

$$t_{quant} \ll \sqrt{t_{class}}$$

для анн. моря

символ

Конечные модели квант. механики

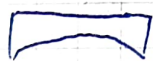
Jaynes-Cummings, Tavis-Cummings, Jay-Cummings-Hubbard, Tavis-C.-H.

осн. квант. ур-е (master equation)

оператора Линдблада: неунитарная динамика. Точн. решение

J.-C.

$H \rightarrow \infty$



опт. полость
(резонатор)

размер ≈ 7 мкм

Сверхотражающие зеркала из ниобия (отр. $\sim 99,9\%$)

1000+ отражений (осциллирует)

мкр. с.: удержание
атома - много

двухуровн. атом (н.д., 3, 4 ур-на и т.д.)

Rb^{85} : сост. 0 или 1 $\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}$

Запускаем атом:

1) поглощение фотона атомом

2) релаксация атома (после переш в полость)

$$1) |m\rangle_{ph} |0\rangle_{at} \rightarrow c' |m-1\rangle |1\rangle_{at}$$

$$2) |m\rangle_{ph} |1\rangle_{at} \rightarrow c'' |m+1\rangle |0\rangle_{at}$$

Рождаются
составные

$|0\rangle_{ph}$ - вакуумное сост.

операторы:

- возбуждения

- релаксация атом.

$$b |1\rangle_{at} = |0\rangle_{at}$$

$$b^+ |0\rangle_{at} = |1\rangle_{at}$$

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

$$b^+ = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Операторы рождения/уничтожения фотона:

$$a |m\rangle_{ph} = \sqrt{m} |m-1\rangle_{ph} - \text{уничт.}$$

$$a^\dagger |m\rangle_{ph} = \sqrt{m+1} |m+1\rangle_{ph} - \text{рожд.}$$

А. Мелин
и Квант. мех.

$$a = \begin{pmatrix} \langle 0|_{ph} & \langle 1|_{ph} & \langle 2|_{ph} & \dots \\ |0\rangle_{ph} & 0 & 1 & 0 \\ |1\rangle_{ph} & 0 & 0 & \sqrt{2} \\ |2\rangle_{ph} & 0 & 0 & 0 \end{pmatrix}$$

Канонический.

$$H_{JC} = \hbar \omega_c a^\dagger a + \sum_{i=1}^n g_i (a^\dagger + a) (b_i^\dagger + b_i) \quad (1) \quad (2) \quad (3)$$

н.р. частота фотона в полости $(\hbar \omega_c)$

точечный $\uparrow$ гамильтониан

① энергия фотонов

② энергия атомов

③ энергия взаимодействия атом-поле

$$H_{int} =$$

ω_a - частота атом. перехода $(|0\rangle \leftrightarrow |1\rangle)$

g_i - интенсивность (сила) взаимо-в атом-поле

i -го атома с полем

$$= \sum_{i=1}^n g_i (a^\dagger b_i^\dagger + a^\dagger b_i + a b_i^\dagger + a b_i)$$

↓ ↓ ↓ возб. фот. ↓ возб. фот. +

релекс. фот. + релекс. фот. +

не сохраняющие энергию (аналогично поглощ.-фот и возб. атом.)

Но закон сохр. энергии работает (локально м.б. losing, но суммарно всегда сохр.)

Сильно растёт базис $|0\rangle \quad |1\rangle \quad |2\rangle \quad |3\rangle \dots$

Приближение RWA

rotation wave approxm.
приблиз. вращения-волны

Ум. RWA ($a^\dagger b + a b^\dagger$)

$$1) |\omega_c - \omega_a| \ll \omega_c \ll \omega_a$$

$$2) \frac{g}{\frac{1}{\hbar} \omega} \ll 1, \quad g = 0,01 \text{ kW}$$

$a^\dagger a =$ число фотонов
в модосе

$$H_{TC}^{RWA} = \hbar \omega_c a^\dagger a + \sum_{i=1}^n \hbar \omega_a b_i^\dagger b_i + \sum_{i=1}^n g_i (a^\dagger b_i + a b_i^\dagger)$$

max. взаимодействие: 2 ph 2 атома



max: $|2\rangle_{ph} |0\rangle_{at}$

определ: $|2\rangle |00\rangle$
 $|1\rangle |10\rangle$
 $|1\rangle |01\rangle$
 $|0\rangle |11\rangle$

$$H = \begin{pmatrix} 200 & 101 & 110 & 011 \\ 200 & 2\hbar\omega_c & \sqrt{2}g_2 & \sqrt{2}g_1 & 0 \\ 101 & \sqrt{2}g_2 & \hbar(\omega_c + \omega_a) & 0 & g_2 \\ 110 & \sqrt{2}g_1 & 0 & \hbar(\omega_c + \omega_a) & g_1 \\ 011 & 0 & g_2 & g_1 & 2\hbar\omega_a \end{pmatrix}$$

(упрощен)

$$200 \rightarrow 101: a b^\dagger |2\rangle |00\rangle = \sqrt{2} |1\rangle |01\rangle_{at}$$

$$H = \begin{pmatrix} 2\hbar\omega_c & \sqrt{2}g_2 & \sqrt{2}g_1 & 0 \\ \sqrt{2}g_2 & \hbar(\omega_c + \omega_a) & 0 & g_2 \\ \sqrt{2}g_1 & 0 & \hbar(\omega_c + \omega_a) & g_1 \\ 0 & g_2 & g_1 & 2\hbar\omega_a \end{pmatrix}$$

$$(1) = \hbar \omega_c a^\dagger a \otimes I_2^{(1)} \otimes I_2^{(2)}$$

$$(2) = \hbar \omega_a (I_{ph+1}^{(ph)} \otimes b_1^\dagger b_1 \otimes I_2 \otimes \dots \otimes I_2 \otimes I_{ph}^{(ph)} \otimes I_2 \otimes b_n^\dagger b_n)$$

$$|\psi(t)\rangle = e^{-\frac{iHt}{\hbar}} |\psi(0)\rangle \quad |\psi(0)\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$dt \approx 100 \text{ HC}$
 50 HC
 10 HC
 $\dots$

$$|\psi(dt)\rangle = \exp(-\frac{iHdt}{\hbar}) |\psi_0\rangle$$

$$|\psi(2dt)\rangle = \exp(-\frac{iH2dt}{\hbar}) |\psi(dt)\rangle = U_{dt} |\psi(dt)\rangle$$

$$U_{dt} = e^{-\frac{iH}{\hbar} dt}$$

коллапс $|\psi\rangle = 1 - \epsilon \ll 1$
 $\rightarrow 0,001$
 $0,0001, \dots$

$|\psi\rangle$ амплитуда, амплитуда

Основное квант. ур-е Операторы Линдблада

Унитарная динамика: $i\dot{\rho} = \frac{1}{\hbar} [H, \rho]$ $\dot{\rho} = -\frac{i}{\hbar} [H, \rho]$

Неунитарная динамика: (потери, утечки, необр. процессы и т.д.)

$$i\dot{\rho} = \frac{1}{\hbar} [H, \rho] + \underbrace{\frac{i}{\hbar} L(\rho)}_{\text{неунитарная часть}}$$

$$L(\rho) = \sum_i \ell_i \left(L_i \rho L_i^\dagger - \frac{1}{2} (L_i^\dagger L_i \rho + \rho L_i^\dagger L_i) \right)$$

$\{L_i^\dagger L_i, \rho\}$ — антикоммутатор

$$\rho_0 = |\psi(0)\rangle\langle\psi(0)|$$

ℓ_i — интенсивности Линдбладовск. процесса, опр. матрицей L_i

Профитирование: 1) унитар. эволюция. $\rho(t+dt) = U_{dt} \rho(t) U_{dt}^\dagger$

$$2) \rho(t+dt) = \rho(t) + \frac{i}{\hbar} L(\rho) dt$$

система: max в полости 2 фот.
2 2-уровня атома

$$|\psi(0)\rangle = |2\rangle_{ph} |00\rangle_{at}$$

$\omega_c = \omega_a$ $g = 0.01 \hbar$ $\omega_c \gg g_1 = g_2$
утечка из полости с интенсивно
 $\ell_0 = g$

есть сток
 $|2\rangle |00\rangle |0\rangle_s$

лазер: $|m\rangle_{ph} \dots$

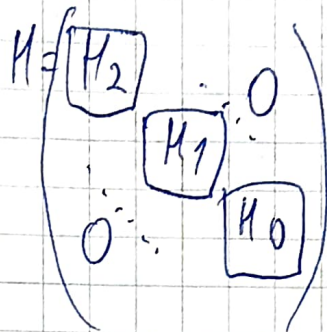
без стока $\left\{ \begin{array}{l} |2\rangle |00\rangle |0\rangle_s \\ |1\rangle |01\rangle |0\rangle_s \\ |1\rangle |10\rangle |0\rangle_s \end{array} \right.$

и др. нечетками в сток

$$H_1 \begin{cases} |12\rangle|00\rangle|1\rangle_S \\ |10\rangle|01\rangle|1\rangle_S \\ |10\rangle|10\rangle|1\rangle_S \end{cases}$$

$$H_0 \{ |0\rangle|00\rangle|2\rangle_S \}$$

$$L_0 = g$$



пер-м канонич
 $\angle 2$ в строке:
 след $H_2 + H_1$

$$L_0: \begin{pmatrix} |1\rangle|00\rangle|1\rangle_S & |10\rangle|01\rangle|1\rangle_S \\ |2\rangle|00\rangle|0\rangle_S & \vdots \\ |1\rangle|01\rangle|0\rangle_S & \vdots \\ \vdots & \vdots \end{pmatrix}$$

запрещен только
 переходы отомона
 из полноты
 в строке

оператор
 Лундберга

$$L_0 = a \text{ уперка в строке}$$

проблема хранения самого состояния

$$|\psi\rangle \in L = L_1 \otimes L_2$$

$$\sum_{i_1, i_2} \psi_{i_1 i_2} |i_1\rangle |i_2\rangle$$

Т. Минько

что не всю матрицу хранить: выбрать особую базис в L_1, L_2

Т. $\forall$ любого сост $|\psi\rangle \in L_1 \otimes L_2$ можно выбрать базис

$$|0\rangle_1, |1\rangle_1, \dots, |N_1-1\rangle_1; |0\rangle_2, |1\rangle_2, \dots, |N_2-1\rangle_2 : \text{т.т. состояние } |\psi\rangle =$$

$$= \sum_{j=0,1,\dots, \min(N_1-1, N_2-1)} \lambda_j |j\rangle_1 |j\rangle_2$$

одно и то же j , но $j_1 \in L_1, j_2 \in L_2$

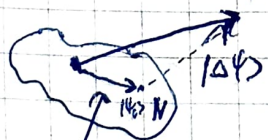
$$\frac{|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2}{\sqrt{2}}$$

Вместо $\psi_{i_1 i_2}$ хранить вектор λ_j

Док-во: 1. Сост. $|\psi\rangle$ не запутано $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$

2. запутан. идентифицировать по $\min(N_1-1, N_2-1)$

остаточно
базисные
вект.
как обычно



мн-во не
запут. сост.
-опр. (т.к. норма 0)

$$|\psi_1\rangle \otimes |\psi_2\rangle \text{ сж?}$$

мн-во всех сост. компактно

$$|\psi_1\rangle \rightarrow |\psi_1^{\infty}\rangle \Rightarrow |\psi_1^{\infty}\rangle \otimes |\psi_2^{\infty}\rangle$$

$$|\psi_2\rangle \rightarrow |\psi_2^{\infty}\rangle$$

структурируем
(найти т. расст.
от ком. ψ_0 $|\psi\rangle$
будет миним.)

$$\text{расст.}(\psi, \psi_0) = \min_{\psi \in N}$$

$$|\psi_0\rangle = |\psi_0^1\rangle \otimes |\psi_0^2\rangle$$

$$|\psi_0^1\rangle = |0\rangle_1 |1\rangle_2 \dots |(N_1-1)\rangle_1$$

$$|\psi_0^2\rangle = |0\rangle_2 |1\rangle_2 \dots |(N_2-1)\rangle_2$$

$$|\psi\rangle = |\psi_0\rangle + |\Delta\psi\rangle$$

$$|\psi\rangle = |\phi_0\rangle = \lambda_0' \lambda_0'' |o_1\rangle |o_2\rangle + |\Delta\psi\rangle$$

> в разложении $|\Delta\psi\rangle$ нет ни $|o_1\rangle$, ни $|o_2\rangle$
 предположим обратное

$$|\Delta\psi\rangle = \sum_{j \neq 0} \epsilon_j |j\rangle |\phi_2^j\rangle$$

Вектор $|\psi_0'\rangle$ взять можно $|\psi_0'\rangle \neq \epsilon |o_1\rangle = |\tilde{\psi}_0'\rangle$
 ортогональные матр.

$$\|\Delta\psi\|$$

$$|\psi_0'\rangle = |\tilde{\psi}_0'\rangle |\psi_0^2\rangle$$

тогда $d_1 < d$, но d - мин. расст. по построению $\Rightarrow$

$\Rightarrow$ нет ни o_1 , ни o_2
 (для o_2 дано)

тогда $|\Delta\psi\rangle$ лежит в простр. меньшей размерности

$\Delta\psi \equiv \psi$ и далее по индукции

Следствия: • эквивалентное представление квант. сост.

• Т. (SVD) СВА - разложение произвольной матрицы

$\forall$ матр A $\exists$ унитарные S и V : $SAV = D$ - диагональная матр.
 где S, V - квадратные

$$A = (a_{ij}) = \sum |i\rangle \langle j|$$

$$|\psi\rangle = \sum_{i,j} a_{ij} |i\rangle \langle j| \quad \sum_j \lambda_j |j_1\rangle \langle j_2|$$

Лекция 17.10

Программа Гровера

$$(1) f(x) = 1$$

$$f: \{0,1\}^n \rightarrow \{0,1\}$$

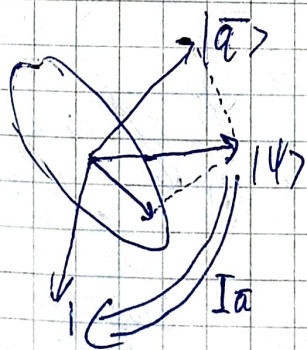
x_{tar} - единств. р-м. (1)

$$(2) U_f: |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$$

$$U_g = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$U_g = O(\sqrt{t_n})$$

для дискриминации амплитуд.



$$|\psi\rangle = \sum_{j=0}^{N-1} \frac{1}{\sqrt{N}} |j\rangle$$

$$|Q_f|G_z^{Anc}|Q_f\rangle$$

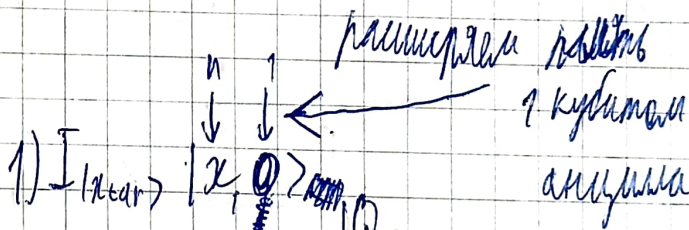
$$(-1)^{z-1} |x, x\rangle$$

$$|j\rangle \in \begin{cases} 100 \dots 01 \\ 100 \dots 11 \\ \vdots \\ 111 \dots 11 \end{cases} \leftarrow |x_{tar}\rangle$$

Классический алг-м с оракулом f
Находит р-м. ⁽¹⁾ за время $\Omega(N)$ $N=2^n$

$I_{\vec{a}}$ - инверсия относительно вектора $|\vec{a}\rangle$

$$(3) I_{\vec{a}}|\vec{b}\rangle = \begin{cases} |\vec{b}\rangle, & \text{если } \langle \vec{a} | \vec{b} \rangle = 0 \text{ (ортон.)} \\ -|\vec{b}\rangle, & \text{если } |\vec{a}\rangle = |\vec{b}\rangle \end{cases}$$



$$|x, z\rangle$$

$$x \neq x_{tar}, z=0$$

$$x = x_{tar}, z=1$$

$$|G_z^{Anc}|Q_f\rangle$$

$$(-1)^{z-1} |x, z\rangle$$

Прежде чем выбирать anc,
нужно убедиться, что она не
запутана с основным регистром
с квантовой памятью

для этого ещё
раз применяем Q_f

Получили и проверили ответ. Вектора, который неизвестен.

Но есть такая операция, 2 оракула.

Можно ли за 1? Экономичный способ реализации $I_{|x_{\text{tar}}\rangle}$:

$$|anc\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$U_{\phi} |x, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\rangle = \begin{cases} -|x, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\rangle, & x = x_{\text{tar}} \\ |x, anc\rangle, & x \neq x_{\text{tar}} \end{cases}$$

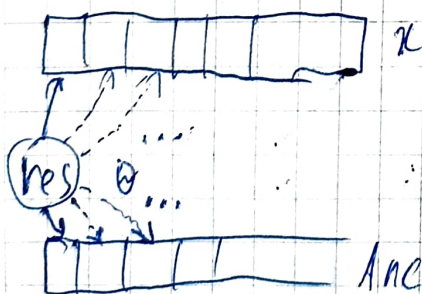
2) $I_{|0\rangle} |x\rangle |res\rangle$

$$|0\rangle = |00\dots 0\rangle$$

Мат. Риторика:

Встретились 1- ноль

и в стр. 1- инверсия



$$\theta_1^{-1} \theta_2^{-1} \dots \theta_n^{-1} (-\theta_z^{res}) \theta_n \dots \theta_2 \theta_1 = I_{|0\rangle}$$

Очисти Anc: применить в обр. пор. эти операторы

$$|\tilde{0}\rangle = |00\dots 0\rangle$$

$$|\tilde{0}\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$$

3) $I|\tilde{0}\rangle$

$$WH|\tilde{0}\rangle = |\tilde{0}\rangle$$

$$WH|\tilde{0}\rangle = |\tilde{0}\rangle$$

$$WH \cdot I_{|\tilde{0}\rangle} \cdot WH = I_{|\tilde{0}\rangle}$$

Оператор Гровера

$$(4) G = -I_{|\tilde{0}\rangle} I_{|x_{tar}\rangle}$$

Пример

$$G^{\tau} |\tilde{0}\rangle \approx |x_{tar}\rangle \quad (\text{мощность оракула} \sim O(\frac{1}{N^2}))$$

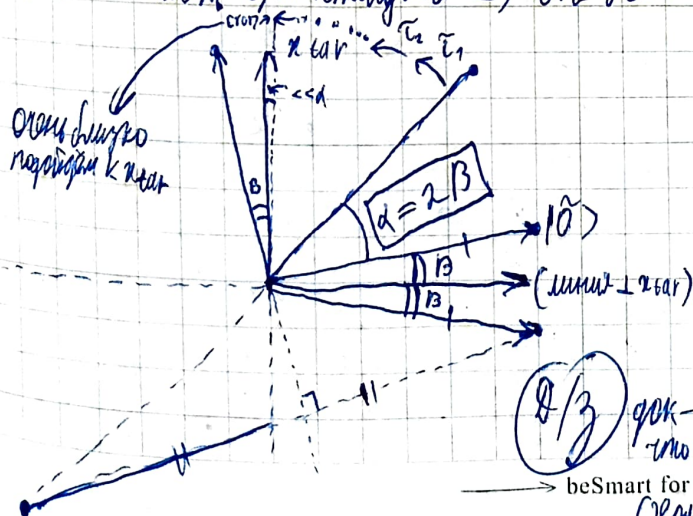
$$\tau = \left\lceil \frac{\pi}{4} \sqrt{N} \right\rceil$$

Век-во $L_R(|\tilde{0}\rangle, |x_{tar}\rangle)$ - базис. пр-во $\cong \mathbb{R}^2$

инвариантно относительно $I_{|x_{tar}\rangle}$ и $I_{|\tilde{0}\rangle}$

G не меняет ориентацию $\Rightarrow$ он явл. поворотом

$\Rightarrow G$ тоже инвар.



L_R на угол d

$$\langle \tilde{0}, x_{tar} \rangle = \frac{1}{\sqrt{N}}$$

$$\beta = \arcsin \frac{1}{\sqrt{N}}$$

$$d = 2 \arcsin \frac{1}{\sqrt{N}} \approx \frac{d}{\sqrt{N}}$$

$$\langle x_{tar} | G^{\tau} | \tilde{0} \rangle = 1 + \epsilon$$

$$\epsilon \sim \frac{1}{N^2}$$

8/3 гек-нб
что d=2*beta

beSmart for you
(рекламный)

Если рещ. нет, что будет с ам?

Случай нескольких рещений ур-я (1)

а) число рещ. известно: L

б) число рещ. неизвест.

а) пусть $\alpha_1, \alpha_2, \dots, \alpha_L$ - рещ. (1)

нужно найти одно из них

$$|\alpha_{\text{tar}}\rangle = \frac{1}{\sqrt{L}} \sum_{k=1}^L |\alpha_k\rangle$$

применим нашу схему из теоремы

$$L_R(|\tilde{0}\rangle, |\alpha_{\text{tar}}\rangle)$$

Инвариант. относ. G ?

$$Q_f(|\alpha_{\text{tar}}, \alpha_{\text{nc}}\rangle) = -|\alpha_{\text{tar}}, \alpha_{\text{nc}}\rangle$$

$$Q_f(|\perp \alpha_{\text{tar}}, \alpha_{\text{nc}}\rangle) = |\perp \alpha_{\text{tar}}, \alpha_{\text{nc}}\rangle$$

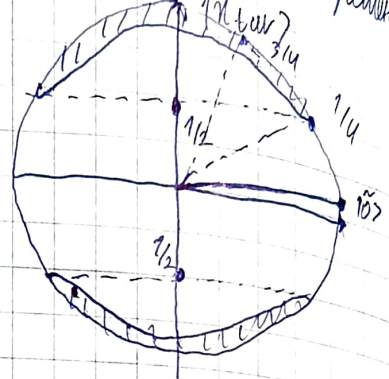
далее аналогично, но β будет другим

$$\beta = \arcsin \frac{\sqrt{L}}{\sqrt{N}} = \arcsin \sqrt{\frac{L}{N}}$$

$$\tau = \left\lceil \frac{1}{\beta} \sqrt{\frac{N}{L}} \right\rceil$$

если нет, то
квант комп. не нужен,
можно найти наугад

б) не знаем, сколько рещений



• не знаем, когда останавливаться.

• хорошо бы перейти в записку (1/2)

$|\chi_0=2$, далее наращиваем

$$\tilde{\chi}_s = \left[\left(\frac{3}{2} \right)^s \cdot \frac{2}{\tilde{\chi}_0} \right] \quad \tilde{\chi}_1=3 \quad \tilde{\chi}_2=4 \dots$$

• примерно геом. прогрессия, быстро
достигает границы окруж.

Сложности итерацион. алгоритма?

$$\tau_0 + \tau_1 + \dots + \tau_M, \quad \epsilon_M = O\left(\sqrt{\frac{M}{L}}\right)$$

не менее чем $\frac{1}{4}$
не более чем $\frac{3}{4}$ ← попадем

$$\left(\frac{3}{4}\right)^C - \text{err} \quad C=700 \quad \text{err} < \frac{1}{1000}$$

очень быстро придет
к верному рещ.

Сложн. ограничивается геометр. прогрессией

$$\text{Сложн. алг.: } \tau_q = O\left(\sqrt{\frac{M}{L}}\right) \quad \text{const} > \frac{1}{4} \text{ будет}$$

программ. квант. преобр. Фурье

Возвращение скрытых параметров с пом. QFT

$$\text{QFT: } |a\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{c=0}^{N-1} e^{\frac{2\pi i a c}{N}} |c\rangle$$

$$|c\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} e^{\frac{2\pi i a c}{N}} |a\rangle$$

U - преобразование унитар
заданный квант. состоян.

содержит знан. U имеет вид: $e^{i\varphi_k}$
 $\varphi_k = 2\pi \omega_k$
 $\omega_k \in [0, 1)$

$$\omega_k \in [0, 1) \quad \omega_k \in \{0, \dots, N-1\}$$

ω_k имеет вид $\frac{w_k}{N}$

наша цель: найти ω_k
поиск по битам составные

$$|\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}\rangle; \quad \omega_k = \varepsilon_0 + 2\varepsilon_1 + \dots + 2^{n-1}\varepsilon_{n-1}$$

n кубитов

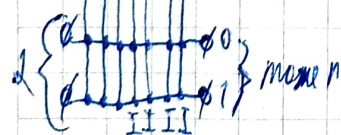
Найти состояние $\Rightarrow$ найти ω_k

• Вычислительный оператор:

$$U_{\text{cond}} |\psi\rangle |d\rangle = \begin{cases} |\psi\rangle, & \text{если } d=0 \\ U |\psi\rangle, & \text{если } d=1 \end{cases} \quad (1)$$

$$U_{\text{cond}} |\psi\rangle |d\rangle = U^d |\psi\rangle \quad (2) \quad 0 \leq d \leq N-1$$

$N=2^n$



$$d_0 + 2d_1$$

$d_1=0 \Rightarrow$ всегда

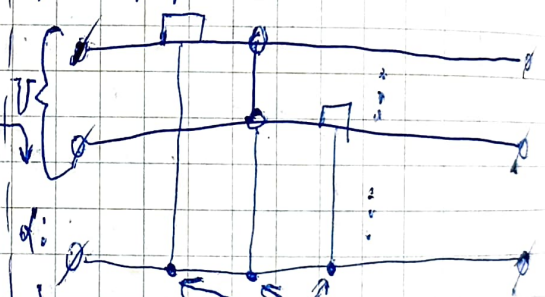
$d_1=1$

всегда $\text{cond} = 0$ - не нужен

2^{n-1} применений U

матр. 3, для 3 куб. и 7 применений $U_{\text{cond}} (1)$

реализация U :



матр. операторы

дано I , если $d=0$
и исходный ритм

$$\text{Rev}_U |\psi\rangle |d\rangle = \text{QFT}_d \cdot U_{\text{cond}} \quad (3)$$

$$|d(0)\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle - \text{нач. сост. амплитуды}$$

подерем произвол. $|\psi\rangle$ и применим Rev_U и измерим энергию,
с большой вероятностью там будет какое-то W_k

$$\text{Rev}_U |\psi\rangle |0\rangle = QFT_d \cdot U_{\text{cond}} |\psi\rangle \underbrace{\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle}_d = \sum_{k=0}^{N-1} \lambda_k \underbrace{\frac{1}{\sqrt{N}} QFT_k^{-1} U_{\text{cond}} |\varphi_k\rangle |j\rangle}_{U^j |\varphi_k\rangle |j\rangle}$$

$$|\psi\rangle = \sum_{k=0}^{N-1} \lambda_k |\varphi_k\rangle \quad (4)$$

$$(5) U |\varphi_k\rangle = e^{2\pi i W_k}$$

$$Q_k = \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} \frac{1}{N} e^{2\pi i j W_k} e^{-\frac{2\pi i j S}{N}} |\varphi_k\rangle |S\rangle = \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} \frac{1}{N} e^{\frac{2\pi i j (W_k - S)}{N}} |S\rangle$$

$$\text{амплитуда} = \sum_{S=0}^{N-1} \beta_S |S\rangle$$

$$\beta_S = \sum_{j=0}^{N-1} \frac{1}{N} e^{\frac{2\pi i j (W_k - S)}{N}} \quad (6)$$

Теперь измерим энергию, мы получим

W_k с вер-то $P_k = |\lambda_k|^2$

Нравится и Montgomery (2000г.) для упрощения алг. тогда факторизацию ищем.

теперь проп. $e^{2\pi i (W_k - S)}$ $\rightarrow$ значения

q - простое число $2^{n-1} < q \leq 2^n$ и кубитов

Нам нужно разложить $q = q_1 \cdot q_2$

Число простое число $S \leq q$ имеет порядок $\log(q)$

$$\frac{j}{r} \approx 0, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$$

$j \leq r$

Алгоритмический период натур. числа $y \pmod{q}$ -

- малое r , что $y^r \equiv 1 \pmod{q}$ и r - наименьшее с этим св-вом

$$y^r = 1 + q \cdot S$$

$$S \in \mathbb{N}$$

beSmart for you

• если $W_k = S$, то все

наз состоит из $\frac{1}{N}$, и в том.

$$\beta_S = 1$$

• если $W_k \neq S$ то пропустит

$$\beta_S = \frac{1 - e^{\frac{2\pi i (W_k - S)}{N}}}{1 - e^{\frac{2\pi i (W_k - S)}{N}}} = 0$$

выкинут только слагаемые

в ком. $(W_k = S)$

Выберем произвольн y . С не исчезающей вер-ю y окажется простым

Рассмотрим оператор: $U_y: |x\rangle \rightarrow |xy \pmod q\rangle$, действ. только на $|x\rangle \rightarrow |x\rangle$, если $x = q, q+1, \dots, 2^n-1$ на $x = 0, 1, \dots, q-1$

Нормальный

взаимно обратн

оператор, т.к. y — простое

нужно найти r

Don. $\mathbb{F}$ P. Shor (1994)

с неизм. вер-ю $\mathbb{F}$ будет факториз

собств. числа U_y :

$$\varphi_{j,s} = \frac{1}{\sqrt{r}} \sum_{k=0}^r e^{\frac{2\pi i k j s}{r}} |y^k s\rangle$$

$$y^{r-1} = (y^{r/2} - 1)(y^{r/2} + 1) = q \cdot s$$

собств. значения: $W_{j,s} = \left(\frac{j}{r} \right) \approx 0, \varepsilon_1 \varepsilon_2 \dots \varepsilon_n$
 $j = 0, 1, \dots, r$
 и макс r канальн

$$d = 0, 1, \dots, N-1 \sim 2^n$$

$$\text{Сложн. } U_{\text{cond}}: 2^n$$

это бьн бн прямого перебор.

Но из-за вида (7) можно эквивалентн образом применить U^d :

$$1) \cdot y; \cdot y^2; \cdot y^{2^2}; \cdot y^{2^3}; \dots; y^{2^{m_0}} \quad 2^{m_0} \leq d < 2^{m_0+1}$$

подержим до m_0 битов (лог)

$$2) \cdot y^{d-2^{m_0}} = ? \quad (\text{отбрасываем от } d \text{ эквивалентн. биты, битово подержим до } k)$$

Сложн.:

$$\sim \log^2 q$$

Итератив. сложн. факторизации q :

$$O(\log^2 q (\log \log q)^3)$$

фактически флнк записи в квадрате

Скорость сравннл со скор. умножнл

Классич. алгоритм Ленстры $O(e^{\sqrt[3]{\log q}})$
 почти экспоненциальное ускорение

Готовы квант с.к.: $n=2$ 1999

$n=3$

$n=5$

$n=10$?

очень важный рубеж

$n \leq 30$ больше 30 — принципиальное ограничение

Лекция 7.11

Алгоритмы: ~5 штук разобрано

Алгоритмы квантовой телепортации

$\langle CNOT | \chi, 0 \rangle \rightarrow | \chi, \chi \rangle$ скопировать битовое состояние
 $|\psi\rangle$ - произвольное сост. можно?

лекция 7.11

существует ли U -унитарный: $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$

нельзя!

доказано:

от противного: I можно скопировать и такой U унитар.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$U|\psi\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \stackrel{U}{\rightarrow} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle + |01\rangle + |11\rangle)$$

$$U|00\rangle = |00\rangle$$

$$U|10\rangle = |11\rangle, U \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}U|00\rangle + \frac{1}{\sqrt{2}}U|10\rangle =$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \leftarrow \text{но то же самое}$$

Теореме квантового клонирования

классическую информацию легко скопировать

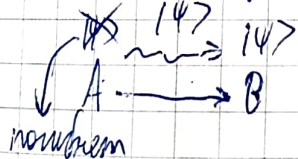
Квантовый канал передачи информации более запутан.

$A \rightarrow B$

$\uparrow_E$

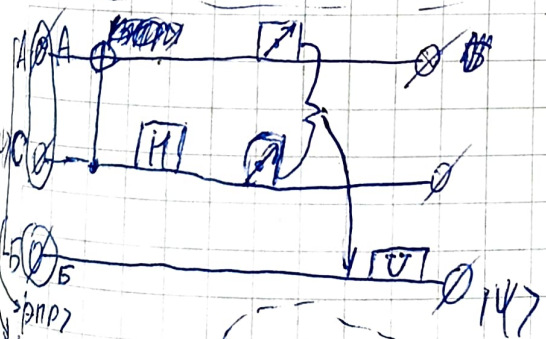
Ева может вмешаться, скопировать состояние, и никто об этом не узнает

Можно ли передать информацию о состоянии с помощью только классической информации.



это возможно!

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



□ - измерение, уничтожающее состояние $|\psi\rangle$ у Алисы

Боб по полученной информации восстанавливает $|\psi\rangle$.

потому Алиса его не узнала

Проверим:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|A, C, B\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle|0\rangle + |1\rangle|\psi\rangle|1\rangle)$$

измерили A, C: получили: $|0\rangle|00\rangle + |1\rangle|00\rangle$

$$\frac{1}{\sqrt{2}}(|0\rangle_A \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B) + |1\rangle_A \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B)) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

beSmart for you

- Упражнения:
- 1) $\lambda_0 |000\rangle + \lambda_1 |001\rangle$ — нигде не меняю основы
 - 2) $\lambda_0 |010\rangle - \lambda_1 |011\rangle \Rightarrow$ изм. (σ_z) меняю знак.
 - 3) $\lambda_0 |100\rangle + \lambda_1 |101\rangle \Rightarrow$ изм. (σ_x) меняю местами
 - 4) $-\lambda_1 |110\rangle + \lambda_0 |111\rangle \Rightarrow$ ~~изм.~~ меняю место и знак $\Rightarrow (-\sigma_z) \sigma_x$

Квантовое взаимодействие

$$|\Phi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

H — эрмитов оператор, от физ. интерпретации. Наблюдение, соответствующее H — наблюд. в базисе с.в. H .

Ориентация детектора A :

$$\sigma_x, \sigma_z$$

$|\varphi_0\rangle, |\varphi_1\rangle$ — с.в., то наблюдаемые с.в. H

есть с.в. велич. с распред. $\begin{matrix} \frac{1}{2} & | & E_0 & | & E_1 \\ \hline p & | & p_0 & | & p_1 \end{matrix}$

$$p_0 = |\langle \psi | \varphi_0 \rangle|^2 \quad p_1 = |\langle \psi | \varphi_1 \rangle|^2$$

$$H = \sigma_x : |\varphi_0\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \quad |\varphi_1\rangle = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$$

$E_0 = 1 \quad E_1 = -1$

σ_z φ_0, φ_1 другие

Вероятности выбора ориентации A и B :

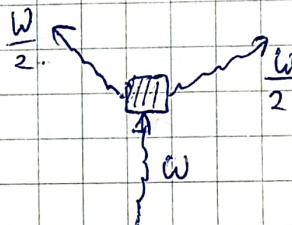
$$A: \begin{matrix} \sigma_x & \frac{1}{2} \\ \sigma_z & \frac{1}{2} \end{matrix}$$

Выбор делается быстро и за

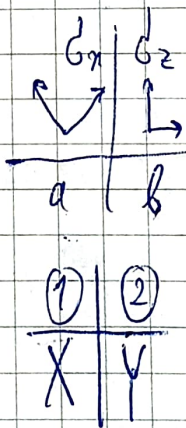
~ 1 метр до приёма фотона в детектор

Какая инф. о ориентации одного детектора не попала в другой.
Э? мгновенное действие на расстоянии

$D = 100 \text{ км}$



подходит в детекторы A и B почти одновременно



Ориентация детектора

$$(1) \frac{\sigma_x + \sigma_z}{\sqrt{2}}$$

$$(2) \frac{\sigma_x - \sigma_z}{\sqrt{2}}$$

наблюдаемое тоже ± 1

Исследовать статистику: какова прибыль и каков результат.

A \ B	Y	X
a	-1	+1
a	+1	+1
b	+1	-1
a	-1	-1
b	-1	-1

Сходится и соответствует сумм. велич.

X_i	вер-ти
$a \cdot X$	1/4
$a' \cdot Y$	1/4
$b \cdot X$	1/4
$-b' \cdot Y$	1/4

мат. ожидание:

$$MX = \frac{1}{4}(aX + a'Y + bX - b'Y) = \frac{1}{4}(a(X+Y) + b(X-Y)) \leq \left(\frac{1}{2}\right) \text{ кер-во Белла (1)}$$

одна из скобок равна 0, другой ≤ 2 , т.к. $a, b, X, Y = \pm 1$

Выводим мат. от. считая что у нас ЭПР пара:

N -наблюдения ее средн. знач. в сост $|\psi\rangle$

$$\langle \psi | H | \psi \rangle \equiv$$

$$|\psi\rangle = \lambda_0 |\varphi_0\rangle + \lambda_1 |\varphi_1\rangle$$

$$P_0 = |\lambda_0|^2 \quad P_1 = |\lambda_1|^2$$

$$E_0 P_0 + E_1 P_1 = \langle H \rangle_\psi$$

$$\equiv (\lambda_0 \langle \varphi_0 | + \lambda_1 \langle \varphi_1 |) (H |\lambda_0 |\varphi_0\rangle + \lambda_1 |\varphi_1\rangle) = \langle H \rangle_\psi$$

$$\langle H \rangle_\psi = \langle \psi | H | \psi \rangle$$

$$\langle H \rangle_\psi = \text{tr}(\langle \psi | H | \psi \rangle) = \text{tr}(|\psi\rangle \langle \psi | H) = \text{tr}(S \cdot H)$$

$$\text{tr} AB = \text{tr} BA \Rightarrow$$

$$\langle H \rangle_S = \text{tr}(S \cdot H) \quad (2)$$

$$\text{Смешанное сост: } S = \sum_j P_j |\varphi_j\rangle \langle \varphi_j|$$

$$MX = \frac{1}{4}(M(a \cdot X) + M(a' \cdot Y) + M(b \cdot X) - M(b' \cdot Y)) = \frac{1}{4} \cdot \frac{\sqrt{2}}{2} = \left(\frac{\sqrt{2}}{2}\right)$$

$$aX = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\langle aX \rangle_{\text{state}} = \frac{1}{2} \cdot \frac{1}{\sqrt{2}} + \frac{1}{2} \cdot \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}$$

beSmart for you

(2) $\Leftrightarrow$ (1)
противоречие
ошибка?
В кер-ве Белла!

a и a' разные?
 b и b' разные? $\rightarrow$ нельзя считать по (1)
квант. замкнутые
существуют
но не являются