SAMSUNG SDS

Foresee

Techtonic 2021

Partner

Disrupt

양자 컴퓨터 오류와 기계학습

제정우 프로

AGENDA

양자 컴퓨터란? — 제정우 프로

양자 컴퓨터의 오류와 극복 노력 — 제정우 프로

머신 러닝의 역할 — 제정우 프로

양자 컴퓨터란?

제정우 프로

양자 컴퓨터

양자 물리의 원리를 정보 처리에 활용하는 컴퓨터

기존 (고전) 컴퓨팅

고전 컴퓨터가 이룩한 것들...

- 정보의 폭발적 증가
- 저장/연산 장치 집적도의 한계
- 계산 복잡도가 높은 문제들

양자 컴퓨팅

좀 더 잘 계산하기 위한 대안들 중 하나

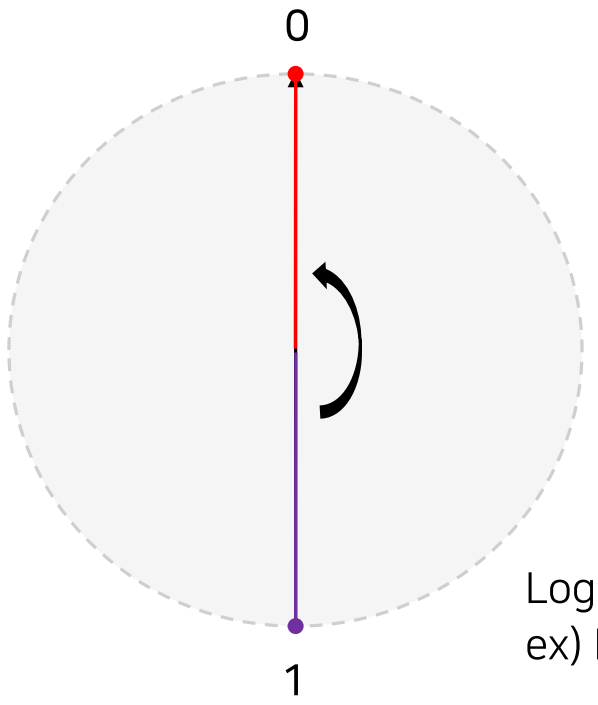
ex) Neuromorphic, Cloud computing

→ 저장/연산 능력 효율성

양자 bit - Qubit

양자 컴퓨팅에서 정보를 저장하기 위한 기본 단위
초전도체, 이온 포획, 양자점 등으로 구현 가능

고전 bit

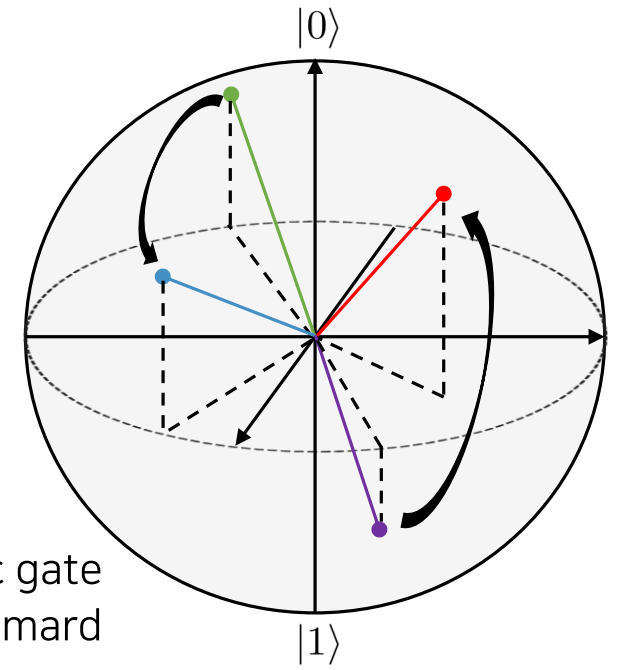


0 또는 1

Logic gate
ex) Not, And

Quantum bit

0과 1의 중첩

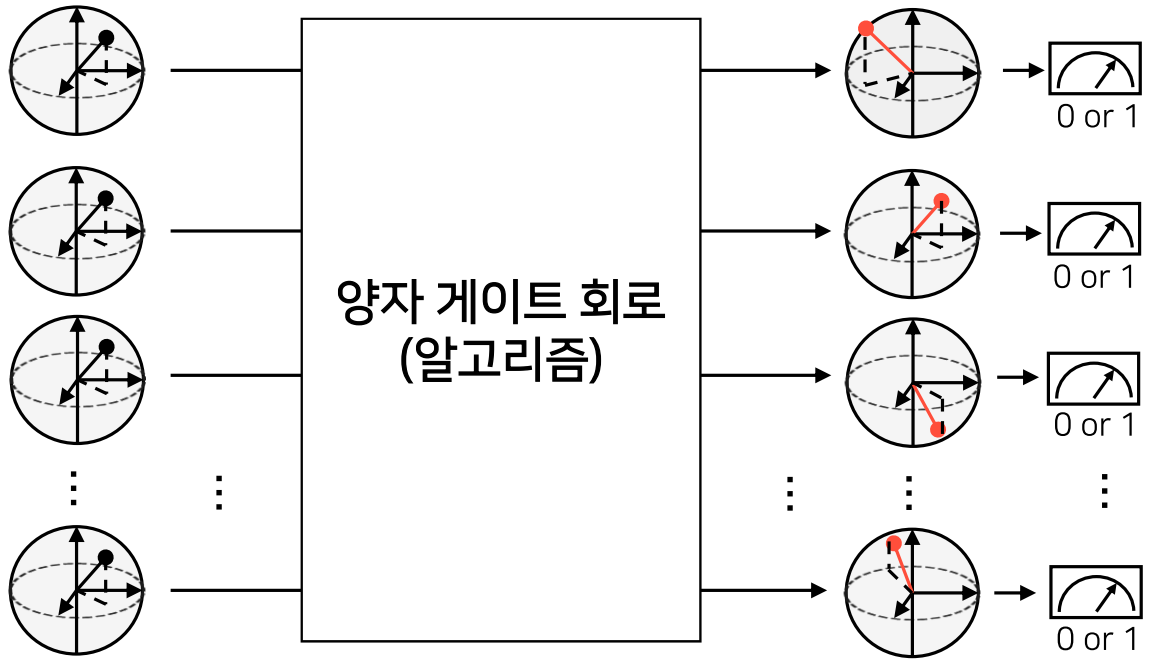


Quantum logic gate
ex) Hadamard

양자 컴퓨터 구성

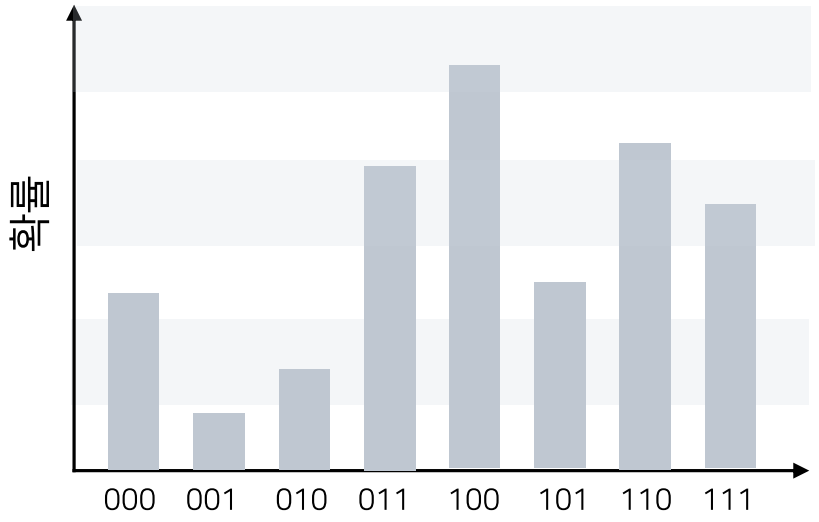
양자 컴퓨터는 1) 정보를 저장해 양자 상태를 만드는 encoding과 2) 양자 상태를 변환하는 양자 회로,
3) 변환된 양자 상태에서 정보를 추출하는 측정으로 구성되어 있다.

1) 상태 입력 **2) 상태 변환** **3) 측정**



출력 값

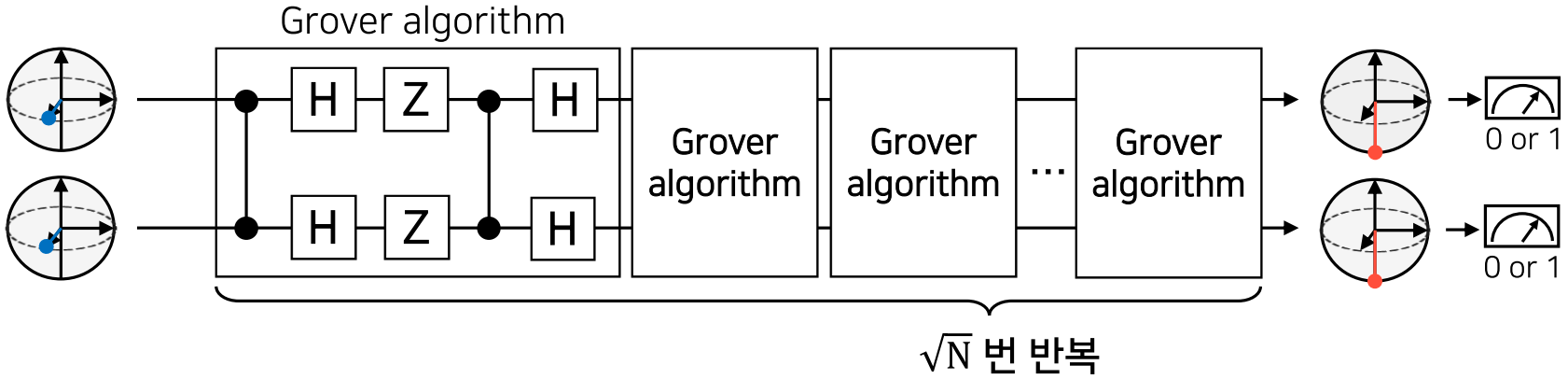
반복 측정의 결과 예) 3-qubit



예시: Grover 검색 알고리즘

N개의 데이터에서 원하는 데이터를 찾는 작업
고전 알고리즘은 N/2번의 연산이 필요한 반면 양자 알고리즘은 $\sqrt{N}$ 번의 연산으로 문제를 해결 할 수 있다.

✔ {00,01,10,11} 중 11 을 찾고자 할 경우



✔ 알고리즘 적용에 따른 확률 분포 변화: 11의 확률 증폭

Qubit의 특성

양자 컴퓨터는 Qubit의 파동성과 병렬연산에 적합한 구조를 이용해 많은 정보를 빠르게 처리한다..

Qubit의 파동성

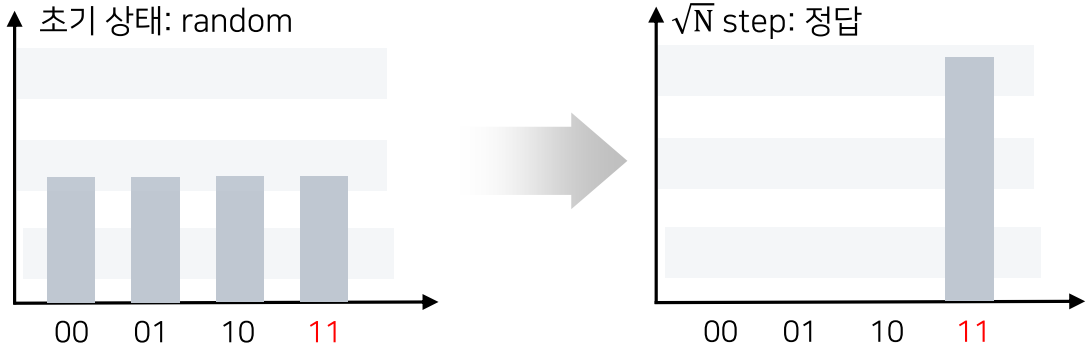
0과 1의 중첩 상태

- 측정에서 0이 나올 확률과 1이 나올 확률 공존

정보의 간섭

- 확률의 상쇄 및 보강을 이용한 알고리즘 가능

*Grover 알고리즘 예



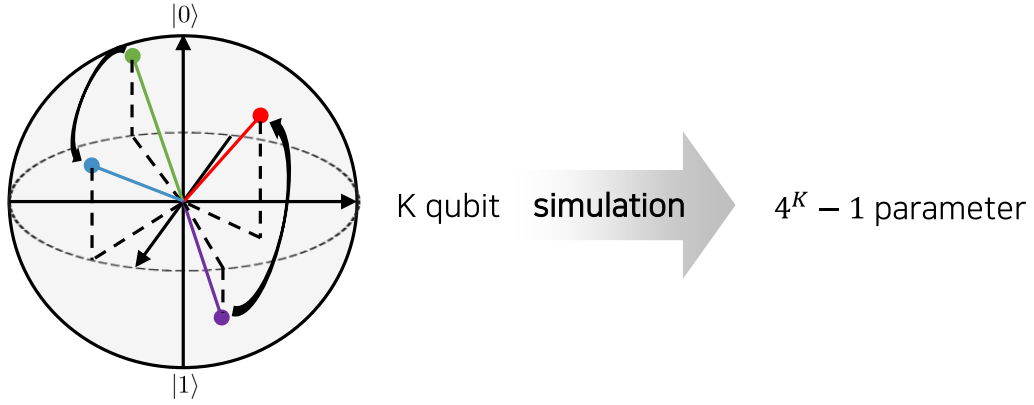
병렬 연산에 적합

얽힘 (entanglement)

- 여러 qubit들간의 상관 관계의 중첩

Qubit에 담을 수 있는 bit

- 2 bit → 1qubit
- 2^{50} bit (1petabit) → 50 qubit
- 100 qubit 이 가진 정보는 고전 컴퓨터로 흉내내기 어려움



양자 알고리즘의 speed-up

Qubit의 성질을 효과적으로 이용하면 기존의 고전 알고리즘의 계산 성능을 뛰어넘는 양자 알고리즘 고안 가능

기존 (고전) 알고리즘

소인수분해
- 정수 N에 대해 $e^{1.9\sqrt[3]{logN}}$ time

푸리에 변환
- 2^n 개의 진폭 $O(n2^n)$게이트

선형 방정식 $A\vec{x} = \vec{y}$
- N 변수와 A condition k 방정식 O(kN)

자료 검색
- 크기 N의 자료에 대해 N query 필요

양자 알고리즘

Shor 알고리즘
- $O(logN)$ 양자게이트

양자 푸리에 변환 알고리즘
- $O(n^2)$

Harrow-Hassidim-Lloyd (HHL) 알고리즘
- A가 sparse 행렬인 경우 $O(k^2 logN)$

Grover 알고리즘
- $\sqrt{N}$ query

양자 소인수분해 알고리즘

양자 컴퓨터는 고전 컴퓨팅 대비 적은 시간에 소인수분해 가능

기존 (고전) 알고리즘

150자리 숫자

- 2003년 PC 100대 1달
- 2018년 PC 100대 1시간

300자리 숫자

- 2018년 PC 100대 천년

양자 알고리즘

150자리 숫자

- 2500-qubit 양자 컴퓨터 수 초

300자리 숫자

- 5000-qubit 양자 컴퓨터 수십 초

※ Reference : S. M. Hamdi, et. al., ICEEICT, 2014 International Conference on.

양자 컴퓨터가 고전 컴퓨터를 대체 할 수 있을까?

No! 양자 컴퓨터의 특성 + 기술적 한계

양자 컴퓨터는 특정 연산에 탁월함

- 모든 연산에서 고전 컴퓨터보다 뛰어난 성능을 내지 않음
- 어떤 연산에 특화되어있는지 잘 알지 못함

양자 컴퓨터의 오류 문제를 해결해야 speed-up 가능

- Qubit 양자 상태는 오류에 취약 → 오류 발생 시 파동성 상실
- 양자 오류는 보정하기가 힘듦

데이터의 I/O

- Quantum random access memory (QRAM)
- 고전 데이터 → 양자 상태

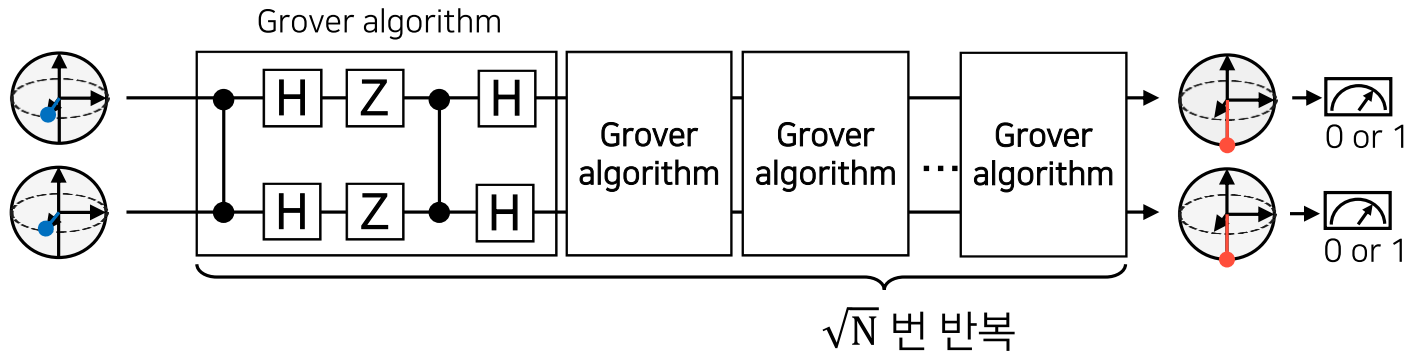
양자 컴퓨터의 오류와 극복 노력

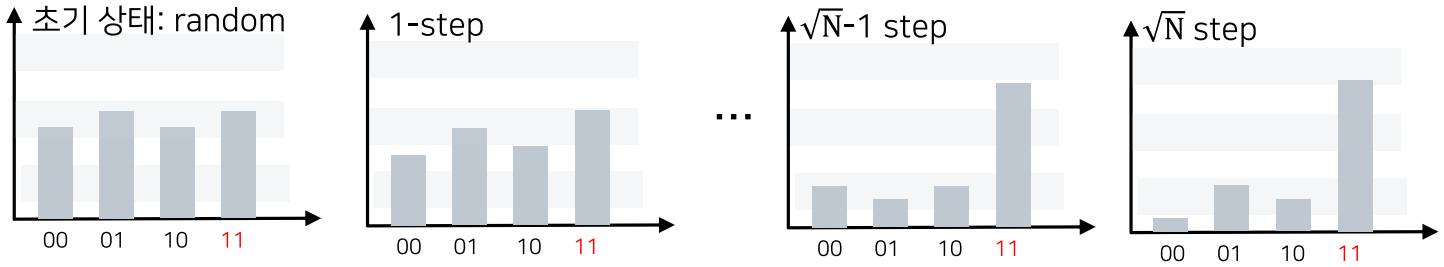
제정우 프로

NISQ computer

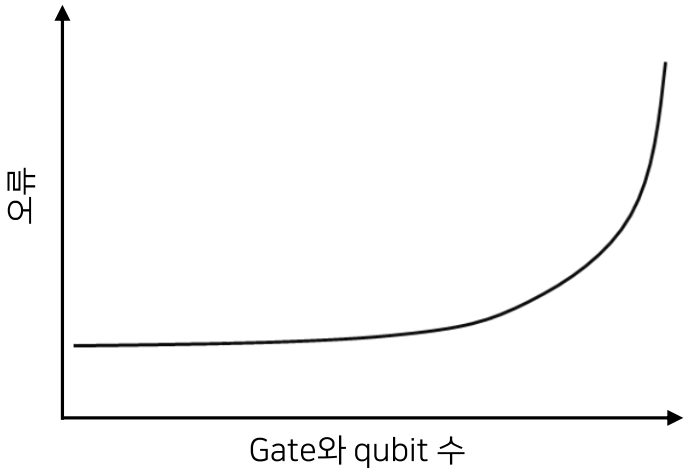
Noisy intermediate-scale quantum (NISQ) computer
현재는 수십 qubit 규모의 오류가 많은 양자 컴퓨터 존재

2-qubit Grover algorithm





오류의 누적



→실용적인 목적에 사용하기 위해서는 오류 없이 수백개의 양자 게이트를 수십개의 qubit에 적용할 수 있어야 함.

양자 오류의 특성

양자 오류는 기존의 방법으로 보정이 불가능 하다.

고전 오류 보정

정보 복제를 통한 오류 보정

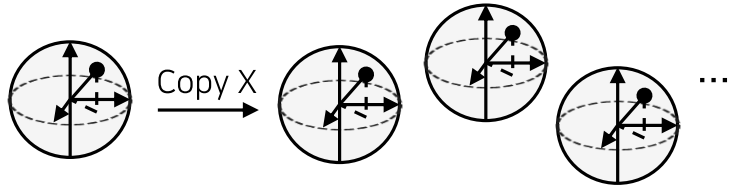
- 고전 오류 보정에서는 bit을 복제하여 오류 방지
- 정보를 읽고 쓰는 것이 가능

data	copy	read	majority voting	write
00100	00100	00100	00100	00100
	00100	00100	00100	00100
	00100	01100	01100	00100
	00100	00100	00100	00100
	⋮	⋮	⋮	⋮

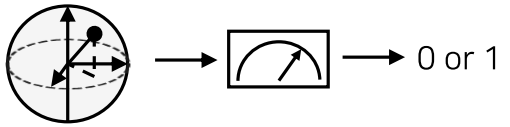
연속적인 값의 전기 신호는 오류에 둔감

양자 오류

양자 정보는 복제가 불가능

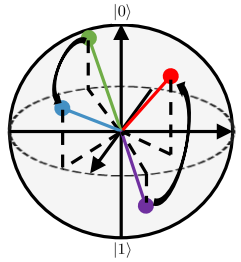


측정 후 양자 정보는 사라짐



오류가 다양함

정보의 간섭을 결정하는 phase에 오류 발생



양자 오류의 결과

양자 알고리즘의 speed-up을 얻을 수 없음

기존 (고전) 알고리즘

- **소인수분해**
  - 정수 N에 대해 $e^{1.9\sqrt[3]{logN}}$ time
- **푸리에 변환**
  - 2^n 개의 진폭 O($n2^n$)게이트
- **선형 방정식 $A\vec{x} = \vec{y}$**
  - N 변수와 A condition k 방정식 O(kN)
- **자료 검색**
  - 크기 N의 자료에 대해 N query 필요

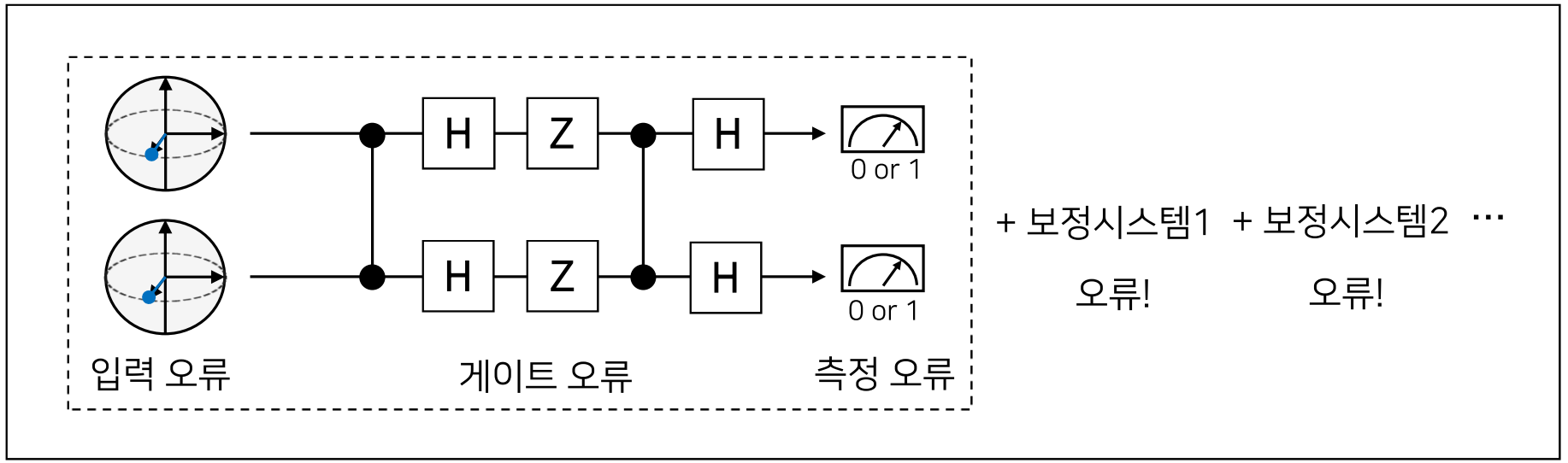
양자 알고리즘

- **Shor 알고리즘**
  - $O(logN)$ 양자게이트
- **양자 푸리에 변환 알고리즘**
  - O(n^2)
- **Harrow-Hassidim-Lloyd (HHL) 알고리즘**
  - A가 sparse 행렬인 경우 O($k^2 logN$)
- **Grover 검색 알고리즘**
  - $\sqrt{\mathrm{N}}$ query

Fault-tolerant quantum computer

어떻게 오류 내성 양자 컴퓨팅을 구현할 수 있을까?

Fault-tolerant device란?
구성 요소들에 오류가 있음에도 목적한 기능을 효과적으로 수행할 수 있는 장치



오류 보정의 문제 → Qubit을 여러 개 쌓는 문제.. 어떻게 쌓을 것인가? 몇 개까지 쌓아야 하는가?

양자 오류 보정 예시1: 3-qubit 반복 코드

Bit flip을 보정하는 방법
3개의 데이터 qubit과 2개의 측정 qubit을 통해 하나의 logical qubit을 만들 수 있다.

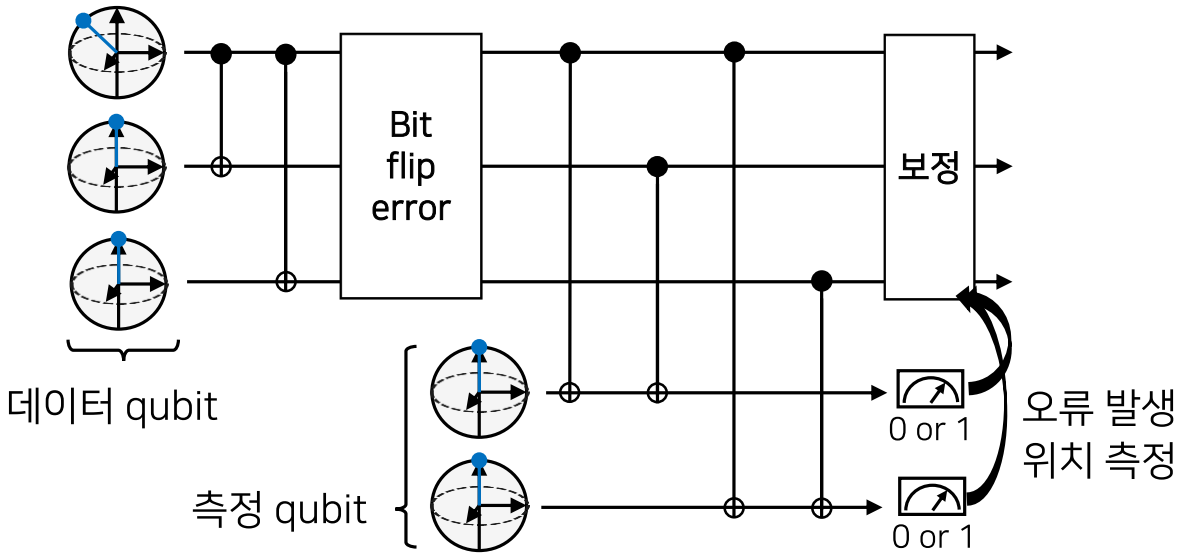
Bit flip 오류

- 0→1 로 1→0 으로 만드는 오류

오류 보정 방법

- 추가적인 qubit 필요
  → 데이터 qubit 3개 + 측정 qubit 2개
- 오류 발생 위치만 측정
  → 상태 정보 자체의 손실X

Bit flip 오류를 보정하기 위한 3-qubit 회로



양자 오류 보정 예시1: 3-qubit 반복 코드

Bit flip을 보정하는 방법
3개의 데이터 qubit과 2개의 측정 qubit을 통해 하나의 logical qubit을 만들 수 있다.

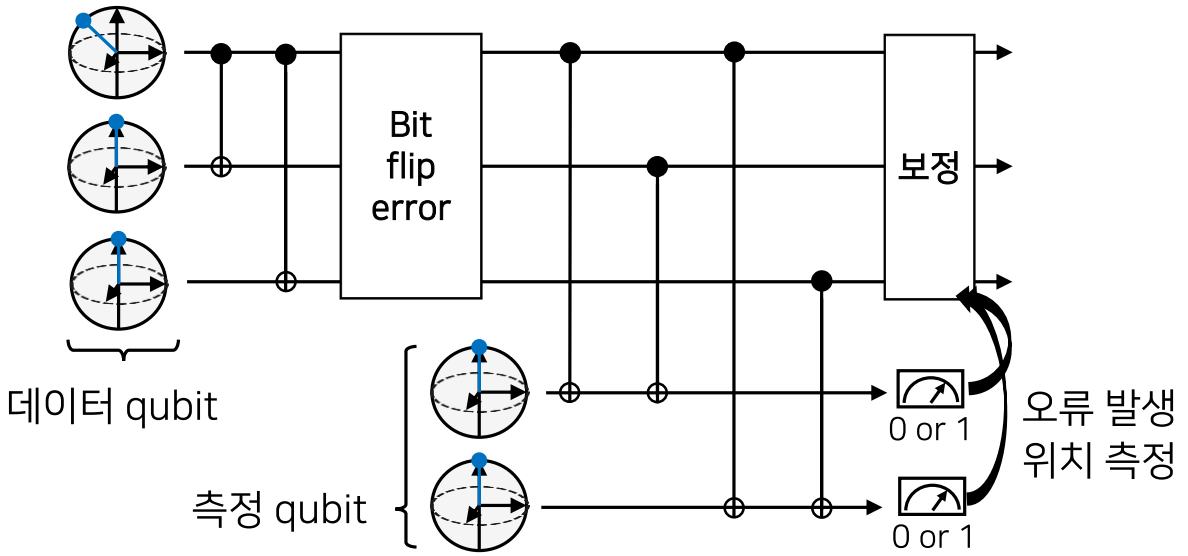
Bit flip 오류

- 0→1 로 1→0 으로 만드는 오류

오류 보정 방법

- 추가적인 qubit 필요
  → 데이터 qubit 3개 + 측정 qubit 2개
- 오류 발생 위치만 측정
  → 상태 정보 자체의 손실X

Bit flip 오류를 보정하기 위한 3-qubit 회로

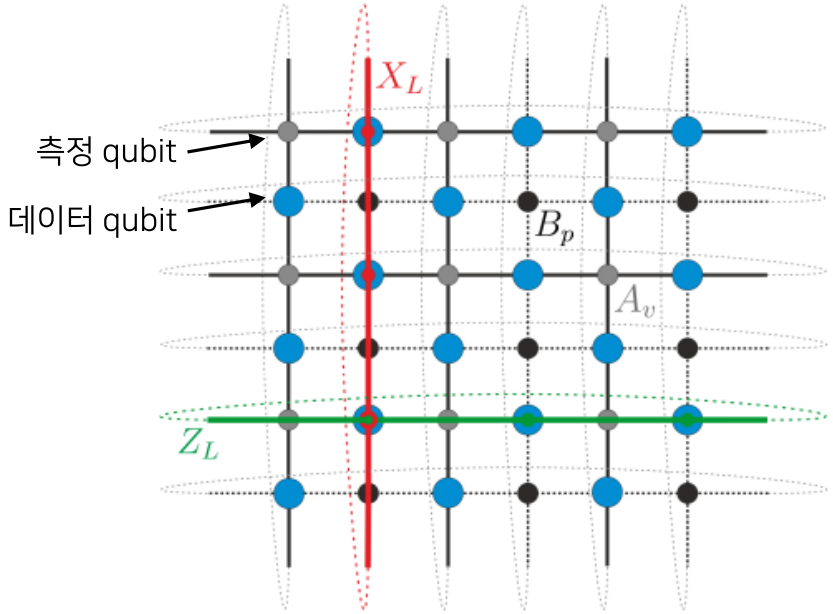


양자 오류 보정 예시2: surface code

오류를 보정하지 않고 오류 존재 검출
양자 컴퓨터 오류가 문턱 값 이하면 qubit이 많아질수록 오류 감소
→ 오류 검출 방법을 이해하는 것이 양자 컴퓨터 개발 상황을 이해하는데 핵심적인 역할을 함

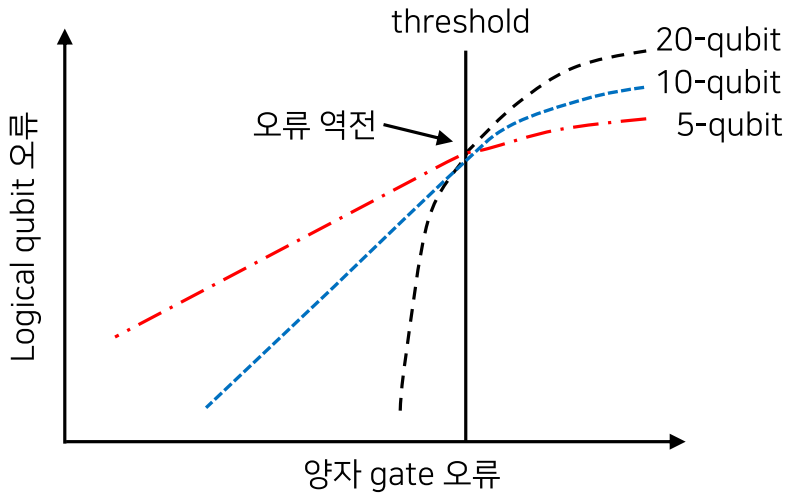
More qubits

- 18 데이터 qubit + 18 측정 qubit = 1 logical qubit



오류 누적 방지

- 문턱 오류 값 이하에서 qubit이 많은 경우가 이득



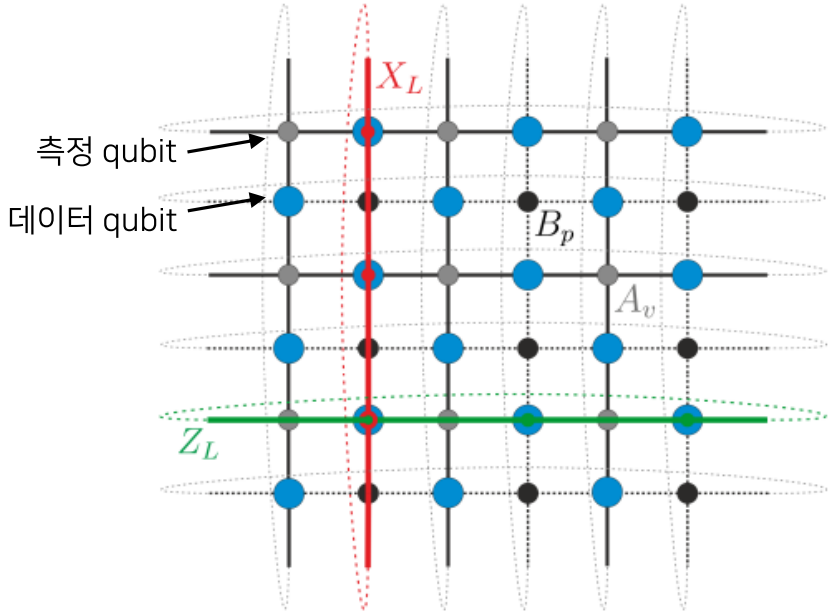
※ Reference : Hendrik Poulsen Nautrup, et. al., Quantum 3, 215 (2019); Austin G. Fowler, et. al., Phys. Rev. A 86, 032324 (2012).

양자 오류 보정 예시2: surface code

오류를 보정하지 않고 오류 존재 검출
양자 컴퓨터 오류가 문턱 값 이하면 qubit이 많아질수록 오류 감소
→ 오류 검출 방법을 이해하는 것이 양자 컴퓨터 개발 상황을 이해하는데 핵심적인 역할을 함

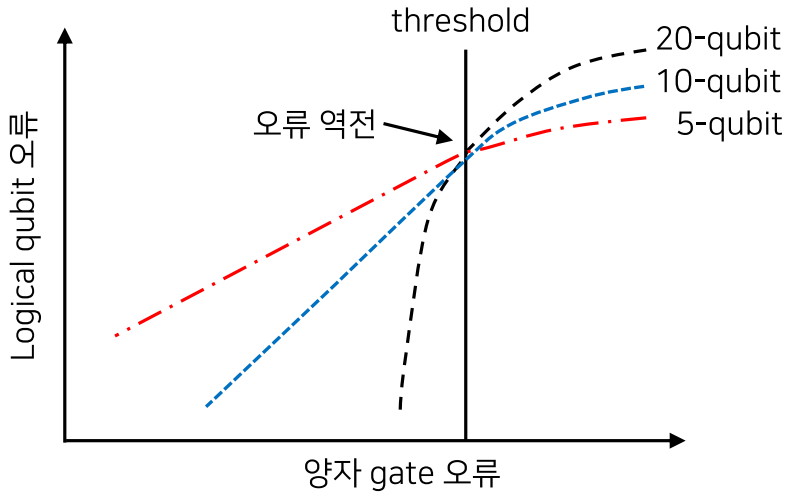
More qubits

- 18 데이터 qubit + 18 측정 qubit = 1 logical qubit



오류 누적 방지

- 문턱 오류 값 이하에서 qubit이 많은 경우가 이득



※ Reference : Hendrik Poulsen Nautrup, et. al., Quantum **3**, 215 (2019); Austin G. Fowler, et. al., Phys. Rev. A **86**, 032324 (2012).

Global quantum computer 기업1: Google

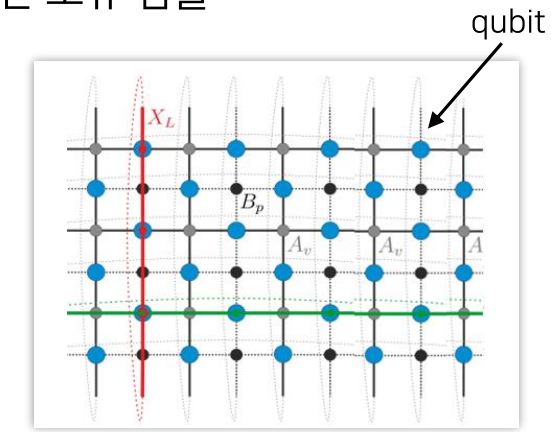
초전도 qubit을 이용해 2029년 오류 보정된 실용적인 1000-qubit 양자 컴퓨터 개발을 목표로 하고 있다.

2019년 Quantum supremacy

고전 컴퓨팅으로 계산이 힘든 작업 수행

- 무작위 양자 회로에서의 출력 샘플링
- Surface code를 이용한 오류 검출

Sycamore 54-qubit
Quantum computer



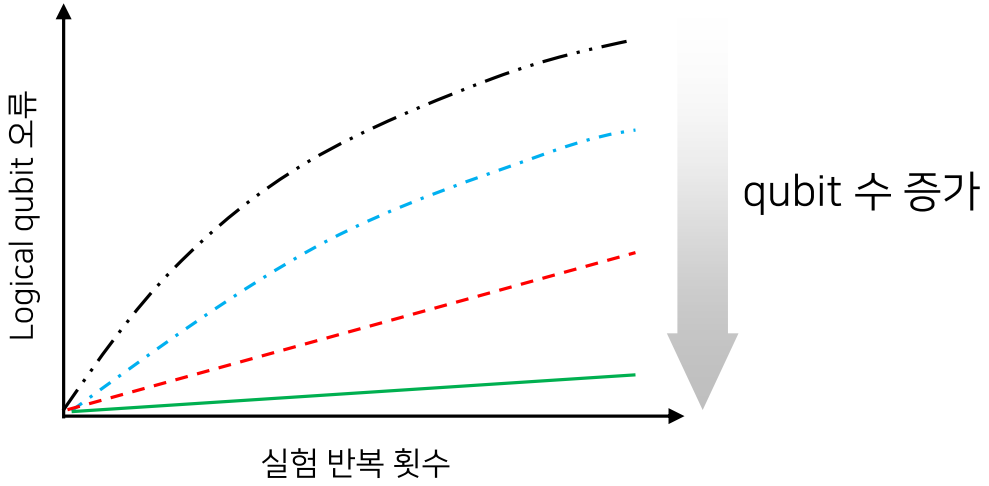
- 오류 발생 비율
  1 qubit ~ 0.15%, 2 qubit ~ 0.6%, Readout ~ 3%

※ Reference : Frank Arute, et.al., Nature **574**, 505 (2019); Google Quantum AI, Nature **595**, 383 (2021).

2021년

Advanced error detection scheme

- 지수함수적 오류 감소 가능



2029년까지 10^6 qubit 컨트롤 → 1000 logical qubit

Global quantum computer 기업1: Google

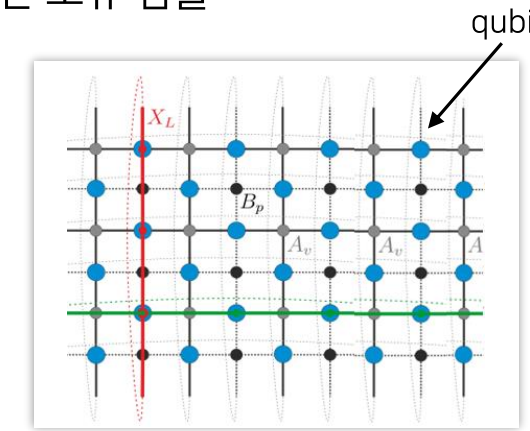
초전도 qubit을 이용해 2029년 오류 보정된 실용적인 1000-qubit 양자 컴퓨터 개발을 목표로 하고 있다.

2019년 Quantum supremacy

고전 컴퓨팅으로 계산이 힘든 작업 수행

- 무작위 양자 회로에서의 출력 샘플링
- Surface code를 이용한 오류 검출

Sycamore 54-qubit
Quantum computer



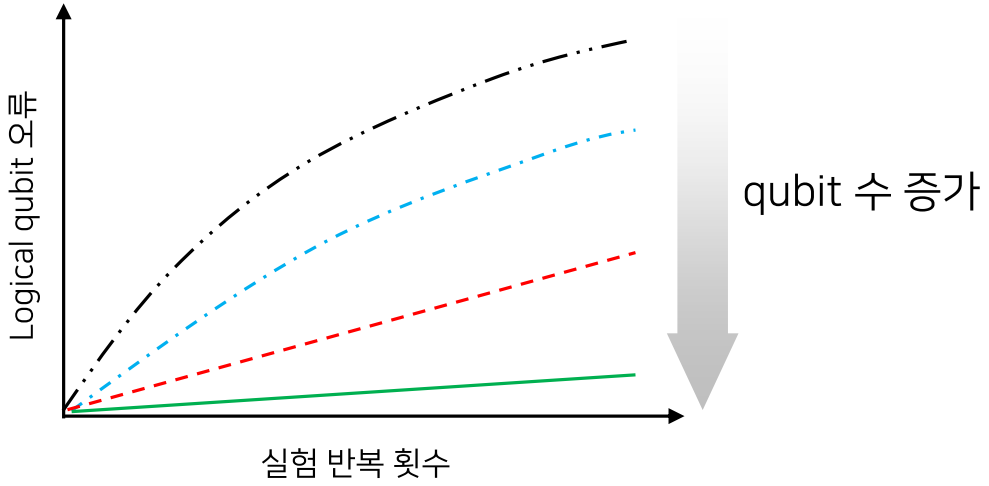
- 오류 발생 비율
  1 qubit ~ 0.15%, 2 qubit ~ 0.6%, Readout ~ 3%

※ Reference : Frank Arute, et.al., Nature **574**, 505 (2019); Google Quantum AI, Nature **595**, 383 (2021).

2021년

Advanced error detection scheme

- 지수함수적 오류 감소 가능



2029년까지 10^6 qubit 컨트롤 → 1000 logical qubit

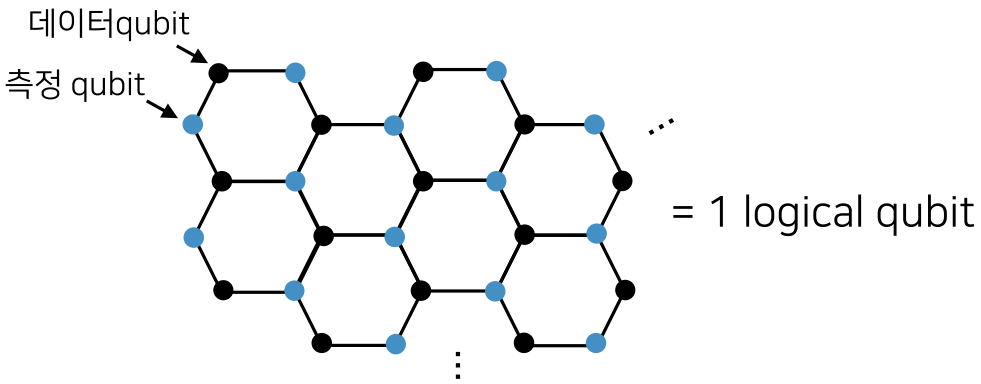
Global quantum computer 기업2: IBM

IBM은 초전도 qubit 설계에 최적화된 양자 오류 보정 방법 개발 중
2023년말 1000 qubit (수 - 수십 logical qubit) 양자 컴퓨터 개발 목표

Hexagon code

육각형 구조를 오류 검출에 활용

- 40~50 qubit을 이용 → 1 logical qubit



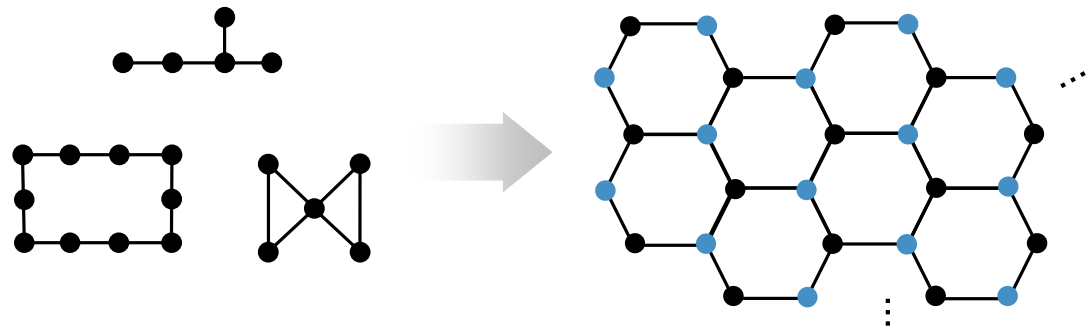
- 초전도체 qubit control 에 적합하도록 최적화

※ Reference : C. Chamberland, et. al. Phys. Rev. X **10**, 011022 (2020)

2021년

Architecture의 변화

- 사각형 → 육각형



2023년말 1000 qubit 양자 컴퓨터

- 1000 qubit ~ 수 - 수십 logical qubit

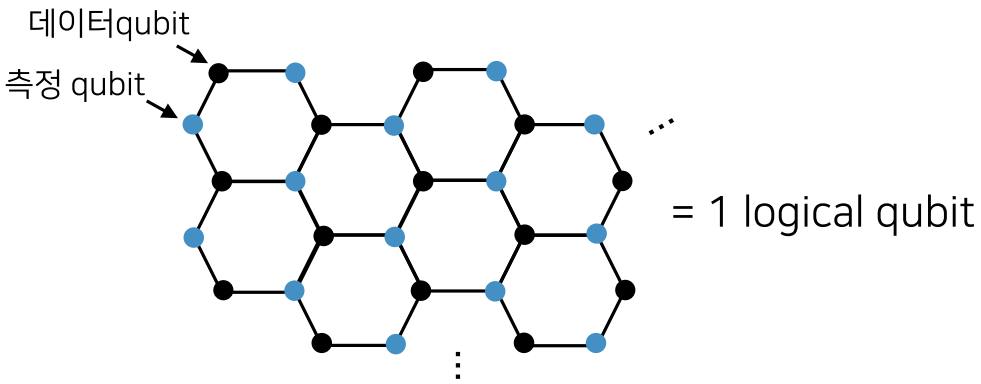
Global quantum computer 기업2: IBM

IBM은 초전도 qubit 설계에 최적화된 양자 오류 보정 방법 개발 중
2023년말 1000 qubit (수 - 수십 logical qubit) 양자 컴퓨터 개발 목표

Hexagon code

육각형 구조를 오류 검출에 활용

- 40~50 qubit을 이용 → 1 logical qubit



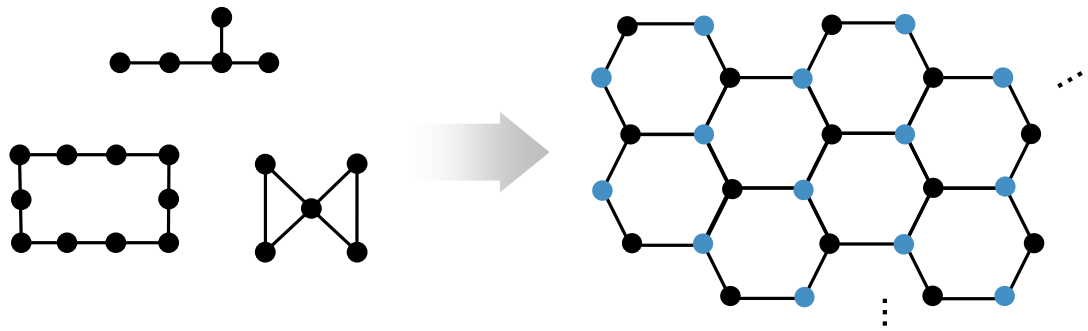
- 초전도체 qubit control 에 적합하도록 최적화

※ Reference : C. Chamberland, et. al. Phys. Rev. X **10**, 011022 (2020)

2021년

Architecture의 변화

- 사각형 → 육각형



2023년말 1000 qubit 양자 컴퓨터

- 1000 qubit ~ 수 - 수십 logical qubit

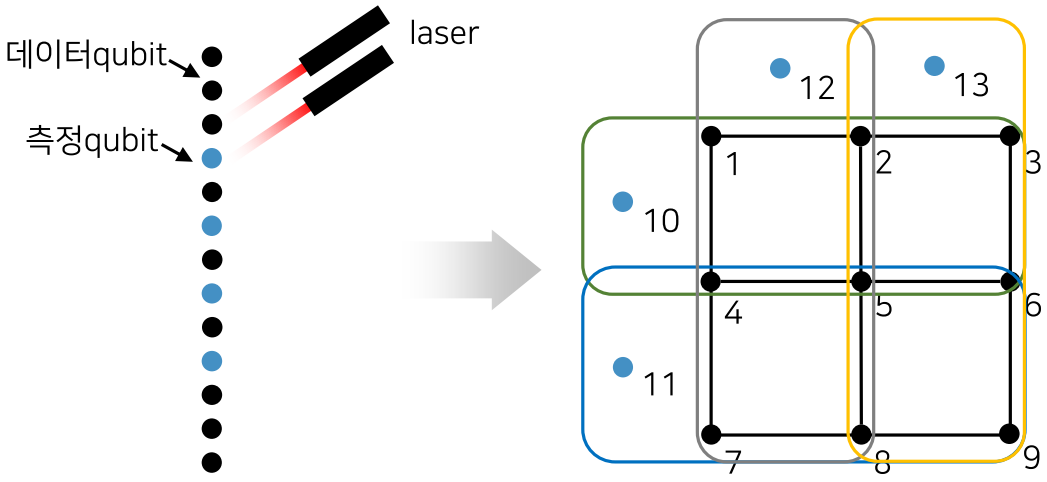
Global quantum computer 기업3: IONQ

이온 포획 qubit에서 오류 검출 코드의 간소화 13 qubit = 1 logical qubit
2028년까지 1000 algorithmic qubit 양자 컴퓨터 목표

2021년 Fault-tolerant control

오류 검출 코드의 간소화 가능

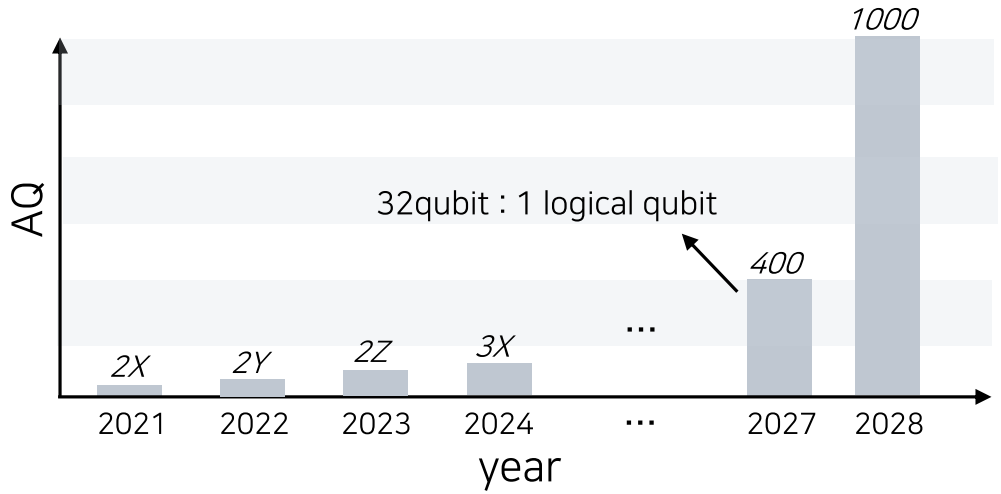
- 이온 포획은 qubit간 연결성이 좋음
- 9 데이터 qubit + 4 측정 qubit → 1 logical qubit



Road map

Algorithmic qubit (AQ)

- 양자 상태 준비 + 양자 회로에서 오류 없이 정상 작동하는 qubit



2028년까지 1000 AQ 달성 목표

※ Reference : Laird Egan, et. al., Nature **598**, 281 (2021); https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap

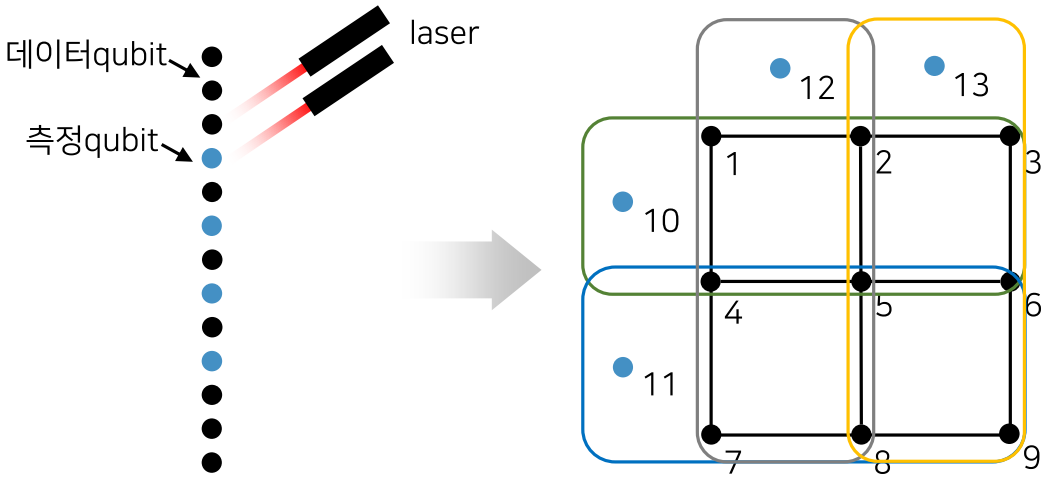
Global quantum computer 기업3: IONQ

이온 포획 qubit에서 오류 검출 코드의 간소화 13 qubit = 1 logical qubit
2028년까지 1000 algorithmic qubit 양자 컴퓨터 목표

2021년 Fault-tolerant control

오류 검출 코드의 간소화 가능

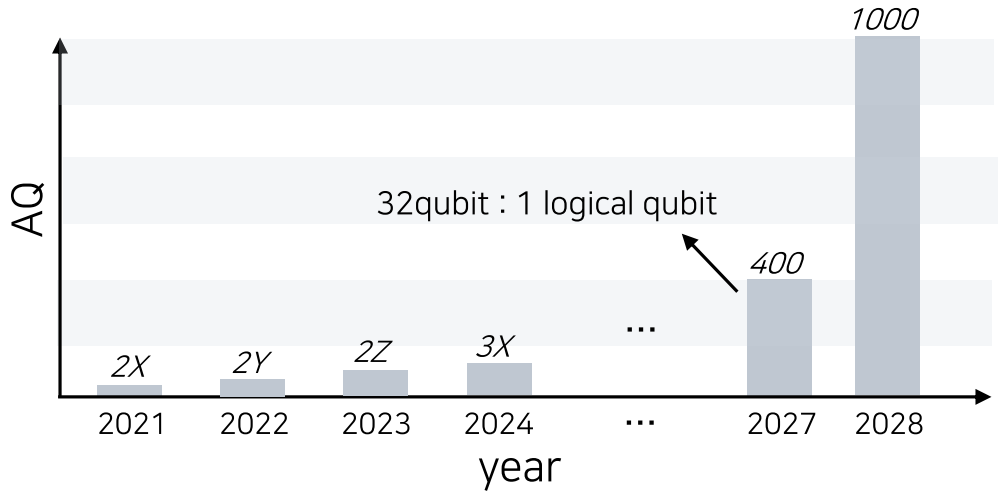
- 이온 포획은 qubit간 연결성이 좋음
- 9 데이터 qubit + 4 측정 qubit → 1 logical qubit



Road map

Algorithmic qubit (AQ)

- 양자 상태 준비 + 양자 회로에서 오류 없이 정상 작동하는 qubit



2028년까지 1000 AQ 달성 목표

※ Reference : Laird Egan, et. al., Nature 598, 281 (2021); https://ionq.com/posts/december-09-2020-scaling-quantum-computer-roadmap

Quantum computer 기업들의 Roadmap

낙관적으로 볼 때 2030년경 1000 logical qubit 양자 컴퓨터 출현
양자 기술 선점을 위해 무엇을 ~~해야 하는가?~~ 하고 있는가?

Quantum computer (QC) Roadmap

2021년: 수십 qubit QC에 대한 오류 검출

2023~2025년: 수십 logical qubit QC

⋮

2030년: 1000 logical qubit QC

무엇을 하고 있는가?

- **양자 컴퓨터 디자인** } H/W
  - 오류 검출 방법의 개선
- **오류 모델링** } H/W + S/W
  - 특수한 연산에 적합하도록 모델링
- **오류에 적응된 양자 알고리즘** } S/W
  - 오류가 있는 적은 수의 qubit으로 풀 수 있는 문제

→ 머신 러닝

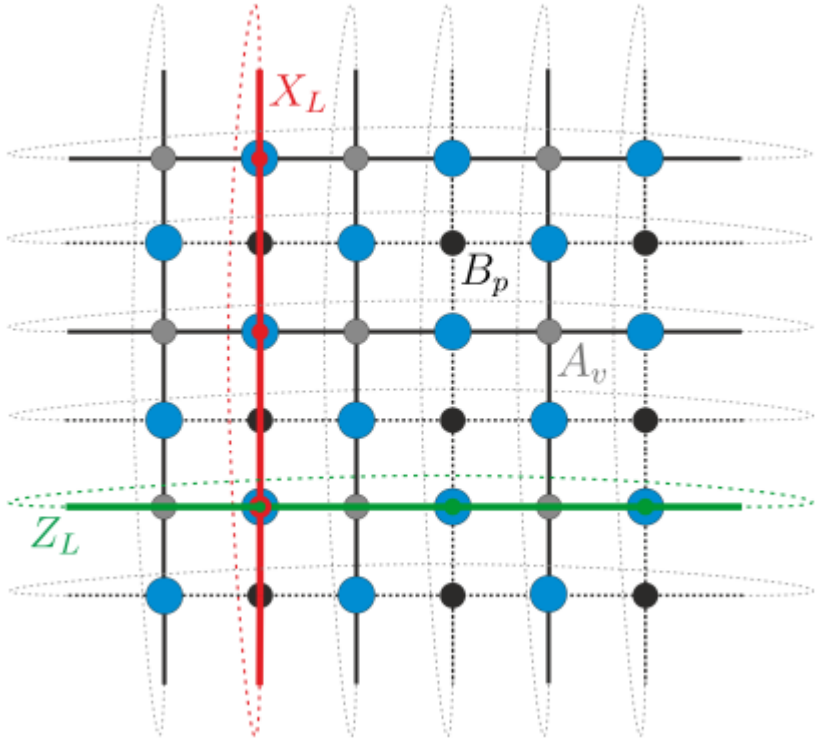
머신 러닝의 역할

제정우 프로

오류 검출 코드 최적화 (양자 컴퓨터 H/W)

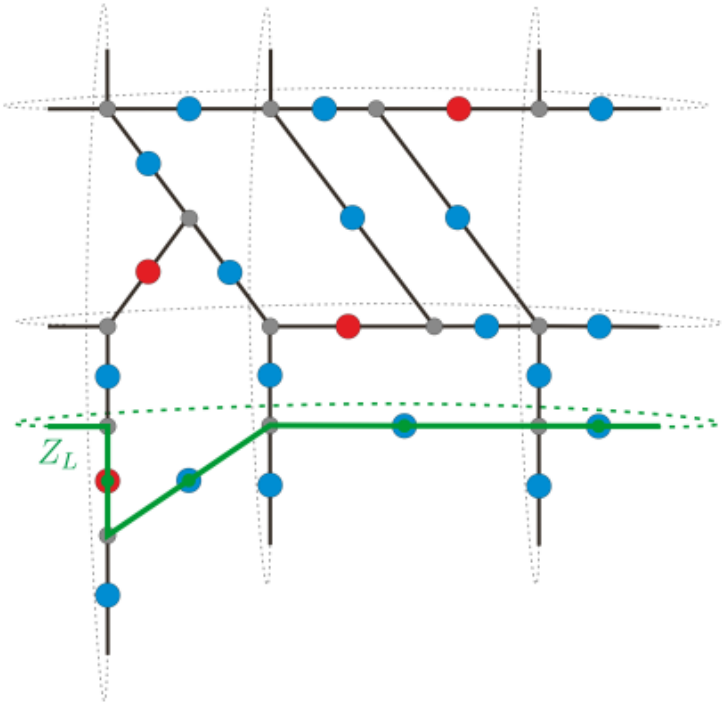
Reinforcement learning을 이용한 최적화

기존 Surface code



qubit 추가

RL 제안



※ Reference : Hendrik Poulsen Nautrup, et. al., Quantum 3, 215 (2019).

사용자를 위한 오류 보정 (양자 컴퓨터 H/W + S/W)

H/W에 접근하기 어려운 양자 컴퓨터 사용자가 오류를 보정 하는 방법들
양자 컴퓨터 domain knowledge 필요

오류 모델링

측정 출력 값을 선형 보정

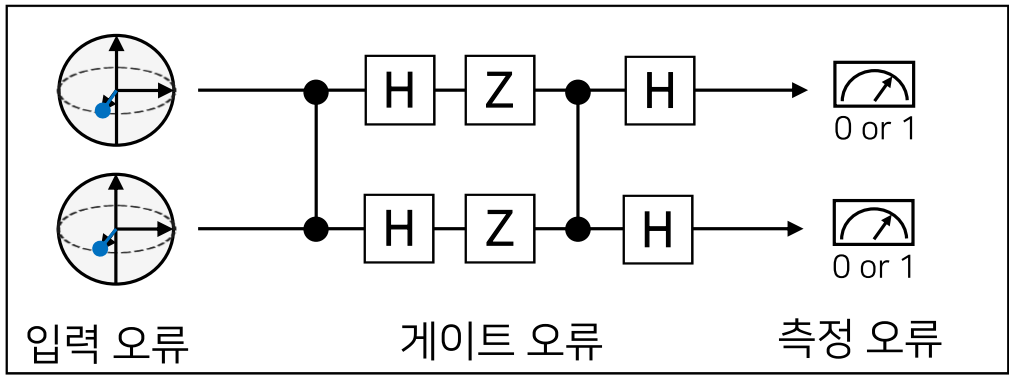
- 이상적인 출력 값과 실제 출력 값을 선형 모델링

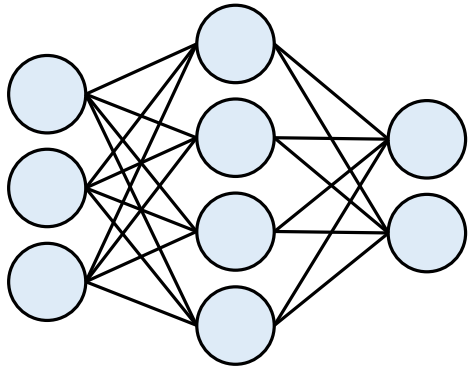
$$Probability_{noise} = M \times Probability_{ideal}$$

양자 회로 최적화

- H/W에서 최적화된 양자 게이트로 양자 회로를 변환

머신 러닝을 통한 오류 모델링





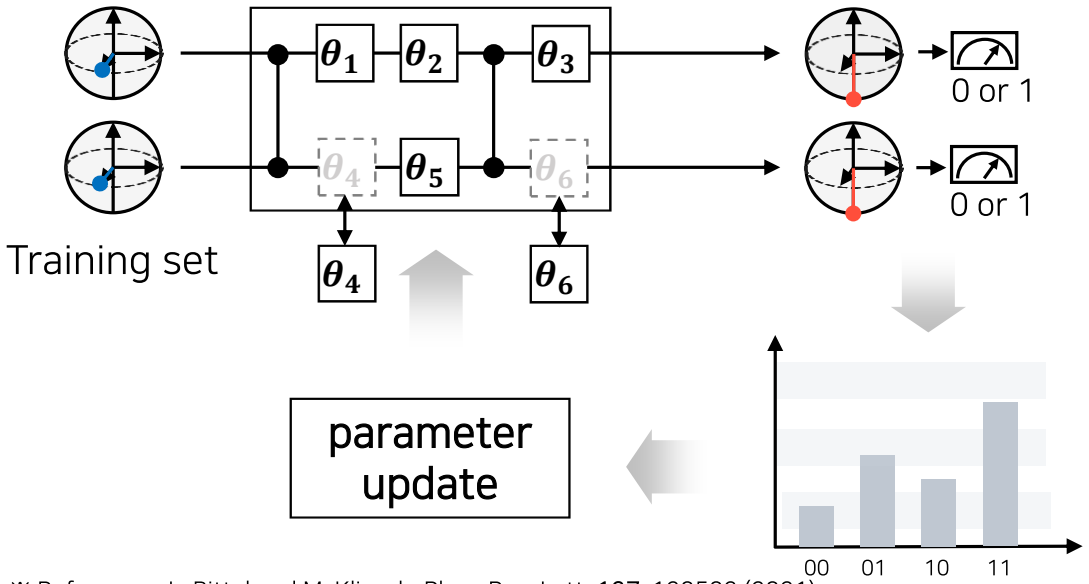
Neural network

학습 가능한 양자 알고리즘 (S/W)

고전 컴퓨팅의 도움을 받아 오류에 적응된 양자 회로를 설계하는 방법

양자 회로 구조 학습

고전-양자 하이브리드 알고리즘



※ Reference : L. Bittel and M. Kliesch, Phys. Rev. Lett. 127, 120502 (2021).

문제의 특성

조합 최적화 + 함수 최적화

문제 공간의 복잡성

- NP-hard problem
- 파라미터 초기 값 설정
- Barren Plateaus 현상

목적 함수 설계 & Data encoding

→ *Quantum Lab*

Thank you

SAMSUNG SDS