Квантовые компьютеры

АНТОН КАРПУТКИН

В действительности все не так, как на самом деле (С. Е. Лец)

Содержание

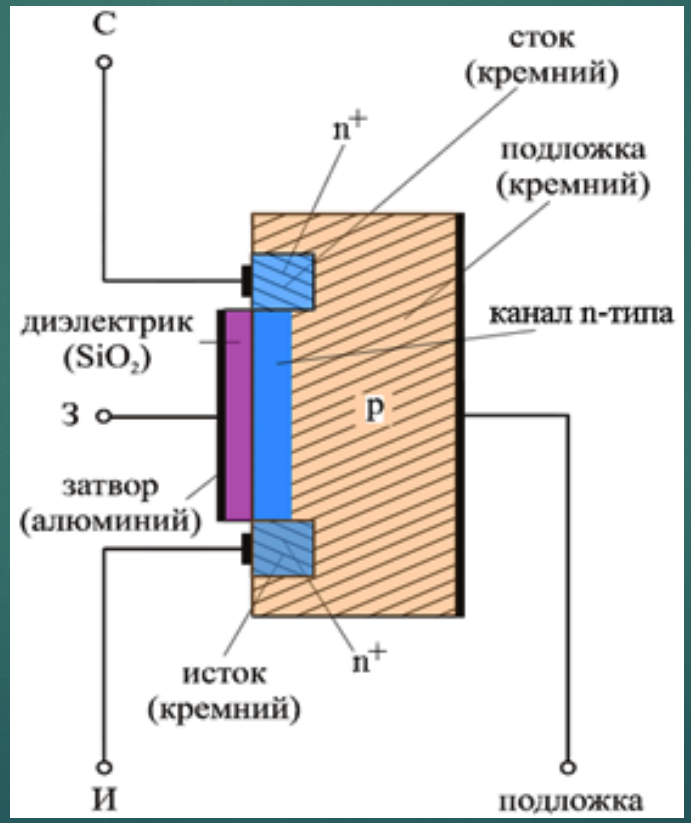
- О классических вычислениях и их пределах
- Квантовые биты
- Квантовые алгоритмы
- Реализация

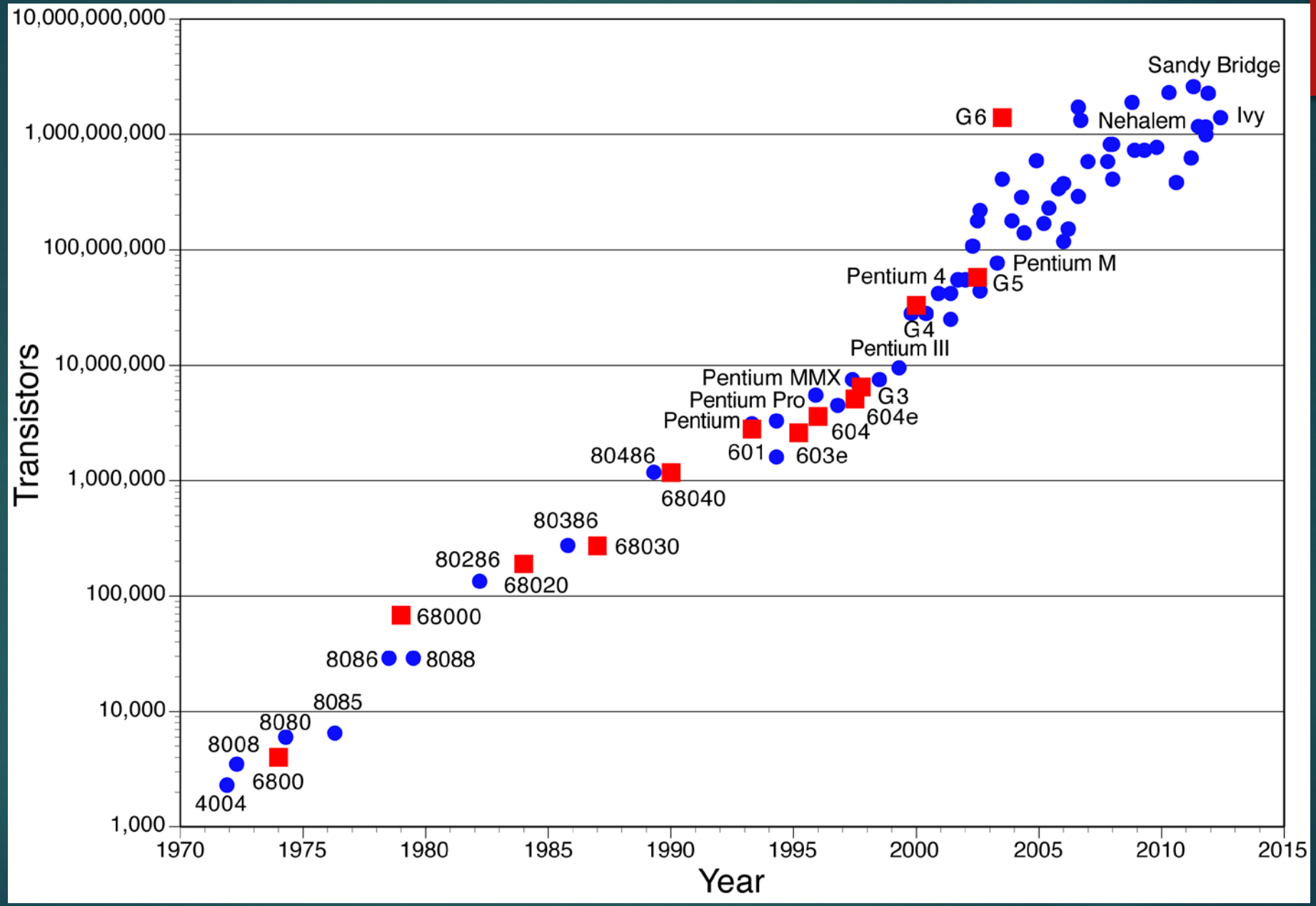
WTF?

- Квантовый компьютер – устройство, использующее квантовые эффекты, такие как *суперпозиция* и *запутывание* для проведения вычислений
- Квантовый компьютер ≠ параллельный компьютер
- Квантовый компьютер не всегда дает экспоненциальный прирост производительности
- Квантовый компьютер не всегда дает прирост производительности

О классических вычислениях и их пределах

- MOSFET-транзисторы




10,000,000,000
1,000,000,000
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
Transistors
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
Year
Sandy Bridge
Ivy
Nehalem
G6
Pentium M
Pentium 4
G5
G4
Pentium III
Pentium MMX
Pentium Pro
Pentium
G3
604e
604
601
603e
80486
68040
80386
68030
80286
68020
68000
8086
8088
8085
8080
8008
6800
4004

О классических вычислениях и их пределах

- Intel roadmap
  - 65 nm – 2006
  - 45 nm – 2008
  - 32 nm – 2010
  - 22 nm – 2012
  - 14 nm – 2014
  - *10 nm – 2016-2017*
  - *7 nm – 2017-2018*
  - *5 nm – 2020-2021*
- Что дальше?

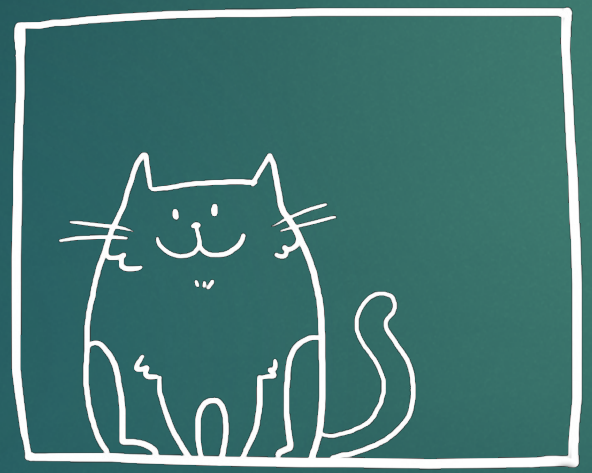
Диаметр атома - 0.2 нм

О классических вычислениях и их пределах

- Туннельный эффект:
  - $\Delta x \Delta p \geq \frac{\hbar}{2}$
  - При ограничении частицы в пространстве увеличивается вероятность больших скоростей
  - Частица перепрыгивает через препятствие
- Bug or feature?

Кубит

$|1\rangle$



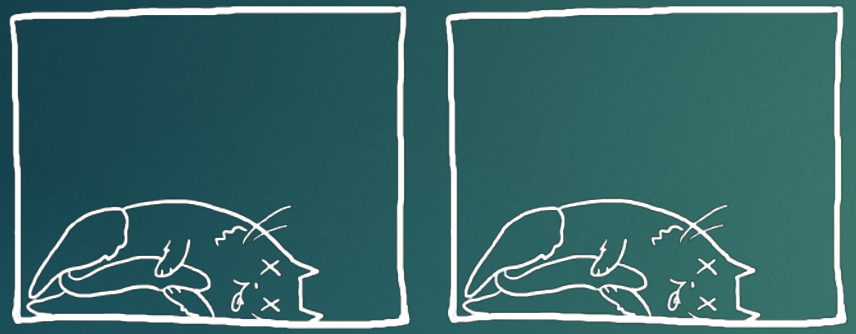
$|0\rangle$

Кубит

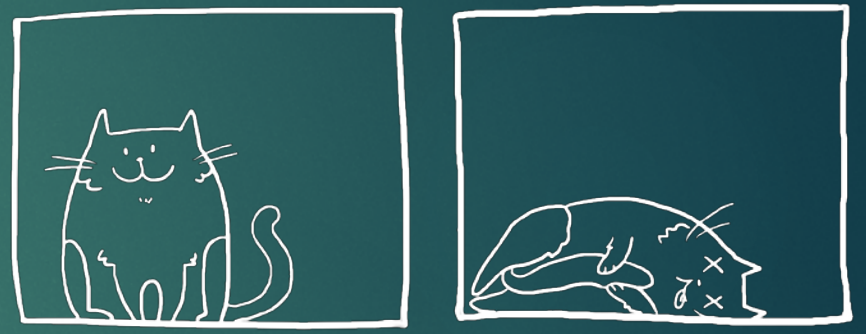
$$\alpha|0\rangle + \beta|1\rangle$$
$$\alpha, \beta \in \mathbb{C}$$
$$|\alpha|^2 + |\beta|^2 = 1$$

Кубиты

$|00\rangle$

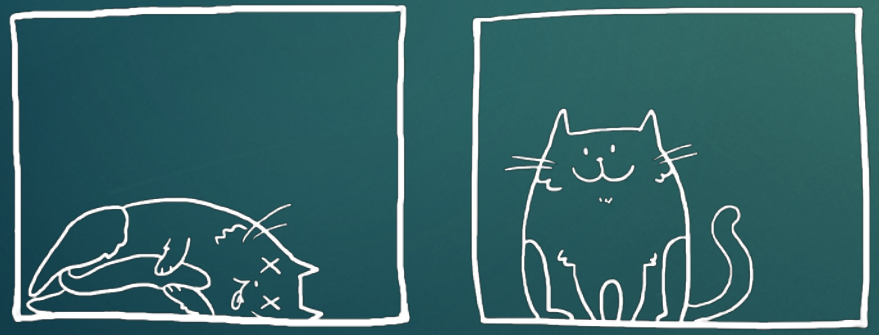


$|10\rangle$

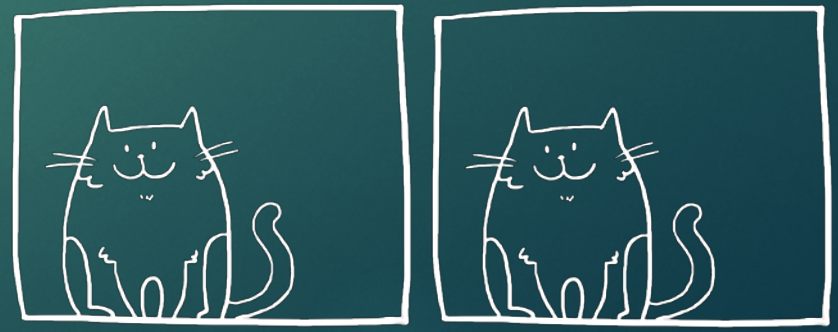


$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$
$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

$|01\rangle$

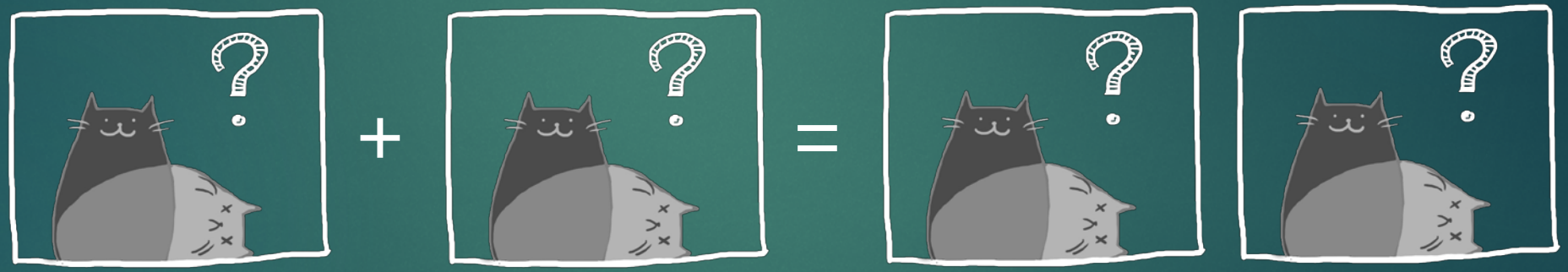


$|11\rangle$



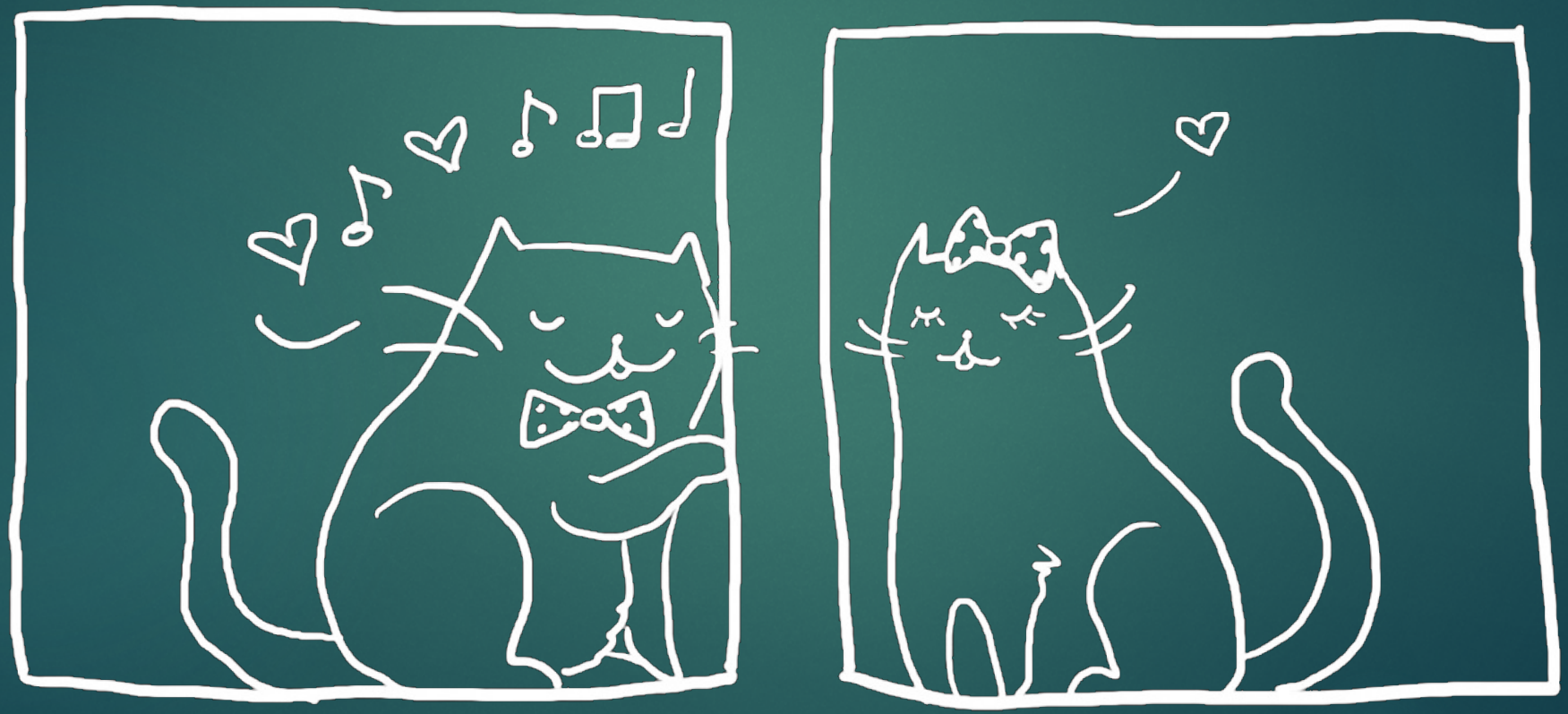
Кубиты

$\alpha|0\rangle + \beta|1\rangle$ $\gamma|0\rangle + \delta|1\rangle$ $(\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) =$
$\alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$



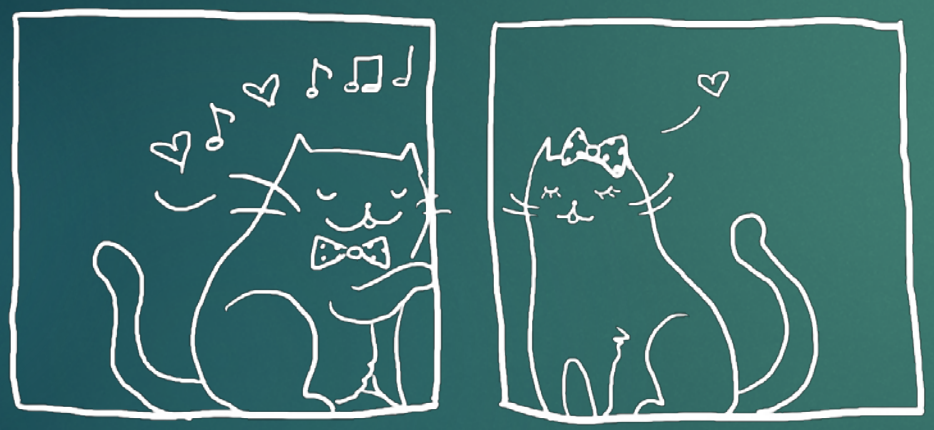
Кубиты

- Квантовое запутывание

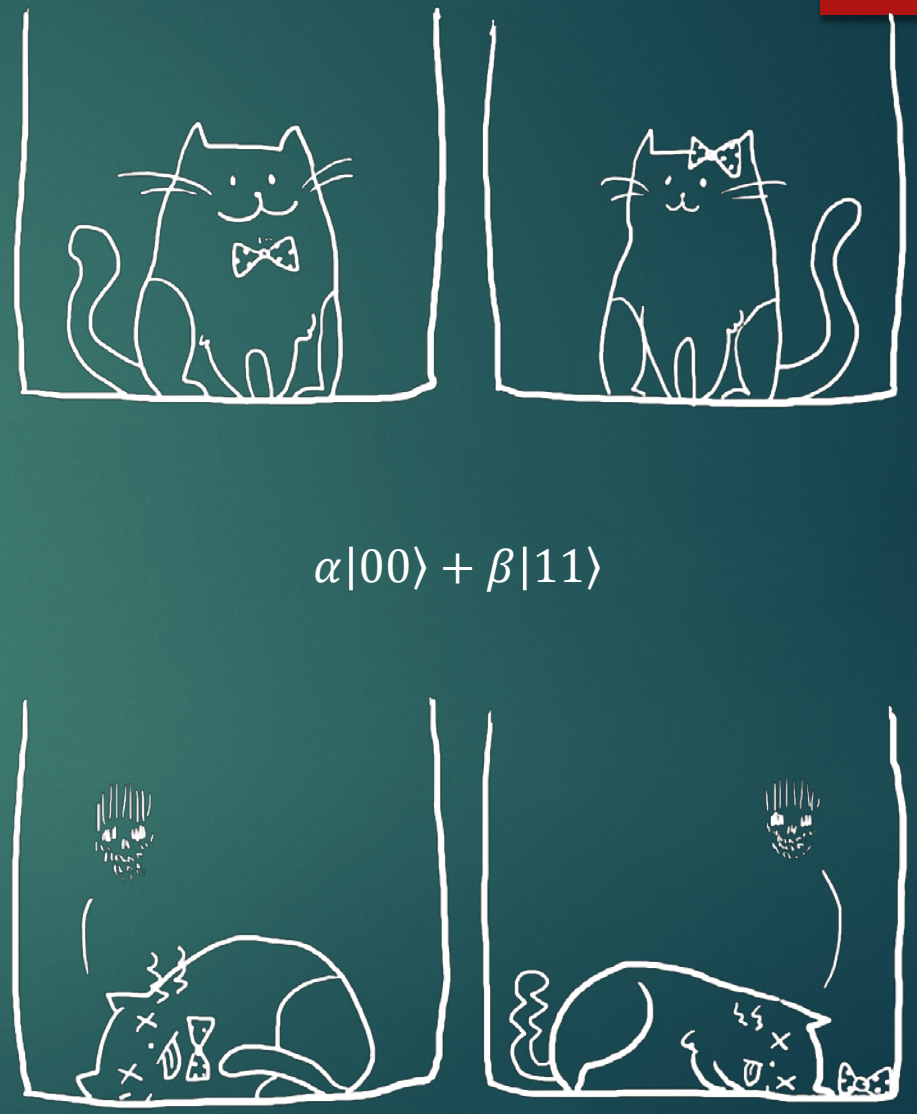


Кубиты

- Квантовое запутывание



$\alpha|00\rangle + \beta|11\rangle$



Квантовые вычисления

- Квантовый алгоритм = унитарное преобразование системы кубитов
  - n кубитов - матрица размера $2^n \times 2^n$
  - Унитарная матрица $A = (a_{ij}) \Rightarrow A^* = \overline{A^T} = (\overline{a_{ji}}) = A^{-1}$
    - Сохраняет длины векторов: $\sum_i |\alpha_i|^2 = 1 \Rightarrow \sum_i |\alpha_i'|^2 = 1$
  - Квантовые вычисления обратимы
  - x = y превращается в $|xy\rangle \rightarrow |x(x \oplus y)\rangle$
  - $x\&y$ превращается в $|xy0\rangle \rightarrow |xy(0 \oplus (x\&y))\rangle$
- Для любой вычислимой классическим алгоритмом функции существует соответствующий квантовый алгоритм

Квантовые вычисления

- Операция Адамара
  - $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
  - $H(\alpha|0\rangle + \beta|1\rangle) = \frac{1}{\sqrt{2}}(\alpha + \beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha - \beta)|1\rangle$
  - $|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Квантовые алгоритмы

- Поиск Грувера

```
int searchSomething(int a[]){
    for(int i = 0; i < a.length; i++){
        if(someFunction(a[i])){
            return i;
        }
    }
    return -1;
}
```

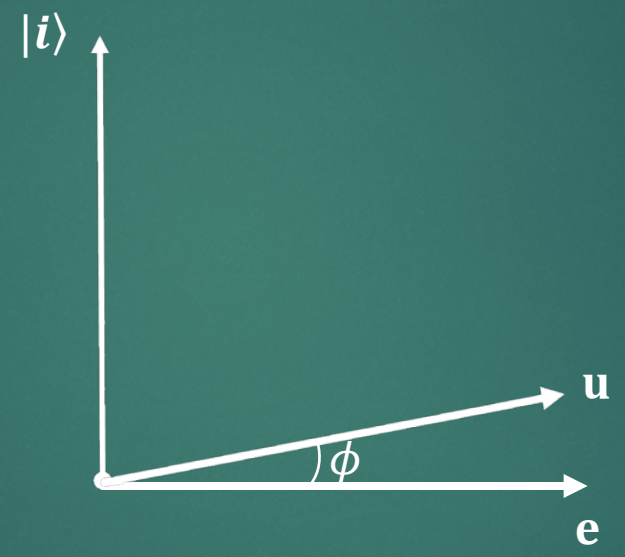
Квантовые алгоритмы

- Поиск Грувера
  - Длина массива $N = 2^n$
  - Только один элемент `a[i]`, удовлетворяющий условию
  - ТВ данных ~ 10^{12} запросов
  - Квантовому алгоритму хватает миллиона запросов

Квантовые алгоритмы

- Поиск Грувера
  - n основных кубитов и некоторое количество дополнительных для промежуточных вычислений
  - $|i\rangle$ искомый вектор
  - $\mathbf{e} = \frac{1}{2^{(n-1)/2}} \sum_{j \neq i} |j\rangle$
  - $\mathbf{u} = \frac{1}{2^{n/2}} \sum |j\rangle$
  - $\langle \mathbf{e} | i \rangle = 0 \Rightarrow \mathbf{e} \perp |i\rangle$
  - $\mathbf{e}, \mathbf{u}, |i\rangle$ лежат в одной плоскости
  - ϕ – угол между $\mathbf{e}$ и $\mathbf{u}$

Квантовые алгоритмы



Квантовые алгоритмы

- Начинаем с вектора $|00 \ldots 0\rangle$
- Операцией Адамара переводим $|00 \ldots 0\rangle$ в $\mathbf{u}$
- $\mathbf{v} := \mathbf{u}$

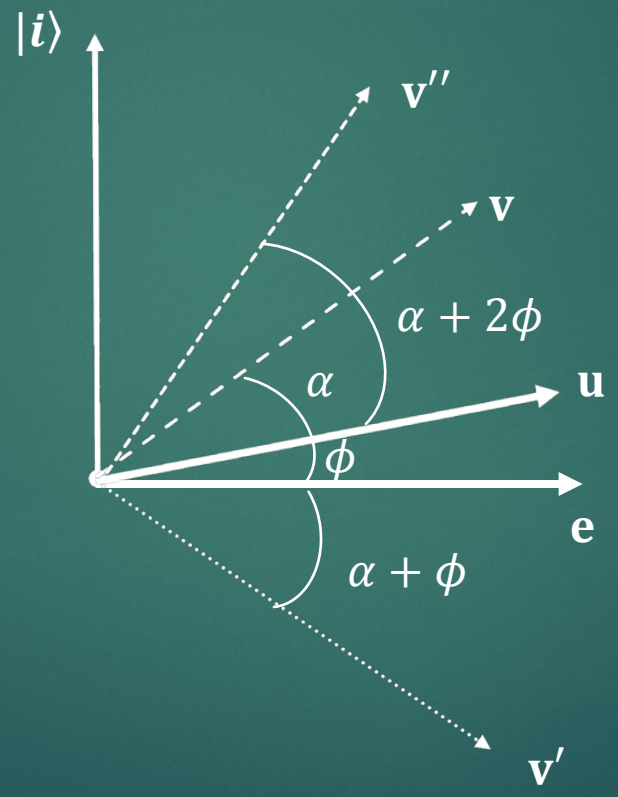
Квантовые алгоритмы

- Отражение вокруг **e**
  - Добавим дополнительный кубит $|0\rangle$
  - $\sum_j a_j|j0\rangle \to \sum_j a_j|j(0 \oplus f(j))\rangle = \sum_{j\neq i} a_j|j0\rangle + a_i|i1\rangle$
  - Над последним кубитом применим Z gate: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{cases} |0\rangle \to |0\rangle \\ |1\rangle \to -|1\rangle \end{cases}$
  - Снова $\sum_j a_j|j0\rangle \to \sum_j a_j|j(0 \oplus f(j))\rangle$
  - В конце получим $\sum_{j\neq i} a_j|j0\rangle - a_i|i0\rangle$

Квантовые алгоритмы

- Отражение вокруг $\mathbf{u}$
  - $\mathbf{u} \rightarrow |0\rangle$
  - Отразить вокруг $|0\rangle$, используя $g(x) = \begin{cases} g(0) = 0 \\ g(x) = 1, x \neq 0 \end{cases}$
  - $|0\rangle \rightarrow \mathbf{u}$

Квантовые алгоритмы



Квантовые алгоритмы

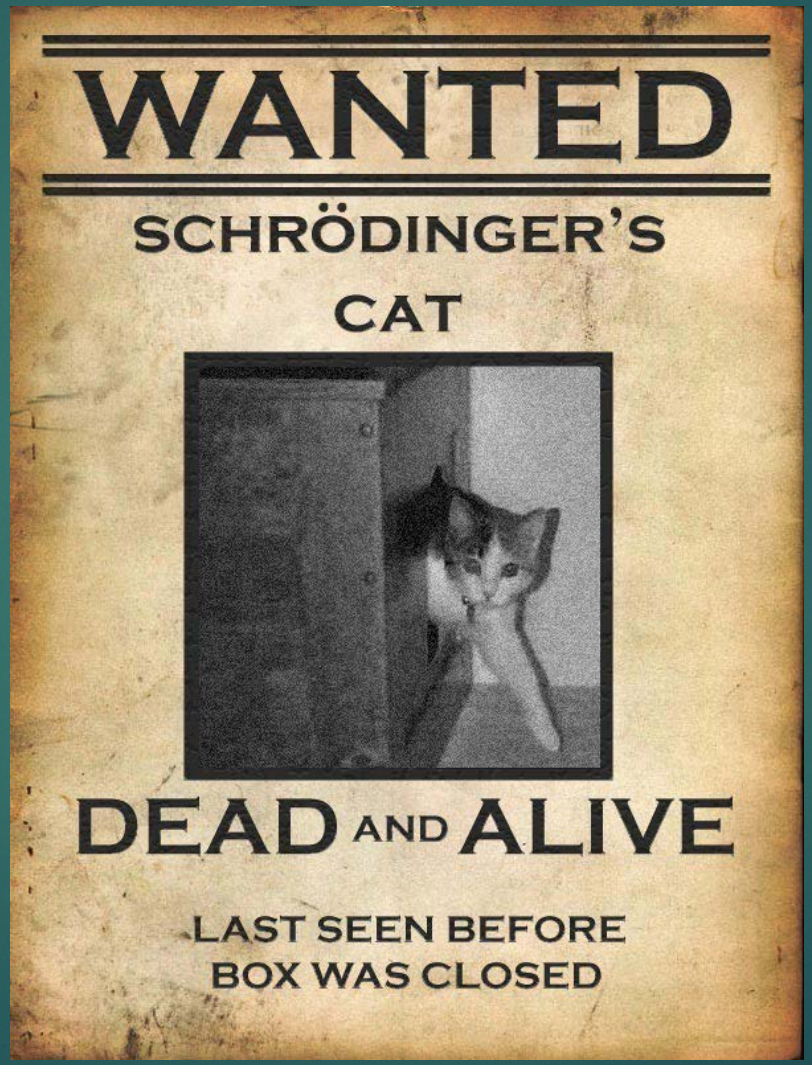
- Количество итераций?
  - $\sin\phi = \sin\angle(\mathbf{u},\mathbf{e}) = \cos\left(\frac{\pi}{2} - \angle(\mathbf{u},\mathbf{e})\right) = \cos\angle(\mathbf{u},|i\rangle) = \langle\mathbf{u}|i\rangle = \frac{1}{2^{n/2}}$
  - $\phi \approx \sin\phi = \frac{1}{2^{n/2}}$
  - Каждую итерацию поворачиваем на 2ϕ к цели
  - Всего $\frac{\pi}{2\cdot 2\phi} = \frac{\pi}{4}2^{n/2}$ итераций
  - Сложность $O(\sqrt{N})$

Квантовые алгоритмы

- RSA шифрование
  - Выберем 2 больших простых числа p и q
  - $N = pq$
  - $\phi(N) = (p-1)(q-1)$
  - Выберем $1 < e < \phi(N)$, взаимно простое с $\phi(N)$
  - Вычислим d, такое что $de \equiv 1 (\mathrm{mod}\ \phi(N))$
  - $\{e, N\}$ – открытый ключ
  - $\{d, N\}$ – закрытый ключ
- Атака: разложение N на множители
  - Классический алгоритм: $\sim O\left(2^{\sqrt[3]{\log N}}\right)$
  - Квантовый алгоритм (Шора): $O((\log N)^3)$

Квантовые алгоритмы

- Симуляция различных физических и химических квантовых систем
  - Нужно решить систему уравнений Шредингера для множества частиц
  - $i\hbar\frac{\partial}{\partial t}\Psi(\mathbf{r},t) = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial \mathbf{r}^2}\Psi(\mathbf{r},t) + V(\mathbf{r},t)\Psi(\mathbf{r},t)$
- Другие алгоритмы
  - http://math.nist.gov/quantum/zoo/


WANTED
SCHRÖDINGER'S
CAT
DEAD AND ALIVE
LAST SEEN BEFORE
BOX WAS CLOSED

Computers in the future may weigh no more than 1.5 tons. –
Popular Mechanics, forecasting the relentless march of science, 1949

I think there is a world market for maybe five computers. –
Thomas Watson, chairman of IBM, 1943

Реализация

- Основные задачи
  - Выбор физической системы в которой можно определить состояния $|0\rangle$ и $|1\rangle$
  - Инициализация
  - Преобразования
  - Измерение
- Декогеренция

Реализация

- Спин электрона
  - Магнитный момент
  - Унитарные операции – повороты внешним магнитным полем
  - Измерение – Stern-Gerlach
- Фотоны
- Сверхпроводники
- Квантовая точка
- …

Реализация

- D-Wave

Реализация

- D-Wave
  - Адиабатический компьютер
  - Реализует алгоритм квантовой нормализации
  - D-Wave One – 128 кубитов
  - D-Wave Two – 512 кубитов
- Квантовые языки программирования
  - QCL – C-like
  - Quipper – библиотека к Haskell
- 1QBit – 1st quantum software development company

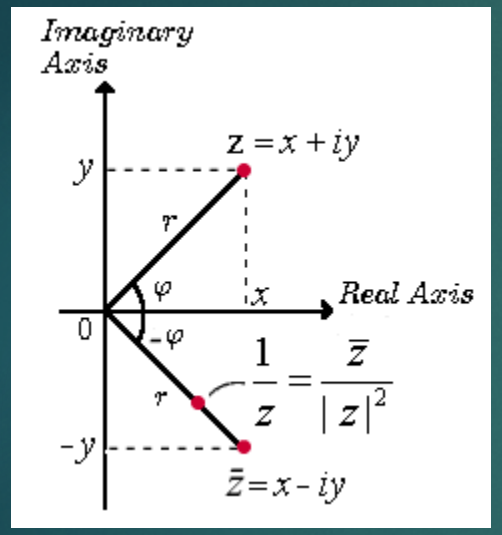
Реализация

Acknowledgements

- Котики – Кристина Вербицкая, Instagram: @tinabitspics


CAMBRIDGE

Математика и физика



- Комплексные числа $\mathbb{C}$
  - $i = \sqrt{-1}$
  - $z = x + iy = r(\cos\phi + i\sin\phi)$
  - $\bar{z} = x - iy = r(\cos\phi - i\sin\phi) = r(\cos(-\phi) + i\sin(-\phi))$
  - $\cos\phi = 1 - \frac{\phi^2}{2!} + \frac{\phi^4}{4!} - \frac{\phi^6}{6!} + \cdots = 1 + \frac{(i\phi)^2}{2!} + \frac{(i\phi)^4}{4!} + \frac{(i\phi)^6}{6!} + \cdots$
  - $i\sin\phi = i\phi - \frac{i\phi^3}{3!} + \frac{i\phi^5}{5!} - \frac{i\phi^7}{7!} + \cdots = i\phi + \frac{(i\phi)^3}{3!} + \frac{(i\phi)^5}{5!} + \cdots$
  - $e^{i\phi} = 1 + i\phi + \frac{(i\phi)^2}{2!} + \frac{(i\phi)^3}{3!} + \frac{(i\phi)^4}{4!} + \cdots$
  - $z = re^{i\phi}, \bar{z} = re^{-i\phi}$
  - $z\bar{z} = r^2 = \sqrt{x^2 + y^2} = |z|^2$

Математика и физика

- Линейная алгебра над $\mathbb{C}$
  - Вектор $\mathbf{z} = (z_1, \ldots, z_n) \in \mathbb{C}^n$
  - Скалярное произведение $\langle \mathbf{u}, \mathbf{v} \rangle = \sum_i u_i \overline{v_i}$
  - Норма вектора (“длина”) $\|\mathbf{z}\| = \sqrt{\langle \mathbf{z}, \mathbf{z} \rangle}$
  - $\cos(\widehat{\mathbf{u}, \mathbf{v}}) = \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\| \|\mathbf{v}\|}$
  - Матрица $A = (a_{ij}) \in \mathbb{C}_{m \times n}$
  - Транспонирование матрицы $A^T = (a_{ji}) \in \mathbb{C}_{n \times m}$
  - Сопряженная матрица $\overline{A} = (\overline{a_{ij}})$
  - Сопряженная транспонированная матрица $A^* = (\overline{a_{ji}})$

Математика и физика

- Линейная алгебра над $\mathbb{C}$
  - Произведение матриц $C = AB$, $(c_{ij}) = (\sum_k a_{ik} b_{kj})$
  - Тензорное произведение $A \otimes B$
  - Обратная матрица A^{-1}, $A^{-1}A = AA^{-1} = I$
- Унитарные матрицы
  - $A^*A = AA^*$

Математика и физика

- Уравнение Шредингера
- $i\hbar\frac{\partial}{\partial t}\Psi(x,t) = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2}\Psi(x,t) + V(x,t)\Psi(x,t)$
- Решение – волновая функция $\Psi(x,t)$
- $\int_a^b |\Psi(x,t)|^2 dx$ - Вероятность нахождения частицы между $x = a$ и $x = b$
- $\int_{-\infty}^{\infty} |\Psi(x,t)|^2 dx = 1$