양자 컴퓨팅이란

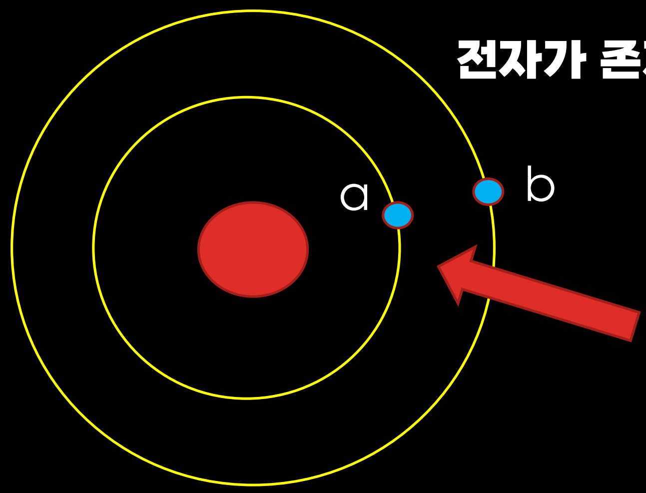
동명대학교 게임공학과
강영민

1. 양자의 기묘함

양자란 무엇인가?

- 양자(quantum)
  - 에너지, 운동량, 퍼텐셜 등의 물리량이 연속값을 취하지 않고 **특정 최소 단위의 정수배로 표현**가능할 때, 그 **최소 단위의 양**을 가리키는 용어
- 우주는 양자
  - 모든 물리량에는 기본단위가 있으며, **우주의 물리량은 이 기본 단위의 정수배만 존재**한다.
  - 우주는 연속체가 아니다! (도대체 우주란 무엇일까?)

전자가 존재할 수 있는 궤도



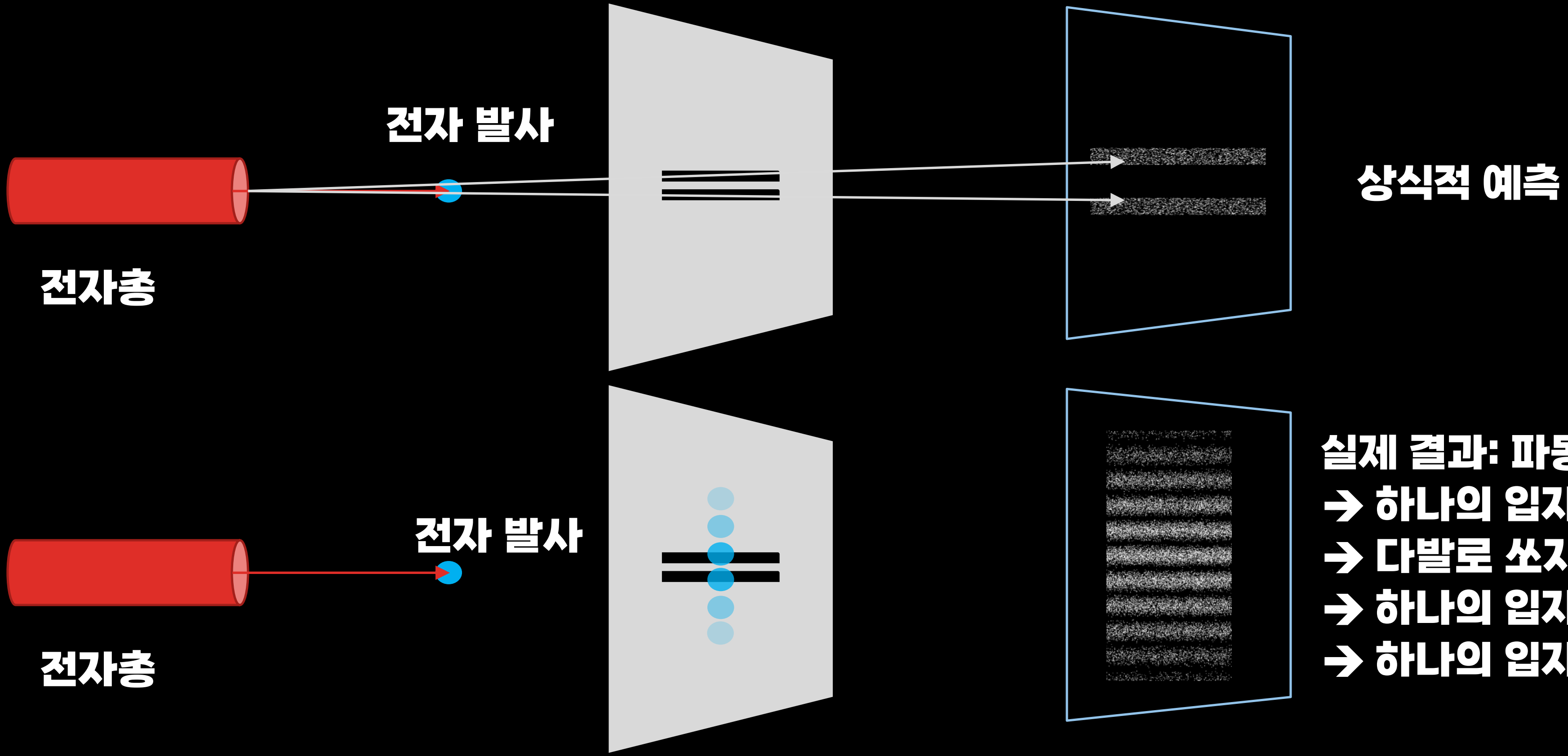
이런 공간에 전자가 놓일 수 없음
→ a의 궤도에 있는 전자가 b 궤도로 에너지를 받아 이동할 때
→ 중간 공간을 거치지 않고 b 궤도로 순간이동함: quantum jump (무한의 속도?)

양자의 기묘함

- 우주는 거시적으로 보면 연속체처럼 보이지만 미시적으로는 양자화=이산적 값으로 이루어짐
  - 양자화 예
    - 빛 알갱이 = 광자
      - 단일 양자로 광자 = 광양자
    - 전자의 에너지는 양자화 되어 있어 특정 값의 정수배인 값만 취할 수 있음 = 이를 통해 원자가 안정화
  - 양자는 미시세계의 기본 골조
- 이 양자는 직관에 반하는 특성을 가짐
  - 불확정성의 원리
  - 양자의 상태는 확률적으로 파악되며, 서로 다른 상태가 동시에 존재하는 "중첩"을 보임
    - 이 고양이는 죽었을 확률이 50%이고 살았을 확률이 50%라고 말할 때
      - 죽은 고양이와 산 고양이가 함께 존재한다는 의미 (실제로 이런 일은 벌어지지 않는다. 고양이=관찰자)
  - 양자는 서로 다른 상태가 함께 존재하는 중첩(superposition)의 특성을 갖는다
  - 이게 어떤 상태인지 관찰하면 중첩은 하나의 상태로 붕괴(collapse)된다.

증거 – 이중슬릿 실험

- 전자빔을 두 개의 틈을 향해 쏜다: 전자 입자는 둘 중 하나를 통과할 것이다 (전통적인 물리학)

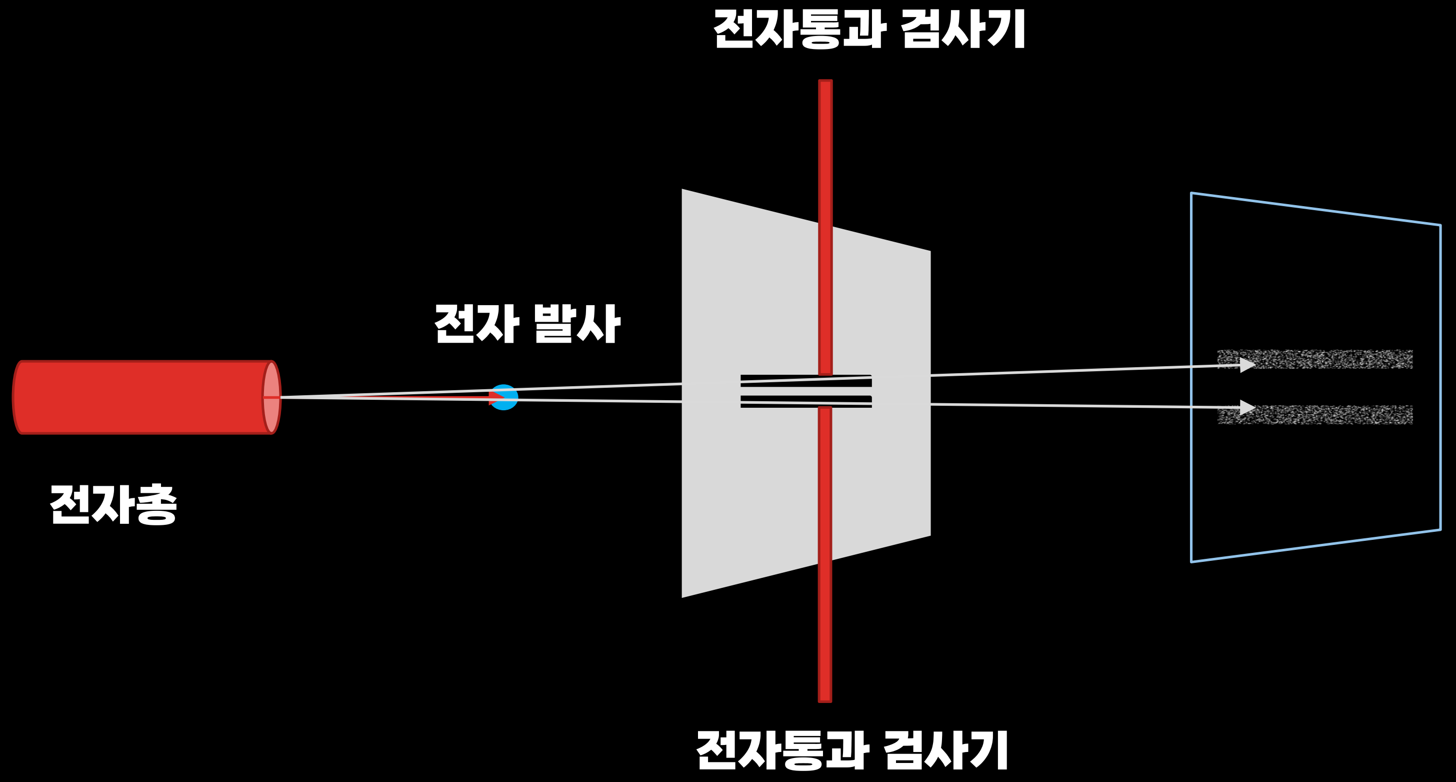


실제 결과: 파동과 같은 간섭무늬
→ 하나의 입자가 두 틈새를 동시에 통과
→ 다발로 쏘지 않고 하나씩 쏘아도 간섭
→ 하나의 입자가 두 슬릿을 통과한다
→ 하나의 입자는 **두 곳에 동시에 존재**

하나의 전자는 매우 많은 상태가 존재
일부는 통과하는 상태, 일부는 통과하지 못하는 상태 (확률은 다름)

증거 – 측정이 중첩을 붕괴시킴

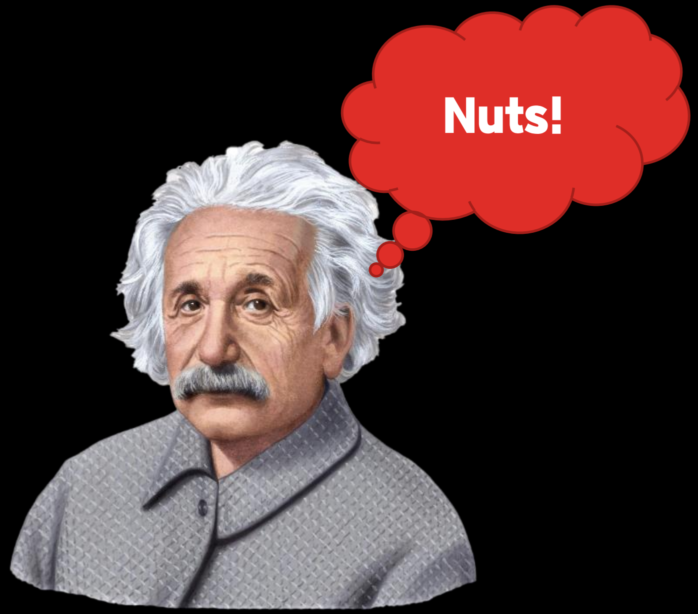
- 전자빔을 두 개의 틈을 향해 쏜다
  - 각각의 슬릿에 전자가 통과하는지를 확인하는 검사기를 설치



간섭무늬 사라짐
: 상태를 확인하면 중첩이 붕괴
→ 하나의 상태만 존재

달은 존재하지 않는다. 보기 전까지는

- 우리가 달을 쳐다 보지 않을 때, 우리가 예상하는 곳에 달은 존재하지 않는다.
- 우리가 달을 쳐다 본 순간 달은 그 상태에 붕괴되어 있게 된다



양자의 세계

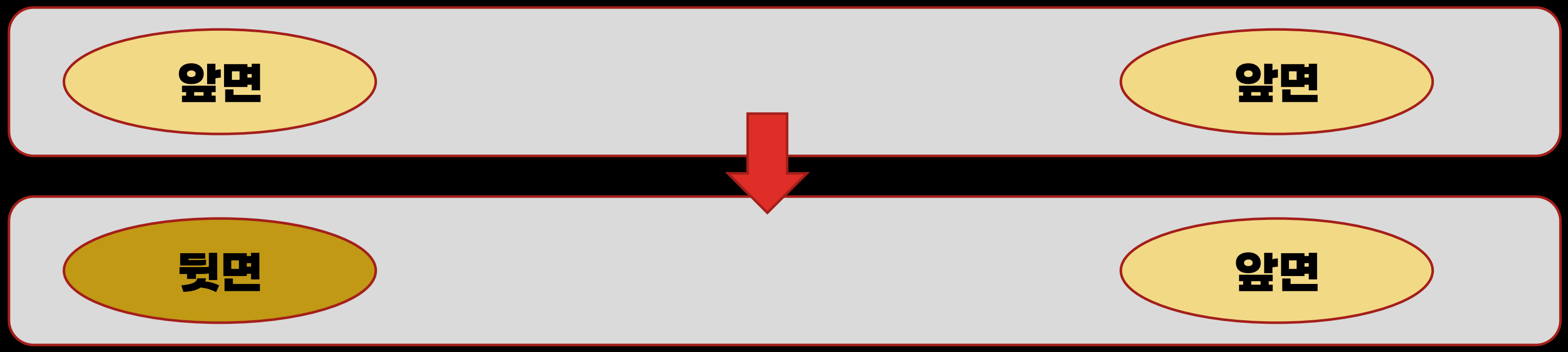
관측 이전의 상태는 중첩되어 있다.
관측은 상태를 붕괴시킨다.
내가 알지 못 하는 관찰자의 관측도 상태를 붕괴시킨다.
하지만, 나는 관측 이전에 붕괴된 상태를 알 수는 없다.
내가 모르지만 붕괴된 상태라는 실재가 존재하지 않을까?

양자역학은 현상에 부합하는 틀을 제공하지만,
이를 해석하는 방법은 다양

- 코펜하겐 해석은 실재의 존재를 부정하지 않음
- 다중 우주 해석은 가능한 모든 상태가 병렬적으로 존재
- 상대적 양자 역학과 Qbism 등은 붕괴된 상태도 상대적이라 봄

양자의 또다른 기묘함

- 얽힘(entanglement)
  - 두 물체가 얽혀 있다 = 하나의 상태가 다른 상태를 결정한다.
- 얽히지 않은 상태 = 서로 독립적인 상태
  - 두 개의 동전



왼쪽 동전을 뒷면으로 뒤집는다고 오른쪽 동전이 뒤집어지지 않는다.

- 얽힌 동전
  - 두 개의 동전은 더 이상 독립적인 상태를 갖지 않고, 하나의 상태가 다른 하나의 상태를 결정한다.
  - 앞-뒷면 상태가 얽혀 있다면, 하나를 뒤집으면 다른 하나도 뒤집힌 상태가 된다.

SPOOKY ACTION AT A DISTANCE

- 아인슈타인이 이해할 수 없었던 얽힘

얽힌 동전을 우주의 양쪽 끝에 보내고, 한 쪽을 뒤집으면 우주 반대쪽에 가보지 않고도 다른 동전의 상태를 알 수 있다.
아인슈타인 가라사대, "어떤 정보도 빛의 속도보다 빠르게 전달될 수 없다"
이렇게 먼 거리의 정보를 시간 흐름 없이 바로 알 수 있다는 것은 물리학의 법칙을 벗어난다고 생각

아이슈타인에 동의하며 양자 얽힘을 이해하는 해석
→ 얽힘이 연관을 보여주지만, 이를 이용해 전통적 정보를 보낼 수 없으며, 얽힌 입자의 상태를 측정했을 때 얻는 결과는 순전히 랜덤하며, 미리 정한 메시지를 실을 수 없다.
→ 이 측정의 결과를 조작하거나 제어하여 정보를 실을 수 없다
→ 얽힘을 이용하여 정보를 무한의 속도로 전달할 방법은 없다.

"정보를 무한의 속도로 전달할 수는 없지만, 양자가 얽히는 것은 명백한 사실이고 이는 양자 암호 등에 사용될 수 있다."

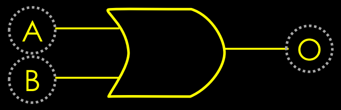
2. 컴퓨팅에 대하여

컴퓨팅이란 무엇인가?

- 컴퓨팅 = 정보를 처리하는 일
- 컴퓨팅에는 무엇이 필요한가
  - 정보를 저장하는 방법 = 하드웨어
  - 정보를 연산하여 새로운 정보를 만드는 방법 = 연산 장치
  - 정보와 연산을 조합하고 조건에 따라 연산 흐름을 제어하여 필요한 정보를 생산하는 일 = 알고리즘
- 현대 문명의 총아, 디지털 컴퓨터
  - 정보 저장: 비트(bit) – 트랜지스터를 통해 전류를 보내면 1, 보내지 않으면 0
  - 연산: 부울 게이트(Boolean gates) – 논리 합, 논리 곱, XOR, Not 연산을 수행하는 회로
  - 게이트를 조합하고, 조건 분기와 반복이 가능한 회로를 연결함으로써
    - 디지털 컴퓨터는 알고리즘을 표현되는 모든 문제를 해결할 수 있는 Universal Turing Machine
      - 메모리가 유한하다는 등의 물리적 한계를 무시하고 볼 때 UTM

컴퓨팅의 예

- 비트(bit)
  - 전기가 흐르면 1 ●
  - 전기가 흐르지 않으면 0 ○
- 논리 연산 게이트
  - OR



전기

A	B	O
○	○	○
○	●	●
●	○	●
●	●	●

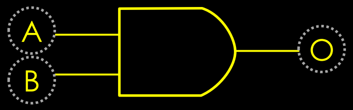
논리

A	B	O
거짓	거짓	거짓
거짓	참	참
참	거짓	참
참	참	참

수치

A	B	O
0	0	0
0	1	1
1	0	1
1	1	1

  - AND

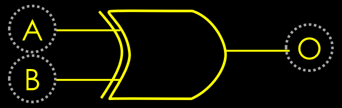


A	B	O
○	○	○
○	●	○
●	○	○
●	●	●

A	B	O
거짓	거짓	거짓
거짓	참	거짓
참	거짓	거짓
참	참	참

A	B	O
0	0	0
0	1	0
1	0	0
1	1	1

  - XOR



A	B	O
○	○	○
○	●	●
●	○	●
●	●	○

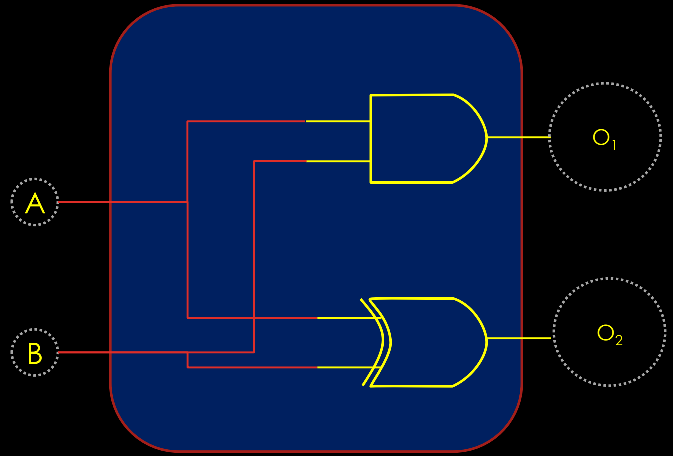
A	B	O
거짓	거짓	거짓
거짓	참	참
참	거짓	참
참	참	거짓

A	B	O
0	0	0
0	1	1
1	0	1
1	1	0

덧셈 연산

- 이진수 덧셈
  - 0 + 0 = 0 0
  - 0 + 1 = 0 1
  - 1 + 0 = 0 1
  - 1 + 1 = 1 0

덧셈기



A	B	O_1	O_2
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

양자 컴퓨팅은?

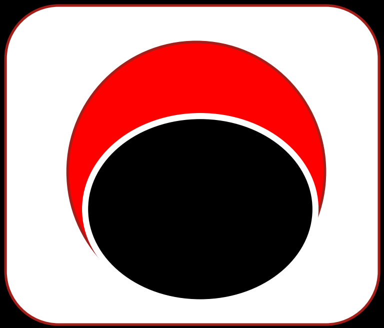
- 정보의 저장 장치를 바꾼다
  - 비트(bits) → 큐비트(Qubits)
    - 큐비트는 양자의 특성을 갖는다
- 양자의 기묘함을 이용한다
  - 양자의 이해하기 어려운 기묘함 – 중첩(superposition) / 얽힘(entanglement)
  - 큐비트는 중첩과 얽힘을 갖는다.
  - 이러한 특성을 이용하여 큐비트를 연산하는 컴퓨터를 만들어 보자
- 그러면 무엇이 좋은가?

QUBITS

- 비트가 하나일 때: (   )
  - (●) 일 수도 있고, (○)일 수도 있다. 그런데 둘 중의 하나로만 존재할 수 있음
  - 1인 상태와 0인 상태를 모두 표현하려면 1비트 저장장치가 2개 필요
    - 장치 1: (●)
    - 장치 2: (○)
- 비트가 두 개일 때 표현할 수 있는 상태의 수 : (   ) (   )
  - 4 가지 상태가 가능
    - (○) (○)
    - (○) (●)
    - (●) (○)
    - (●) (●)

네 가지 상태를 다 표현하려면
두 비트 저장장치가 4개 필요

Qubit

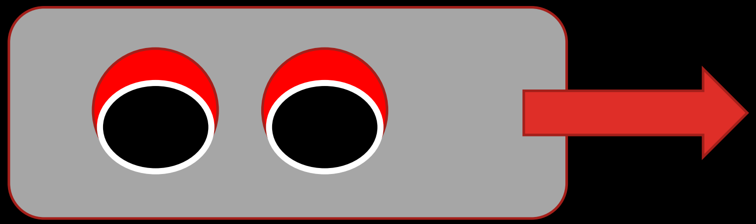


0과 1의
상태가 중첩

두 가지 상태가 중첩될 수 있을 때 qubit
세가지 상태가 중첩되면 qutrit
N 상태 중첩이 가능하면 quNit라고 하는데
현재 양자컴퓨터의 주대상은 qubit

QUBITS

- 00, 01, 10, 11의 네 가지 상태를 모두 표현하는 큐비트
  - 두 개의 큐비트를 가진 저장장치 1개면 충분



이 큐비트에 적용되는 “양자 효과quantum effects"을 이용하여 계산

- 그러면 이 큐비트의 신호를 처리하는 게이트는?
  - OR, XOR, AND 게이트가 아님
  - 양자 게이트
    - 항등(Identity) 게이트
    - 파울리(Pauli) 게이트
    - 아다마르(Hadamard) 게이트

뭘 할 수 있는지 나중에 살펴 보자

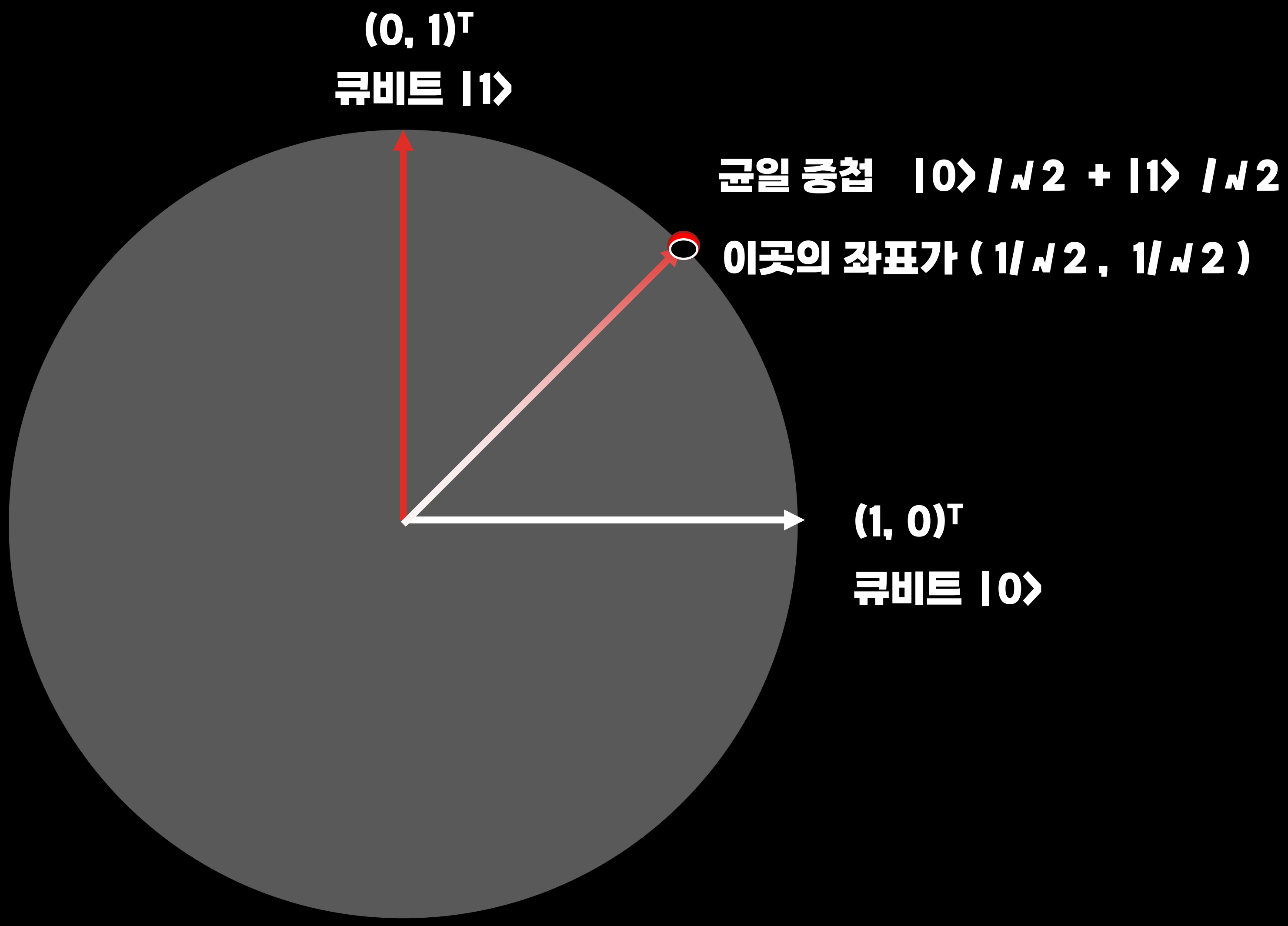
양자컴퓨터에 적용되는 양자효과

- 계산에 활용하는 효과
  - 중첩(superposition)
    - 중첩은 하나의 양자 시스템이 동시에 여러 상태를 가질 수 있게 함 (측정 전까지)
    - n 개의 비트로는 2^n 가지 상태를 표현할 수 있고, 이 모든 상태를 동시에 저장하려면 2^n 장치가 필요
    - 2^n 가지 상태를 단지 n 개의 큐비트로 표현 가능
  - 얽힘(entanglement)
    - 양자 얽힘을 이용하여 계산의 효율을 얻으려 함
  - 간섭(interference)
    - 양자는 파동처럼 간섭의 성질을 갖는다.
- 계산을 방해하는 양자 효과
  - 결어긋남(decoherence)
    - 양자를 조작하면 양자의 완벽한 고립을 파괴한다 이것은 양자의 중첩과 얽힘이 예측대로 거동하지 않게 하고 이는 시스템이 무작위적이며 특징이 없는 상태로 만들어 버린다.
  - 복사 불능 정리(non-cloning theorem)
    - 알려지지 않은 임의의 양자 상태와 동일한 복제를 생성하는 것은 물리적으로 불가능하다는 정리

큐비트를 표현하는 아주 간단한 수학

- 양자 게이트
  - 물론 디지털 컴퓨터에 사용하는 부울 논리 게이트는 아님
- 큐비트를 표현하는 방법
  - 약간의 수학, 선형대수를 사용해 보자
    - 큐비트는 0과 1의 두 가지 상태를 중첩해 가질 수 있음
    - 이것은 각각 같은 차원에 존재하는 스칼라 값이 아니고 서로 다른 기저벡터(basis vector)
      - 0의 상태는 $(1, 0)^T$ 벡터 → 이를 $|0\rangle$로 표현
      - 1의 상태는 $(0, 1)^T$ 벡터 → 이를 $|1\rangle$로 표현
      - 중첩이 이루어진 상태는 이 두 벡터의 선형 결합: $\alpha|0\rangle + \beta|1\rangle = |\varphi\rangle$
        - $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha(1,0)^T + \beta(0,1)^T$
        - 0일 확률은 α^2, 1일 확률은 β^2. 둘중의 하나일 확률은 1이므로 $\alpha^2 + \beta^2 = 1$
  - **균일 중첩** 상태의 양자 – uniform superposition state: **양자 컴퓨팅에서 매우 중요**
    - 0일 확률이 ½, 1일 확률이 ½인 큐비트: **이 상태를 이용하여 양자 컴퓨팅이 동작**
      - $$|\varphi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

큐비트를 이해하는 아주 간단한 기하



이런 큐비트를 조작하는 게이트는?

- 양자 게이트
  - 부울 대수에 기반한 논리 게이트가 아닌

- 파울리 게이트
  - 양자의 상태가 |0>, |1>, |φ> 로 표현하는 데, 이를 흔히 사용하는 벡터로 표현하면 각각
    - (1, 0)^T, (0, 1)^T, (1/√2, 1/√2,)^T 의 2차원 벡터이므로 2x2 행렬을 곱해 새로운 2차원 벡터를 만듦
    - 이 2x2행렬 중 구현이 가능한 것들이 게이트의 역할을 함 = 파울리(Pauli) 게이트

  - I : 항등 행렬
    - I |0> = |0> , I |1> = 1>
  - X : 양자 Not 게이트로서 |0>을 |1>로, |1>을 |0>으로 바꿈
    - X |0> = |1> , X |1> |0>
  - Y : 큐비트의 상태를 반대로 바꾸고 위상 변화를 일으킨다
    - Y |0> = i | 1> , Y |1> = - i | 0>
  - Z : |0> 큐비트는 그대로 두고, |1>에 대해서는 위상변화를 일으킨다
    - Z |0> = |0> , Z |1> = - | 1>
  - H : 아다마르(Hadamard) 게이트로 기저상태의 큐비트를 중첩상태로 바꿈
    - H |0> = α|0> + α|1> , H|1> = α|0> - α|1> (α는 모두 1/√2)

양자의 상태를 바꾸는 기본 게이트
파울리 게이트

양자를 중첩상태로 바꾸는 중요한 게이트
아다마르 게이트

수학 좋아하는 사람들에게만…

진지한 명조체로

큐비트 상태

$$|0>=\begin{pmatrix}1\\0\end{pmatrix}$$

$$|1>=\begin{pmatrix}0\\1\end{pmatrix}$$

$$|\psi>=\alpha\,|0>+\beta\,|1>=\begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

Uniform Superposition State:

$$|\psi>=\tfrac{1}{\sqrt{2}}\,|0>+\tfrac{1}{\sqrt{2}}\,|1>=\tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$$

$$X\,|0>=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}=|1>$$

$$X\,|1>=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}=|0>$$

$$Y\,|0>=\begin{pmatrix}0&-i\\i&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\i\end{pmatrix}=i\,|1>$$

$$Y\,|1>=\begin{pmatrix}0&-i\\i&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}-i\\0\end{pmatrix}=-i|0>$$

$$Z\,|0>=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}=|0>$$

$$Z\,|1>=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\-1\end{pmatrix}=-|1>$$

파울리 게이트 적용 결과

양자 게이트

$$X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

$$Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$$

$$Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

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

$$H\,|0>=\tfrac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}=\tfrac{1}{\sqrt{2}}|0>+\tfrac{1}{\sqrt{2}}|1>$$

$$H\,|1>=\tfrac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}=\tfrac{1}{\sqrt{2}}|0>-\tfrac{1}{\sqrt{2}}|1>$$

아다마르 게이트 적용 결과: 양자 중첩 상태를 만드는 결과

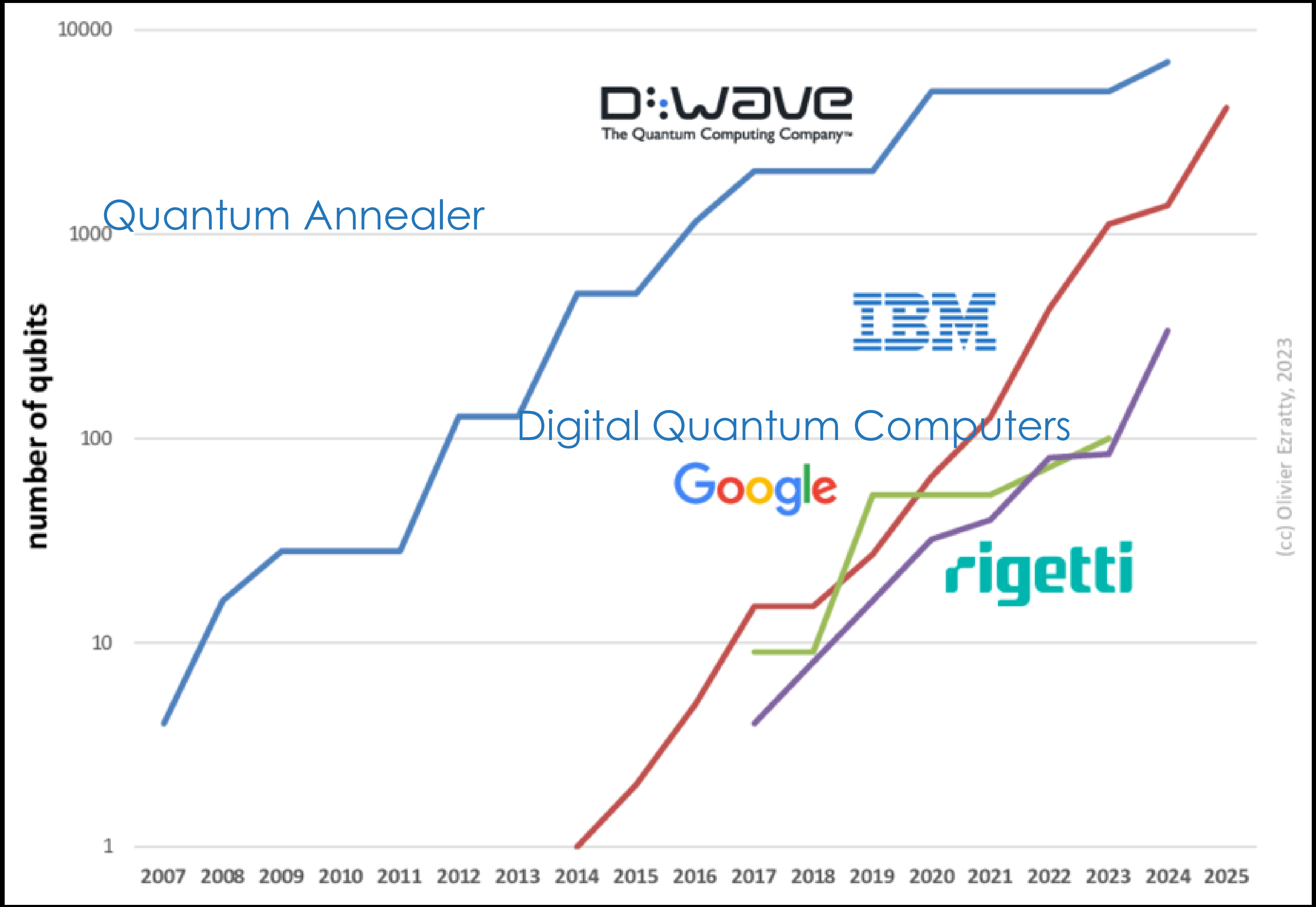
양자 컴퓨터의 현재 한계와 유형

- 양자 컴퓨터의 계산 우위 가능성
  - 중첩과 얽힘을 이용하여 계산 상의 이익을 취할 수 있다고 보고 있음
  - 현실적으로 우리는 NISQ(noisy intermediate scale quantum) 시대에 머물러 있음
- 양자 컴퓨터의 유형
  - **추상개념**: Quantum Turing Machine: **양자 튜링 기계**
    - 추상적 모델: 전통적 컴퓨터가 따르는 튜링 기계 개념을 양자 역학 모델로 나타낸 것
  - **디지털**: Universal Quantum Computer: **범용 양자 컴퓨터**
    - 양자 게이트로 만든 양자 회로로 논리 연산을 수행 – 디지털 양자 컴퓨터라고도 함
    - 현재의 NISQ 단계에서 오류가 없는 실효적 알고리즘을 개발하는 것이 매우 어려움
  - **아날로그**: Quantum Annealer: **양자 담금질 기계**
    - 금속의 온도를 높여 결합을 강화하는 담금질처럼 오류에 강한 최적화를 통해 문제 해법을 찾는 기계
  - 기타 하이브리드 모델: 디지털-아날로그 퀀텀 컴퓨터

양자 컴퓨터 유형별 특징 비교

	동작방식	계산 방법의 특징	적용 분야	현재 최대 큐비트 수
QTM Quantum Turing machine	추상개념	튜링 기계를 양자역학 모델로 표현	튜링 기계로 풀 수 있는 모든 문제 풀이 가능	NA
UQC Universal Quantum Computer	디지털	양자 게이트의 조합으로 논리 연산 – 오류에 취약	튜링 완전이 아니어도 양자 논리 게이트만 있으면 이로 분류	수 백 큐비트
QA Quantum Annealer	아날로그	양자를 단열과정처럼 고에너지에서 저에너지 상태로 바꾸며 안정상태 찾기 – 오류에 강건	최적화나, 이를 활용하는 기계학습에 응용	수 천 큐비트
Hybrid	혼합	두 모델을 결합	가까운 미래에 출현 예상	NA

큐비트 수의 증가 추세



Olvier Ezratty.
Is there a Moore's law for quantum computing, 2023. Preprint.

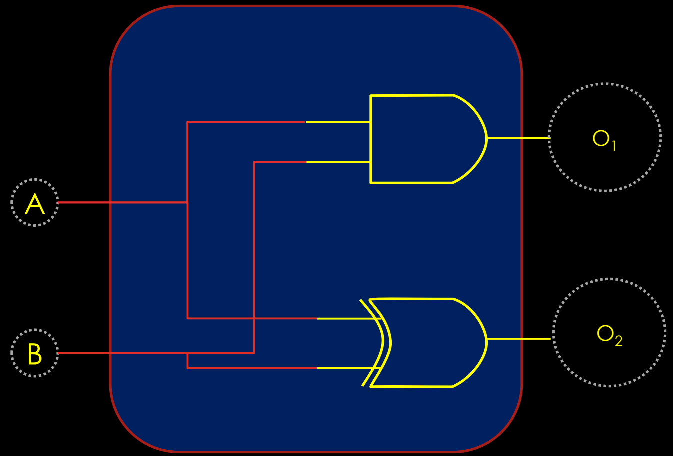
얼마만큼의 큐비트가 필요한가?

- RSA 암호 풀기
  - 양자 계산에서 가장 잘 알려진 알고리즘 쇼어의 알고리즘(Shor's Algorithm)
  - 대규모 숫자의 소인수 분해를 전통적 컴퓨터보다 기하급수적으로 빠르게 할 수 있다
  - Shor의 주장: 2n + O(log n) 큐비트로 n-bit RSA 공격가능
    - 현재의 2048-bit RSA를 공격하는 데에 4096 + 오류 수정
  - .
- 현재의 양자 컴퓨터
  - Noisy Intermediate-scale Quantum 시대: 오류 보정에 많은 큐비트가 필요
  - 그럼에도 노이즈 감소와 오류 수정 기술에 적극적인 노력 투입
  - RSA를 문제를 푸는 데에 필요한 큐비트의 수가 줄고 있음
    - Preskill: 계산상 요구되는 큐비트보다 훨신 많은 수의 수백만 개 이상의 큐비트가 필요 (10여년 전)
    - Microsoft Research의 추정: 4,000 큐비트 정도로 2048-bit RSA 무력화 가능 (2023)

BTQ, How Far Away Is The Quantum Threat?

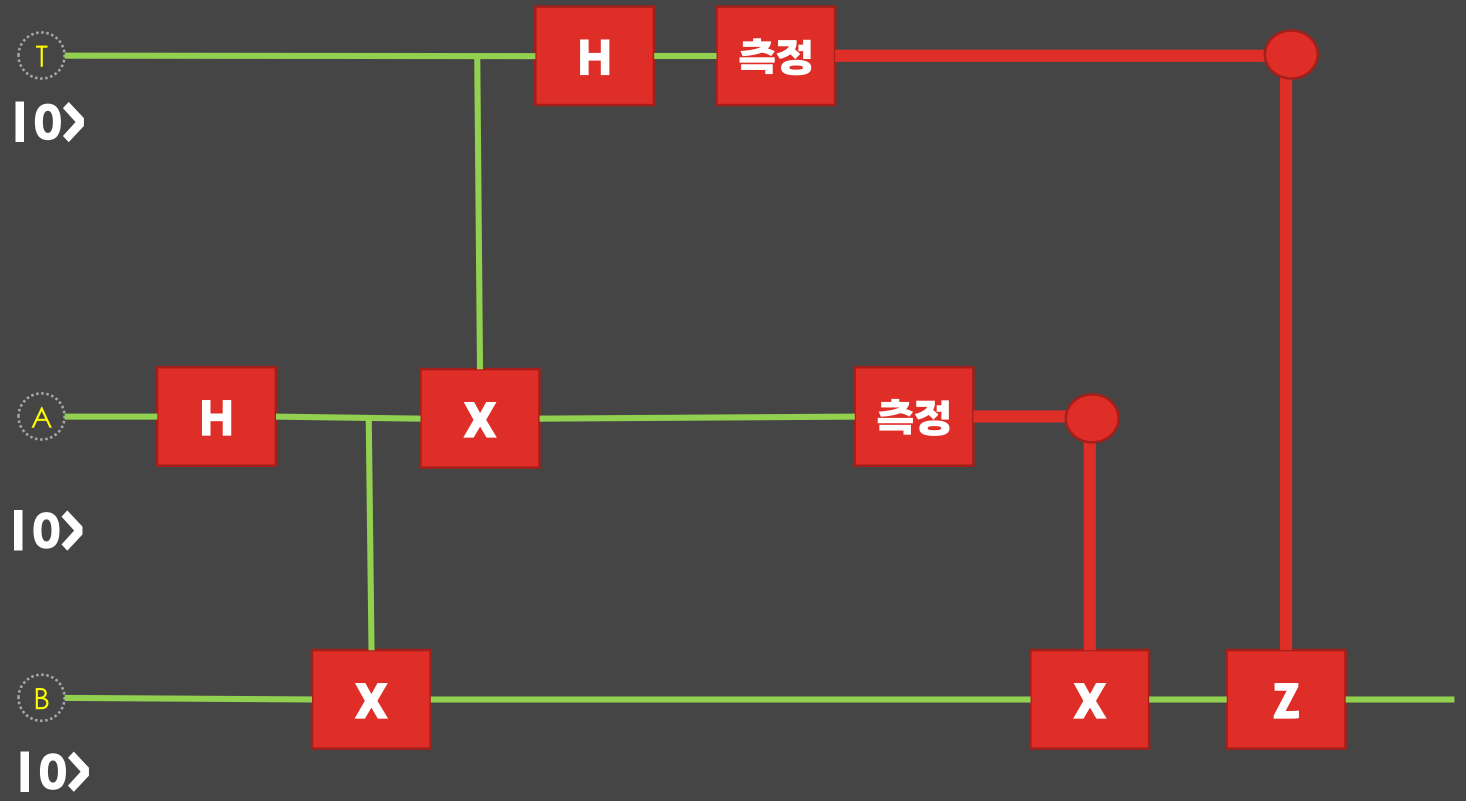
디지털 컴퓨터와 양자 컴퓨터

디지털 컴퓨터의 1비트 덧셈기



양자 컴퓨터의 Teleportation 회로

양자 전송 회로 (양자의 상태를 전송할 수 있는 양자 컴퓨터의 핵심 장치)



A가 T의 상태를 B에게 보내고 싶을 때, 이 회로를 사용한다.

양자 컴퓨팅 알고리즘

- **Deutsch-Jozsa 알고리즘**
  - **실용성은 없지만, 고전 알고리즘보다 빠른 첫 양자 알고리즘으로서의 의미**
  - **고전 컴퓨터에서는 어렵고, 양자 컴퓨터에서 쉽도록 만든 문제를 해결**

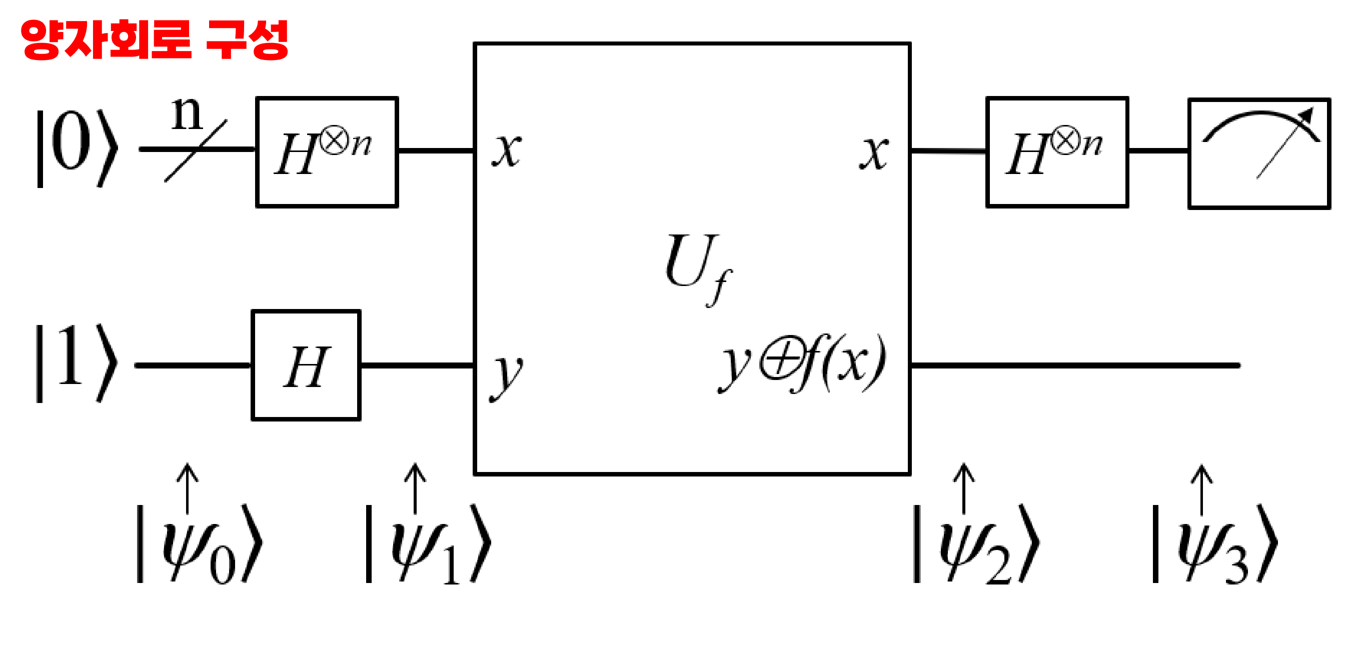
n 비트 2진수 입력
01001010101001011 0 → 블랙박스 함수 → 한 자리수의
0 또는 1 출력

블랙박스 함수는
언제나 같은 값을 내 보내는 상수함수이거나
모든 정의역의 변수 반에 대해 0을 출력하고
나머지 반에 1을 출력하는 균형함수 둘 중 하나

  - **고전 알고리즘**
    - **입력값과 출력을 살피는 일은 $O(2^n)$, 즉 지수적 계산복잡도로 어려운 문제**

양자 컴퓨팅 알고리즘

- Deutsch-Jozsa 알고리즘



양자 알고리즘

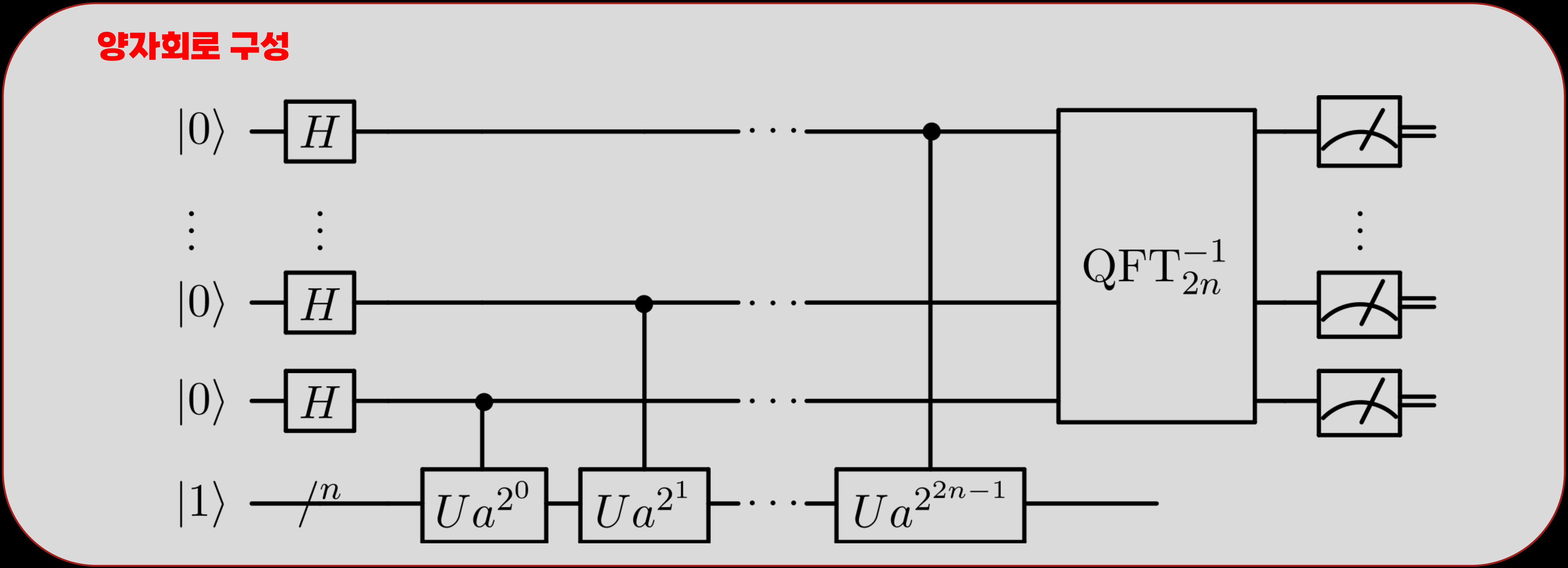
- Shor's 알고리즘
  - 소인수 분해를 빠르게 처리할 수 있는 양자 알고리즘
    - 크기 N인 수를 소인수 분해할 때 O(log3N) 시간과 O(logN) 저장 공간 필요
    - 소인수 분해를 쉽게 하는 고전 알고리즘은 없다. 이를 빠르게 처리하면 소인수 분해의 어려움에 기반한 RSA 암호를 쉽게 깰 수 있다.

  - 현재의 양자 컴퓨터는 보안의 위협이 되는가/
    - 아직은…
      - 현재의 양자 컴퓨터는 지나치게 많은 오류가 있음
      - 현재의 양자 컴퓨터는 양자 오류 수정에 쓰기에는 너무 적은 큐비트를 가짐
      - 실험실 환경에서의 소인수 분해 역시 여러 시도 끝에 답을 얻음

  - 그간의 성과
    - 2001년 IBM이 7개 큐비트로 15를 소인수 분해 함 (3x5)
    - 2012년 15의 소인수 문제를 고체 큐비트에서 구현하고 21의 소인수 분해에 도달
    - 2019년 IBM Q system One으로 35의 소인수 분해에 도전 → 실패 (누적 오차)

양자 컴퓨팅 알고리즘

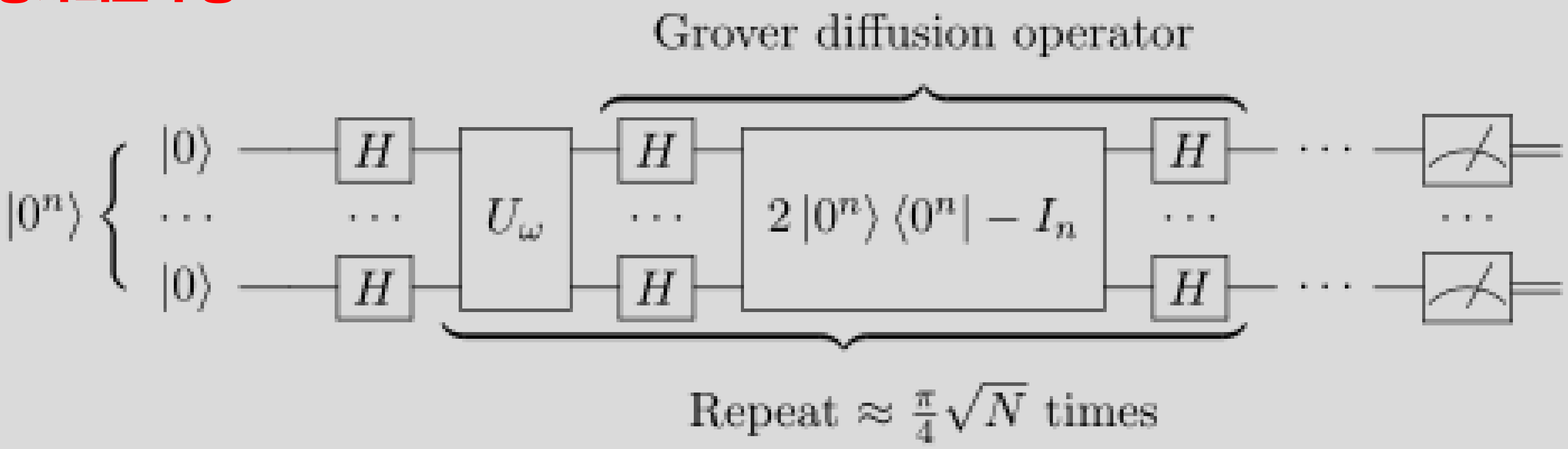
- Shor's 알고리즘



양자 컴퓨팅 알고리즘

- Grover's 알고리즘
  - 양자 검색 알고리즘: 단방향 함수에서 출력으로 입력을 찾는 문제
    - 정의역의 크기가 N일 때, O(√N) 검사로 답을 찾을 수 있음
  - 대표적인 함수: 해시(hash) 함수
    - y = hash(x) → x를 이용하여 y를 얻는 것은 간단하지만, y를 안다고 x를 알 수는 없다.

양자회로 구성



양자 컴퓨팅 알고리즘

- 현재까지 양자 알고리즘
  - 양자 컴퓨팅이 우월한 특수한 문제를 다룸
  - 대규모 큐비트가 오류 없이 동작하는 상태를 가정한 "수학적 모델"
  - 실제로 적용은 매우 어려운 문제
    - 우리는 NISQ 시대를 살고 있다
      - 양자 컴퓨터는 오류와 결어긋남이 지속적으로 계산을 방해함

- 현재의 양자 컴퓨팅 연구
  - 더 좋은 양자 컴퓨터 – 양자 컴퓨팅이 실현될 수 있도록
  - 양자 우위를 확보할 수 있는 알고리즘 개발
    - 계산 복잡도 이론 + 알고리즘 연구 → 순수한 수학의 영역

응용?

15의 소인수가 5와 3이라는 것.
어디에 쓸 수 있을까?

양자 컴퓨터에 대한 비관적 전망

- 현재의 하드웨어로는 여러 가지 한계
  - 대규모 데이터를 다룰 수 있는가?
    - GPU를 이용한 시뮬레이터에서 기존 GPU 컴퓨팅에 비해 낮은 성능 보임
      - 시뮬레이션에 사용된 큐비트 수는 1만개로 현재의 기술적 수준을 크게 넘은 것
    - 대규모 데이터를 다루기에는 대역폭(bandwidth)이 너무 작다
      - "양자 컴퓨팅은 작은 데이터에 대한 대규모 계산에나 쓸모가 있을 것"
        - The Register, A lone Nvidia GPU speeds past the physics-straining might of a quantum computer – in these apps at least
    - 양자 컴퓨터가 맞고 있는 냉혹한 현실
      - LeCun(Meta), "실질적으로 유용한 양자 컴퓨터를 실제로 제작할 가능성에 대해 별로 확신하지 않는다."
      - Mattias Troyer (MS)
        - "10년간 제안된 것들이 효과가 없다. 간단한 이유를 발견했다. 오류 수정이 어렵다. 그리고 큐비트를 조작하는 것은 트랜지스터를 다루는 것보다 훨씬 오래 걸린다. 앞으로 수세기 이상 계산용으론 GPU가 낫다. "
        - 모든 문제가 아니라 일부 문제라도 다룰 수 있다면 양자 컴퓨터의 가치는 있다

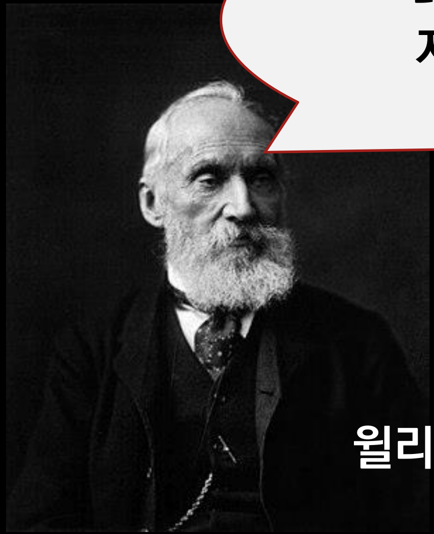
Edd Gent. Quantum Computing's Hard, Cold Reality Check. IEEE Spectrum. https://spectrum.ieee.org/quantum-computing-skeptics

WHO KNOWS

절대온도 K의 단위가 된 물리학자.
물리학을 오늘과 같은 형태로 정립한 이
켈빈 경, 윌리엄 톰슨이 말한다….

나는 풍선이 아닌 다른 항공 운항에
대해서는 일말의 신뢰도 갖지 않고 있다.
지금 들리는 모든 시도에 대해서도 좋은
결과가 나올 것이라 기대하지 않는다.

1895



윌리엄 톰슨

1903년 12월 17일

동생, 비행기
날리러 가자!

라이트 형제들

참고문헌

- Zebo Yang, Maede Zolanvari. A survey of important issues in quantum computing and communications, IEEE Communications Surveys & Tutorial, 25(2):1059-1094, IEEE, 2023.
- N David Mermin. Is the moon there when nobody looks? Reality and the quantum theory, Physics Today, April 1985, pp. 38-47. American Institute of Physics, 1985.
- Quantum 101 – Quantum Science Explained, https://perimeterinstitute.ca/quantum-101-quantum-science-explained, Perimeter Institute for Theoretical Physics, 2023.
- BTQ, How Far Away Is The Quantum Threat? https://www.btq.com/blog/how-far-away-is-the-quantum-threat
- Edd Gent. Quantum Computing's Hard, Cold Reality Check. IEEE Spectrum. https://spectrum.ieee.org/quantum-computing-skeptics