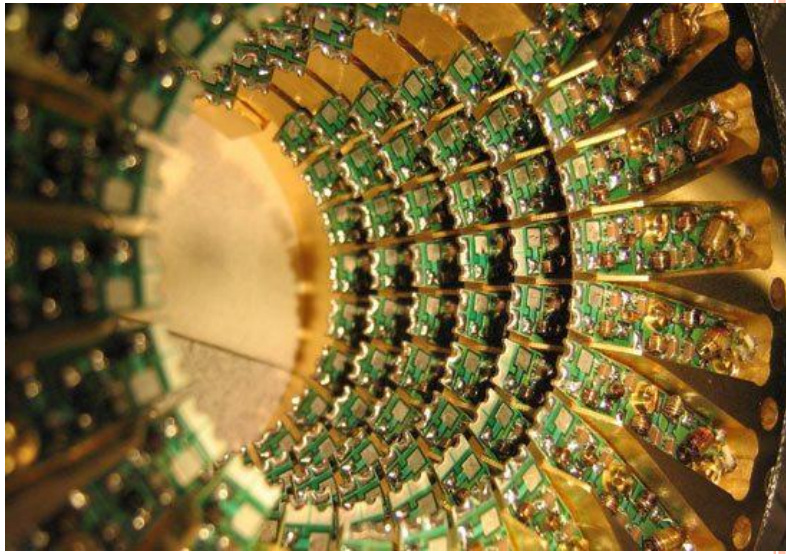
НАНОЭЛЕКТРОНИКА



7. Квантовые компьютеры

«Область квантовых вычислений продолжает оставаться далёкой от ясности»

http://www.3dnews.ru/903591

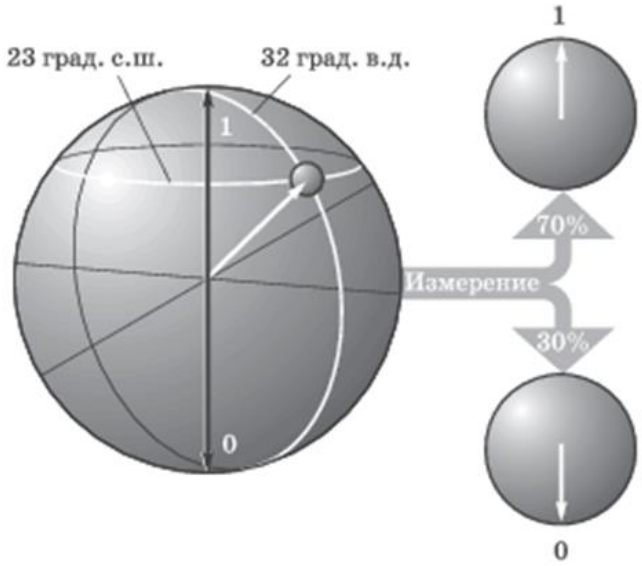
Принципы квантовой теории информации

Квантовый компьютер – вычислительное устройство, спроектированное и работающее на принципах квантовой механики.

Состояния «классического» компьютера: $F = |0\rangle, |1\rangle, \ldots |n\text{-}1\rangle$

Состояния квантового компьютера: $\Psi = \sum_{j=0}^{n-1} \lambda_j |\psi_j\rangle$
где λ - амплитуда (комплексная)

Измерение – случайная величина, принимающая значения $|j\rangle$, $j = 0,1,\ldots n\text{-}1$ с вероятностями $|\lambda_j|^2$



Кубит (quantum bit) представляет собой когеррентную суперпозицию двух базисных состояний системы:

$|\Psi_1\rangle = a|0\rangle + b|1\rangle,$

где $|a|^2 + |b|^2 = 1$

Принципы квантовой теории информации

Принцип квантового параллелизма:

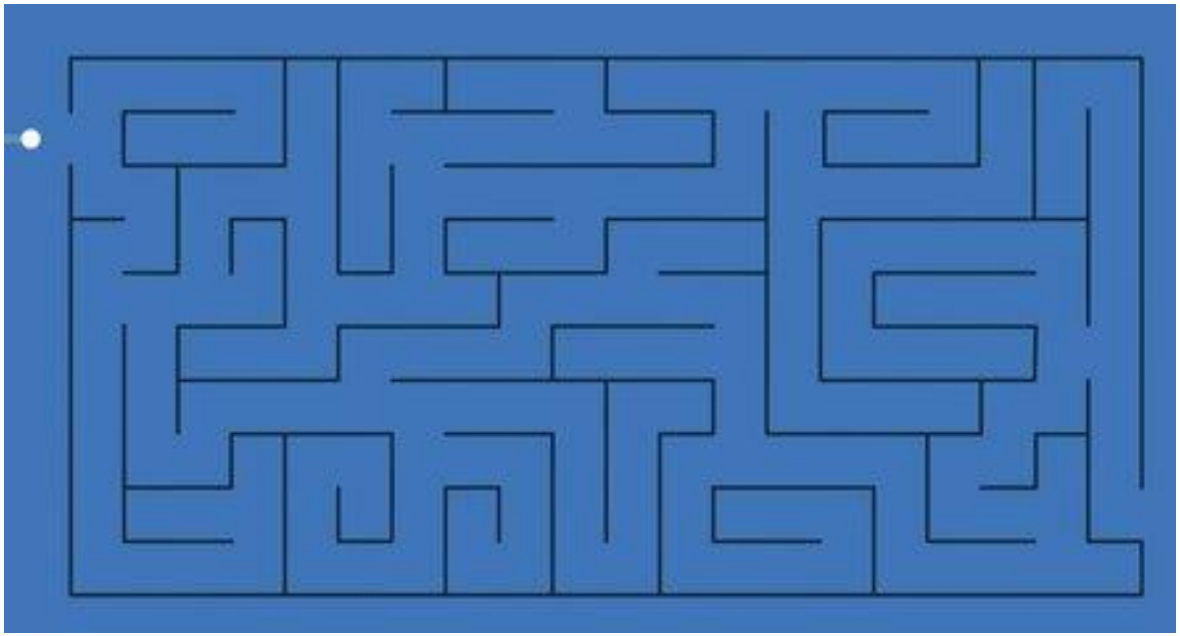
Если один кубит может быть в двух суперпозиционных состояниях, то два кубита – уже в четырёх (00, 01, 10, 11). При этом общее квантовое состояние системы выражается так: $\Psi = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

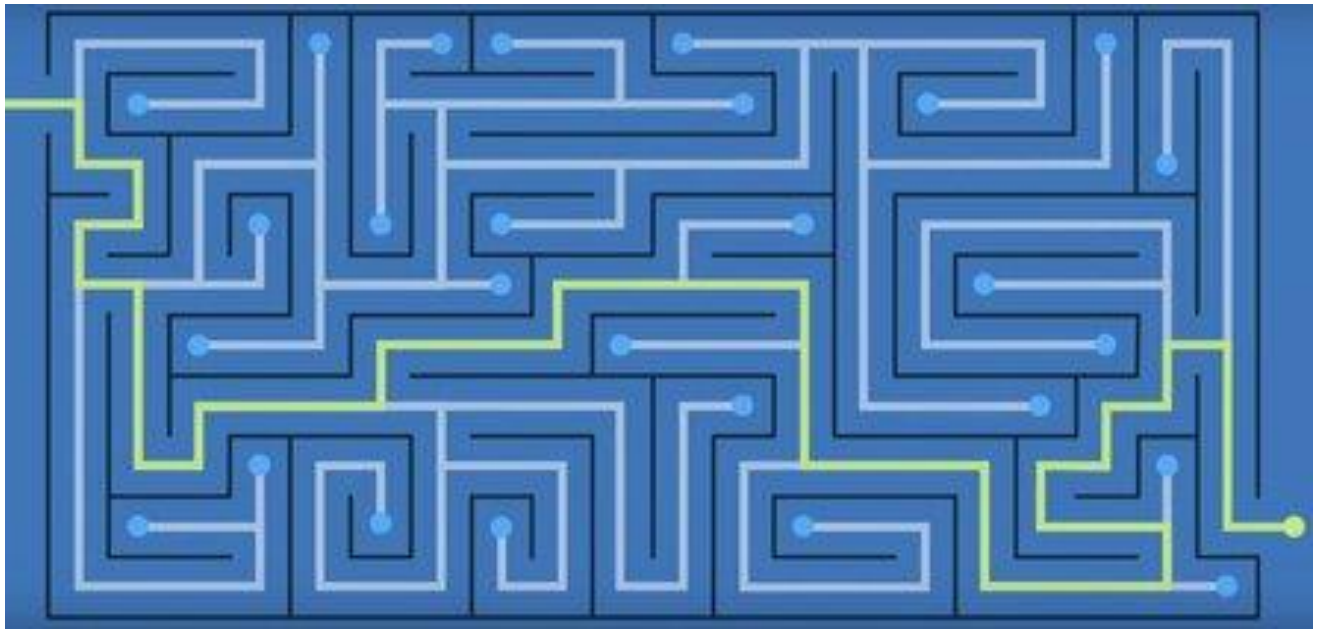
На n кубитах можно провести математическую операцию одновременно (и только одновременно) с $\mathbf{2^n}$ состояниями.

В качестве *регистра кубитов* может быть выбрана любая система, подчиняющаяся законам квантовой механики. Например, поляризационные состояния фотонов, электронные состояния изолированных атомов или ионов, спиновые состояния ядер атомов, и т. п.

Схема вычислений: берётся регистр кубитов, куда записывается начальное состояние. Затем состояние системы изменяется посредством *унитарных* преобразований, соответствующих логическим операциям. Измерение конечного состояния регистра кубитов будет являться результатом работы компьютера.

классический алгоритм вычислений

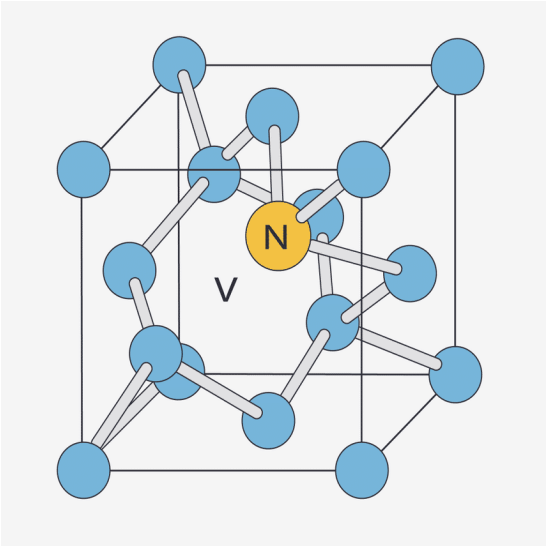


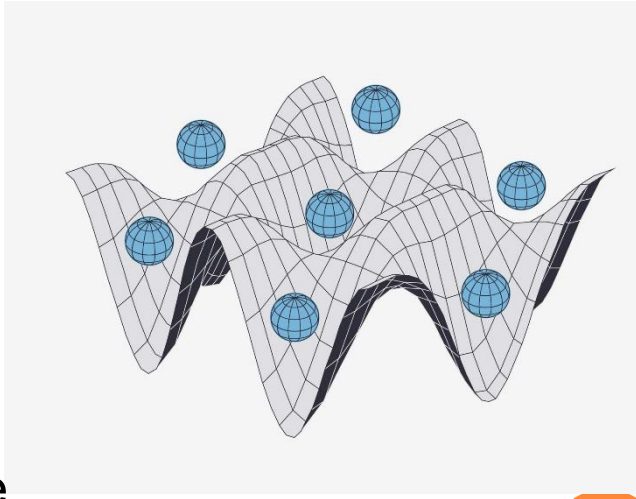


квантовый алгоритм вычислений

Примеры реализации кубитов

- В некоторых случаях в регулярной кристаллической решетке алмазов могут возникать дефекты — например, один из атомов углерода может быть замещен атомом азота.Такого типа дефекты называют NV-центрами. Электрон в NV-центре может находиться в суперпозиции двух спиновых состояний, а значит, может играть роль кубита.
- Главное преимущество «алмазных» кубитов – хорошая устойчивость: электроны в них могут удерживать своё состояние несколько секунд, что очень много по сравнению с другими типами кубитов. Кроме того, они могут успешно работать даже при комнатной температуре. Однако создать из них большие массивы кубитов – проблематично.





Примеры реализации кубитов

- **Полупроводниковые квантовые точки**: в качестве кубитов используются либо зарядовые состояния (нахождение или отсутствие электрона в определённой точке) либо направление электронного и/или ядерного спина в данной квантовой точке. Управление осуществляется через внешние потенциалы или лазерным импульсом.

- **Сверхпроводящие элементы** (джозефсоновские переходы, СКВИДы и др.). Кубит: присутствие/отсутствие куперовской пары в определённой пространственной области, либо направление магнитного поля. Управление: внешний потенциал либо магнитный поток.

- **Ионы или атомы в ловушках**. Кубиты: основное/возбуждённое состояния внешнего электрона в ионе. Управление: лазерные импульсы.

- **Смешанные технологии**: использование заранее приготовленных запутанных состояний фотонов для управления атомными ансамблями.

Принципы реализации квантового компьютера

Свойство когерентных квантовых состояний иметь сумму вероятностей, равную единице, называется **запутыванием** (сцеплением) состояний. Запутанные квантовые объекты связаны между собой независимо от того, насколько далеко они расположены друг от друга.

Максимальное время жизни квантовой системы из нескольких запутанных кубитов, в течение которого она сохраняет свои квантовые свойства и может быть использована для произведения вычислений, называют **временем декогеренции**.

Основные проблемы реализации квантового компьютера

Кубиты в запутанном состоянии крайне нестабильны: любое внешнее воздействие может разрушить связь между ними. Незначительное изменение температуры, давления, пролетевшая рядом частица (например, фотон) — все это дестабилизирует систему и приводит к некорректному результату вычислений.

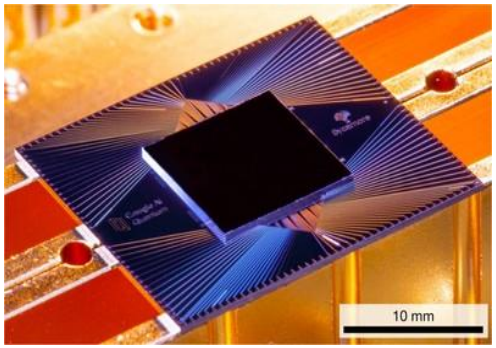
Учитывая, что даже без внешних воздействий время удержания запутанного состояния не превышает десятков микросекунд, по истечению этого времени вычислительная система кубитов начнет выдавать на выходе вместо вероятностного распределения правильных решений — белый шум.

Кроме того, к фундаментальным проблемам квантовых вычислений можно отнести:

- Накопление ошибок при вычислениях.
- Сложности с начальной инициализации состояний кубитов.
- Сложности с сопряжением кубитов в единую систему.

«Самопровозглашённый» квантовый компьютер

Популярными реализациями квантовых компьютеров остаются устройства канадской компании *D-Wave*, хотя сама квантовая природа этих компьютеров до сих пор вызывает сильные сомнения.

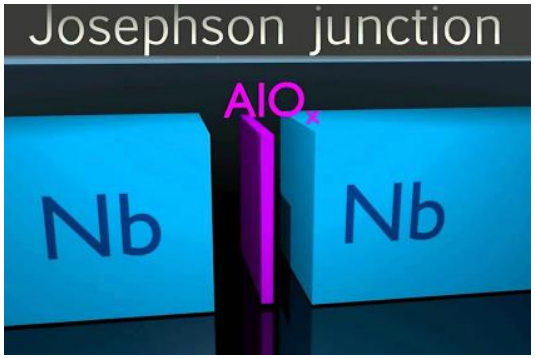


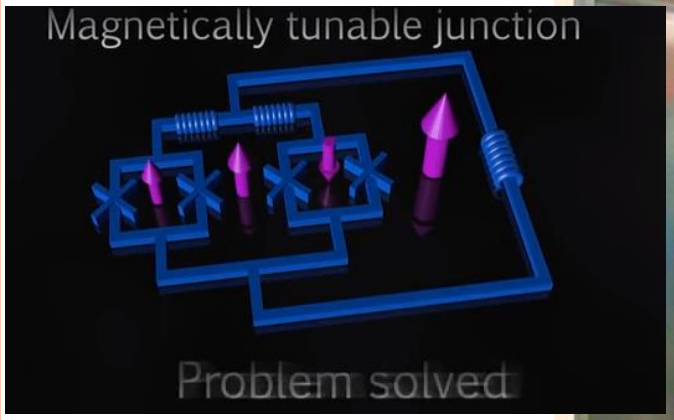
Рабочая версия компьютера продемонстрирована в 2011 году. Тип процессорной логики – адиабатическая сверхпроводящая. Искомый результат определяется в результате изменения энергетического состояния кубитов.

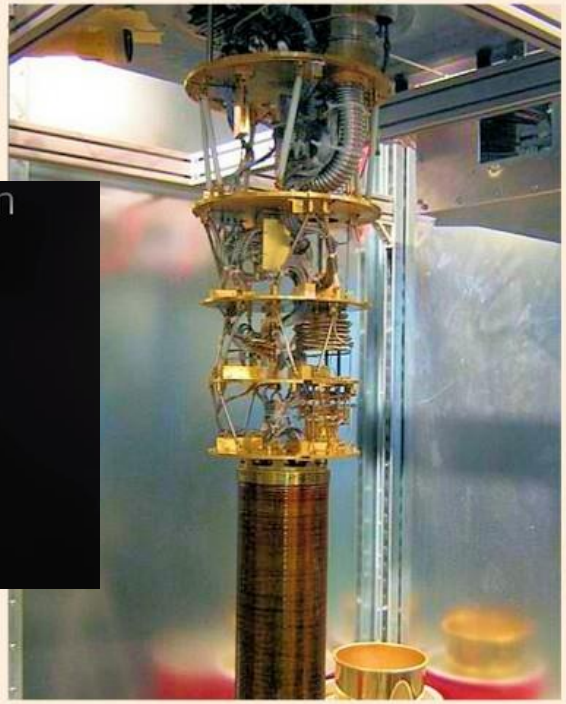
На физическом уровне кубиты представлены джозефсоновскими переходами, которые, объединяясь попарно, формируют SQUID (квантовый интерферометр). Сверхпроводящий ток способен преодолевать участки микроразрывов за счёт эффекта туннелирования электронов. Электроны образуют куперовские пары и приобретают дополнительную энергию. После прохождения электронами джозефсоновского перехода эта энергия выделяется в виде электромагнитного излучения, частота которого зависит от величины падения напряжения.

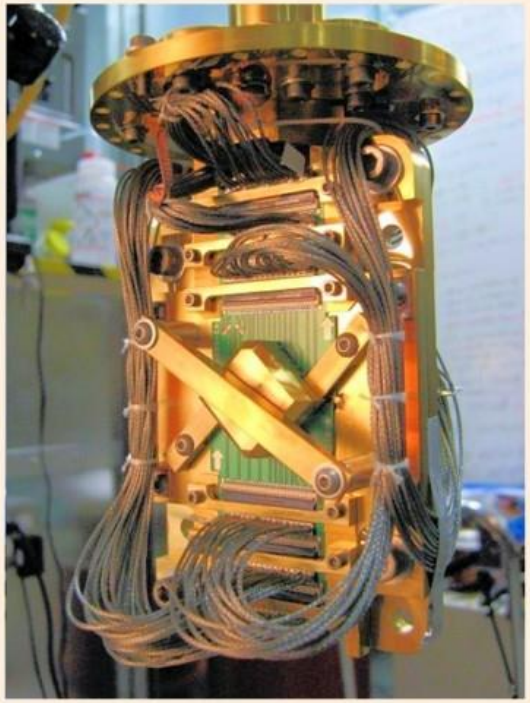
«Железо» квантового компьютера

D-Wave (one, two)

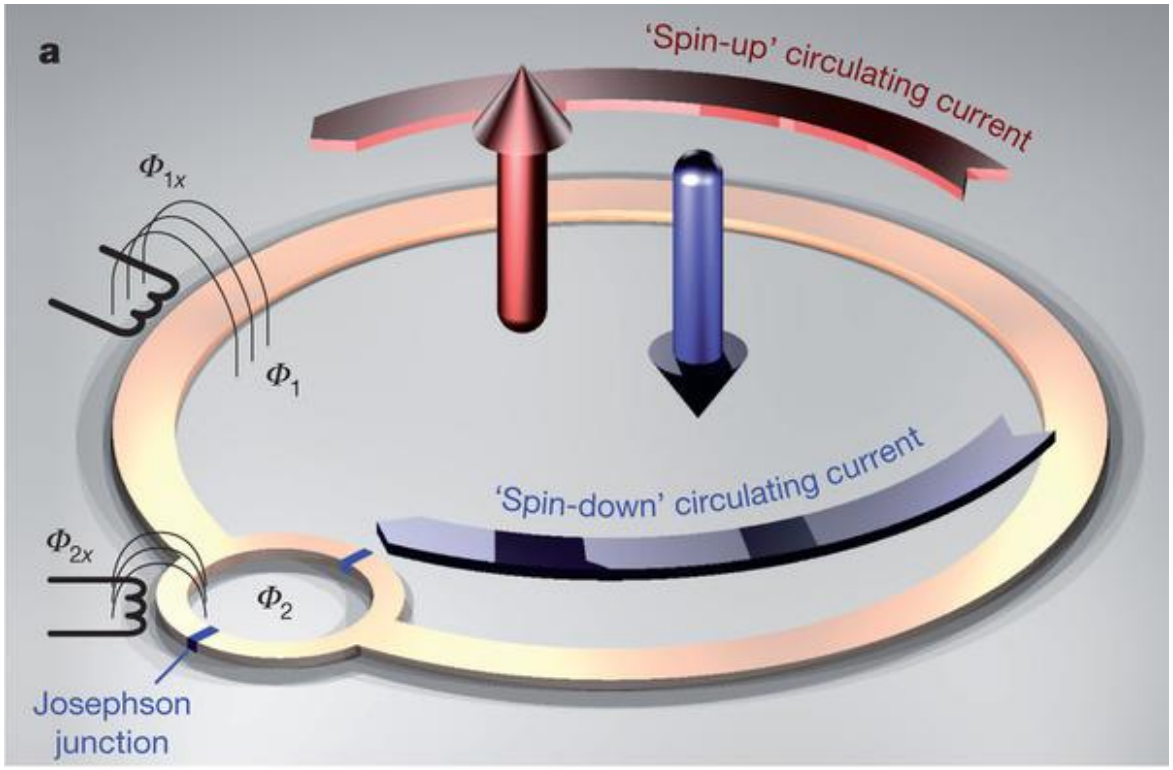


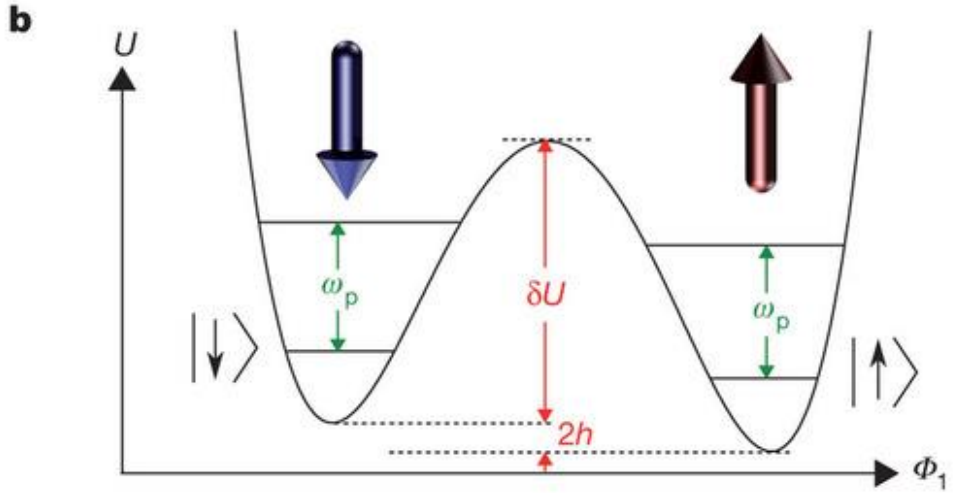






«Железо» квантового компьютера





Реализация кубита на джозефсоновских переходах: ток может течь одновременно в двух направлениях.

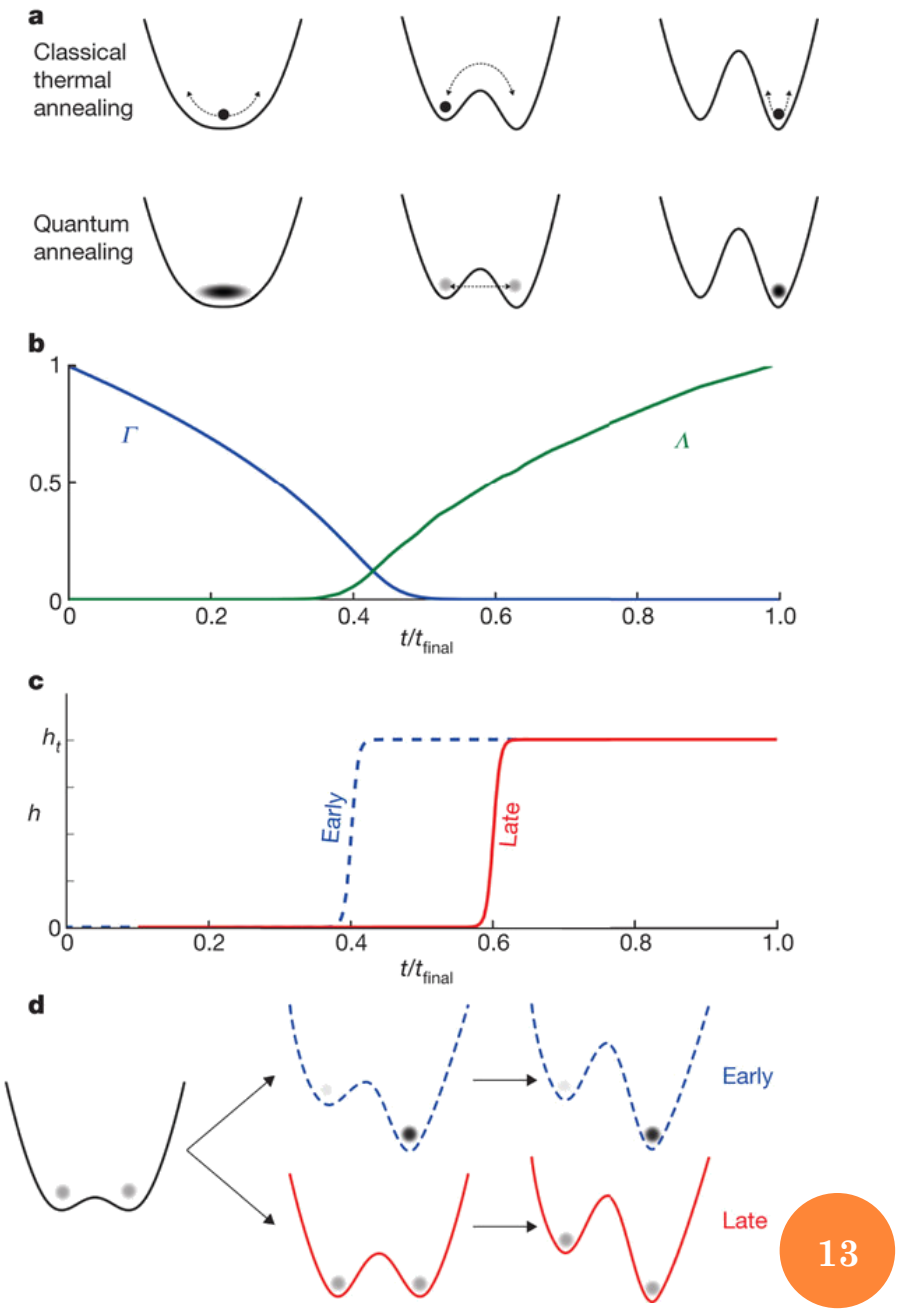
«Софт» и идеология D-Wave

Компьютер создан для решения одной задачи – дискретной оптимизации.

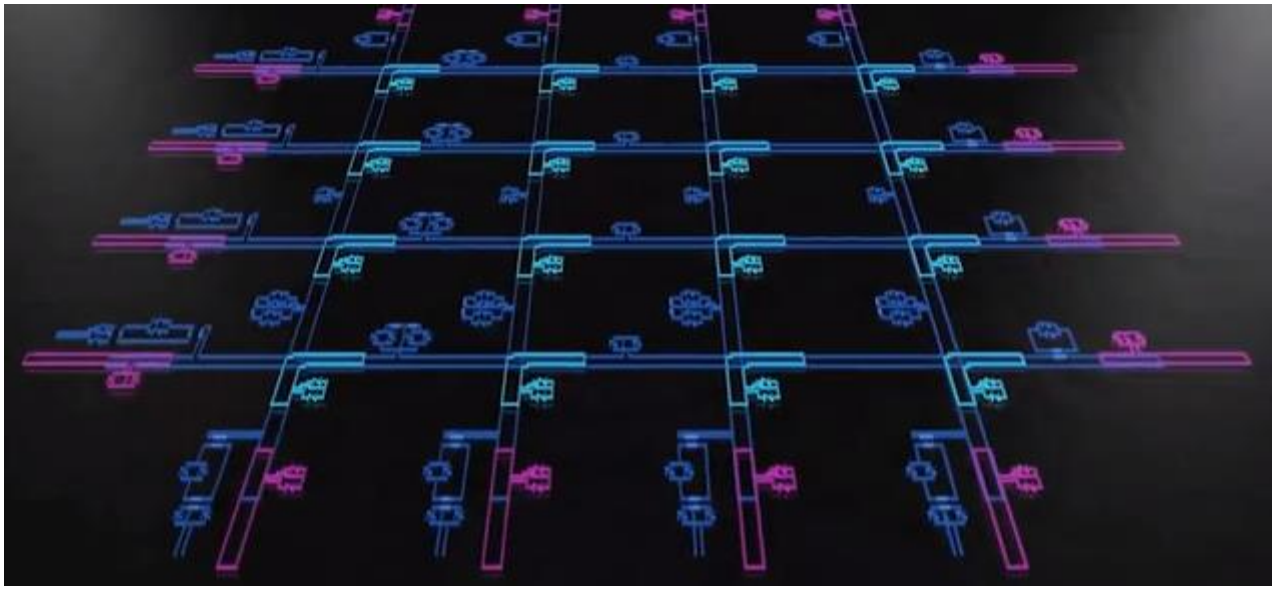
Задача решается на основе метода адиабатических квантовых вычислений.

Алгоритм реализации этого метода – квантовый отжиг (quantum annealing). Квантовый отжиг – это метод поиска глобального минимума некоторой целевой функции с помощью эффекта квантового туннелирования.

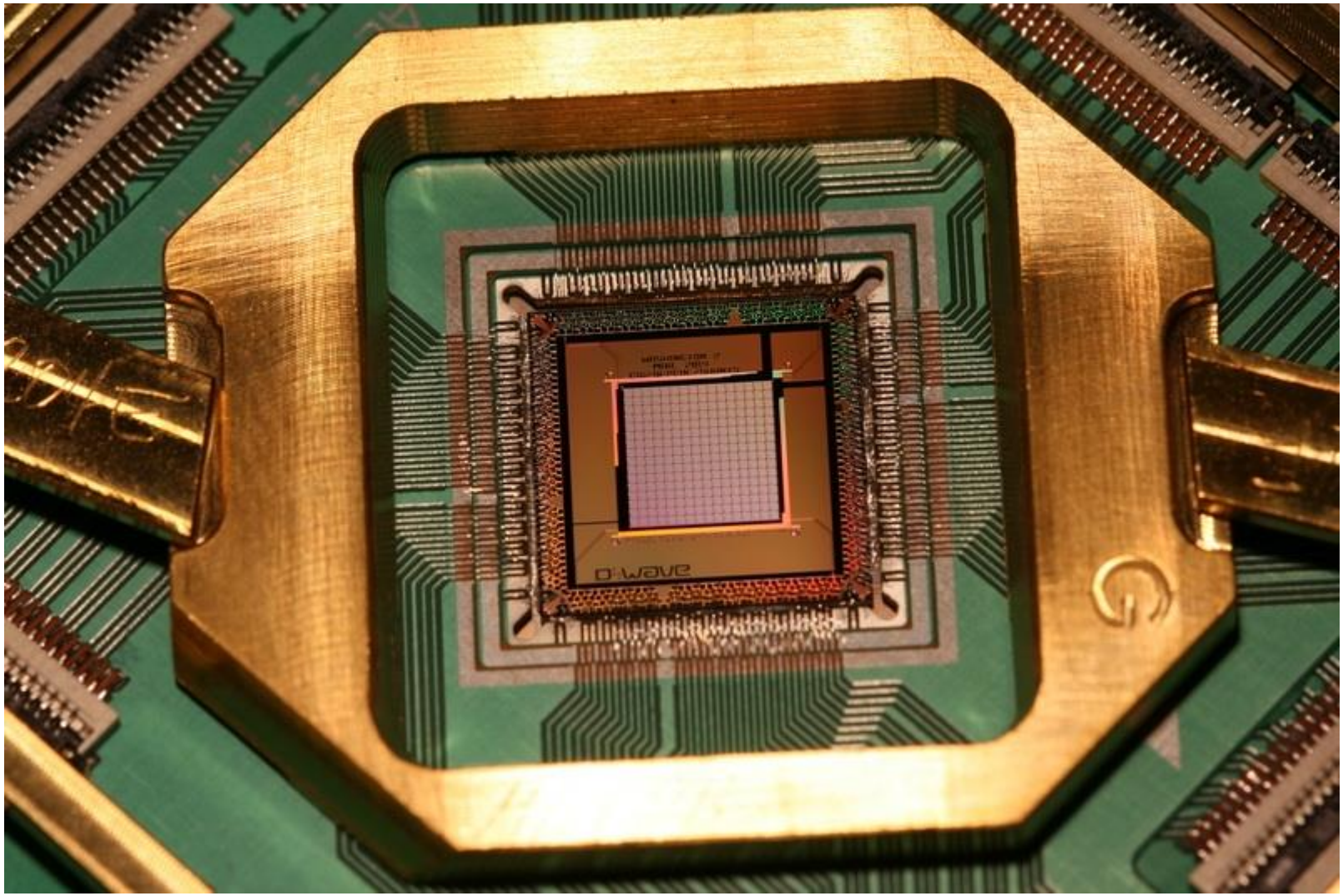
Задачей, построенной на этом алгоритме, является, в частности, квантовая бинарная классификация (QBC), т.е. метод обучения.



«Железо» квантового компьютера



«Железо» квантового компьютера



Что может решить D-Wave?

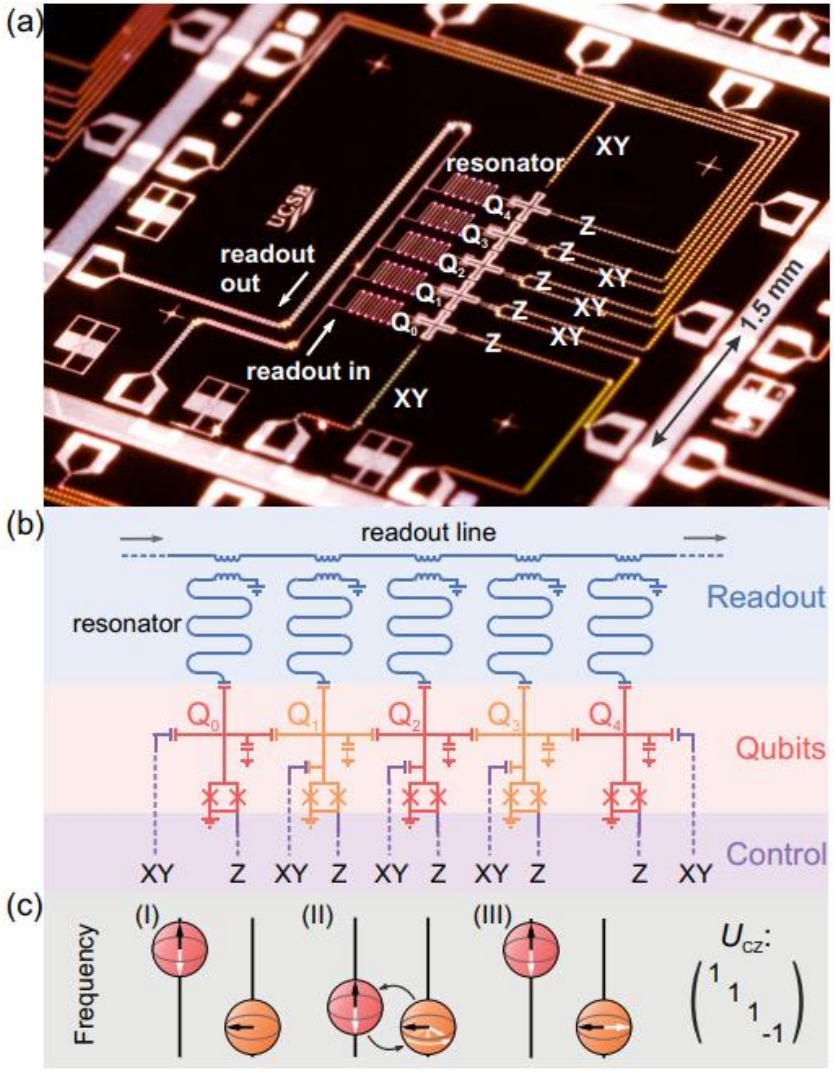
Примеры приложений для квантовых процессоров D-Wave

Задача о 3-выполнимости	Анализ дерева отказов	Моделирование атомных магнитометров
Трехмерная томография	Задача расписания	Моделирование квантово-решеточных переходов
Байесовский вывод на изображениях	Линейный метод наименьших квадратов	Проектирование телекоммуникационных сетей
Факторизация бинарных матриц	Оптимизация списка заказов	Топологический анализ данных
Балансировка бюджета при аукционной торговле	Моделирование молекулярной динамики	Оптимизация транспортных потоков
Задача маршрутизации транспортных средств	Моделирование террористических сетей	Выбор маршрутов эвакуации при цунами
Химический структурный анализ	Оптимизация маршрутов производственного транспорта	Машинное обучение: ускорение глубинного обучения
Вычислительная гидрология	Филогенетика	Машинное обучение: задача классификации
Ограниченная задача о кратчайшем пути	Подбор инвестиционных портфелей	Машинное обучение: квантовый бустинг
Моделирование выборов	Планирование расписаний спутников	Машинное обучение: тренировка нейросетей
Факторинг	Моделирование фазового перехода Костерлица — Таулеса	Машинное обучение: обучение с подкреплением
Диагностика сбоев в вычислительных сетях	Моделирование структуры материалов	Машинное обучение: обучение без учителя

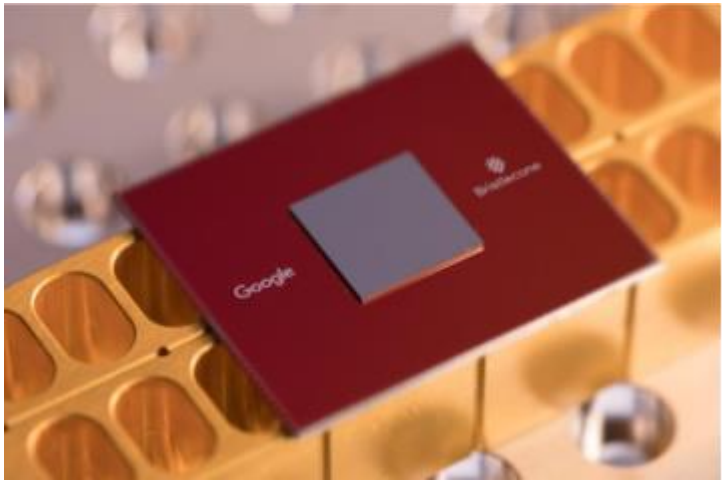
Исследовательские институты и коммерческие организации разработали около сотни приложений для квантовых процессоров D-Wave. Их уровень готовности варьируется от стадии прототипа до близкой к промышленной версии.

Среди вещей, которые можно радикально ускорить квантовыми вычислениями (по различным технологиям) — оптимизация маршрутов транспорта, секвенирование ДНК, предсказание биржевых котировок и подбор криптографических ключей.

«Bristlecone», Google's New Quantum Processor, 2018

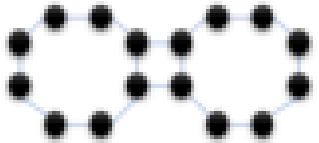


принцип на 5-кубитном варианте

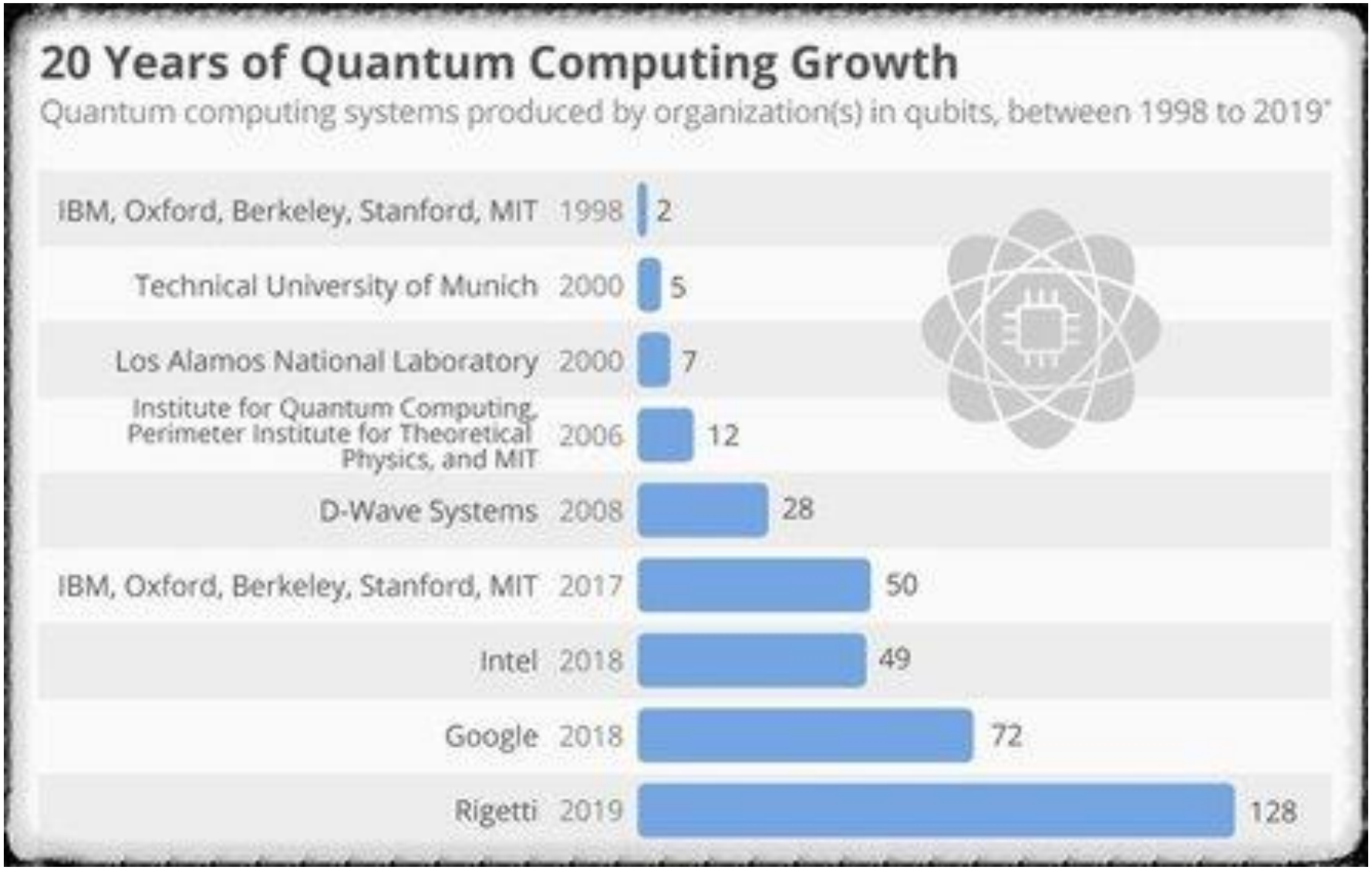


Конфигурация процессора Bristlecone включает 72 кубита.
Разработан квантовый код коррекции ошибок, который измеряет квантовое состояние кубита, запутанного с соседними кубитами. Это позволяет сохранить его исходное состояние. При этом с увеличением числа кубитов коррекция ошибок улучшается.

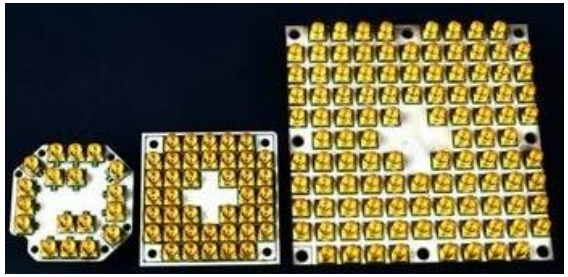
Больше всего сомнений относительно текущего состояния квантовых вычислений вызывает разброс между сообщениями об их теоретических возможностях и реально достижимыми результатами.

Machine	Qubits	2Q Gates	Coherence Time (us)	1Q Error (%)	2Q Error (%)	RO Error (%)	Qubit Topology
IBM Q5 Tenerife	5	6	40	0.2	4.76	6.21	
IBM Q14 Melbourne	14	18	30	1.19	7.95	9.09	
IBM Q16 Rüschlikon	16	22	40	0.22	7.14	4.15	
Rigetti Agave	4	3	15	3.68	10.8	16.37	
Rigetti Aspen1	16	18	20	3.43	8.92	5.56	
Aspen3	16	18	20	3.79	5.37	6.65	
UMD Ion Trap	5	10	1.5×10^6	0.2	1.00	0.6	

Все существующие квантовые процессоры построены таким образом, что обеспечивают приемлемое запутывание одного кубита только со своими соседями, которых не больше шести. Больше операций → больше ошибок → сильнее влияние декогерентности.

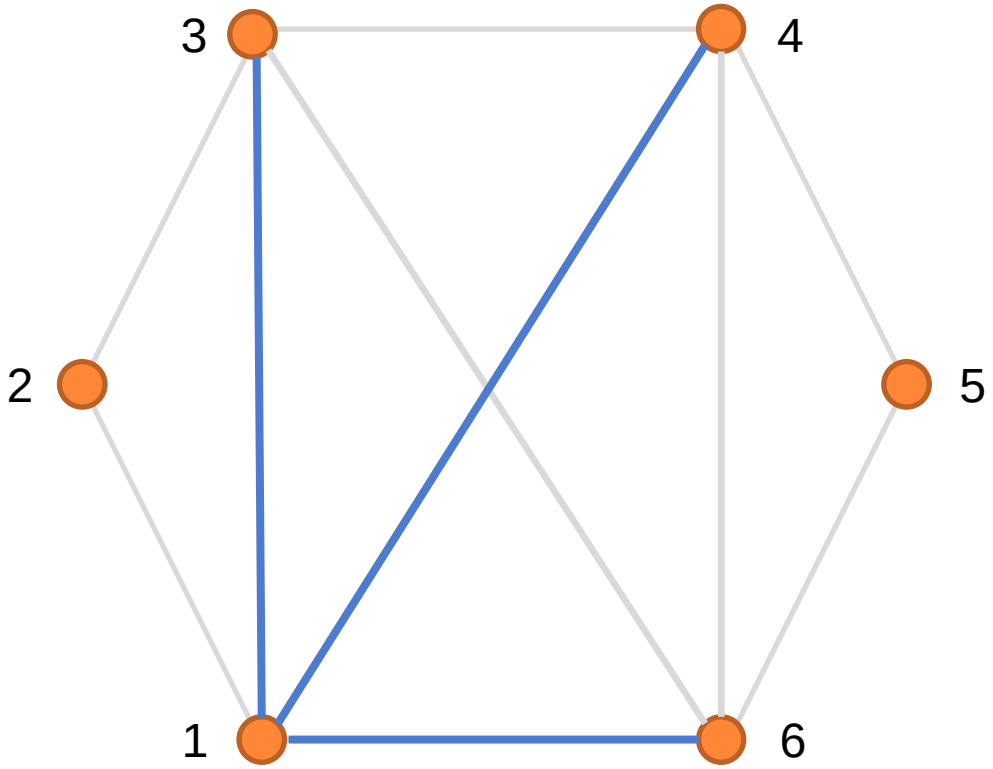


Всего, по данным аналитической компании CB Insights, над задачей создания квантового компьютера бьются не менее 18 корпораций.



Тест для квантового компьютера: числа Рамсея

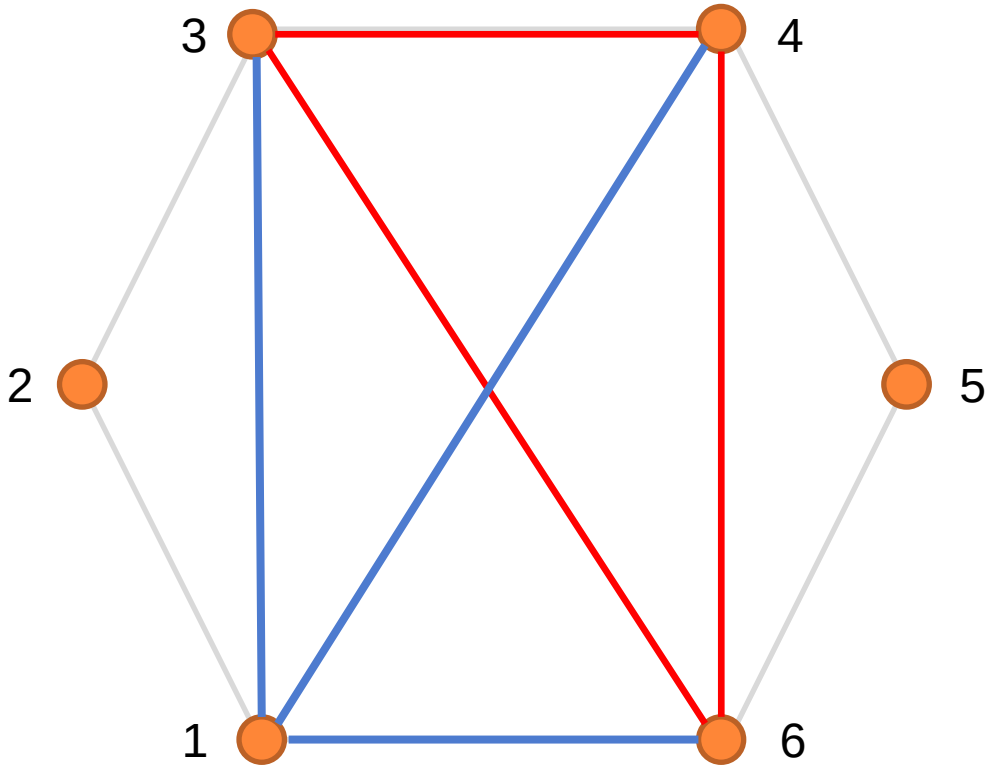
Задача: Какова наименьшая полная сеть, которая будучи произвольным образом раскрашена в красный и синий цвет (в два цвета), обязательно содержала бы либо красную сеть из трёх точек (треугольник), либо синюю сеть из трёх точек?



Пусть есть группа из шести человек. Докажите, что в этой группе обязательно найдутся три человека, которые будут попарно знакомы друг с другом, либо которые будут попарно незнакомы друг с другом.

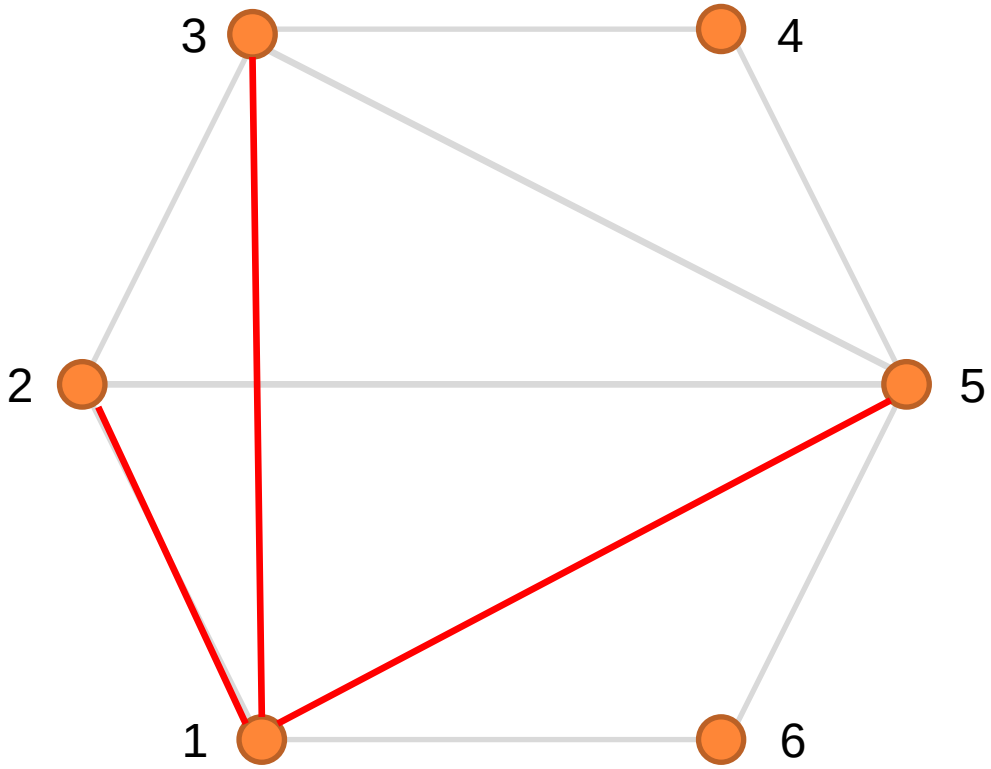
К вопросу о числах Рамсея

Задача: Какова наименьшая полная сеть, которая будучи произвольным образом раскрашена в красный и синий цвет (в два цвета), обязательно содержала бы либо красную сеть из трёх точек (треугольник), либо синюю сеть из трёх точек?



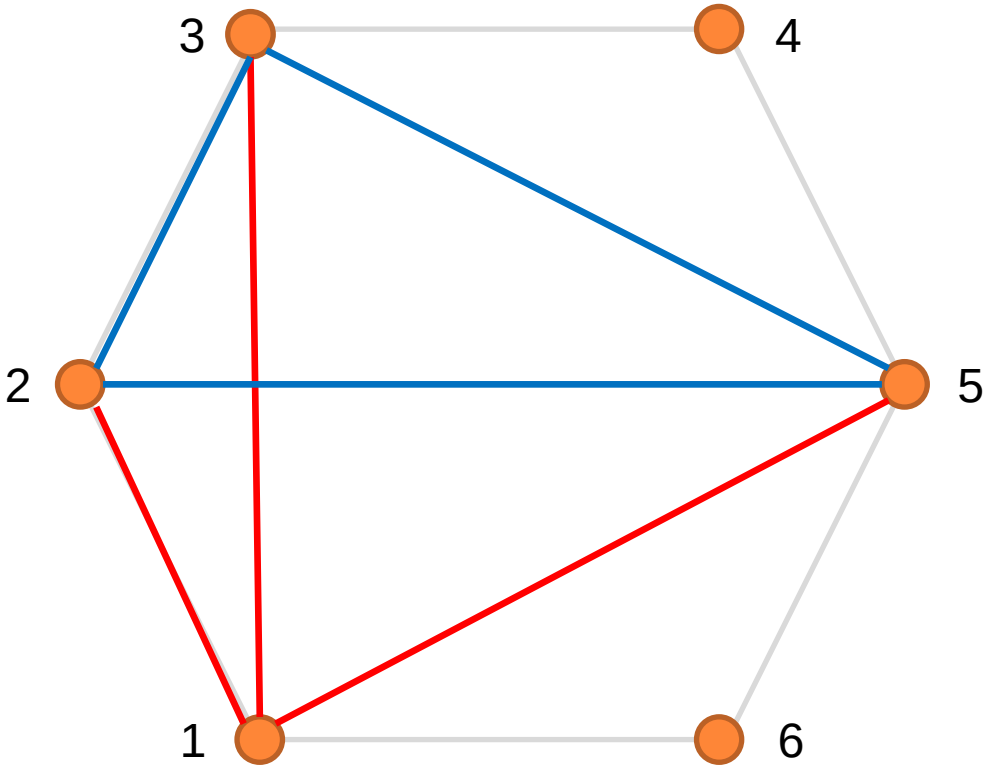
К вопросу о числах Рамсея

Задача: Какова наименьшая полная сеть, которая будучи произвольным образом раскрашена в красный и синий цвет (в два цвета), обязательно содержала бы либо красную сеть из трёх точек (треугольник), либо синюю сеть из трёх точек?



К вопросу о числах Рамсея

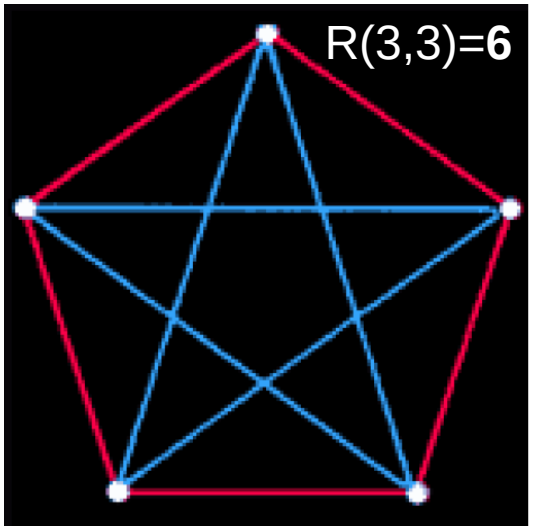
Задача: Какова наименьшая полная сеть, которая будучи произвольным образом раскрашена в красный и синий цвет (в два цвета), обязательно содержала бы либо красную сеть из трёх точек (треугольник), либо синюю сеть из трёх точек?

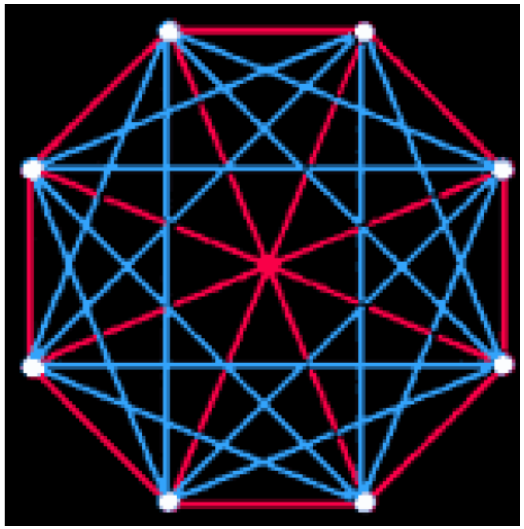


R(3,3)=6

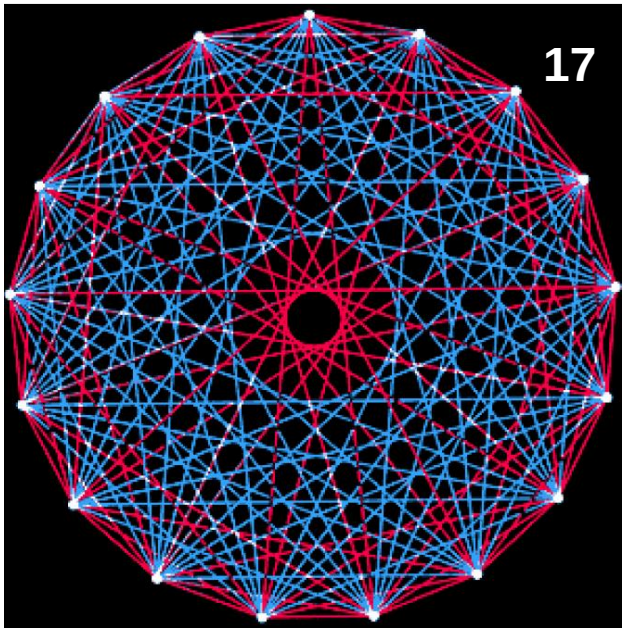
Пример задачи для квантового компьютера

Задача построения двухцветных графов чисел Рамсея





R(3,4)=**9**



Ответ: R(4,4)=**18**

D-Wave на решение этой задачи потребовалось 270 миллисекунд, было задействовано 28 кубитов, остальные - корректировали ошибки.

R(5,5) = ???

И когда же будет решение?

Таблица значений [править | править код]

Для $N(q_1, q_2, \ldots, q_t; t)$ при $t > 2$ имеется очень мало данных[3]. Следующая таблица значений чисел Рам
Радзишевского[en][4], данные приведены по состоянию на 2020 год.

r, s	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10
3	1	3	6	9	14	18	23	28	36	[40, 42]
4	1	4	9	18	25	[36, 41]	[49, 61]	[59, 84]	[73, 115]	[92, 149]
5	1	5	14	25	[43, 48]	[58, 87]	[80, 143]	[101, 216]	[133, 316]	[149, 442]
6	1	6	18	[36, 41]	[58, 87]	[102, 165]	[115, 298]	[134, 495]	[183, 780]	[204, 1171]
7	1	7	23	[49, 61]	[80, 143]	[115, 298]	[205, 540]	[217, 1031]	[252, 1713]	[292, 2826]
8	1	8	28	[59, 84]	[101, 216]	[134, 495]	[217, 1031]	[282, 1870]	[329, 3583]	[343, 6090]
9	1	9	36	[73, 115]	[133, 316]	[183, 780]	[252, 1713]	[329, 3583]	[565, 6588]	[581, 12677]
10	1	10	[40, 42]	[92, 149]	[149, 442]	[204, 1171]	[292, 2826]	[343, 6090]	[581, 12677]	[798, 23556]

https://ru.wikipedia.org/wiki/Теорема Рамсея

Почему не получается?

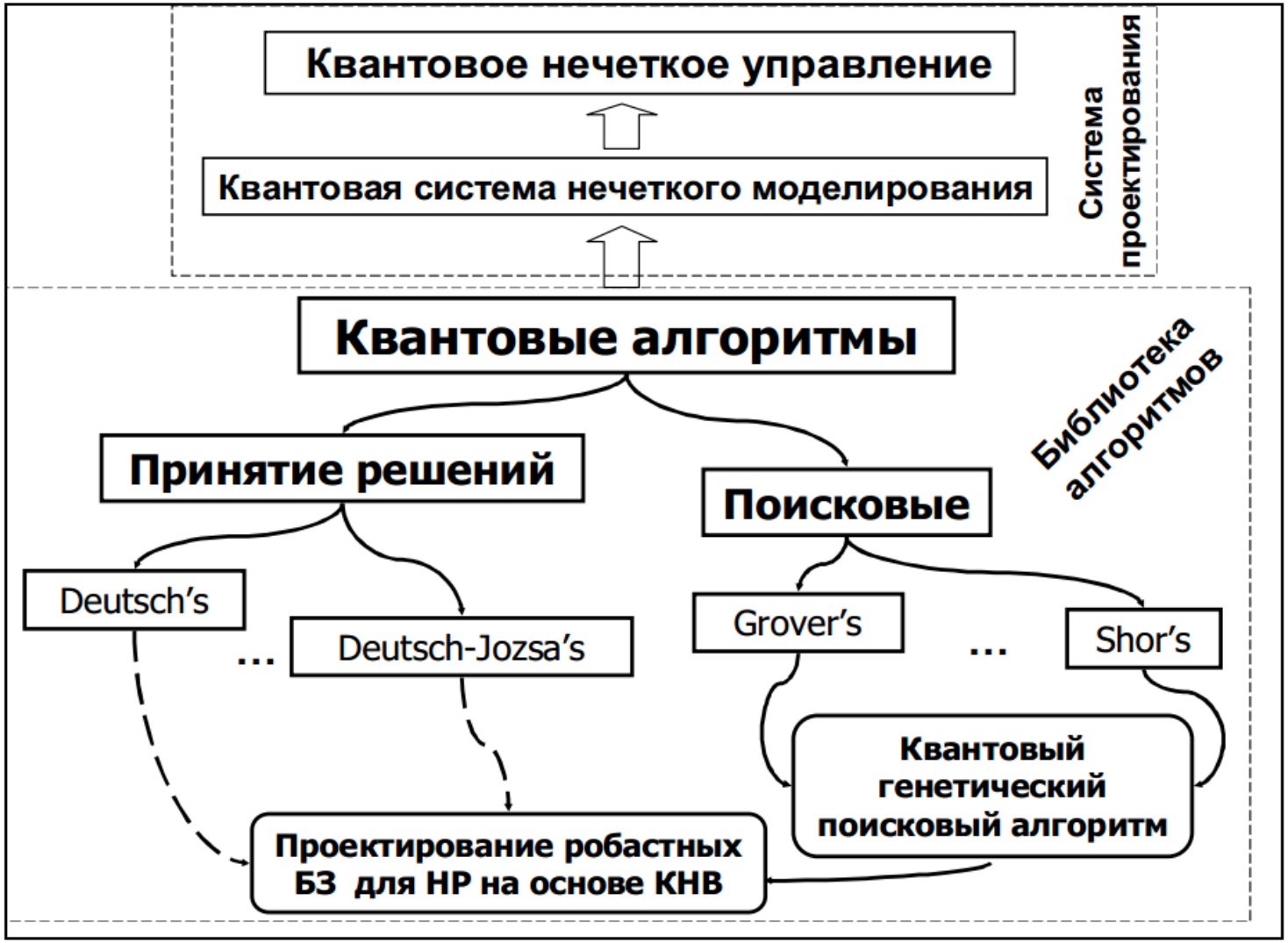
1. Чем больше кубитов находятся в связанном состоянии, тем менее стабильной является система. Для достижения «квантового превосходства» требуется компьютер со многими десятками связанных кубитов, работающими стабильно и с малым числом ошибок.

2. Надо решить поставленную задачу, пока кубит «не умер». Чем больше кубитов – тем меньше время жизни их связанного состояния.

Пути решения:

- Использование криокамер с предельно низкими температурами.
- Использование максимально защищенных от внешних воздействий процессорных блоков.
- Использование систем квантовой коррекции ошибок (Логический кубит).
- Использование оптимизаторов при программировании схем для конкретного процессора.

Классификация квантовых алгоритмов



"Состояние на выходе системы может быть когерентной суперпозицией состояний, соответствующих различным ответам, каждый из которых является решением задачи".

Другие задачи для (других) квантовых компьютеров

1) **Алгоритм Дойча — Йожи** (1992) позволяет «за одно вычисление» определить, является ли функция двоичной переменной $f(n)$ постоянной (принимает либо значение 0, либо 1 при любых аргументах) или сбалансированной (для половины области определения принимает значение 0, для другой половины 1).

2) **Алгоритм Шора** (1994) — квантовый алгоритм факторизации (разложения числа на простые множители). С его помощью (при использовании квантового компьютера с несколькими сотнями логических кубитов) становится возможным взлом криптографических систем любой реально используемой сложности с открытым ключом за время, не превышающее время шифрования. Используется квантовое Фурье-преобразование.

3) **Алгоритм Гровера** (1996) — квантовый алгоритм решения задачи перебора, то есть нахождения решения уравнения $f(x)=1$, где f есть булева функция от n переменных. На основе данного алгоритма созданы, в частности, схема поиска экстремума целочисленной функции и алгоритм поиска совпадающих строк в базе данных.

Faith, trust and pixie dust