스핀과 큐비트

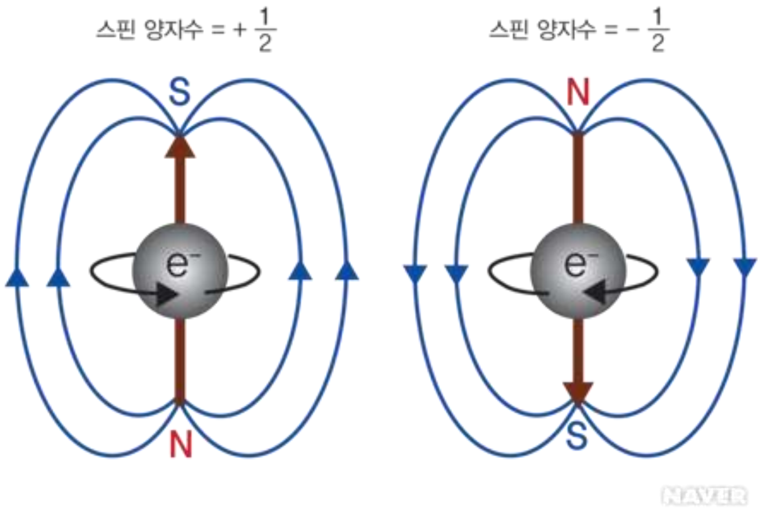
2025113574 권나현

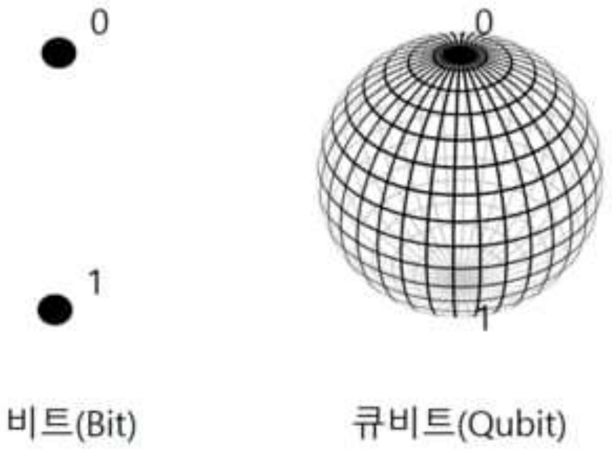
2025.11.12

System Software Lab.

목차

1. 확률
2. 양자스핀을 설명하는 수학적 모델
3. 동치 상태 벡터
4. 특정 스핀 방향의 기저
5. 광자 편광: 수학 모델, 특정 편광 방향의 기저
6. 큐비트
7. 확률 진폭과 간섭





1. 확률

※ 확률 개념

- 가정 : 실험 결과 $E_1, E_2, \ldots, E_n$ 중 하나

P_i : 결과 E_i가 일어날 확률

→ 0~1 값

모든 확률 총합=1

1. 확률

· 스핀 → 가정 0° 방향 측정

실험 결과 N, S 중 하나

P_N : N 얻을 확률

P_S : S 얻을 확률

ex) 전자가 0° 방향으로 스핀 N 갖는다는 결과

→ 같은방향 다시 측정 : $P_N=1$, $P_S=0$

ex) ~~가~~ 90° 방향으로 스핀 N 〃

→ 0° 방향 측정 : $P_N = P_S = 0.5$

2. 양자스핀을 설명하는 수학적 모델

· 양자 스핀을 설명하는 수학적 모델 : 행렬과 벡터

기본모델 = 벡터 공간

측정 결과 개수 = 벡터공간 "차원"

ex) 스핀 : 2개의 결과만 가능하므로 2차원 → $\mathbb{R}^2$

$\mathbb{R}^2$: 표준적인 2차원 평면 → 평면에서 측정장치 회전

(3차원 회전 → 벡터 공간은 2차원 이지만 복소수 계수의 벡터)

(↳ 벡터공간: 2차원 복소수 공간, → $\mathbb{C}^2$)

ex) 가정: $c_1^2+c_2^2=1$을 만족하는 $|v\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$로 제한.

· 스핀 측정할 방향 선택 = 순서가 있는 정규직교 기저 선택

($|b_1\rangle, |b_2\rangle$)

↓ 기저 내 2개 벡터

2개의 가능한 측정결과에 대응함.

첫번째 벡터 = N, 두번째 벡터 = S

· 스핀 측정 전 입자 → $|b_1\rangle$과 $|b_2\rangle$의 선형결합

→ $c_1|b_1\rangle + c_2|b_2\rangle$로 주어지는 스핀상태

⇒ "상태 벡터", "상태"

· 측정 수행 → 상태 벡터는 $|b_1\rangle$이나 $|b_2\rangle$로 바뀜.

2. 양자스핀을 설명하는 수학적 모델

⇒ 측정 행위는 상태 벡터를 바꾼다.

· 새로운 상태 : 측정에 관련된 기저 벡터 중 하나

(어느 벡터가 될지의 확률은 초기상태로 주어짐)

i.e) $|b_1\rangle$가 될 확률 = c_1^2, $|b_2\rangle$가 될 확률 = c_2^2

(2장 p.54)

c_1, c_2 : "확률진폭"

∴ 확률진폭 ≠ 확률

(+/-)   (=확률진폭^2)

2. 양자스핀을 설명하는 수학적 모델

Ex) 수직방향, 수평방향 스핀 측정 실험

· 수직 방향 스핀 측정에 해당하는 두 개 정규직교기저 ⇒ $(|\uparrow\rangle, |\downarrow\rangle)$

$$\left(|\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$$

→ 첫번째 벡터: 0° 방향으로 스핀이 N인 전자

→ 두번째 벡터: 0° 방향으로 스핀이 S인 전자

· 수평방향 스핀 " ⇒ $(|\rightarrow\rangle, |\leftarrow\rangle)$

$$\left(|\rightarrow\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix}, |\leftarrow\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}\right)$$

→ 첫번째 벡터: 90° 방향으로 스핀이 N인 전자

→ 두번째 벡터: 90° 방향으로 스핀이 S인 전자

<실험 1>

1: 수직방향으로 스핀 측정, 2: 수직방향으로 스핀 측정

1

전자의 초기 스핀상태는 모르지만 단위벡터인 것은 분명함

→ $c_1^2+c_2^2=1$ 만족하는 $c_1|\uparrow\rangle + c_2|\downarrow\rangle$

측정 수행 → 전자는 위로 편향되거나 아래로 편향됨

(상태가 $|\uparrow\rangle$) (상태가 $|\downarrow\rangle$)

위로 편향될 확률: c_1^2

아래로 편향될 확률: c_2^2

2

이전상태(위로 편향): $|\uparrow\rangle = 1|\uparrow\rangle + 0|\downarrow\rangle$

측정 수행 → $1^2=1$의 확률로 $|\uparrow\rangle$

$0^2=0$의 확률로 $|\downarrow\rangle$ ⇒ $|\uparrow\rangle$ 상태 유지

이전상태(아래로 편향): $|\downarrow\rangle = 0|\uparrow\rangle + 1|\downarrow\rangle$

즉) 이 전자를 수직 방향으로 몇 번을 측정해도 상태 그대로 유지

실험 반복 → 똑같이 편향된 상태 유지

2. 양자스핀을 설명하는 수학적 모델

<실험 2>

1: 수직방향으로 스핀 측정, 2: 수평방향으로 스핀 측정

1

가정
1: 수직방향 측정 → 0° 방향으로 스핀 N ⇒ $|\uparrow\rangle$

2

2: 수평방향 측정 → 수평 방향에 해당하는 정규직교기저로 벡터 나타내야 함.

→ $|\uparrow\rangle = x_1|\rightarrow\rangle + x_2|\leftarrow\rangle$

만족하는 x_1, x_2 값 구하기

구하는 방법

① 정규직교기저 이루는 것을 나란히 놓아 행렬 A 만들기.

$$A = [\,|\rightarrow\rangle \; |\leftarrow\rangle\,] = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

② $A^T|\uparrow\rangle$ 계산 (새로운 기저에 대한 확률진폭)

$$A^T|\uparrow\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|\rightarrow\rangle + \frac{1}{\sqrt{2}}|\leftarrow\rangle$$

x_1 $\quad$ x_2

2. 양자스핀을 설명하는 수학적 모델

결론

∴ 수평방향 측정 → 상태는 $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ 확률로 $|\rightarrow\rangle$

→ $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ 확률로 $|\leftarrow\rangle$

∴ 전자가 90° 방향으로 스핀 N 가질 확률 $= \frac{1}{2}$
(= $|\uparrow\rangle$)

전자가 90° 방향으로 스핀 S 가질 확률 $= \frac{1}{2}$
(= $|\downarrow\rangle$)

2. 양자스핀을 설명하는 수학적 모델

3

2: 수평방향 측정 이후 전자의 상태벡터: $|\rightarrow\rangle$ or $|\leftarrow\rangle$

3: 수직방향 측정 ⇒ 수직 정규직교 기저들의 선형결합으로.

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle$$

$$|\leftarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$$

3. 동치 상태 벡터

* 동치 상태 벡터

Q: 전자의 스핀(주어진) : $|\uparrow\rangle$ or $-|\uparrow\rangle$ 구별 가능?

A: X

구별하는 측정 수행

(∵) 임의 정규직교기저 선택 → $(|b_1\rangle, |b_2\rangle)$

if 전자상태: $|\uparrow\rangle \rightarrow |\uparrow\rangle = a|b_1\rangle + b|b_2\rangle$ 만족시키는

a, b 구해야 함.

측정 → 스핀이 N일 확률 $= a^2$

→ 스핀이 S일 확률 $= b^2$

if 전자상태: $-|\uparrow\rangle \rightarrow -|\uparrow\rangle = -a|b_1\rangle - b|b_2\rangle$

측정 → 스핀이 N일 확률 : $(-a)^2 = a^2$

→ 스핀이 S일 확률 : $(-b)^2 = b^2$

⇒ 두 경우의 확률 같음 ⇒ $|\uparrow\rangle, -|\uparrow\rangle$ 상태벡터 전자

구별하는 측정 존재 X.

i.e) $|v\rangle$, $-|v\rangle$ 도 구별 불가능 ⇒ "동치 관계"

(equivalent)

∴ 전자가 $|v\rangle$ 스핀 가짐 ⇔ 전자가 $-|v\rangle$ 스핀 가짐.

3. 동치 상태 벡터

(ex) 다음과 같이 4개의 켓이 존재

① $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$ ② $-\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle$ ①,②: 동치벡터

③ $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle$ ④ $-\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$ ③④: 동치벡터

Q: $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$와 $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle$의 관계?

A: 측정방향 → 0°: 구별 불가능.

(두 경우 모두 $\frac{1}{2}$ 확률로 $|\uparrow\rangle$ 이나 $|\downarrow\rangle$

→ 90°: 첫번째: S, 두번째: N) 구별가능

(∵) $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle = |\leftarrow\rangle$, $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle = |\rightarrow\rangle$

Q: 측정방향에 대한 기저는 어떻게 선택?

(수직방향(0°) 측정 시 기저: $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$

수평방향(90°) 〃 $= \left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix}, \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}\right)$)

A: 다음 장

4. 특정 스핀 방향의 기저

측정장치 회전

↳ 90° 회전 → 수평방향 측정

↳ 180° 회전 → 수직방향 측정

전제

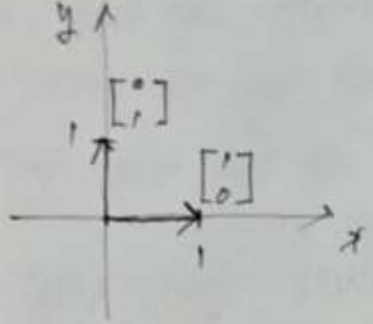
0° 방향으로 스핀이 N ⇔ 180° 방향으로 스핀이 S

0° 방향으로 스핀이 S ⇔ 180° 방향으로 스핀이 N

∴ 장치 회전 시 0°~180° 까지만 고려해도 모든 방향 포함.

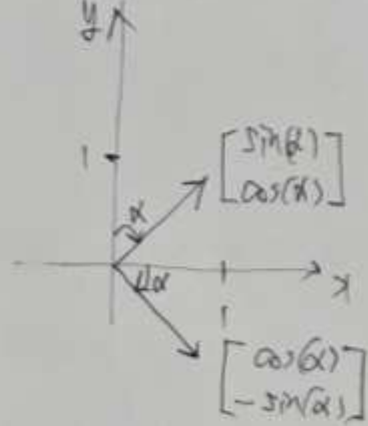
기저 시작점 : 표준기저 $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$

2차원 벡터로 표현 ↳



회전 { α° 만큼

벡터 $\begin{bmatrix}1\\0\end{bmatrix} \rightarrow \begin{bmatrix}\cos(\alpha)\\-\sin(\alpha)\end{bmatrix}$, $\begin{bmatrix}0\\1\end{bmatrix} \rightarrow \begin{bmatrix}\sin(\alpha)\\\cos(\alpha)\end{bmatrix}$



∴ α° 만큼 회전 시

최초의 두 개 직교기저 $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$

$\rightarrow \left(\begin{bmatrix}\cos(\alpha)\\-\sin(\alpha)\end{bmatrix}, \begin{bmatrix}\sin(\alpha)\\\cos(\alpha)\end{bmatrix}\right).$

4. 특정 스핀 방향의 기저

회전 ↙ 90° 만큼

$$\left(\begin{bmatrix}\cos(90^\circ)\\-\sin(90^\circ)\end{bmatrix},\begin{bmatrix}\sin(90^\circ)\\\cos(90^\circ)\end{bmatrix}\right)=\left(\begin{bmatrix}0\\-1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix}\right)$$

$\begin{bmatrix}0\\-1\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}$ → 동치 → 90° 회전하면 원래와 동치인 기저로 돌아옴

(단, 기저 원소들의 순서는 바뀜)

x 와 s

4. 특정 스핀 방향의 기저

(설정)

θ = 측정장치 회전 각도

α = 기저벡터 회전 각도

$0° \le \theta \le 180°$ → 모든 방향 나타낼 수 O

$0° \le \alpha \le 90°$ → 기저의 회전 모두 나타낼수 O

$\theta = 180°$와 $\alpha = 90°$ 도달 → 0° 방향으로 측정된 N, S 서로 바뀜.

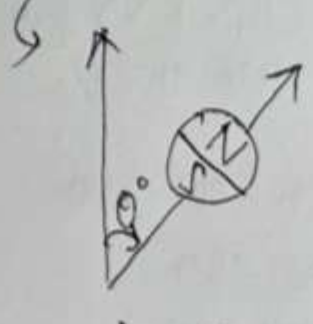
(∵) Bloch 구면의 반각 법칙

물리적 회전각 = 2 × 기저벡터 회전각

$\theta = 2\alpha$

∴ θ만큼 측정 장치 회전한 경우

$$\text{기저} = \left(\begin{bmatrix} \cos\left(\frac{\theta}{2}\right) \\ -\sin\left(\frac{\theta}{2}\right) \end{bmatrix}, \begin{bmatrix} \sin\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \right)$$



측정 각도

$$\left(\begin{bmatrix} \cos\left(\frac{\theta}{2}\right) \\ -\sin\left(\frac{\theta}{2}\right) \end{bmatrix}, \begin{bmatrix} \sin\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \right)$$

4. 특정 스핀 방향의 기저

<예제: 60도만큼 장치 회전>

Q: 스핀 처음 측정 → 전자가 0° 방향의 스핀 N 가짐.

60° 회전한 장치로 다시 측정 → 결과가 N으로 나올 확률은?

sol) 최초 측정 이후 상태벡터 :

0° 방향 스핀 N이므로 $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$

↓ 새로운 기저벡터들의 선형결합으로 표현.

기저의 벡터로 구성된 행렬 × 상태벡터

$$\begin{bmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$$

$$\therefore \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{\sqrt{3}}{2} \begin{bmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix} + \frac{1}{2} \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$$

N 얻을 확률 : $\left(\frac{\sqrt{3}}{2}\right)^2 = \frac{3}{4}$.

5. 광자 편광: 수학 모델, 특정 편광 방향의 기저

※ 광자 편광을 위한 수학 모델

관찰 전자스핀 측정 → 광자 편광
유사성?

실험 수직방향의 편광 필터 → 0°
(수직으로 편광된 광자 통과시키는)

⇒ 수평으로 편광된 광자는 이 필터에 흡수됨.

실험 표준기저 $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$ → 0°에 대한 기저

⇒ 벡터 $\begin{bmatrix}1\\0\end{bmatrix}$: 수직으로 편광된 광자
벡터 $\begin{bmatrix}0\\1\end{bmatrix}$: 수평으로 편광된 광자
대응.

ex) 필터를 β° 만큼 회전

↳ β°로 편광된 광자 통과시킴
β°에 수직으로 편광된 광자 차단시킴

정리 · 각각의 방향에 대해 특정 정규직교기저 ($|b_1\rangle$, $|b_2\rangle$) 존재
(그 방향의 편광 측정과 관련)

→ $|b_1\rangle$: 주어진 방향으로 편광된 (필터 통과) 광자
$|b_2\rangle$: 주어진 방향에 수직으로 편광된 광자
(필터에 의해 흡수)

- 광자 : $|v\rangle$로 주어지는 편광상태 가짐.

선형 조합 → $|v\rangle = \alpha_1 |b_1\rangle + \alpha_2 |b_2\rangle$

5. 광자 편광: 수학 모델, 특정 편광 방향의 기저

(측정) 특정 기저의 방향으로 편광 측정

→ 광자 = α_1^2 확률로 그 방향으로 편광

α_2^2 확률로 그와 수직인 방향으로 편광.

i.e) 광자가 필터 통과할 확률 : α_1^2

필터에 흡수될 확률 : α_2^2

∴ 광자가 주어진 방향으로 편광됐다면 광자상태 = $|b_1\rangle$

(= 광자가 필터 통과)

5. 광자 편광: 수학 모델, 특정 편광 방향의 기저

* 특정 편광 방향의 기저

review · 표준기저 $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right) \xrightarrow{\alpha^\circ \text{ 회전}} \overset{\text{정규직교기저}}{\left(\begin{bmatrix}\cos(\alpha)\\-\sin(\alpha)\end{bmatrix}, \begin{bmatrix}\sin(\alpha)\\\cos(\alpha)\end{bmatrix}\right)}$

· 90° 회전: 기저요소 순서 바뀌나, 표준기저로 돌아감

실험 β° 만큼 편광필터 회전

$\beta = 0^\circ$, $\beta = 90^\circ$ 일 때 각각 측정 (수직, 수평)

$\beta = 0^\circ$ ↓ 수직: 통과, 수평: 흡수

$\beta = 90^\circ$ ↓ 수직: 흡수, 수평: 통과

$\therefore \beta = 90^\circ \xrightarrow{\text{대응}} \alpha = 90^\circ$, $\alpha = \beta$.

$\therefore$ β° 만큼 편광필터 회전시킬 때 해당 정규직교기저

$: \left(\begin{bmatrix}\cos(\beta)\\-\sin(\beta)\end{bmatrix}, \begin{bmatrix}\sin(\beta)\\\cos(\beta)\end{bmatrix}\right)$

5. 광자 편광: 수학 모델, 특정 편광 방향의 기저

* 편광필터 실험

(과정)

① 정사각형 모양의 선형 편광필름 3개

② 2장의 필름 중 하나를 다른 하나의 앞에 배치

1: ③ 하나는 고정시키고 다른 하나를 90° 회전

⇒ 빛이 완전히 차단

2: ④ 2 상태에서 45° 회전된 3번째 필터를 2장의 필터 사이에 배치

⇒ 빛은 3장이 겹치는 영역 통과

(분석) - 1번째 실험 : 2개의 정방형 편광필름.

0° 방향 90° 방향 편광 측정

∵ 0° 일때 기저 = 90° 일때 기저

(순서 바뀌게 되면)

빛 → $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \xrightarrow[\text{흡수}]{} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

∴ 첫번째 필터 통과한 광자는 2번째 필터에서 흡수됨.

5. 광자 편광: 수학 모델, 특정 편광 방향의 기저

- 2번째 실험

(앞 2장의 배치는 동일)

· 45° 회전된 3번째 필름 삽입 → 빛 통과

· 3장의 순서 기저

$$\left(\begin{bmatrix}1\\0\end{bmatrix},\begin{bmatrix}0\\1\end{bmatrix}\right),\left(\begin{bmatrix}\frac{1}{\sqrt2}\\\frac{-1}{\sqrt2}\end{bmatrix},\begin{bmatrix}\frac{1}{\sqrt2}\\\frac{1}{\sqrt2}\end{bmatrix}\right),\left(\begin{bmatrix}0\\1\end{bmatrix},\begin{bmatrix}1\\0\end{bmatrix}\right)$$

3장 모두 통과하는 광자 → 3번 측정

1번째 필터 통과하는 광자 상태: $\begin{bmatrix}1\\0\end{bmatrix}$

2번째 측정에서 광자 상태

$$\begin{bmatrix}1\\0\end{bmatrix}=\frac{1}{\sqrt2}\begin{bmatrix}\frac{1}{\sqrt2}\\\frac{-1}{\sqrt2}\end{bmatrix}+\frac{1}{\sqrt2}\begin{bmatrix}\frac{1}{\sqrt2}\\\frac{1}{\sqrt2}\end{bmatrix}$$

1번째 필터 통과한 광자가 2번째 필터 통과할 확률

$: \left(\frac{1}{\sqrt2}\right)^2=\frac{1}{2}$

∴ 첫번째 필터 통과하는 광자의 절반이 두번째 필터 통과.

상태: $\begin{bmatrix}\frac{1}{\sqrt2}\\\frac{-1}{\sqrt2}\end{bmatrix}$

3번째 필터: 세번째 기저 사용해서 측정

광자상태: $\begin{bmatrix}\frac{1}{\sqrt2}\\\frac{-1}{\sqrt2}\end{bmatrix}=\frac{-1}{\sqrt2}\begin{bmatrix}0\\1\end{bmatrix}+\frac{1}{\sqrt2}\begin{bmatrix}1\\0\end{bmatrix}$

∴ 상태 $\begin{bmatrix}0\\1\end{bmatrix}$인 광자 통과, 확률: $\left(\frac{1}{\sqrt2}\right)^2=\frac{1}{2}$

2개 필터 통과한 광자의 절반이 세번째 필터 통과.

6. 큐비트

* 큐비트

(정의) $\mathbb{R}^2$ 공간 내에서의 임의의 단위 벡터

큐비트 주어짐 → 측정 → $|b_0\rangle$아 $|b_1\rangle$ 결과

- 측정 방향 고려 : 두개 정해지고 기저 $(|b_0\rangle, |b_1\rangle)$ 도입
- 형태 : $\alpha_0|b_0\rangle + \alpha_1|b_1\rangle$ (기저벡터의 선형결합)
- $|b_0\rangle$ 확률 : $(\alpha_0)^2$
- $|b_1\rangle$ 확률 : $(\alpha_1)^2$

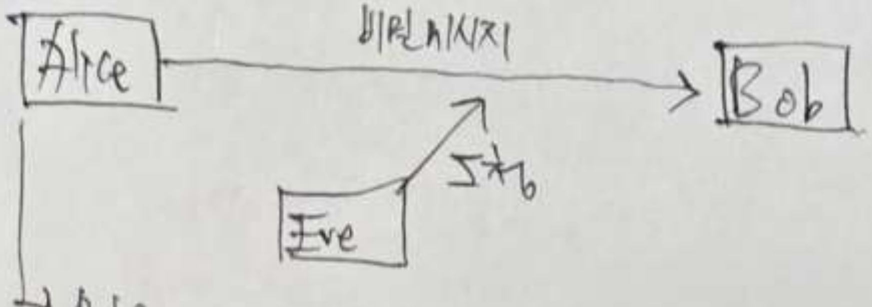
· 큐비트 = 단위 벡터 → 무한히 많음. ≠ 고전적 컴퓨터

· 큐비트로부터 정보 얻으려면 큐비트 측정 필요

· 측정 → 0 아 1 결과 = 최종결과 : 고전적인 비트

* 예제 : 앨리스, 밥, 이브 (암호학)

· 암호학의 핵심 목표



→ Bob은 메시지 읽고 Eve는 못 읽게 하려면?
어떻게 암호화?

6. 큐비트

큐비트

Alice → Bob 큐비트 스트림 보내는 방법

Alice : 자신의 정규직교기저 $(|a_0\rangle, |a_1\rangle)$ → 큐비트 측정

Bob : Alice가 보낸 큐비트를 자신의 정규직교기저 $(|b_0\rangle, |b_1\rangle)$ 사용해 측정

ex) Alice가 0을 보내려 한다

Alice : 자신의 측정장치 → 큐비트 상태 $|a_0\rangle$와 $|a_1\rangle$ 생성가능

상태 $|a_0\rangle$인 큐비트 보냄.

Bob : 자신의 순서기저 사용해 측정 하기 위해 $|a_0\rangle$을 Bob의 기저 벡터들의 선형결합으로 나타내야 함.

$\therefore |a_0\rangle = d_0|b_0\rangle + d_1|b_1\rangle$ 형태.

측정 시 d_0^2 확률로 $|b_0\rangle$, d_1^2 확률로 $|b_1\rangle$

Q: Bob과 Alice가 같은 기저 사용하지 않는 이유

A: Eve도 같은 기저 사용하면 Bob과 같은 메시지 받음 → 도청가능

6. 큐비트

ex) Alice, Bob이 기저 $\left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right)$ 와 $\left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix}, \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}\right)$

사용해 자신들의 큐비트 측정

→ 스핀 계산과 동일하게 계산
($N, S \to 0, 1$)

· 둘이 동일한 기저 사용할 때만 Bob은 Alice가 의도했던 비트 받음

- 서로 다른 기저 사용 → B: Alice 의도에 $\frac{1}{2}$ 받음
(틀린 비트 $\frac{1}{2}$)

· Alice와 Bob이 서로 다른 2개의 기저를 사용하면서 안전한 통신을 주고받는 방법이 있음.

ex) Alice와 Bob이 3개 기저 中 1 무작위로 선택
↳ 전자스핀을 0°, 120°, 240° 방향 측정

Q. Alice가 240°, Bob이 120° 방향으로 측정한다면?

A: Alice의 기저: $\left(\begin{bmatrix}-\frac{1}{2}\\ -\frac{\sqrt{3}}{2}\end{bmatrix}, \begin{bmatrix}\frac{\sqrt{3}}{2}\\ -\frac{1}{2}\end{bmatrix}\right)$

Bob의 기저: $\left(\begin{bmatrix}\frac{1}{2}\\ -\frac{\sqrt{3}}{2}\end{bmatrix}, \begin{bmatrix}\frac{\sqrt{3}}{2}\\ \frac{1}{2}\end{bmatrix}\right)$

(∵ θ방향 정규직교기저: $\left(\begin{bmatrix}\cos\left(\frac{\theta}{2}\right)\\ -\sin\left(\frac{\theta}{2}\right)\end{bmatrix}, \begin{bmatrix}\sin\left(\frac{\theta}{2}\right)\\ \cos\left(\frac{\theta}{2}\right)\end{bmatrix}\right)$)

6. 큐비트

케이스 (ㄱ) 중해도 동치

↳ Alice의 기저: $\left(\begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}, \begin{bmatrix} \frac{\sqrt{3}}{2} \\ -\frac{1}{2} \end{bmatrix} \right)$

= 60° 방향의 기저와 같음

(벡터 순서 다름)

(240° 방향으로 N측정 = 60° 방향으로 S측정)

Alice: 0을 보내고 싶으면 큐비트 $\begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$를 보냄.

Bob의 측정 결과: 확률진폭 구하기

(Bob 기저벡터의 선형조합)

(기저벡터 보다 확률 X 큐비트?) (정리)

$$\begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} -\frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$$

$$\therefore \begin{bmatrix} -\frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} = -\frac{1}{2} \begin{bmatrix} \frac{1}{2} \\ -\frac{\sqrt{3}}{2} \end{bmatrix} + \frac{\sqrt{3}}{2} \begin{bmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{bmatrix}$$

$\rightarrow \left(-\frac{1}{2}\right)^2 = \frac{1}{4}$ 확률로 0

$\left(\frac{\sqrt{3}}{2}\right)^2 = \frac{3}{4}$ 확률로 1

⊕ Alice: 1 보내면 → Bob: $\frac{1}{4}$ 확률로 1

$\frac{3}{4}$ 확률로 0 얻음.

i.e) Alice, Bob이 3개의 기저 중 하나 선택하되, 3번째 기저가 표준기저고 둘이 나머지 2개 중에서 하나씩 사용

-> Bob은 언제나 1/4 확률로 정확한 비트 얻음.

7. 확률 진폭과 간섭

* 확률 진폭과 간섭

· 보강간섭 : 두 파동의 위상이 같을 때 (마루, 골 일치)

→ 파동의 진폭 커짐 ⊕

· 상쇄간섭 : 두 파동의 위상이 반대일 때 (마루 + 골)

→ 파동의 진폭 감소 ⊖

큐비트

형태: $\alpha_0|b_0\rangle + \alpha_1|b_1\rangle$

확률진폭 → ⊕, ⊖ 가능

(확률진폭)^2 = 해당 기저벡터로 바뀔 확률

ex). 2개의 큐비트 $|\leftarrow\rangle$, $|\rightarrow\rangle$

↓ 표준기저로 측정

$|\uparrow\rangle$와 $|\downarrow\rangle$로 바뀜.

확률: $\frac{1}{2}$ $\frac{1}{2}$

비트로 해석 => 0 와 1을 같은 확률로 얻음.

· 2개의 큐비트 중첩

$|v\rangle = \frac{1}{\sqrt{2}}|\leftarrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$

↓ 수평방향으로 $|v\rangle$ 측정 ↓ 수직방향으로 측정

$|\leftarrow\rangle$와 $|\rightarrow\rangle$ 같은 확률로 얻음. 0

(∵) $|v\rangle = \frac{1}{\sqrt{2}}|\leftarrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix}$

$= 1\begin{bmatrix}1\\0\end{bmatrix} + 0\begin{bmatrix}0\\1\end{bmatrix}$

↓ 보강간섭 ↓ 상쇄간섭

7. 확률 진폭과 간섭

⇒ 이러한 성질은 양자 알고리즘에서 중요
선형결합 선택 → 관심 있는 항만 골라서 증폭
나머지 항들은 없앰.

예고: BB84 프로토콜

감사합니다.