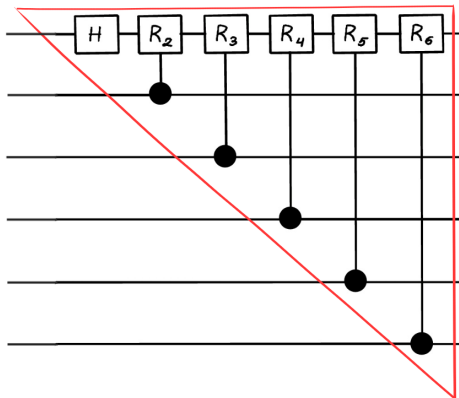
където използваните базисни
гейтове са :

• гейта на Адамар $\boxed{H}$

Отговаря на
матрицата $2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H|x\rangle = 2^{-1/2} (|0\rangle + (-1)^x |1\rangle)$$

$$= 2^{-1/2} \sum_{y=0,1} \exp\left(2\pi i \frac{xy}{2}\right) |y\rangle$$

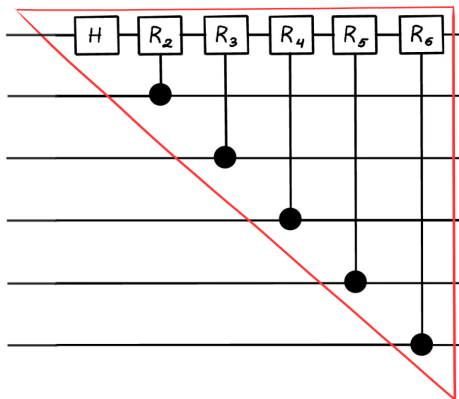


където използваните базисни
гейтове са :

• гейта на Адамар 

$$H|x\rangle = 2^{-1/2} (|0\rangle + (-1)^x |1\rangle)$$

$$= 2^{-1/2} \sum_{y=0,1} \exp\left(2\pi i \frac{xy}{2}\right) |y\rangle$$



където използваните базисни
гейтове са :

• гейта на Адамар $\text{---} \boxed{H} \text{---}$

$$H|x\rangle = 2^{-1/2} (|0\rangle + (-1)^x |1\rangle)$$

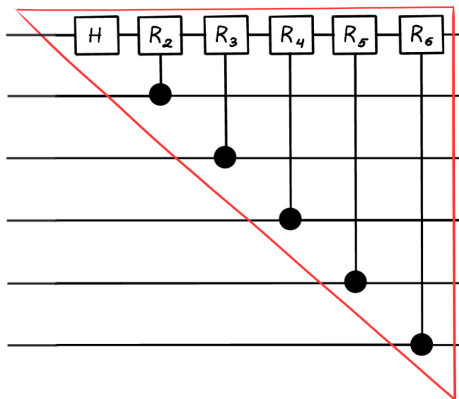
$$= 2^{-1/2} \sum_{y=0,1} \exp\left(2\pi i \frac{xy}{2}\right) |y\rangle$$

$$1 = e^0$$

$$y=0$$

$$y=1$$

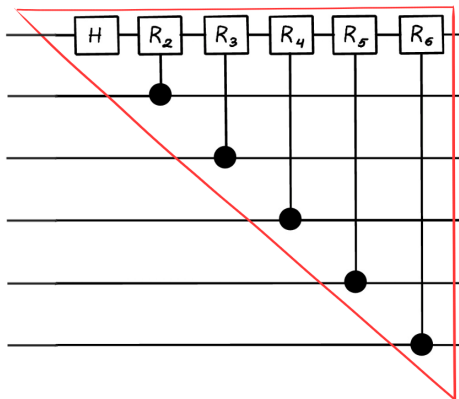
$$\boxed{e^{\frac{2\pi i}{2} x} = (-1)^x}$$



където използваните базисни
гейтове са :

- **гейтове** за всяко $a \in \{1, 2, \dots\}$



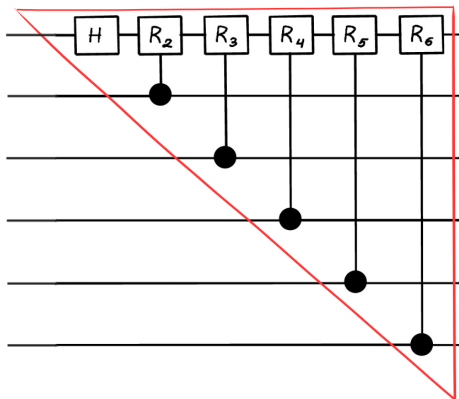


където използваните базисни гейтове са :

- **гейтове** за всяко $a \in \{1, 2, \dots\}$



алтернативно
означение

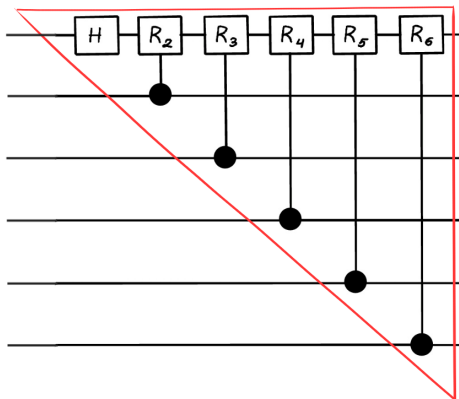


където използваните базисни гейтове са :

- **гейтове** за всяко $a \in \{1, 2, \dots\}$



} алтернативно
означение
(тип "условна
операция")

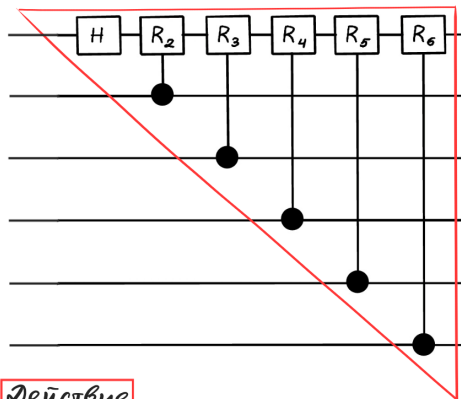


където използваните базисни гейтове са :

- **гейтове** за всяко $a \in \{1, 2, \dots\}$

$\left. \begin{array}{l} \text{---} [R_a] \text{---} \\ \text{---} [R_a] \text{---} \end{array} \right\}$ алтернативно
 означение
 (тип "условна
 операция")

$$R_a |xy\rangle := \exp\left(2\pi i \frac{xy}{2^a}\right) |xy\rangle$$



$$|x_1\rangle \xrightarrow{\text{H}} 2^{-1/2} (|0\rangle + (-1)^{x_1} |1\rangle)$$

$$|x_2\rangle \longrightarrow |x_2\rangle$$

$$|x_3\rangle \longrightarrow |x_3\rangle$$

$$|x_4\rangle \longrightarrow |x_4\rangle$$

$$|x_5\rangle \longrightarrow |x_5\rangle$$

$$|x_6\rangle \longrightarrow |x_6\rangle$$

Действие

$$|x_1\rangle \xrightarrow{\text{H}} 2^{-1/2} (|0\rangle + e^{2\pi i \frac{x_1}{2}} |1\rangle)$$

$$|x_2\rangle \longrightarrow |x_2\rangle$$

$$|x_3\rangle \longrightarrow |x_3\rangle$$

$$|x_4\rangle \longrightarrow |x_4\rangle$$

$$|x_5\rangle \longrightarrow |x_5\rangle$$

$$|x_6\rangle \longrightarrow |x_6\rangle$$

Действие

$$|x_1\rangle \xrightarrow{\text{H}} 2^{-1/2} (|0\rangle + e^{2\pi i [0.x_1]_2} |1\rangle)$$

$$|x_2\rangle \longrightarrow |x_2\rangle$$

$$|x_3\rangle \longrightarrow |x_3\rangle$$

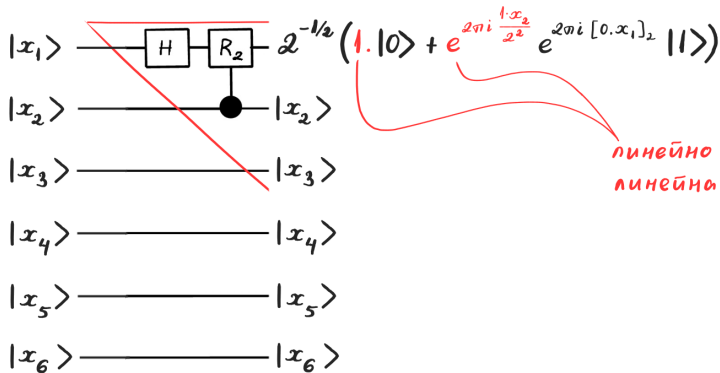
$$|x_4\rangle \longrightarrow |x_4\rangle$$

$$|x_5\rangle \longrightarrow |x_5\rangle$$

$$|x_6\rangle \longrightarrow |x_6\rangle$$

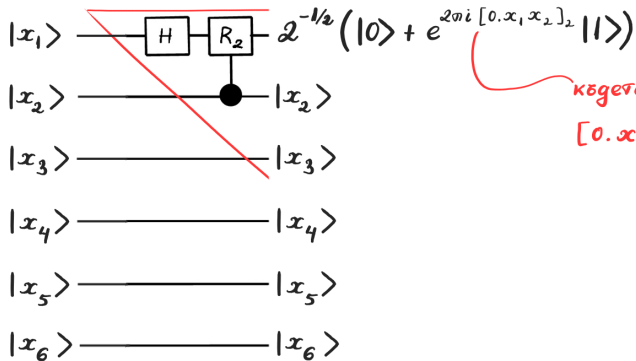
където това е двоична дроб
 $[0.x_1]_2 := x_1 2^{-1}$

Действие



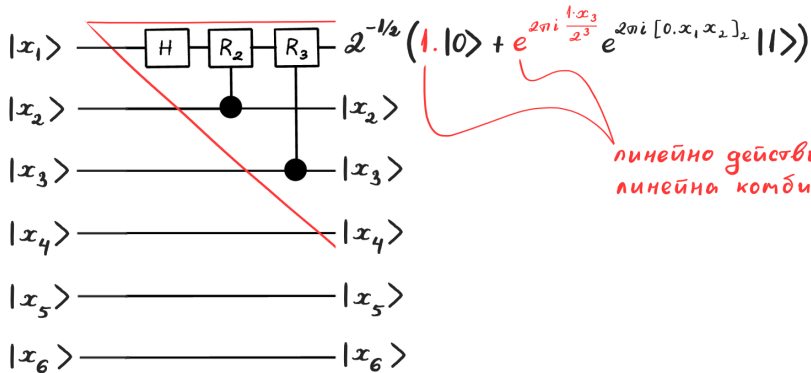
линейно действие върху
линейна комбинация

Действие



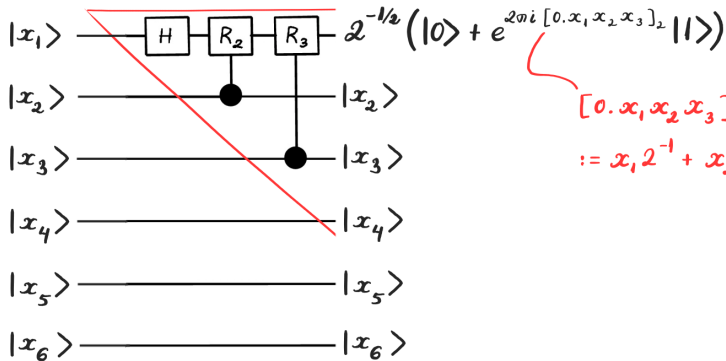
където това е двоична дроб
 $[0.x_1 x_2]_2 := x_1 2^{-1} + x_2 2^{-2}$

Действие



линейно действие върху
линейна комбинация

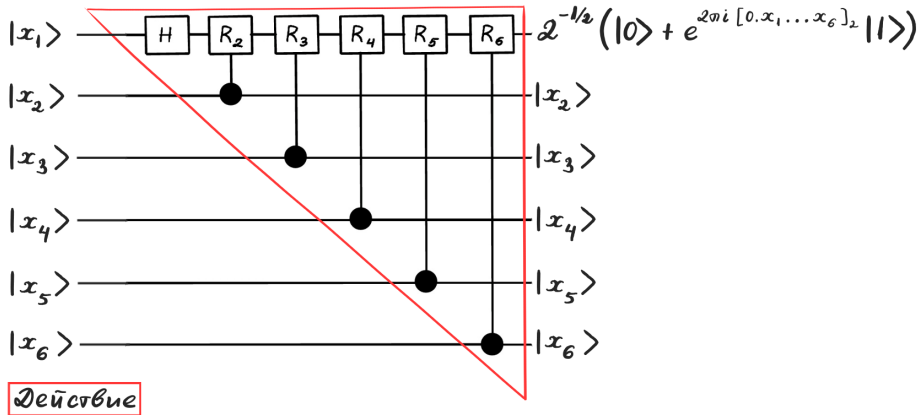
Действие



$$[0.x_1 x_2 x_3]_2$$

$$:= x_1 2^{-1} + x_2 2^{-2} + x_3 2^{-3}$$

Действие



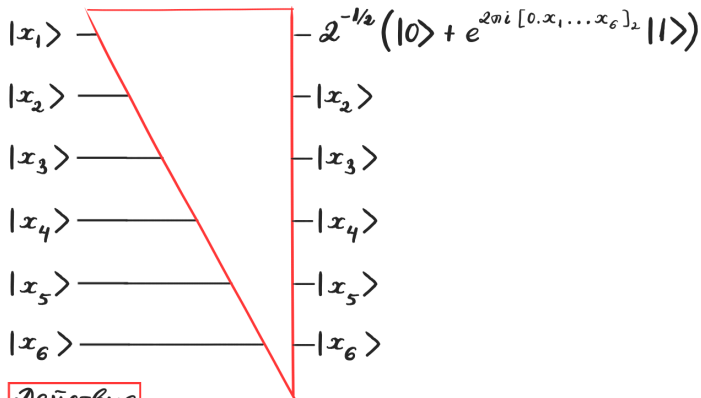
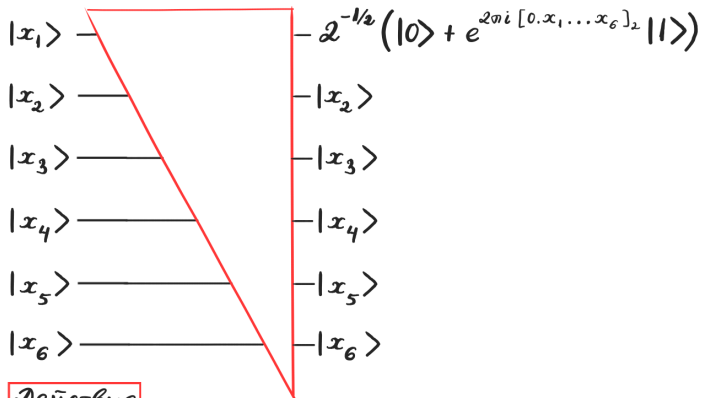
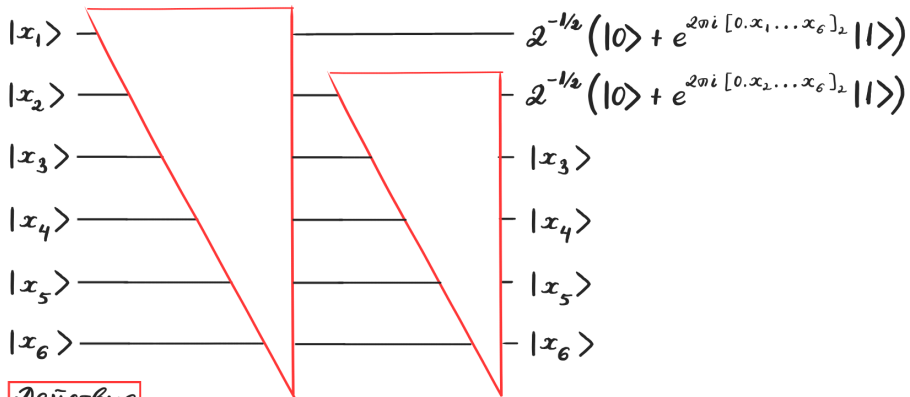


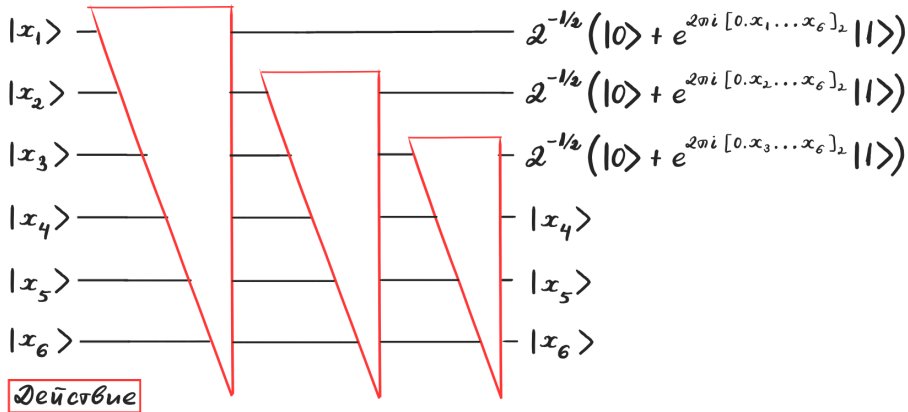
Diagram illustrating a quantum operation (action) on a system of qubits $|x_1\rangle, |x_2\rangle, |x_3\rangle, |x_4\rangle, |x_5\rangle, |x_6\rangle$. The operation is represented by a red triangle and a curly brace, leading to the expression:

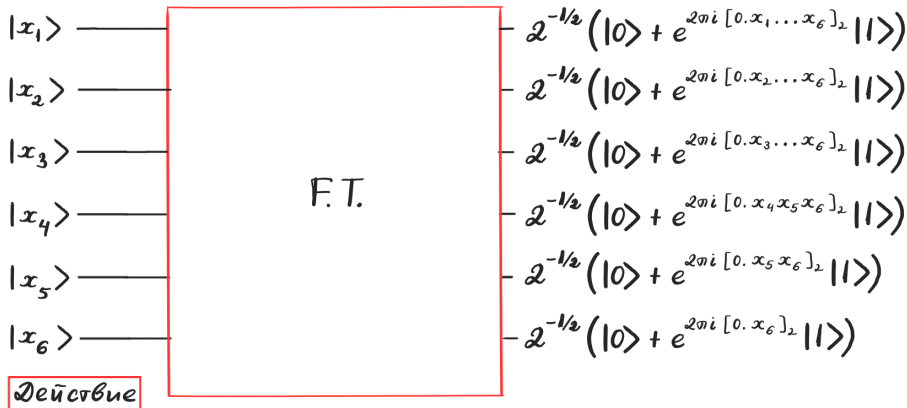
$$2^{-1/2} (|0\rangle + e^{2\pi i [0.x_1 \dots x_6]_2} |1\rangle) \otimes |x_2 \dots x_6\rangle$$

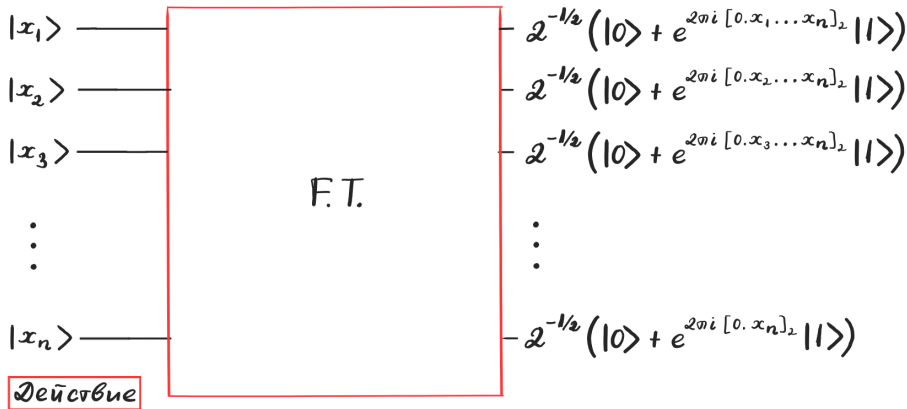
Действие











$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

$\Downarrow$ F.T.

$$2^{-n/2} (|0\rangle + e^{2\pi i [0.x_1 \dots x_n]_2} |1\rangle) \otimes (|0\rangle + e^{2\pi i [0.x_2 \dots x_n]_2} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i [0.x_3 \dots x_n]_2} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i [0.x_n]_2} |1\rangle)$$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

↓ F.T.

$$2^{-n/2} (|0\rangle + e^{2\pi i [0.x_1 \dots x_n]_2} |1\rangle) \otimes (|0\rangle + e^{2\pi i [0.x_2 \dots x_n]_2} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i [0.x_3 \dots x_n]_2} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i [0.x_n]_2} |1\rangle)$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

$\downarrow$ F.T.

$$2^{-n/2} (|0\rangle + e^{2\pi i [0.x_1 \dots x_n]_2} |1\rangle) \otimes (|0\rangle + e^{2\pi i [0.x_2 \dots x_n]_2} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i [0.x_3 \dots x_n]_2} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i [0.x_n]_2} |1\rangle)$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

$\Downarrow$ F.T.

$$2^{-n/2} (|0\rangle + e^{2\pi i \bar{X}/2^n} |1\rangle) \otimes (|0\rangle + e^{2\pi i [0.x_2 \dots x_n]_2} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i [0.x_3 \dots x_n]_2} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i [0.x_n]_2} |1\rangle)$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

$\Downarrow$ F.T.

$$2^{-n/2} (|0\rangle + e^{2\pi i \bar{X}/2^n} |1\rangle) \otimes (|0\rangle + e^{2\pi i \bar{X}/2^{n-1}} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i [0.x_3 \dots x_n]_2} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i [0.x_n]_2} |1\rangle)$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

$\Downarrow$ F.T.

$$2^{-n/2} (|0\rangle + e^{2\pi i \bar{X}/2^n} |1\rangle) \otimes (|0\rangle + e^{2\pi i \bar{X}/2^{n-1}} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i \bar{X}/2^{n-2}} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i [0, x_n]_2} |1\rangle)$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}_{\downarrow \text{F.T.}}$$

$\downarrow \text{F.T.}$

$$2^{-n/2} (|0\rangle + e^{2\pi i \bar{X}/2^n} |1\rangle) \otimes (|0\rangle + e^{2\pi i \bar{X}/2^{n-1}} |1\rangle) \\ \otimes (|0\rangle + e^{2\pi i \bar{X}/2^{n-2}} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i \bar{X}/2} |1\rangle)$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}_{\downarrow \text{F.T.}}$$

$\downarrow \text{F.T.}$

$$2^{-n/2} (|0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}} |1\rangle) \otimes (|0\rangle + e^{\frac{2\pi i}{2^n} \bar{X} 2} |1\rangle) \otimes (|0\rangle + e^{\frac{2\pi i}{2^n} \bar{X} 2^2} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{\frac{2\pi i}{2^n} \bar{X} 2^{n-1}} |1\rangle)$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

$\downarrow$ F.T.

$$2^{-n/2} \left(e^0 |0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}(1 \cdot 2^0)} |1\rangle \right) \otimes \left(e^0 |0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}(1 \cdot 2^1)} |1\rangle \right) \\ \otimes \left(e^0 |0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}(1 \cdot 2^2)} |1\rangle \right) \otimes \dots \otimes \left(e^0 |0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}(1 \cdot 2^{n-1})} |1\rangle \right)$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}_{\downarrow \text{F.T.}}$$

$\downarrow \text{F.T.}$

$$2^{-n/2} \left(e^0 |0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}(1 \cdot 2^0)} |1\rangle \right) \otimes \left(e^0 |0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}(1 \cdot 2^1)} |1\rangle \right) \\ \otimes \left(e^0 |0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}(1 \cdot 2^2)} |1\rangle \right) \otimes \dots \otimes \left(e^0 |0\rangle + e^{\frac{2\pi i}{2^n} \bar{X}(1 \cdot 2^{n-1})} |1\rangle \right)$$

↑ Разкриваме скобите: получаваме 2^n събираеми, в които ако сме избрали в първия член лявото събираемо пишем $y_1 = 0$, а ако десното - $y_1 := 1$; за втория член имаме $y_2 = 0$ или 1 и т.н.

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

↓ F.T.

$$2^{-n/2} \sum_{y_1, y_2, y_3, \dots, y_n=0}^1 e^{\frac{2\pi i}{2^n} \bar{X}(y_1 2^0)} e^{\frac{2\pi i}{2^n} \bar{X}(y_2 2^1)} e^{\frac{2\pi i}{2^n} \bar{X}(y_3 2^2)} \dots e^{\frac{2\pi i}{2^n} \bar{X}(y_n 2^{n-1})} \\ \times |y_1\rangle \otimes |y_2\rangle \otimes |y_3\rangle \otimes \dots \otimes |y_n\rangle$$

↑ Разкриваме скобите: получаваме 2^n събираеми, в които ако сме избрали в първия член лявото събираемо пишем $y_1 = 0$, а ако десното - $y_1 := 1$; за втория член имаме $y_2 = 0$ или 1 и т.н.

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$
 $\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

↓ F.T.

$$2^{-n/2} \sum_{y_1, y_2, y_3, \dots, y_n=0}^1 e^{\frac{2\pi i}{2^n} \bar{X}(y_1 2^0)} e^{\frac{2\pi i}{2^n} \bar{X}(y_2 2^1)} e^{\frac{2\pi i}{2^n} \bar{X}(y_3 2^2)} \dots e^{\frac{2\pi i}{2^n} \bar{X}(y_n 2^{n-1})} \\ \times |y_1\rangle \otimes |y_2\rangle \otimes |y_3\rangle \otimes \dots \otimes |y_n\rangle$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \cdots \otimes |x_n\rangle}$$

↓ F.T.

$$2^{-n/2} \sum_{y_1, y_2, y_3, \dots, y_n = 0}^1 e^{\frac{2\pi i}{2^n} \bar{X}(y_1 2^0 + y_2 2^1 + y_3 2^2 + \cdots + y_n 2^{n-1})} \times |y_1\rangle \otimes |y_2\rangle \otimes |y_3\rangle \otimes \cdots \otimes |y_n\rangle$$

Нека $X := x_1 + x_2 2^1 + \cdots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n 2^0$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \cdots \otimes |x_n\rangle}$$

↓ F.T.

$$2^{-n/2} \sum_{y_1, y_2, y_3, \dots, y_n=0}^1 e^{\frac{2\pi i}{2^n} \bar{X}(y_1 2^0 + y_2 2^1 + y_3 2^2 + \cdots + y_n 2^{n-1})} \\ \times |y_1\rangle \otimes |y_2\rangle \otimes |y_3\rangle \otimes \cdots \otimes |y_n\rangle$$

Нека $X := x_1 + x_2 2^1 + \cdots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n 2^0$

$Y := y_1 + y_2 2^1 + \cdots + y_n 2^{n-1}$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

↓ F.T.

$$2^{-n/2} \sum_{y_1, y_2, y_3, \dots, y_n = 0}^1 e^{\frac{2\pi i}{2^n} \bar{X} Y}$$

$$\times |y_1\rangle \otimes |y_2\rangle \otimes |y_3\rangle \otimes \dots \otimes |y_n\rangle$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$Y := y_1 + y_2 2^1 + \dots + y_n 2^{n-1}$

$$\underbrace{|x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \dots \otimes |x_n\rangle}$$

↓ F.T.

$$2^{-n/2} \sum_{y_1, y_2, y_3, \dots, y_n = 0}^1 e^{\frac{2\pi i}{2^n} \bar{X} Y} |y_1\rangle \otimes |y_2\rangle \otimes |y_3\rangle \otimes \dots \otimes |y_n\rangle$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$Y := y_1 + y_2 2^1 + \dots + y_n 2^{n-1}$

$$\begin{array}{c}
 |X\rangle \\
 \downarrow \text{F.T.} \\
 2^{-n/2} \sum_{Y=0}^{2^n-1} e^{\frac{2\pi i}{2^n} \bar{X}Y} |Y\rangle
 \end{array}$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$Y := y_1 + y_2 2^1 + \dots + y_n 2^{n-1}$

$|X\rangle$ $\downarrow \text{F.T.}$

$$2^{-n/2} \sum_{Y=0}^{2^n-1} e^{\frac{2\pi i}{2^n} \bar{X}Y} |Y\rangle$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$ $\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$ $Y := y_1 + y_2 2^1 + \dots + y_n 2^{n-1}$

Всъщност, ние използвахме друга формула:

$$|X\rangle \xrightarrow{\text{F.T.}} 2^{-n/2} \sum_{Y=0}^{N-1} e^{\frac{2\pi i}{N} X\bar{Y}} |Y\rangle$$

$|X\rangle$ $\downarrow \text{F.T.}$

$$2^{-n/2} \sum_{Y=0}^{2^n-1} e^{\frac{2\pi i}{2^n} \bar{X}Y} |Y\rangle$$

Нека $X := x_1 + x_2 2^1 + \dots + x_n 2^{n-1}$

$\bar{X} := x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n 2^0$

$Y := y_1 + y_2 2^1 + \dots + y_n 2^{n-1}$

Всъщност, ние използвахме друга формула:

$$|X\rangle \xrightarrow{\text{F.T.}} 2^{-n/2} \sum_{Y=0}^{N-1} e^{\frac{2\pi i}{N} X\bar{Y}} |Y\rangle$$

- не е проблем: просто трябва обрнем мрежата по вертикала.

И така, начерихме мрежа за Фурие трансформацията.

И така, намерихме мрежа за Фурие трансформацията.

Упражнение (извън основния материал).

Сравнете с последната точка на Лекция 10, където работата на мрежата е дадена върху координатите на вектор, докато тук е пресмятана върху базисен вектор.

И така, намерихме мрежа за Фурие трансформацията.

Упражнение (извън основния материал).

Сравнете с последната точка на Лекция 10, където работата на мрежата е дадена върху координатите на вектор, докато тук е пресмятана върху базисен вектор.

От линейната алгебра знаем, че ако $A(e_j) := \sum_{k=1}^N a_{jk} e_k$
- трансформация на базис

И така, намерихме мрежа за Фурие трансформацията.

Упражнение (извън основния материал).

Сравнете с последната точка на Лекция 10, където работата на мрежата е дадена върху координатите на вектор, докато тук е пресмятана върху базисен вектор.

От линейната алгебра знаем, че ако $A(e_j) := \sum_{k=1}^N \overbrace{a_{jk}}^{\text{матрица}} e_j$
- трансформация на базис

И така, намерихме мрежа за Фурие трансформацията.

Упражнение (извън основния материал).

Сравнете с последната точка на Лекция 10, където работата на мрежата е дадена върху координатите на вектор, докато тук е пресмятана върху базисен вектор.

От линейната алгебра знаем, че ако $A(e_j) := \sum_{k=1}^N \overbrace{a_{jk}}^{\text{матрица}} e_j$
- трансформация на базис

тогава $y_k = \sum_{j=1}^N a_{jk} x_j$ - трансформация на координати

И така, намерихме мрежа за Фурие трансформацията.

Упражнение (извън основния материал).

Сравнете с последната точка на Лекция 10, където работата на мрежата е дадена върху координатите на вектор, докато тук е пресмятана върху базисен вектор.

От линейната алгебра знаем, че ако $A(e_j) := \sum_{k=1}^N \overbrace{a_{jk}}^{\text{матрица}} e_k$
- трансформация на базис

тогава $y_k = \sum_{j=1}^N a_{jk} x_j$ - трансформация на координати

Затова в лекция 10 посоката на изпълнение вървеше на обратно.