양자컴퓨터의 수학적 기초 탐구

2025-07-31

황태준
중앙고등학교
2025
20731

Contents

친구 몇 명이 보여달라고 해서 설명문 형식이 될 수도 있음을 양해 부탁드립니다.

I. 고전 정보

양자역학 이전에는, ($F = ma$로 대표되는) 고전적인 물리 법칙이 "확정"적으로 기술되었고, 그것이 상식이었다. 인간적인 상식에 따라 정보 또한 당연히 확정적으로 표현되었다.

I.1. 고전 정보와 확률벡터

전형적인 고전 정보를 취하는 계(系, system)의 예시는, 고전적인 "상태"(state)인 0과 1로 이루어진 컴퓨터의 비트(bit, binary digit)이다. 다른 예시로는 여섯 면을 가진 주사위가 있다. 주사위가 가진 고전적인 상태는, 윗면의 숫자에 대응시킨다고 했을 때, 1, 2, 3, 4, 5, 6이다. DNA의 염기서열은 A, T, C, G를 가지고, 선풍기 풍량은 끔, 미풍, 약풍, 강풍 등의 상태를 가지게 된다.

이때, 이러한 계를 X라고 하고, 이 계가 가질 수 있는 상태의 집합을 Σ라고 하자. 우리는 이렇게 놓음으로써 Σ는 유한집합이고, 공집합이 아니라고 정하게 된다. 이것을 간단히 수식으로 표현하면

$$X \in \Sigma \qquad \text{s.t. } \Sigma \neq \varnothing \wedge |\Sigma| \neq \infty \tag{1.1}$$

몇 가지 예시는 다음과 같다.

- X가 비트라면, $\Sigma = \{0, 1\}$
- X가 주사위라면, $\Sigma = \{1, 2, 3, 4, 5, 6\}$
- X가 뉴클레오타이드라면, $\Sigma = \{\mathrm{A}, \mathrm{T}, \mathrm{C}, \mathrm{G}\}$
- X가 선풍기라면, $\Sigma = \{$끔, 미풍, 약풍, 강풍$\}$

이처럼, 계 X의 상태 집합 Σ의 원소들은 특정 의미를 갖는 문자에 대응되어 정보를 효율적으로 기술한다. 예를 들어 우리가 선풍기를 조작하고 있다고 생각해 보자. 이 상황에서는 상태가 무엇인지 바로 알 수 있다. 바람이 너무 세다고 느끼는 것은 선풍기를 코앞에서 강풍으로 틀어놨기 때문일 것이다. 우리는 선풍기가 강풍으로 되어 있음을 확인할 수 있고, 임의로 미풍으로 바꿀 수 있다. 하지만 모든 정보가 이렇게 확정적으로 처리될 수는 없다(물론 선풍기도, 풍량을 확인하기 전에는 무슨 풍량으로 되어 있는지 알 수 없기도 하다).

주사위를 던진다고 생각해 보자. 주사위가 구르다가 멈추기 전에는 주사위가 어떤 상태를 가질지 알 수가 없다. 사실, 대부분의(또는 모든) 정보가 이러한 성질을 갖는데, 우리는 이것을 확률로 표현한다. 일반적인 경우 주사위가 상태 2를 가질 확률은 아래와 같이 표현한다.

$$P(\mathsf{X} = 2) = \frac{1}{6} \tag{1.2}$$

각 상태가 점유하는 확률을 모두 표현해 보면

$$\begin{aligned} P(\mathrm{X}=1) &= \frac{1}{6} \\ P(\mathrm{X}=2) &= \frac{1}{6} \\ P(\mathrm{X}=3) &= \frac{1}{6} \\ P(\mathrm{X}=4) &= \frac{1}{6} \\ P(\mathrm{X}=5) &= \frac{1}{6} \\ P(\mathrm{X}=6) &= \frac{1}{6} \end{aligned} \tag{1.3}$$

또는 이것을 간단하게 열벡터로 나타낸다.

$$\begin{pmatrix} \frac{1}{6} \\ \frac{1}{6} \\ \frac{1}{6} \\ \frac{1}{6} \\ \frac{1}{6} \\ \frac{1}{6} \end{pmatrix} \tag{1.4}$$

우리는 아래 두 가지를 가정하면 모든 확률 분포를 열벡터로 나타낼 수 있다.

1. 모든 원소는 음이 아닌 실수이다.
2. 모든 원소의 합은 1이다.

반대로, 위 두 속성을 만족하는 열벡터는 확률 분포로 해석할 수 있다. 앞으로 우리는 이런 벡터를 '확률벡터'라고 하자.

I.2. 확률 상태의 측정

어떤 계를 측정한다는 것은 그 계가 어떤 상태에 있는지를 명확히 확인하는 것이다. 또, 측정을 하게 되면 확률벡터가 새로 정의되는데, 계가 현재 상태에 있는 것이 확실하게 되므로 현재 상태의 확률은 1, 나머지 상태들은 0이 된다.

어떤 계에서 상태가 $a \in \Sigma$에 있다면, 우리는 확률벡터를 아래와 같이 나타낼 수 있다.

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{1.5}$$

이 벡터는 이 계가 확실히 상태 a에 있다는 것을 의미하고, 이 벡터를 $|a\rangle$라고 한다[1].

하나의 동전을 계라고 보면 상태에 대한 기저 벡터는 다음과 같이 정할 수 있다.

$$|\text{앞면}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |\text{뒷면}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.6}$$

이제, 계의 확률벡터는 각 기저 벡터의 선형 결합식으로 나타내어질 수 있다. 우리의 예에서는

$$\begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{2}|\text{앞면}\rangle + \frac{1}{2}|\text{뒷면}\rangle \tag{1.7}$$

꽤나 뻔한 소리처럼 보일 수 있으나, 양자 정보도 고전 정보와 비슷하게 기술하게 되며, 우리는 고전 정보를 이렇게 표현함으로써 양자 정보를 이해하는 데 조금 더 가깝게 다가갈 수 있다.

II. 양자 정보

II.1. 양자 상태벡터

계의 양자 상태는 고전 정보의 확률벡터와 비슷하게 열벡터로 나타낸다. 하지만, 확률벡터와 달리 양자 상태벡터의 원소는 복소수이다. 그에 따라 모든 원소의 절댓값 제곱의 합이 1이 되어야한다. 이것은 곧 해당 벡터의 유클리드 노름이 1이라는 것과 동치이다.

[1] 물론 $\vec{a}$나 $\mathbf{a}$처럼 표현할 수도 있겠지만, 양자역학에서는 디랙 표기법에 따라 $|a\rangle$를 사용한다.

Definition 2.1.1 (열벡터의 유클리드 노름)

열벡터

$$v = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix} \tag{2.1}$$

의 유클리드 노름(Euclidian norm)은

$$\|v\| = \sqrt{\sum_{k=1}^{n} |\alpha_k|^2} \tag{2.2}$$

즉, 양자 상태벡터는 유클리드 노름이 1임을 만족하는 힐베르트 공간 상의 단위 벡터이다.

II.2. 큐비트

큐비트(qubit)란 상태를 $\Sigma = \{0, 1\}$로 가지는 양자 계이다. 즉, 양자 상태를 가질 수 있는 비트이다.

$$|0\rangle \triangleq \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ |1\rangle \triangleq \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.3}$$

이때, 큐비트의 상태로 가능한 몇 가지 예는 아래 같은 것들이 있다.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$\begin{pmatrix} \frac{1+2i}{3} \\ -\frac{2}{3} \end{pmatrix} = \frac{1+2i}{3}|0\rangle + -\frac{2}{3}|1\rangle \tag{2.4}$$

그 중에서도 아래 두 상태는 자주 등장하여 별도의 기호가 있다.

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{2.5}$$

II.3. 디랙 표기법

우리가 가능한 상태 $a \in \Sigma$를 가진 상태벡터 $|\psi\rangle$에 대해 행렬곱은 해당 인덱스의 원소 값을 출력한다.

$$|\psi\rangle = \frac{1+2i}{3}|0\rangle + -\frac{2}{3}|1\rangle = \begin{pmatrix} \frac{1+2i}{3} \\ -\frac{2}{3} \end{pmatrix} \tag{2.6}$$

이라고 하면

$$\langle 0|\psi\rangle = \frac{1+2i}{3},\ \langle 1|\psi\rangle = -\frac{2}{3} \tag{2.7}$$

또, 임의의 벡터에 대해 행벡터 $\langle\psi|$는 열벡터 $|\psi\rangle$를 켤레 전치(conjugate transpose)한 것이다.

$$\langle\psi| = \frac{1-2i}{3}\langle 0| - \frac{2}{3}\langle 1| = \left(\frac{1-2i}{3}, -\frac{2}{3}\right) \tag{2.8}$$

Definition 2.3.1 (에르미트 전치행렬)

복소수체 상의 행렬 A에 대해 모든 원소에 켤레를 취한 행렬을 A의 켤레 행렬이라고 하고, $\overline{A}$로 쓴다.

이때, 아래를 켤레 전치행렬(conjugate transpose) 또는 에르미트 전치행렬(Hermitian transpose)이라고 한다[2].

$$A^\dagger \equiv A^* \stackrel{\Delta}{=} \overline{A^\mathsf{T}} \tag{2.9}$$

이 표기법에 따라, 상태벡터는 다음을 만족한다고 할 수 있다.

$$\||\psi\rangle\|^2 = \langle\psi|\psi\rangle = 1 \tag{2.10}$$

한 가지 예시로, 가능한 상태 $\Sigma = \{0,1,2,3,4,5,6,7,8,9\}$를 갖는 양자 10진법 자릿수 상태는 아래와 같다[3].

---

[2] †는 단검을 본뜬 모양으로, 칼표라고 한다. 켤레 전치행렬을 표기할 때, 순수 수학에서는 별표를, 물리학에서는 칼표를 쓰는 편이다. 비슷하게, 켤레 복소수를 표기할 때 순수 수학에서는 윗선을, 물리학에서는 별표를 쓴다.

[3] $\frac{1}{\sqrt{385}}$는 벡터를 크기 1로 만들기 위한 계수이다. $|\psi\rangle = \sum_{k=0}^{9}(k+1)|k\rangle$로 두면, 벡터의 노름 제곱은 $\langle\psi|\psi\rangle = \sum_{k=0}^{9}|k+1|^2 = \sum_{k=1}^{10}k^2 = 385$. 상태벡터를 확률로 해석하려면 그 크기가 1이어야 하며, 그렇게 만드는 과정을 정규화라고 한다.

$$\frac{1}{\sqrt{385}}\begin{pmatrix}0\\1\\2\\3\\4\\5\\6\\7\\8\\9\end{pmatrix} = \frac{1}{\sqrt{385}}\sum_{k=0}^{9}(k+1)|k\rangle \tag{2.11}$$

이렇게 상태가 많아질수록 열벡터 표기는 불편해지고, 디랙 표기법이 얼마나 효율적인지를 확인해볼 수 있다. 디랙 표기법은 아직 상태가 확정되지 않았을 때도 그 상태를 표현할 수 있는데, 임의의 고전 상태 집합 Σ에 대해 양자 상태벡터는 아래와 같다.

$$\frac{1}{\sqrt{|\Sigma|}}\sum_{a\in\Sigma}|a\rangle \tag{2.12}$$

II.4. 양자 상태의 측정

양자 상태가 측정될 때는 어떤 일이 일어나는가? 여러 가지 측정 방법이 있지만 그 중에서도 표준 기저[4] 측정(standard basis measurement)라는 방법을 알아보겠다. 확률론적 상황에서처럼, 어떤 양자 상태를 측정하면 관찰자는 양자 상태벡터 그 자체가 아닌, 그 벡터에 속한 어떤 고전 상태 하나만을 보게 된다. 즉, 측정은 양자 정보와 고전 정보 간 연결 고리의 역할을 한다.

양자 상태가 측정될 때, 각 고전 상태는 상태벡터에 대응되는 값의 절댓값 제곱의 확률로 나타난다. 예를 들어, $|+\rangle$ 상태를 측정할 때는

$$\begin{aligned}P(\mathrm{X}=0) &= |\langle 0|+\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}\\ P(\mathrm{X}=1) &= |\langle 1|+\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}\end{aligned} \tag{2.13}$$

해보면 알겠지만, $|-\rangle$도 같은 결과가 나온다.

상태벡터가

$$|\psi\rangle = \frac{1+2i}{3}|0\rangle + -\frac{2}{3}|1\rangle \tag{2.14}$$

[4] 큐비트에서 표준 기저는 $\{|0\rangle, |1\rangle\}$이다.

라면, 측정 시 확률은

$$P(\mathrm{X}=0) = |\langle 0|\psi\rangle|^2 = \left|\frac{1+2i}{3}\right|^2 = \frac{5}{9}$$
$$P(\mathrm{X}=1) = |\langle 1|\psi\rangle|^2 = \left|-\frac{2}{3}\right|^2 = \frac{4}{9} \tag{2.15}$$

II.5. 유니터리 연산

그런데, 양자 정보는 고전 정보와 근본적으로 뭐가 다른가? 지금까지 본 바로는 복소수를 원소로 가진다는 것 외에는 없어 보인다. 그러면 상태벡터의 확률을 그냥 확률벡터로 나타내면 안 되는 것인가?

가장 쉬운 답은, 양자 정보는 고전 정보와 허용된 연산의 집합이 다르다. 확률벡터와 비슷하게 상태벡터에서의 연산도 선형 사상이다. 하지만 고전적인 경우에는 연산이 확률 행렬(벡터)로 표현되는 반면, 양자 상태벡터에 대한 연산은 유니터리 행렬로 표현된다는 점이 다르다.

Definition 2.5.1 (선형 사상)

벡터 공간 V, W 상에서 정의된 함수 $T : V \to W$가 아래 두 조건을 만족시키면 T는 선형 사상(線型寫像, linear map) 또는 선형 변환(線型變換, linear transformation)이라고 한다.

1. 가법성(加法性, additivity)

$$T(\mathbf{u}+\mathbf{v}) = T(\mathbf{u}) + V(\mathbf{v}) \qquad \forall \mathbf{u}, \mathbf{v} \in V \tag{2.16}$$

2. 동차성(同次性, homogeneity[5])

$$T(c\mathbf{v}) = cT(\mathbf{v}) \qquad \forall c \in \mathbb{F}, \mathbf{v} \in V \tag{2.17}$$

여기서 $\mathbb{F}$는 $\mathbb{R}, \mathbb{C}$ 등 벡터 공간 V, W의 스칼라 체이다.

이 두 조건을 합쳐서 표현하면

$$T(a\mathbf{u}+b\mathbf{v}) = aT(\mathbf{u}) + bT(\mathbf{v}) \qquad \forall a, b \in \mathbb{F} \wedge \mathbf{u}, \mathbf{v} \in V \tag{2.18}$$

Definition 2.5.2 (유니터리 행렬)

복소 정사각행렬[6] U는 아래 식을 만족시키면 유니터리 행렬이다[7].

[5] 정확하게는 homogeneity of scalar multiplication(스칼라배의 동차성)

[6] 정방행렬이라고도 한다.

[7] 정사각행렬에 대해서 위 두 식 중 하나가 참이면 나머지 하나도 참이다. 정사각행렬이 아닌 경우, 하나가 성립한다고 나머지 하나가 무조건 성립하지 않을 수 있으며, 이러한 경우는 유니터리 행렬이라고 하지 않는다.

$$UU^\dagger = \mathbb{I}$$
$$U^\dagger U = \mathbb{I} \tag{2.19}$$

여기서 $\mathbb{I}$는 단위행렬이다.

위 두 등식이 성립함은 아래가 성립함과 동치이다.

$$U^{-1} = U^\dagger \tag{2.20}$$

또, 위 정의는 다음과 동치이다.

임의의 벡터에 복소 정사각행렬 U를 곱하여도 유클리드 노름이 변하지 않을 때 U는 유니터리 행렬이다. 즉, $n \times n$ 복소 정사각행렬 U가 유니터리 행렬이라는 것은, 임의의 n 차원 복소수 열벡터 $|\psi\rangle$에 대해

$$\|U|\psi\rangle\| = \||\psi\rangle\| \tag{2.21}$$

가 항상 성립함을 의미한다. 양자 상태벡터의 집합은 유클리드 노름이 1인 벡터들의 집합과 동일하기 때문에, 유니터리 행렬을 양자 상태벡터에 곱하면 또 다른 양자 상태벡터가 된다.

유니터리 행렬(unitary matrices)은 항상 양자 상태벡터를 다른 양자 상태벡터로 변환하는 선형 사상의 집합과 정확히 일치한다. 여기서 고전 확률론과의 유사성을 주목할 수 있다. 고전적인 경우, 확률벡터를 항상 다른 확률벡터로 변환하는 연산은 확률 행렬과 대응된다. 즉, 양자역학에서는 유니터리 행렬이 상태 보존을 보장하며, 고전 확률론에서는 확률 행렬이 확률 보존을 보장한다.

II.6. 유니터리 연산

유니터리 행렬은 양자 상태벡터의 노름을 보존하므로, 양자 컴퓨터에서 큐비트에 가하는 모든 연산은 유니터리 연산이어야 한다. 다음은 1 큐비트에 대한 대표적인 유니터리 연산의 예시이다. 이 행렬들은 연산자처럼 행동하며, 선형 변환이나 로렌츠 변환을 적용하듯이 상태벡터에 작용하게 된다.

파울리 연산

아래 네 개를 파울리 행렬이라고 한다.

$$
\begin{aligned}
\mathbb{I} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
\sigma_x \equiv X &\triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
\sigma_y \equiv Y &\triangleq \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\
\sigma_z \equiv Z &\triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}
\end{aligned}
\tag{2.22}
$$

단, X, Y, Z는 다른 용도로도 많이 쓰인다는 것에 주의하자.

X 연산은 비트에 대해 아래 결과를 내놓기 때문에 NOT 연산자 또는 비트 플립(bit flip)이라고 하기도 한다.

$$
\begin{aligned}
X|0\rangle &= |1\rangle \\
X|1\rangle &= |0\rangle
\end{aligned}
\tag{2.23}
$$

Z 연산은 phase flip(위상 플립?)이라고 하며, 아래와 같은 결과를 내놓는다.

$$
\begin{aligned}
Z|0\rangle &= |0\rangle \\
Z|1\rangle &= -|1\rangle
\end{aligned}
\tag{2.24}
$$

Y 연산은 복소수 위상까지 포함된 회전 연산이다.

아다마르 연산

$$
H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}
\tag{2.25}
$$

비트 $|0\rangle, |1\rangle$을 균등한 중첩상태로 바꾸는 연산으로, 결과는 아래와 같다.

$$
\begin{aligned}
H|0\rangle = |+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
H|1\rangle = |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}
\tag{2.26}
$$

큐비트 상태 벡터에 대해 아래 네 개의 아다마르 연산 결과는 기억해 두자.

$$
\begin{aligned}
H|0\rangle = |+\rangle \quad H|1\rangle = |-\rangle \\
H|+\rangle = |0\rangle \quad H|-\rangle = |1\rangle
\end{aligned}
\tag{2.27}
$$

위상 연산

노름, 즉 확률 분포[8]는 유지하면서 상태 벡터의 복소수 위상만 변화시키는 선형 연산을 위상 연산이라고 한다. 위상이란 복소평면 상의 편각(argument)와 같은 말이다[9].

예를 들어,

$$|\psi'\rangle = e^{i\varphi}|\psi\rangle \tag{2.28}$$

는 원래 상태 $|\psi\rangle$와 측정 확률은 완전히 같지만, 위상이 φ만큼 변한 상태이다.

같은 말을 수식으로 되풀이해보자면, 위상 연산은 상태 벡터에 다음과 같이 작용한다.

$$|\psi\rangle \mapsto e^{i\theta}|\psi\rangle \tag{2.29}$$

일반적인 위상 회전 변환 연산 행렬은 다음과 같이 주어진다.

$$P_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \tag{2.30}$$

그 중 특수한 경우는 간단한 과정이지만 매번 계산하지 말고 따로 기억해 두자.

$$\begin{aligned} S = P_{\frac{\pi}{2}} &= \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \\ T = P_{\frac{\pi}{4}} &= \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} \end{aligned} \tag{2.31}$$

앞서 본 파울리 행렬도 위상 변환의 대표적인 예 중 하나이다.

위상 변환의 필요성과 위상의 물리적 의미를 이해하려면 간단한 예를 들어보자. $|+\rangle$와 $|-\rangle$는 측정 시 동일한 확률인 $\frac{1}{2}$를 가져 구분이 불가능하다. 하지만 아다마르 연산을 적용 후 측정하면 각각 $|0\rangle$과 $|1\rangle$을 출력해 구별이 가능해진다.

따라서, 위상 변화는 물리적으로 의미가 있는 변화이며, 양자 상태 간 구별에 중요한 역할을 한다고 할 수 있다.

II.7. 유니터리 연산의 합성

행렬곱은 벡터기하학적으로 선형변환의 합성의 의미를 가진다. 즉, 유니터리 연산을 합성하려면 행렬곱을 취한다.

---

[8] 양자 상태벡터는 고전 확률벡터와 다르다고 했지만, 상태벡터를 단위벡터로 정함으로써 확률 해석을 할 수 있게 된다.

[9] 임의의 복소수 $z = re^{i\theta} = r(\cos\theta + i\sin\theta)$에서 $\theta = \arg z$가 바로 위상이다.

예를 들어, 아다마르 연산 후 S 연산을 적용하고 다시 아다마르 연산을 적용한다고 하자. R이라고 명명할 이 연산은 아래와 같다.

$$\begin{aligned} R &\triangleq HSH \\ &= \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \end{bmatrix} \\ &= \begin{bmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{bmatrix} \end{aligned} \tag{2.32}$$

R은 흥미로운 경우로, 파울리 X 연산의 제곱근이다.

$$R^2 = \begin{bmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{bmatrix}^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.33}$$

이렇게, NOT 연산을 두 번의 다른 연산으로 하는 것은 고전적인 단일 비트에서는 불가능하다.

III. 다중 계에서의 정보 처리

III.1. 데카르트 곱과 상태 집합

X, Y는 각각 고전 상태 집합 Σ, Γ를 갖는 계라고 하자. 이 두 계가 합쳐져 또 다른 하나의 계를 이룬다고 할 때, (X, Y) 또는 XY로 나타낼 수 있다. 이때, 궁금한 것은 (X, Y)의 고전 상태 집합은 무엇인가에 대한 것이다.

답은 꽤 당연하게 느껴지는데, Σ와 Γ의 데카르트 곱이다.

> **Definition 3.1.1 (데카르트 곱)**
>
> 두 집합 A, B의 데카르트 곱은 아래와 같다.
>
> $$A \times B = \{(a, b) \mid a \in A, b \in B\} \tag{3.1}$$

두 개 이상의 계 $X_1, \ldots, X_n$과 그 상태 집합 $\Sigma_1, \ldots, \Sigma_n$에 대해서도 이 계들을 단일 계 $(X_1, \ldots, X_n)$으로 보았을 때 그 계의 상태 집합은 아래와 같이 된다.

$$\Sigma_1 \times \ldots \times \Sigma_n = \{(a_1, \ldots, a_n) \mid a_1 \in \Sigma_1, \ldots, a_n \in \Sigma_n\} \tag{3.2}$$

이렇게 계가 많아질 때, 그 계의 상태를 순서쌍 $(a_1, \ldots, a_n)$ 대신 간단히 문자열 $a_1 \ldots a_n$으로 나타낼 수 있다.

예를 들어, $\mathsf{X}_0, \ldots, \mathsf{X}_9$가 모두 비트이며, 이들의 고전 상태 집합은 모두 같다고 하자.

$$\Sigma_0 = \ldots = \Sigma_9 = \{0, 1\} \tag{3.3}$$

그렇다면 이 비트들을 묶은 단일 계 $(\mathsf{X}_0, \ldots, \mathsf{X}_n)$은 총 $2^{10} = 1024$ 개의 가능한 상태를 가지며, 이 상태들은 아래 집합의 부분집합이다.

$$\Sigma_0 \times \ldots \times \Sigma_9 = \{0, 1\}^{10} \tag{3.4}$$

문자열로 나타냈을 때 상태들의 사전식 배열은 다음과 같다.

$$\begin{array}{c} 0000000000 \\ 0000000001 \\ 0000000010 \\ 0000000011 \\ 0000000100 \\ \vdots \\ 1111111111 \end{array} \tag{3.5}$$

III.2. 두 계의 독립

확률과 통계에서 배운 우리가 알고 있는 독립의 정의는 다음과 같다.

Definition 3.2.1 (사건의 독립)

두 사건 A, B에 대하여 다음이 성립하면 두 사건은 서로 독립이다.

$$P(A \cap B) = P(A)P(B) \tag{3.6}$$

이와 같은 맥락으로,

Definition 3.2.2 (계의 독립)

상태 집합 Σ, Γ를 갖는 두 계 X, Y가 서로 독립이려면 아래가 성립해야 한다.

$$P((\mathsf{X}, \mathsf{Y}) = (a, b)) = P(\mathsf{X} = a)P(\mathsf{Y} = b) \qquad \forall a \in \Sigma, b \in \Gamma \tag{3.7}$$

이걸 디랙 표기법을 통해 확률벡터로 나타내어 보자. 확률 상태 (X, Y)에 대해

$$\begin{aligned} &\sum_{(a,b)\in\Sigma\times\Gamma} p_{ab}|ab\rangle \\ |\varphi\rangle &= \sum_{a\in\Sigma} q_a|a\rangle \\ |\psi\rangle &= \sum_{b\in\Gamma} r_b|b\rangle \end{aligned} \tag{3.8}$$

라고 할 때, 계가 독립이려면 모든 $a \in \Sigma, b \in \Gamma$에 대해

$$p_{ab} = q_a r_b \tag{3.9}$$

가 성립해야 한다.

III.3. 벡터의 텐서곱

독립의 조건은 간단히 텐서곱으로 나타낼 수 있다. 텐서곱은 일반적인 표기로, 여러 가지 자료구조에 추상적인 방법으로 적용될 수 있지만, 우리는 벡터에 대한 텐서곱의 명확한 정의를 살펴보자.

Definition 3.3.1 (벡터의 텐서곱)

두 벡터

$$\begin{aligned} |\varphi\rangle &= \sum_{a\in\Sigma} \alpha_a |a\rangle \\ |\psi\rangle &= \sum_{b\in\Gamma} \beta_b |b\rangle \end{aligned} \tag{3.10}$$

에 대하여 두 벡터의 텐서곱은 아래와 같다.

$$|\varphi\rangle \otimes |\psi\rangle = \sum_{(a,b)\in\Sigma\times\Gamma} \alpha_a \mathrm{B}_b |ab\rangle \tag{3.11}$$

이 새로운 벡터의 원소들은 $\Sigma \times \Gamma$의 원소들에 대응된다. 또, 이 정의는 $|\pi\rangle \coloneqq |\varphi\rangle \otimes |\psi\rangle$에 대해 아래와 동치이다.

$$\langle ab|\pi\rangle = \langle a|\varphi\rangle\langle b|\psi\rangle \qquad \forall a \in \Sigma, b \in \Gamma \tag{3.12}$$

좀 더 직관적인 이해를 위해 열벡터를 전개하여 텐서곱을 살펴보면

$$\begin{aligned} |\varphi\rangle &= \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_{|\Sigma|} \end{pmatrix} \\ |\psi\rangle &= \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \vdots \\ \beta_{|\Gamma|} \end{pmatrix} \end{aligned} \tag{3.13}$$

$$|\varphi\rangle \otimes |\psi\rangle = \begin{pmatrix} \alpha_1\beta_1 \\ \vdots \\ \alpha_1\beta_{|\Gamma|} \\ \alpha_2\beta_1 \\ \vdots \\ \alpha_2\beta_{|\Gamma|} \\ \vdots \\ \alpha_{|\Sigma|}\beta_1 \\ \vdots \\ \alpha_{|\Sigma|}\beta_{|\Gamma|} \end{pmatrix} \tag{3.14}$$

이제 텐서곱으로 계의 독립 조건을 다시 나타낼 수 있다.

Theorem 3.3.2 (텐서곱을 이용한 계의 독립 조건)

상태 집합 Σ, Γ를 갖는 두 계 X, Y가 각각 확률벡터 $|\varphi\rangle \in \mathbb{R}^{|\Sigma|}, |\psi\rangle \in \mathbb{R}^{|\Gamma|}$로 주어질 때, 두 계가 서로 독립이려면 아래가 성립해야 한다.

$$|\pi\rangle = |\varphi\rangle \otimes |\psi\rangle \qquad \text{where } |\pi\rangle \in \mathbb{R}^{|\Sigma|\times|\Gamma|} \tag{3.15}$$

텐서곱은 이러한 정보 처리에서 자주 쓰이고 중요하기 때문에, 아래와 같은 표기로 기호가 생략 및 간략화되기도 한다.

$$|\varphi\rangle \times |\psi\rangle \equiv |\varphi\rangle|\psi\rangle \equiv |\varphi \otimes \psi\rangle \equiv |\varphi\psi\rangle \equiv |(\varphi, \psi)\rangle \equiv |\varphi, \psi\rangle \tag{3.16}$$

또, 텐서곱 연산에서는 분배 법칙과 스칼라에 한해 결합법칙이 성립한다.

$$(|\varphi_1\rangle + |\varphi_2\rangle) \otimes |\psi\rangle = |\varphi_1\rangle \otimes |\psi\rangle + |\varphi_2\rangle \otimes |\psi\rangle \tag{3.17}$$

$$\begin{aligned} &(\alpha|\varphi\rangle) \otimes |\varphi\rangle = |\varphi\rangle \otimes (\alpha|\psi\rangle) = \alpha(|\varphi\rangle \otimes |\psi\rangle) \\ &\equiv \alpha|\varphi\rangle|\psi\rangle \end{aligned} \tag{3.18}$$

III.4. 확률 상태의 측정

여러 계로 구성된 확률 상태의 측정에 대해 알아보자. 다중 계를 하나의 전체적인 계로 간주한다면, 모든 계를 측정하는 경우 측정이 어떻게 일어나야 하는지에 대한 정의를 자연스럽게 얻을 수 있다.

예를 들어, 두 비트 (X, Y)의 상태가 아래와 같이 주어진다고 하자.

$$\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle \tag{3.19}$$

이 경우, 측정 결과가 00, 즉 X를 측정했을 때 0이고 Y를 측정했을 때도 0일 확률은 1/2 이고, 11일 확률도 1/2이다. 측정 결과가 00이면 상태는 $|00\rangle$으로, 11이면 $|11\rangle$로 바뀐다.

그러나 모든 계를 측정하는 것이 아니라, 일부 계만 측정할 수도 있다. 이 경우에는, 측정된 계에 대해서는 측정 결과를 얻고, 측정하지 않은 계에 대해 우리가 갖고 있는 정보도 변하게 된다. 이것을 설명하기 위해 두 계 중 하나만 측정하는 간단한 경우에 집중하자. 세 개 이상의 계 중 일부만 측정하는 보다 일반적인 상황은, 측정된 계들을 하나의 시스템으로 묶고 측정되지 않은 계들도 하나의 시스템으로 묶으면 결국 두 계로 이루어진 경우로 환원할 수 있기 때문이다.

계 X, Y의 상태 집합을 다시 각각 Σ, Γ라고 두고, 두 계는 어떤 상태를 공유하고 있다고 하자. 이제 이 중 X만 측정하고 Y는 측정하지 않았을 때 무슨 일이 생기는지 알아보자.

X만 측정할 경우 특정 상태 $a \in \Sigma$가 나올 확률은

$$P(\mathsf{X} = a) = \sum_{b \in \Gamma} P((\mathsf{X}, \mathsf{Y}) = (a, b)) \tag{3.20}$$

이는 주변 확률분포(marginal distribution)이라고 하며, 전체 상태로부터 일부 변수만 남긴 분포이다. 만약 이 식이 성립하지 않는다면, 즉 Y의 측정 여부가 X의 확률에 영향을 준다면, 이는 초광속 정보 전달을 허용하게 되는 것이므로 물리학적으로 허용되지 않는다. 즉, 다른 사람이 어디에 있든 측정을 했다는 사실만으로는 측정되지 않은 X의 상태에 아무런 영향을 주지 않아야 한다.

X만 측정된다는 가정 하에서, 여전히 Y의 상태에 대한 불확실성이 존재한다. 그러므로 (X, Y)의 상태를 임의로 특정 상태 $|ab\rangle$로 선언하는 것이 아니라, Y에 대한 불확실성을 반영하는 방법이 필요하다. 이것은 조건부 확률로 표현한다.

$$P(\mathsf{Y} = b \mid \mathsf{X} = a) = \frac{P((\mathsf{X}, \mathsf{Y}) = (a, b))}{P(\mathsf{X} = a)} \qquad \text{s.t. } P(\mathsf{X} = a) \neq 0 \tag{3.21}$$

$P(\mathsf{X} = a) = 0$인 상황은, $\mathsf{X} = a$ 상태가 관측되지 않는 것이 아니라면 발생하지 않기 때문에, 걱정하지 않아도 된다.

이것을 확률벡터로 표현하기 위해, (X, Y)의 확률 상태를 기술하는 벡터 $|\psi\rangle$를 생각하자.

$$|\psi\rangle = \sum_{(a,b) \in \Sigma \times \Gamma} p_{ab} |ab\rangle \tag{3.22}$$

오직 X를 관측해 $\mathsf{X} = a$가 될 확률은

$$P(\mathsf{X} = a) = \sum_{c \in \Gamma} p_{ac} \tag{3.23}$$

이에 따라 X의 상태벡터는

$$\sum_{a\in\Sigma}\left(\sum_{c\in\Gamma} p_{ac}\right)|a\rangle \tag{3.24}$$

측정 결과로 $a \in \Sigma$가 나왔다고 한다면, Y의 상태는 조건부 확률을 통해 반영된다. 이때 Y의 상태벡터는

$$|\pi_a\rangle = \frac{\sum_{b\in\Gamma} p_{ab}|b\rangle}{\sum_{c\in\Gamma} p_{ac}} \tag{3.25}$$

이제 $\mathsf{X} = a$인 사건에 대해 계 (X, Y)에서 해당 확률은 $|a\rangle \otimes |\pi_a\rangle$가 된다.

$|\pi_a\rangle$가 저렇게 나오는 이유 중 하나로 이해해두면 좋은 것은 벡터의 정규화이다.

$$|\pi_a\rangle = \frac{1}{\sum_{c\in\Gamma} p_{ac}} \sum_{b\in\Gamma} p_{ab}|b\rangle \tag{3.26}$$

식을 이렇게 보면, 이 식은 $|b\rangle$에 대한 상태벡터 $\sum_{b\in\Gamma} p_{ab}|b\rangle$를 벡터 원소의 전체 합 $\sum_{c\in\Gamma} p_{ac}$로 나누어 정규화시킨 것이다.

잘 이해가 되지 않으니 구체적인 예를 들어보자. $\Sigma = \{0, 1\}$, $\Gamma = \{1, 2, 3\}$이라고 하고, 상태벡터는 다음과 같이 주어졌다고 하자.

$$|\psi\rangle = \frac{1}{2}|0,1\rangle + \frac{1}{12}|0,3\rangle + \frac{1}{12}|1,1\rangle + \frac{1}{6}|1,2\rangle + \frac{1}{6}|1,3\rangle \tag{3.27}$$

텐서곱의 성질을 이용해 벡터를 X를 기준으로 인수분해하듯 분리해서 정리하자.

$$|\psi\rangle = |0\rangle \otimes \left(\frac{1}{2}|1\rangle + \frac{1}{12}|3\rangle\right) + |1\rangle \otimes \left(\frac{1}{12}|1\rangle + \frac{1}{6}|2\rangle + \frac{1}{6}|3\rangle\right) \tag{3.28}$$

그러므로 확률은

$$\begin{aligned} P(\mathsf{X}=0) &= \frac{1}{2} + \frac{1}{12} = \frac{7}{12} \\ P(\mathsf{X}=1) &= \frac{1}{12} + \frac{1}{6} + \frac{1}{6} = \frac{5}{12} \end{aligned} \tag{3.29}$$

확률 총합이 1이므로 정상적인 분포임을 검산할 수 있다.

이제 Y의 조건부 확률벡터를 구하자. 먼저 $\mathsf{X} = 0$일 때부터 하면

$$|\pi_0\rangle = \frac{1}{\frac{7}{12}}\left(\frac{1}{2}|1\rangle + \frac{1}{12}|3\rangle\right) = \frac{6}{7}|1\rangle + \frac{1}{7}|3\rangle \tag{3.30}$$

$\mathsf{X} = 1$일 때도 똑같이

$$|\pi_1\rangle = \frac{\frac{1}{5}}{12}\left(\frac{1}{12}|1\rangle + \frac{1}{6}|2\rangle + \frac{1}{6}|3\rangle\right) = \frac{1}{5}|1\rangle + \frac{2}{5}|2\rangle + \frac{2}{5}|3\rangle \tag{3.31}$$

IV. 마무리

이렇게 양자 컴퓨팅의 방대한 세계 중에서도 가장 기본적인 내용인 고전 정보와 양자 정보의 기초적 처리 방법에 대한 이론을 알아 보았다. 입문을 위한 흥미를 돋구는 차원에서는 괜찮았지만, 실질적인 실현 방법이나, 게이트 연산과 정보 저장 방식 등 유틸리티 규모의 양자 컴퓨팅까지 가기에는 길이 멀다. 확실히 재미있는 주제는 맞는 것 같다.

IV.1. 추후 탐구 계획

아래의 커리큘럼을 통해 양자컴퓨팅 개론 공부를 완성시킬 계획이다. 대부분 수학과 물리 내용이지만, 이산수학과 암호화 알고리즘, 기본적인 자료구조에 대한 이해, 기존 컴퓨터의 대략적인 작동 개론 등 컴퓨터과학 지식도 필요한 편이다.

- 양자상태
- 관측가능성
- 유니터리 연산자
- 양자얽힘
- 양자암호학
- 밀도 연산자
- 슈미트 디컴퍼지션
- 순간이동
- No Cloning 정리
- 고전 정보 처리
- 고전 정보의 양자역학적 구현
- 그로버 양자 탐색 알고리즘
- 나머지와 군집론
- 공동키 암호학
- DFT, FFT, 양자 FFT
- 가역 양자컴퓨팅
- 애니온, 위상양자컴퓨팅

감사합니다.