

# BT & QT

바이오 기술혁명 앞당기는 **퀀**텀컴퓨팅

고등과학원 김재완

- 양자물리학
- 비트와 큐비트
- 양자컴퓨터
- 양자컴퓨터의 응용: 바이오 기술

# 양자물리학

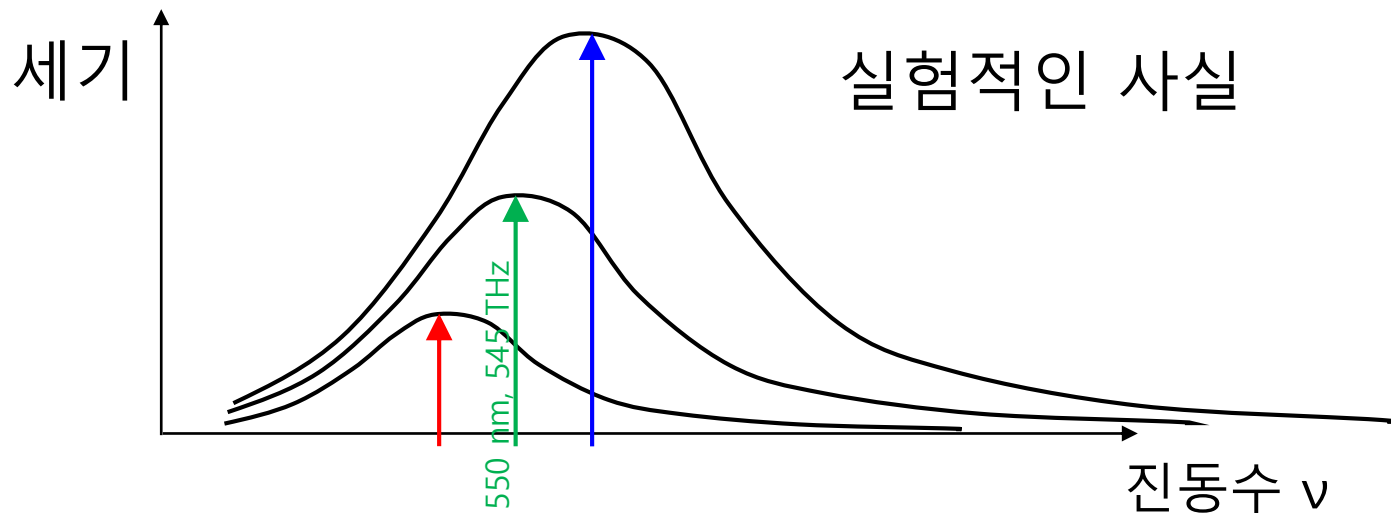
- 1874 , 막스 플랑크의 지도교수  
“이제 물리학 분야에서는 거의 완성되어서 이제 별로 할 일이 없다네 ...”
- 1899: 찰스 두엘, 미국 특허청장  
:( 잘못 알려진 것으로 알려져 있지만 상당수가 이미 그렇게 생각했음)  
“세상에서 발명될만한 것은 다 발명되었다!”  
산업혁명, 백열등, 무선전신, 영화 등등.
- 뉴턴의 고전물리학; 라플라스의 결정론적인 세계관
- 맥스웰의 전자기 이론: 빛은 전자기파

# 1900년, 플랑크, 양자물리학

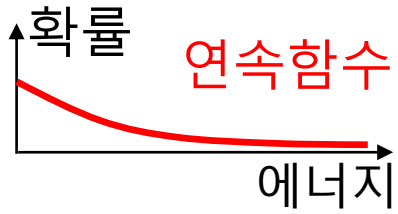
- 흑체복사

뜨거워질수록 붉어지다가 노랗게 되다가 하얗게 빛난다.

(긴 파장/낮은 진동수) → (짧은 파장/높은 진동수)



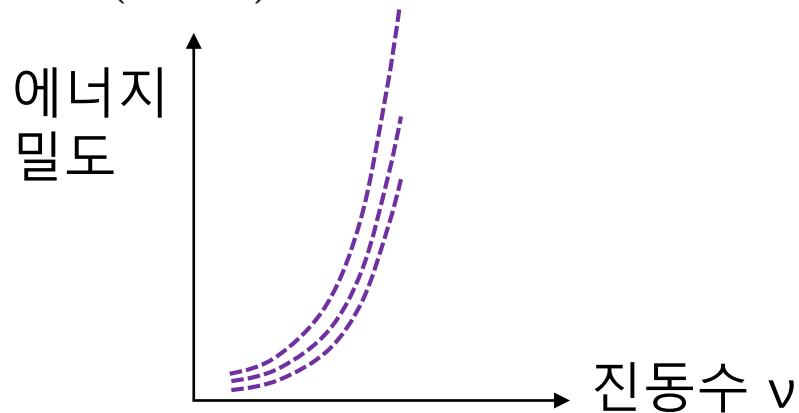
## 고전물리학



$$\langle E \rangle = \frac{\int_0^\infty E e^{-E/kT}}{\int_0^\infty e^{-E/kT}} = kT$$

적분

$$\rightarrow u(\nu, T) \sim \nu^2 kT$$



## 플랑크의 양자가설

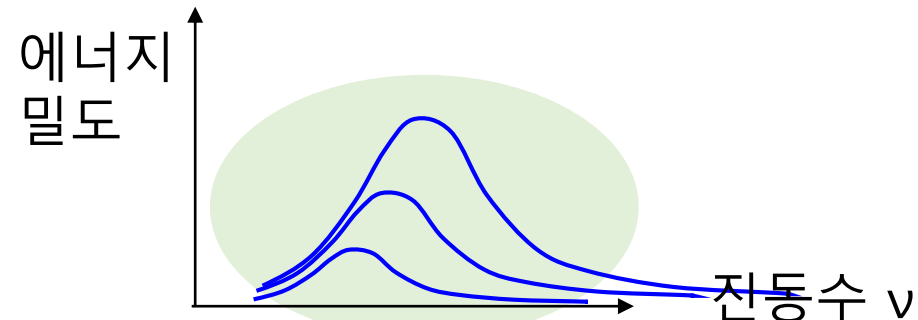
$$E = nh\nu$$

$n$  : 0, 자연수

$h$  : 플랑크 상수

$$\langle E \rangle = \frac{\sum_0^\infty (nh\nu) e^{-nh\nu/kT}}{\sum_0^\infty e^{-nh\nu/kT}} = \frac{h\nu}{e^{h\nu/kT} - 1}$$

$$\rightarrow u(\nu, T) \sim \frac{h\nu^3}{e^{h\nu/kT} - 1}$$



물리량이 연속적이지 않고 덩어리져 있다  
 $\rightarrow$  양자(量子, quantum)

# 양자물리학 : 자연의 궁극적 원리

→ 궁극적 기술

- 연금술 (Alchemy) → 화학 (Chemistry)
- 생명현상: DNA, 시각, 후각, 청각, 광합성 등.
- 반도체, 레이저 → 20세기 정보통신 혁명

# 스무고개

- 동물입니다.
- 다리가 넷인가요?
- 초식성인가요?
- .
- .
- .
- 호랑이입니까?

- 예(1), 아니오(0)
- 예(1), 아니오(0)
- 예(1), 아니오(0)
- .
- .
- .
- 예(1), 아니오(0)

# It from Bit

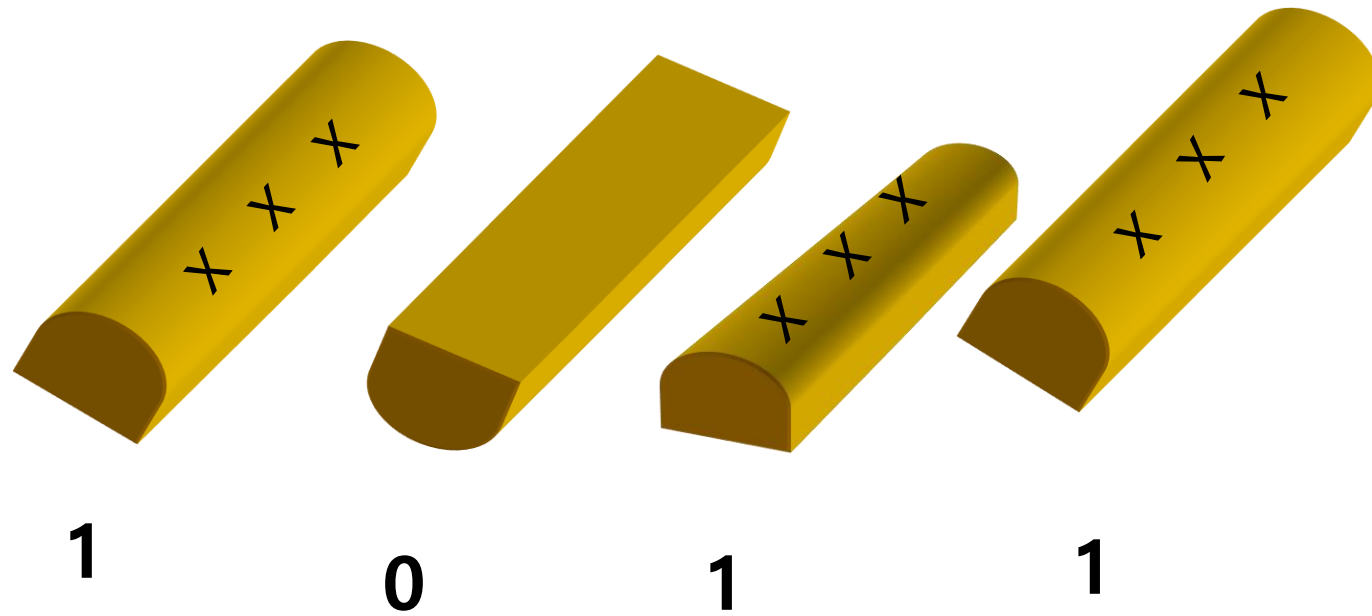
힐러

음(--) 양(—)

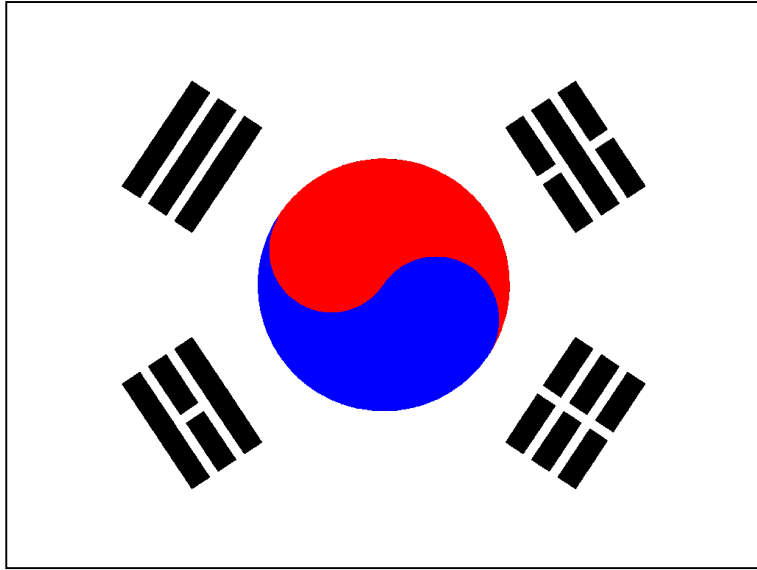
(易經 = 역경 = 주역)



# 숫 (한국형 주사위)



# 태극기



$$|\Psi\rangle = a|0\rangle + b|1\rangle$$

큐비트(Qubit) = 양자비트(quantum bit)



## 21 Ideas for the 21st Century

To 8/30/99

- 10 [CITIES](#)
- 11 [BIOLOGY](#)
- 12 [ARTIFICIAL INTELLIGENCE](#)
- 13 [HEALTH](#)
- 14 [INTERNET](#)
- 15 [MONEY](#)
- 16 [DEMOGRAPHICS](#)
- 17 [POLITICS](#)
- 18 [EDUCATION](#)
- 19 [GENETICS](#)
- 20 [LIFE SCIENCE](#)
- 21 [QUALITY COMPUTERS](#)
- [A PERSPECTIVE](#)
- [A SCIENCE GUIDE](#)
- [ONLINE ORIGINALS](#)

side effects. And there may be pressure--from insurance companies, even from employers--to take the preventive medicine even if we don't want to. Our chances of survival may be greater. The costs of survival may be as well

Video interview with [Alexandra Heerdt](#), director of Memorial Sloan-Kettering Cancer Center's special surveillance breast program

### 15 [MONEY](#)

**In the new financial cosmos, it will be safer to take a dare.**

Imagine a market where hedgers and speculators meet to trade futures, similar to today's betting on the value of corn or soybeans. The wagering will concern the future value of a career, a neighborhood, or even a country. If the risk of a stick-your-neck-out choice is hedged, it's suddenly a whole lot easier to take the plunge

### 17 [POLITICS](#)

**Democracy goes direct--again.**

In many ways, it's back to the 1830s. Candidates will canvass voters in their homes; citizens will question politicians in public forums. The big difference: It will all take place on the Internet. The danger? Net-based splinter groups could factionalize public life

thousands of PCs working in concert have already tackled complex computing problems. In the not-so-distant future, some scientists expect spontaneous computer networks to emerge, forming a "huge digital creature"

Video interview with [Cherry Murray](#), head of Physical Research Lab, Bell Labs

### 16 [DEMOGRAPHICS](#)

**The 'little emperors' can save the world's aging population.**

How will a shrunken generation of fewer, more pampered children worldwide support their retired elders? By using their extra education, ambition, and advantages to become more productive than those who came before them

### 18 [EDUCATION](#)

**Kids were right all along: High school is obsolete.**

Should kids head for college when they're 15 or 16? Some experts think so, and some kids agree. They argue that the last two years of high school just keep students in a holding pattern, when many are independent enough to be starting their advanced education

# 21. 양자컴퓨터

주사위 놀음(양자물리학)으로 가장 어려운 문제들을 풀게 될 것이다.

answer questions beyond the reach of today's computers

### [A SCI-FI GUIDE](#)

**Astounding tales that might come true!**

What high-tech marvels will materialize in the next 100 years? Science fiction is a wellspring of predictions for the next century. Drawing on predictions in the following 30 astounding tales, illustrator David B. Mattingly created this vision of the future

can identify with the human being behind the music. When a machine is making the music, that human connection is broken

### [ONLINE ORIGINALS](#)

**Q&As, Web links, and video interviews**

Additional online-only items found throughout this package are collected here.



양자물리학

정보과학

하드웨어:  
반도체 소자, 레이저

소프트웨어, 운영체제:

양자정보과학

양자병렬성

→ 양자컴퓨터는

디지털보다 지수함수적으로 크고 빠른 계산을 할 수 있다.

양자푸리에변환, 데이터 검색,

양자다체문제 → 나노기술, 계산화학, 바이오

양자정보의 복사불가능성, 양자측정의 비가역성

→ 양자암호 (절대안전한 통신)

양자얽힘의 양자상관성

→ 양자텔레포테이션, 양자초압축코딩, 양자암호, 양자이미징, 양자계측

# 20세기 정보통신기술

- 하드웨어 ← 양자물리학  
반도체, 레이저
- 소프트웨어, 운영체제 ← 수학, 정보과학  
폰노이만, 튜링, 새넌

# 나노기술

- 1 nm(nano meter)= $10^{-9}$ m
  - C-C 결합길이= 0.12~0.15 nm

## • 무어의 법칙

반도체 집적도는 4년에 3배가 된다.

트랜지스터의 크기: cm  $\rightarrow$  nm  $\rightarrow$  ?

kB  $\rightarrow$  MB  $\rightarrow$  GB  $\rightarrow$  TB  $\rightarrow$  PB  $\rightarrow$  EB  $\rightarrow$  ZB  $\rightarrow$  YB  $\rightarrow$  ?

Peta, Exa, Zetta, Yotta, ...

cf. pico, femto, atto, zepto, yocto, xona, weco, ...

# 나노기술의 한계 → 양자정보과학

길이가 나노미터 정도로 된다

→ 미시세계는 양자물리학으로 지배된다

→ 양자 불확정성 원리

→ 0과 1(비트)를 구분하기 어려워짐

→ 디지털 정보에 치명적

→ 무어 법칙의 끝, 나노기술의 한계

→ 양자불확정성을 피하려는 소극적 대응보다

→ 양자현상을 적극적으로 활용하려는 대응

→ 양자정보과학

# 비트 {0,1} → 양자비트/큐비트 $\{|0\rangle, |1\rangle\}$

하다마드  
게이트

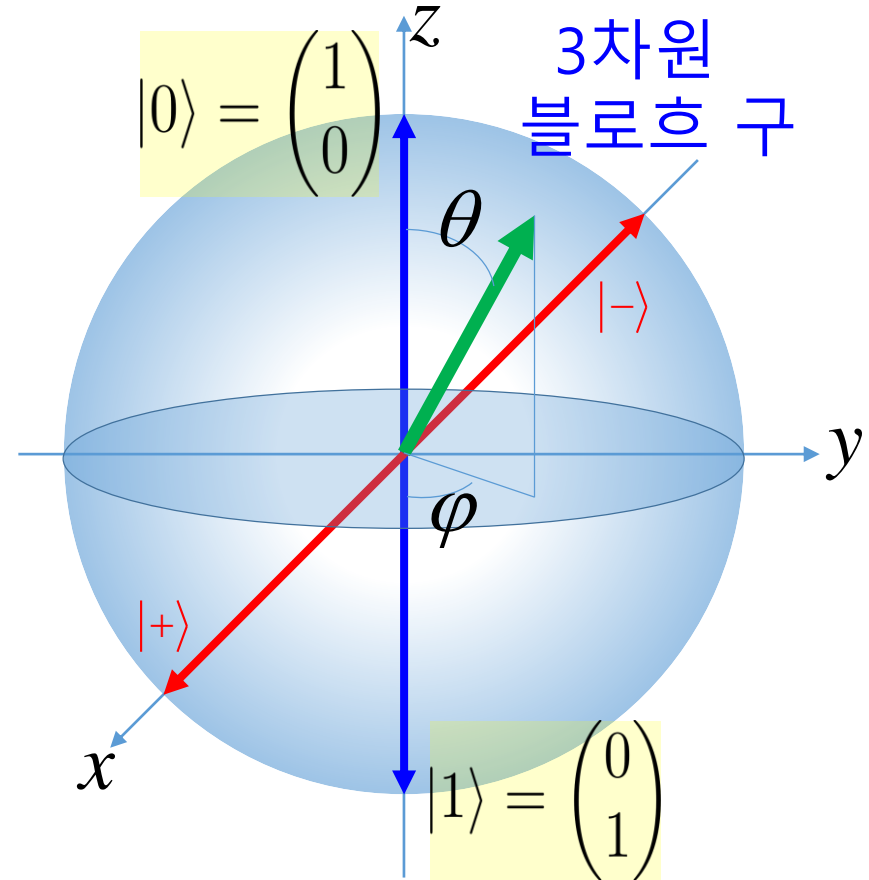
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \equiv |+\rangle$$

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

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \equiv |-\rangle$$



블로흐 구 표면 위의 순수 상태

$$|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right)$$



# 하다마드 게이트

큐비트 한 개

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \quad \text{"0과 1을 한꺼번에"}$$

큐비트  $N$  개

$$\begin{aligned} & H_1 \otimes H_2 \otimes \cdots \otimes H_N \quad |0\rangle_1 \otimes |0\rangle_2 \cdots \otimes |0\rangle_N \\ &= \frac{1}{\sqrt{2}} (|0\rangle_1 + |1\rangle_1) \otimes \frac{1}{\sqrt{2}} (|0\rangle_2 + |1\rangle_2) \otimes \cdots \otimes \frac{1}{\sqrt{2}} (|0\rangle_N + |1\rangle_N) \\ &= \frac{1}{\sqrt{2^N}} (|0_1 0_2 \cdots 0_N\rangle + |1_1 0_2 \cdots 0_N\rangle + \cdots + |1_1 1_2 \cdots 1_N\rangle) \\ &= \frac{1}{\sqrt{2^N}} \sum_{k=0}^{2^N-1} |k(\text{이진법 표현})\rangle \end{aligned}$$

"000...00부터 111...11까지

$2^N$  가지 경우 모두를 한꺼번에"

# 디지털 정보

- 비트
- 0 또는 1, 둘 중의 하나만.

- 비트 4 개로,

0000, 0001, 0010, 0011,  
0100, 0101, 0110, 0111,  
1000, 1001, 1010, 1011,  
1100, 1101, 1110, 1111

모두  $16=2^4$  가지 경우를,  
한 번에 하나씩

# 양자 정보

- 양자비트 = 큐비트
- 0 and 1 의 양자중첩: 둘 다 한꺼번에.  
≠ 퍼지논리 (Fuzzy Logic)

- 큐비트 4 개로

$$\begin{aligned} &(|0\rangle+|1\rangle) \otimes (|0\rangle+|1\rangle) \otimes (|0\rangle+|1\rangle) \otimes (|0\rangle+|1\rangle) \\ &= |0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle \\ &+ |0100\rangle + |0101\rangle + |0110\rangle + |0111\rangle \\ &+ |1000\rangle + |1001\rangle + |1010\rangle + |1011\rangle \\ &+ |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle \end{aligned}$$

$16=2^4$  가지 경우

모두를 한꺼번에.

디지털 컴퓨터

N 비트



$$1 \cdot N$$

N 비트

병렬 디지털 컴퓨터

N 비트



$m$

$$m \cdot N$$

N 비트

양자 컴퓨터: 양자 병렬성

N 비트



$$2^N$$

N 비트

# 성능비교

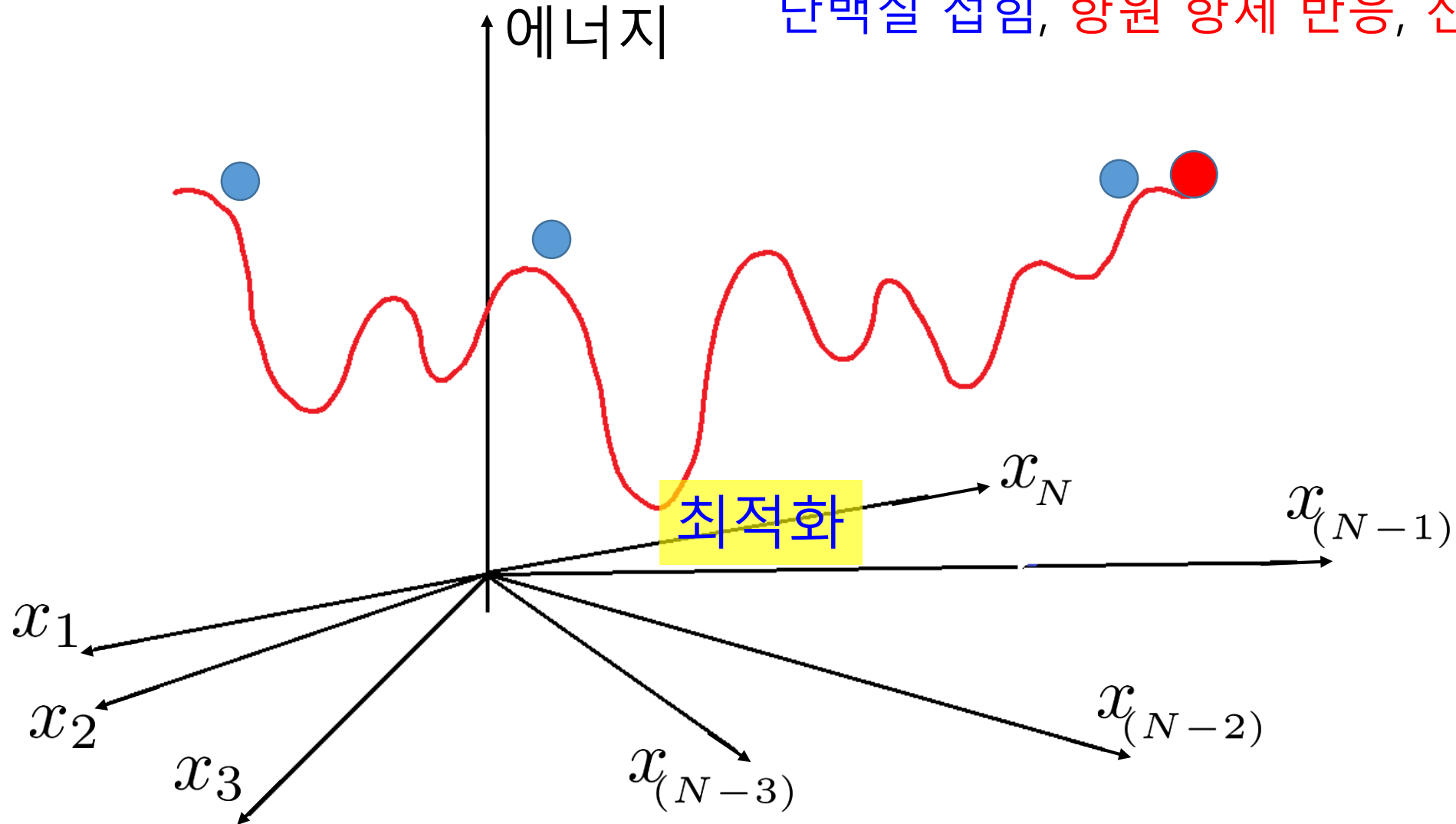
디지털 컴퓨터

양자컴퓨터

양자물리학	하드웨어	양자물리학
정보이론	소프트웨어 /운영체제	양자물리학 + 정보이론
$2^{N^{1/3}}$ 불가능	큰 수의 소인수분해 2000 자릿수	$N^3 \rightarrow IT$ 몇 분 ~ 몇 일
$\frac{N}{2}$ 50만회	데이터 검색 100만 항목	$\sqrt{N} \rightarrow BT, IT$ 수 천회
$2^N$ 불가능	양자다체문제 전자 50개	$N^C \rightarrow NT, IT, BT$ 큐비트 50~1000개

# DNA → RNA → 단백질

단백질 접힘, 항원 항체 반응, 신약 개발 등



# DNA → RNA → 단백질

단백질 접힘, 항원 항체 반응, 신약 개발 등

- 분자 동역학 시뮬레이션  
시뮬레이티드 어닐링(풀림)  
→ 양자 어닐링, Coherent Ising Machine, 단일양자계산
- 정보과학적 방법 (바이오인포매틱스)  
데이터 검색 → 양자검색(그로버), 양자기계학습
- 다체문제  
지수함수적 복잡도 ( $e^N$ ) → 선형적 복잡도 (N)

# 도전은 이제부터

- 구글: 양자 우위 (quantum supremacy)  
2019년 초전도큐비트 53개  
IBM, IonQ, ...
- 오류 수정: 양자 오류는 디지털보다 훨씬 심각  
큐비트 수십 개로 논리 큐비트 1 개 역할
- 니스크=NISQ(Noisy Intermediate Scale Quantum)  
오류 수정 없이도 해 볼만한 중간 규모의 양자 기술
- 양자기계학습 (Quantum Machine Learning), 양자 AI 등.