Въпрос: нека сист. е в чисто състояние с вектор $\Psi \in \mathbb{C}^N$, $\|\Psi\| = 1$. Нека $e_1, \dots, e_N$ – о.н.б. (напр., стандартния).

$$\Psi = \psi_1 e_1 + \dots + \psi_N e_N$$

$$\underbrace{|\psi_1|^2} + \dots + |\psi_N|^2 \left(= \|\Psi\|^2\right) = 1$$

$$\underbrace{|\langle \Psi | e_1 \rangle|^2} = p_1, \dots$$

вероятността за изход, т.е.

$p_1, \dots, p_N$ – вероятности, $p_1 + \dots + p_N = 1$

$\psi_j = x_j + i y_j \quad (j = 1, \dots, N)$

∟ $2N$ - реални числа, 1 - уравнение

$$x_1^2 + y_1^2 + \dots + x_N^2 + y_N^2 = 1$$

– остават $2N-1$ - параметри

НО: $\Psi' = e^{i\alpha} \Psi$ - това определя същото състояние

$\Rightarrow$ можем да направим $\psi_1 \in \mathbb{R}$ (в частност, може да се окаже $\psi_1 = 0$)

$y_1 = 0$ – остават $\boxed{2N-2}$

свободните параметри на състоянието

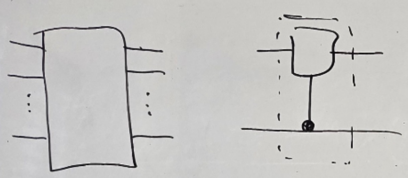
А един експеримент ни дава $N-1$ - параметъра $p_1, \dots, p_{N-1}$

Нужен ни е подходящ втори експеримент $f_1, \dots, f_N$ – о.н.б.

с вероятности $q_1 + \dots + q_N = 1$

$$q_j = |\langle \Psi | f_j \rangle|^2$$

$\Rightarrow \quad 2N - 2 = N - 1 + N - 1$



$e_0, e_1 \in \mathbb{C}^2$ - о.н.б.

$e_0 = \begin{pmatrix}1\\0\end{pmatrix}$, $e_1 = \begin{pmatrix}0\\1\end{pmatrix}$

$|e_0\rangle = e_0$

$|e_1\rangle = e_1$

$$|0\rangle := \begin{pmatrix}1\\0\end{pmatrix} \neq 0$$

$$|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$$

$$|\Psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$$

$\mathbb{C}^2 \otimes \mathbb{C}^2$ - о.н.б. $(j,k=0,1)$

$$|j\rangle \otimes |k\rangle \equiv |j\rangle|k\rangle \equiv |j,k\rangle$$

произведение на Кронекер.

$$\underbrace{\underset{k\times l}{\begin{pmatrix} a_{11} & \cdots & a_{1l} \\ \vdots & A & \vdots \\ a_{k1} & \cdots & a_{kl}\end{pmatrix}} \otimes \underset{n\times m}{\begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & B & \vdots \\ b_{n1} & \cdots & b_{nm}\end{pmatrix}}}_{(kn)\times(lm)} =$$

$$= \left(\begin{array}{c|c|c} a_{11}B & \cdots & a_{1l}B \\ \hline \vdots & \ddots & \vdots \\ \hline a_{k1}B & \cdots & a_{kl}B \end{array}\right)$$

Свойства на тенз. пр-е (по Кронек.)

1) $(A\otimes B)(C\otimes D) = (AC)\otimes(BD)$

матрично, при условие, че съотв. матричното умножение

2) $(A\otimes B)^{\overset{*}{T}} = A^{\overset{*}{T}} \otimes B^{\overset{*}{T}}$

3) асоциативност:

$$(A\otimes B)\otimes C = A\otimes(B\otimes C)$$

Твърдение

За тензорното произведение $e_{j_{n-1}}\otimes\cdots\otimes e_{j_0}$ на стандартните о.н.б. в $\mathbb{C}^2$ - на n-та тенз. ст.:

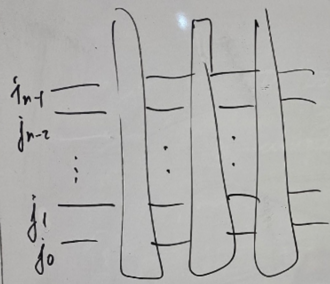
$$\mathbb{C}^2\otimes\cdots\otimes\mathbb{C}^2 = \mathbb{C}^{\underbrace{2\cdot 2\cdots 2}_{n}} = \mathbb{C}^{2^n}$$

$(N := 2^n)$ - резултатът е отново вектор от стандарт. о.н.б. в $\mathbb{C}^N$ - и той е с номер

$$\ell := j_{n-1}2^{n-1} + j_{n-2}2^{n-2} + \dots + j_1 2^1 + j_0 2^0$$

$$= [j_{n-1}\dots j_1 j_0]_2$$

$$\ell \in \{0,1,\dots,2^n-1\}$$



logical circuit "верига" схема

classical quantum

Това което представя логическата схема е изчисляване на булеви функции

$$y_1 = F_1(x_1,\dots,x_n)$$
$$\vdots$$
$$y_m = F_m(x_1,\dots,x_n)$$

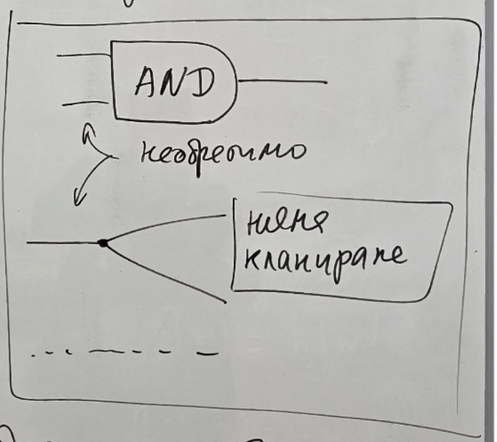
x_j, y_k – булеви променливи $(0,1)$

$$\underline{\underline{y}} = \underline{\underline{F}}(\underline{x})$$

Важна особеност на класическите с/у квантовите лог. схеми

НАЙ-ВАЖНО: квантовите са винаги обратими

Напр.:



Само обратимите булеви функции могат да се моделират квантово

Понятието за "алгоритъм" в този подход:

– това е функция

$$\tilde{F} : \mathbb{N} \to \mathbb{N}$$

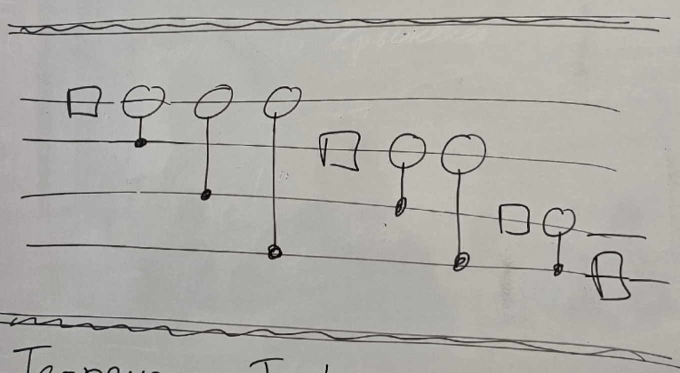
за която има редица от булеви функции

$$\underline{\underline{F}}_1,\ \underline{\underline{F}}_2,\ \dots,\ \underline{\underline{F}}_k,\ \dots$$

с 1 вход, с входа, с 3 входа

ТАКАВА, че

техните логически схеми се пораждат алгоритмично



Теорема на Тофоли:

За всяка булева функция

$$F_1(x_1,\dots,x_n) = y_1$$
$$\vdots$$
$$F_m(x_1,\dots,x_n) = y_m$$

Съществува обратима булева функц.

$$G_1(x_1,\dots,x_{n+k}) = y_1$$
$$\vdots$$
$$G_{m+l}(x_1,\dots,x_{n+k}) = y_{m+l}$$

където $n+k = m+l$

и това е обратима булева ф-я,

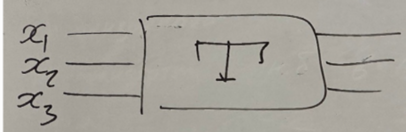
и тя възпроизвежда F

като фиксираме $x_{n+1},\dots,x_{n+k}$ $(=0)$

и не четем $y_{m+1},\dots,y_{m+l}$

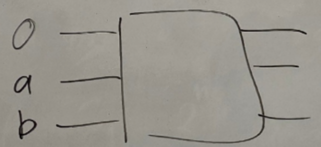
Има алгоритъм, който превежда схемата на F в схема за G и при него сложността не "нараства"

Гейт на Тофоли



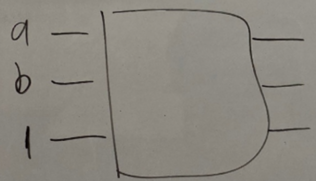
$$y_1 = x_1 + x_2x_3 \mod 2$$
$$y_2 = x_2$$
$$y_3 = x_3$$

$$x_1 = y_1 - x_2x_3 = y_1 - y_2y_3 = y_1 + y_2y_3$$
$$x_2 = y_2$$
$$x_3 = y_3$$



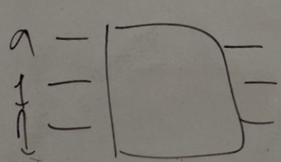
ab = "a и b"

} trash



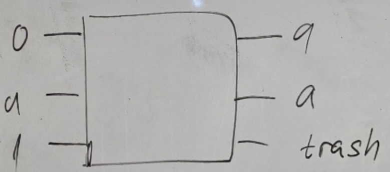
$a+b = a$ XOR b

} trash

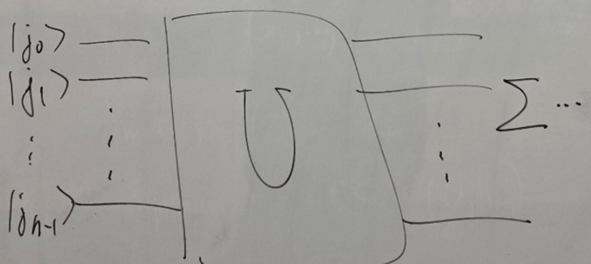


$a+1$ = "не a"

} trash



"Квантуване" на гейта на Тофоли

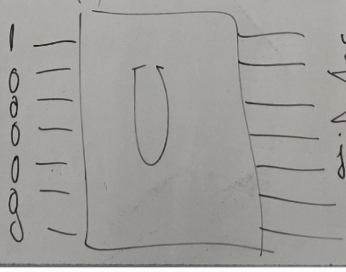


общ квантов гейт — унитарна матрица

	0 (000)	1 (001)	2 (010)	3 (011)	4 (100)	5 (101)	6 (110)	7 (111)
000	1	0	0	0	0	0	0	0
001	0	1	0	0	0	0	0	0
010	0	0	1	0	0	0	0	0
011	0	0	0	0	0	0	0	1
100	0	0	0	0	1	0	0	0
101	0	0	0	0	0	1	0	0
110	0	0	0	0	0	0	1	0
111	0	0	0	1	0	0	0	0

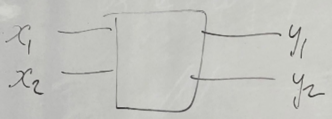
образът на $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$

транспозиция (37)



$$\sum_{j=0}^{7} u_{j,1}\, e_j$$

Забележка:



— всички обратими булеви функции "2 → 2" са "линейно-афинни" (нехомог.) в аритметиката по mod 2

— док. – с проверка

$$(2^2)^{2^2} = 4^4 = 256 \text{ всички}$$

$$(2^2)! = 4! = 24 \text{ обратими}$$

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix}$$

$$x_1, x_2, y_1, y_2, \underbrace{a, b, c, d, u, v}_{\text{параметри}} \in \mathbb{Z}_2$$

$$2^6 = 64$$

— значи ще има дубляж

(00), (01), (10), (11)

( ) ( ) ( ) ( )

Следва:

— лекция 9 – алг. на Гр.

— л. 10 – Д. Фурие Тр.

— л. 11 – алг. на Шор

— л. 12 – кв. маш. на Тюр.

— л. 13 пробл. за шифриране

л. 14, 15 – извънредни