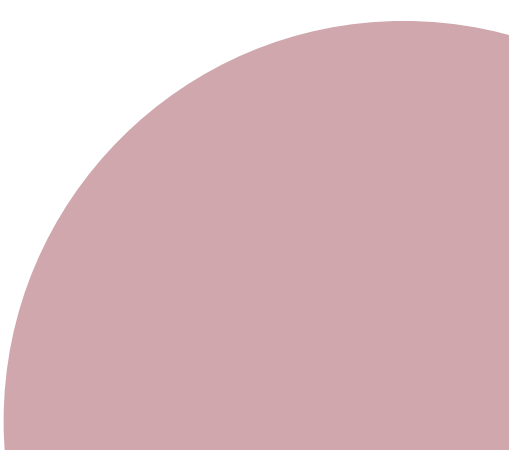


Introduction to Quantum Computing

양자컴퓨팅 기초

2025-10-01

황태준
중앙고등학교
2025
2학년 7반 31번



목차

I. 오리엔테이션	3
II. 양자 상태	10
III. 관측가능량	23
IV. 유니터리 연산자	40
V. 양자 얽힘	48
VI. 양자 암호학	54

I. 오리엔테이션

I.1. 시작하기 전에

표기법 알림

z 의 켈레복소수는 보통 수학에서 \bar{z} , 물리학에서 z^* 처럼 하는 것이 관례이다. 하지만 복잡한 식에 켈레를 씌울 때는 \bar{z} 가 가독성이 좋다고 판단되어 여기서는 켈레를 \bar{z} 로 나타낸다.

벡터는 \mathbf{v} 와 같이 굵은 이탤릭(italic)으로 쓴다. \mathbf{v} 와 같은 굵은 인쇄체(upright roman)보다 가독성이 좋을 것으로 판단되기 때문이다. ISO(국제표준화기구)에서도 벡터는 굵은 이탤릭 \mathbf{v} 또는 이탤릭 화살표 액센트 \vec{v} 로 쓸 것을 권장하고 있다. 다만 \vec{v} 꼴은 가독성이 떨어지며 유클리드 공간 상의 벡터로 그 의미가 한정되기 때문에 현재 고등교육 이상에서는 특별한 경우가 아니면 잘 쓰이지 않는다.

연산자는 \hat{A} 처럼 모두 \wedge 액센트를 붙이는 것이 관례이나, 혼동이 없는 범위에서는 가독성을 위해 붙이지 않았다.

참고문헌 알림

이 문서는 캐나다 Carleton 대학의 수학 교수 Yuly Billig의 온라인 강의 『Quantum Computing』을 강하게 참고하였다. 이외에도 David J. Griffiths 외의 『Introduction to Quantum Mechanics』 3판, R. Shankar의 『Principle of Quantum Mechanics』도 참고했다.

I.2. 무어의 법칙

캘리포니아 공과대학(CalTech) 화학 박사이자 인텔의 공동창립자인 고든 무어(Gordon Moore, 1929 ~ 2023) 교수는 관찰을 통해 일정 시간동안 컴퓨터 반도체에 집적되는 트랜지스터 수가 2배 이상 증가한다는 “무어의 법칙(Moore’s Law)”을 제시했다. 그가 처음 법칙을 제안했을 때 그 “일정 시간”은 1년 정도였다.

The complexity for minimum component costs has increased at a rate of roughly a factor of two per year. Certainly over the short term this rate can be expected to continue, if not to increase. Over the longer term, the rate of increase is a bit more

uncertain, although there is no reason to believe it will not remain nearly constant for at least 10 years.¹

— Gordon Moore, 1965, “Electronics” 紙

10년 뒤인 1975년, 무어는 법칙을 2년 마다 두 배로 증가한다고 수정했다. 열역학 제 2법칙의 등 여러 한계 때문에 증가 속도는 앞으로 줄어들 예정이다. 오늘날 트랜지스터는 대략 50개의 원자 내외의 두께로 되어 있는데, 이대로 간다면 우리는 곧 원자 크기의 한계에 직면할 것이고, 그때 작용하는 물리 법칙은 이전과 달라지게 된다.

한 개의 원자는 한 뭉탱이의 원자와 전혀 다르게 행동하는데(적어도 그렇게 보이는데), 원자 뭉탱이는 고전역학의 지배를 받는 반면 원자 한 개는 양자역학의 지배를 받는다. 원자가 뭉탱이로 있을 때는, 큰수의 법칙에 따라 양자역학에 의한 확률적 현상들이 평균으로 수렴하여 무시해도 될 정도가 된다. 이 말은, 계속해서 트랜지스터 개수를 늘리기 위해 칩의 크기를 줄인다면(즉 집적도를 늘린다면) 곧 디지털 컴퓨터를 설계할 때도 양자 터널링² 등의 양자역학적 효과를 고려해야한다는 뜻이다.

I.3. 배경과 역사

양자역학은 이상하고, 인간적 직관에 부합하지 않는다. 우리는 현대 인간 이전까지 양자역학적 효과를 실감하지 못했다. 즉, 인간은 양자역학이 아닌 고전역학적 사고로 진화했으며, 우리의 뇌는 양자역학을 이해하기에 적합하지 않다.

비록 양자역학의 수학적, 물리적 기반은 이제 잘 다져져 있음에도 불구하고, 양자역학에는 여전히 우리가 해결할 수 없는 문제들이 있다. 처음으로 발견된 양자역학적 현상은 다양한 물질이 방출하는 고유한 선 스펙트럼이었다. 이것을 통해 별의 구성 원소를 알아내기도 한다. 수소 원자의 경우에는 슈뢰딩거 방정식에 따른 꽤 정확한 이론이 있어서, 에너지 준위와 선 스펙트럼의 파장을 계산할 수 있다. 연구가 계속되며, 꽤 작은 원자의 경우라도 스펙트럼의 에너지 준위를 계산해 내려면 막대한 자원이 필요하다는 것을 깨달았다. 슈퍼 컴퓨터가 등장하고도 다중 양자계에서의 에너지 준위 계산은 엄청나게 오랜 시간이 소요된다. 그런데, 자연은 이 막대한 계산을 아무 오류 없이 완벽히 해낼 수 있다.

¹최소 구성 요소 비용에 대한 복잡성은 연간 약 두 배 비율로 증가했습니다. 단기적으로 이 경향은 비용이 증가하지 않더라도 확실히 계속될 것으로 예상할 수 있습니다. 장기적으로 보면 증가율이 다소 불확실하지만 적어도 10년 동안 거의 일정할 것이라고 못 할 이유는 없습니다.

²나중에 자세히 알아볼 것이므로 앞뒤 다 자르고 간단히 설명하자면, 트랜지스터 크기가 ~1 nm 정도로 작아지게 되면, 양자역학적 효과로 인해 전자가 트랜지스터 내부의 절연막을 개무시하고 통과해버릴 수 있다. 즉, 정보 저장 및 계산의 정확성이 보장되지 않는다.

1980년, 유리 마닌(Юрий Манин, 1937 ~ 2023)은 양자역학적 현상과 씨름하는 것 대신, 양자계를 계산 기계로 사용하는 것이 어떻냐고 그의 저서 “Computable and Uncomputable”에서 제안했다. 그는 현재의 양자 컴퓨팅 패러다임을 연 것이다. 비슷한 시기, 폴 베니오프(Paul Benioff, 1930 ~ 2022)는 튜링 머신의 양자역학적 모델을 제안했다.

1982년, 리처드 파인만(Richard Feynmann, 1918 ~ 1988)은 비슷한 이유로, 지금의 계산기가 고전적이기 때문에 양자역학 문제를 쉽게 풀 수 없다고 하며, 계산기를 양자역학적으로 구동하게 만든다면 이런 문제들을 더 쉽고 빠르게 풀 수 있을 것이라고 했다.

1980년대, 90년대부터 양자컴퓨팅은 컴퓨터과학의 한 분야로 간주되어, 소수의 사람들이 이 분야에서 활동했다. 데이비드 도이치(David Deutsch, 1953 ~)는 양자 튜링 머신과 도이치-요샤 알고리즘(Deutsch-Josza algorithm)을 개발하였다. 1994년 피터 쇼어(Peter Shor, 1959 ~)는 RSA 암호화 알고리즘을 무력화하는 양자컴퓨팅 알고리즘을 고안했다. RSA 알고리즘은 현재까지 사용되고 있는 정보 암호화 알고리즘으로, 지금의 슈퍼컴퓨터로도 뚫는 데 너무 오랜 시간이 걸려 사실상 뚫는게 불가능한 알고리즘이다. 이런 이유로 각국 정보기관들은 세계 여러 나라의 각종 데이터를 암호화된 상태로 마구 저장해두고 있다. 신뢰성 있는 양자컴퓨터가 나오게 된다면 이 데이터들의 암호를 풀어 중요한 비밀 정보를 열람할 수 있을지도 모르기 때문이다.

양자컴퓨팅은 여러 분야에 걸쳐 있는 학문이다.

1. 물리학
2. 수학
3. 컴퓨터과학

물론 본 책에서 다루는 내용에 필요한 모든 학문적 기반을 제공할 것이지만, 이 세 분야에 대한 배경 지식은 이해에 큰 도움이 된다.

이제 이 책에서 다룰 전체 내용을 간략하게 미리보기하도록 하겠다.

I.4. 큐비트

큐비트(qubit)는 quantum bit를 줄인 말로, 디지털 컴퓨터에서 정보의 기본 단위가 비트이듯, 양자컴퓨터에서 정보의 기본 단위이다. 그런데, 큐비트는 일반적인 비트와 무슨 차이가 있을까?

어떤 한 전자의 스핀을 생각해 보자. 전자는 전자기장을 만들며, 스핀은 그 중 자기장을 기술하는 물리량이다. 즉, 전자는 하나의 작은 자석처럼 행동한다.

전자는 페르미온으로, $+\frac{1}{2}$ 또는 $-\frac{1}{2}$ 의 스핀을 갖는다. 이때 양수 스핀을 \uparrow , 음수 스핀을 \downarrow 로 표시한다. 물리학의 디랙표기법을 빌려 양수 스핀을 가진 전자의 상태는 $|\uparrow\rangle$ 로 쓰자. 또, 음수 스핀을 가진 전자의 상태는 $|\downarrow\rangle$ 라고 하자. 이 두 상태를 기저(basis) 상태라고 하겠다. 이제 이것을 비트로 해석하기 위해 아래와 같이 정의하자.

$$\begin{aligned} |\uparrow\rangle &=: |1\rangle \\ |\downarrow\rangle &=: |0\rangle \end{aligned} \tag{1.1}$$

그런데, 이 전자는 꼭 위 두 상태 중 하나에 있어야 하는 것이 아니다. 양자역학에 의하면, 전자의 스핀의 일반적인 상태는 양수 스핀과 음수 스핀의 선형 결합으로 표현될 수 있다.

$$\begin{aligned} |\psi\rangle &= \alpha|\downarrow\rangle + \beta|\uparrow\rangle \\ \text{where } \alpha, \beta &\in \mathbb{C} \wedge |\alpha|^2 + |\beta|^2 = 1 \end{aligned} \tag{1.2}$$

이제 우리는 여기서부터 큐비트의 발상을 가져올 수 있다. 두 벡터 $|0\rangle$ 과 $|1\rangle$ 을 기저로 갖는 복소평면 \mathbb{C}^2 를 생각하자. 이제 큐비트 $|\psi\rangle$ 는 이 평면 위에서 크기(정확히는 노름)가 1인 벡터이다³.

이처럼 큐비트는 하나의 값이 아니라, 두 값의 선형 결합을 저장하게 된다. 즉, 고전적인 컴퓨터는 고전적이고 확정적인 원리로 작동하여 비트 하나는 0 또는 1의 값을 갖지만, 큐비트는 양자역학적이고 불확정적인 원리로 작동하여 큐비트 하나는 0과 1을 가중치를 두고 둘 다 갖게 된다. 가중치(α, β 의 계수)를 갖는다는 것은, 어떤 큐비트는 0보다 1에 가까울 수 있고, 어떤 것은 그 반대일 수 있다는 것이며, 그 가까운 정도도 모든 큐비트가 다를 수 있다는 것이다.

이제 입자와의 상호작용이 발생하면 무슨 일이 일어나는지 보자. 하나의 전자가 아니라, 서로 상호작용하는 전자의 쌍이 있다고 하자. 두 전자의 통합된 스핀 상태를 생각하자. 이때 기저상태는 다음과 같이 존재할 수 있다.

$$|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle \tag{1.3}$$

일반적인 상태는 이 기저상태들의 중첩(superposition)이 된다.

³복소수 $a + bi$ 에 대하여 그 절댓값이 $\sqrt{a^2 + b^2}$ 인 이유도 노름에 관련되어 있다.

$$\begin{aligned}
 |\psi\rangle &= \alpha_1|\uparrow\uparrow\rangle + \alpha_2|\uparrow\downarrow\rangle + \alpha_3|\downarrow\uparrow\rangle + \alpha_4|\downarrow\downarrow\rangle \\
 \Leftrightarrow |\psi\rangle &= \alpha_1|11\rangle + \alpha_2|10\rangle + \alpha_3|01\rangle + \alpha_4|00\rangle \\
 \text{where } \alpha_i &\in \mathbb{C} \wedge \sum_i |\alpha_i|^2 = 1
 \end{aligned} \tag{1.4}$$

이것을 2-큐비트라고 한다. 여기서 볼 수 있듯, 2-큐비트는 두 개의 고전적인 비트에서 가능한 모든 고전적 상태를 선형 결합으로 갖는다. 이제, 2-큐비트에서 n -큐비트로 어떻게 갈지 알 수 있다. 고전적 비트 상태 n 개를 저장하는 n -큐비트는 아래와 같이 문자열로 표현할 수 있다.

$$\overbrace{|0100\dots1\rangle}^{n \text{ 비트}} \tag{1.5}$$

이 표현이 번거로우므로 우리는 켓 안에 들어가는 이진수의 십진수 형태를 취하여 간단하게 표현하기로 한다.

$$|k\rangle \tag{1.6}$$

예를 들어 $n = 4$ 이고 $k = 9$ 라면 이 상태는 무엇일까?

$$\begin{aligned}
 k = 9 &= 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\
 &= 1001_{(2)}
 \end{aligned} \tag{1.7}$$

이므로 해당 상태는

$$|9\rangle = |1001\rangle = |\uparrow\downarrow\downarrow\uparrow\rangle \tag{1.8}$$

이 된다.

따라서 n -큐비트는 일반적으로 아래와 같이 나타낼 수 있다.

$$\begin{aligned}
 |\psi\rangle &= \sum_{k=0}^{2^n-1} \alpha_k |k\rangle \\
 \text{where } \alpha_k &\in \mathbb{C} \wedge \sum_{k=0}^{2^n-1} |\alpha_k|^2 = 1
 \end{aligned} \tag{1.9}$$

이때 $|\psi\rangle$ 는 \mathbb{C}^{2^n} 상의 벡터이다. 이것은 n -큐비트의 복잡도가 n 의 지수로 증가함을 보여준다. 즉, n 개의 상호작용하는 전자의 스핀을 기술하기 위해서는 2^n 개의 복소수를 저장해

야 한다. n 이 50만 되어도 그 값은 현재의 디지털 컴퓨터로는 범접할 수 없는 크기의 천문학적 숫자가 된다.

이는 원자와 분자에서 스펙트럼의 에너지 준위를 계산하는 문제가 왜 그리 어려운지를 보여주는 단적인 예시이다. 우리는 전자 50개를 가진 분자를 아주 당연하게 상상해 볼 수 있다. 그리고 우리는 그 다중 계의 상태를 기술하는 것이 현재 컴퓨터의 저장 및 계산 능력으로는 불가능에 가까운 수준이라는 것도 확인했다. 하지만 자연은 50개의 전자를 조종하고 에너지에 맞는 스펙트럼을 만들어내는 데 아무런 지장이 없다.

I.5. 큐비트의 측정

여기서 논점은, 만약 50개의 전자로도 이 정도의 메모리 용량을 만들어낼 수 있다면, 왜 우리는 고전적인 메모리 칩을 버리고 양자역학적 기술로 메모리 칩을 만들지 않냐는 것이다. 이 질문에 대한 답은, 양자계의 가장 큰 문제는 그것이 확률적이라는 것이다. 그에 따라 양자계에 저장된 정보를 불러오는 데 어려움이 생기게 된다.

고전적인 컴퓨터 메모리의 경우, 예를 들어 n -비트 정보를 특정 주소 범위에 저장해 두었다면, 당연하게도⁴ 우리는 나중에 메모리의 해당소에서 정확히 동일한 정보를 불러올 수 있게 된다.

하지만, 식 (1.9)와 같은 양자 상태에서는 그런 식으로 정보를 불러올 수가 없다. 즉, 계수 α_k 들을 불러올 수 없다는 말이다.

양자 상태의 정보를 읽는 유일한 방법은 바로 그 계에 대해 측정(measurement)을 수행하는 것이다. 고전적인 상태들의 중첩인 양자 상태의 측정의 결과는 단일 고전 상태가 된다. 즉, 측정은 확률적이다.

양자 상태 $|\psi\rangle$ 의 값에 대한 측정을 수행하면 $|\alpha_k|^2$ 의 확률로 고전 상태 값 중 하나인 k 를 얻는다. 식 (1.9)가 나타내는 것은 가중치가 적용된 합이다. 어떤 상태는 다른 상태보다 더 높은 확률로 나타날 수 있다. 이 값들은, 측정이라는 시행을 할 때마다 다르게 나타나고, 이것이 양자역학이 여태까지 컴퓨터공학에 사용되지 못했던 이유이다.

정리하자면, 큐비트 체계를 사용할 때의 장점은 엄청난 양의 정보를 저장할 수 있다는 것이고, 단점은 그 정보를 불러오는 것이 매우 어려우며 한 번에 큐비트가 담은 모든 정보를 읽을 수 없다는 것이다.

⁴메모리가 어떻게 작동하는지 생각이라도 해 보았다면 당연하지 않다는 것을 알 수 있지만, 우리가 매일매일 컴퓨터를 사용하며 느끼기에는 그렇다는 말이다.

I.6. 양자 알고리즘

알고리즘이란, 입력과 출력을 가지는 절차를 의미한다. 양자 알고리즘도 알고리즘의 한 종류이다.

입력 상태 $|m\rangle$ 을 가정하자. 이 입력 상태에, 예를 들어 물리적으로 계에 레이저를 쏘는 등의, 특정한 변환 연산을 적용하면, 결과는 $|\psi\rangle$ 는 어떤 중첩된 상태가 될 것이다. 이 상태를 얻었다면 이것에 대한 측정을 수행해 출력으로 단일 상태 $|s\rangle$ 를 얻는다. 양자 알고리즘은 이러한 일련의 과정을 효율적, 효과적으로 조작하여 궁극적으로는 측정의 결과가, 거의 항상이라고 볼 수 있는 충분히 높은 확률로 원하는 정보에 대한 값이 나오도록 하는 것에 목적을 둔다. 알고리즘의 개발 과정에서는 항상 믿음직스러운 고전적인 컴퓨터로 양자 알고리즘의 결과가 올바른지 검산해 볼 수 있다.

보다시피, 양자 알고리즘을 설계하는 것은 매우 어려운 일이다. 현재 알려진 것들 중 실제로 유용한 양자 알고리즘은 얼마 없으며, 양자컴퓨팅 이론을 발전시켜 유용하고 효과적인 양자 알고리즘을 더 많이 만들어서 자연이 제공하는 방대한 양의 메모리 용량을 자유롭게 사용할 수 있게 되는 것이 미래의 목표가 되겠다. 하지만, 양자 알고리즘을 설계하는 것 외에, 실제로 양자컴퓨터를 설계하여 만드는 것도 매우 어려운 일⁵이므로, 이러한 목표를 달성하기 위해서는 수많은 노력이 지속적으로 필요할 것이다.

여기서는 이론적인 부분과 함께, 물리적으로 양자컴퓨터를 실현하는 방법과, 그 앞에 닥친 어려움에 대해서도 이야기해 보겠다.

⁵주석을 작성하는 현재는 좀 더 높은 온도에서 작동하는 양자컴퓨터도 있으나, 여전히 대표적인 대기압들의 선두주자 양자컴퓨터들은 수 켈빈 단위의 초저온에서만 작동하지 못한다.

II. 양자 상태

이번 장에서는 양자역학의 수학적 기반에 대해 알아보도록 하겠다.

그런데, 들어가기 전에 당연히 이걸 읽고 있으면 아는 것이 좋겠지만 모르는 독자를 위해 아래 정의를 선언하고 들어가겠다.

Definition 2.1 (벡터의 유클리드 노름)

벡터의 크기는 노름(norm), 또는 엄밀한 용어로 유클리드 노름(Euclidean norm)⁶ 정의하며, 일반적으로 아래와 같은 벡터

$$\mathbf{v} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \quad (2.1)$$

에 대해 그 노름은

$$\|\mathbf{v}\| \equiv |\mathbf{v}| = \sqrt{\sum_{i=1}^n |a_i|^2} \quad (2.2)$$

기호는 절댓값 기호 $|\cdot|$ 를 사용하거나, 단순한 절댓값이 아닌 노름이라는 것을 보이기 위해 작대기 두 개로 감싼 노름 기호 $\|\cdot\|$ 를 사용하기도 한다.



II.1. 양자역학의 공리

양자역학에서 코펜하겐 해석을 중심으로, 실험적으로 확립된 네 가지 정도의 공리(axiom, postulate)⁷를 양자역학의 공리라고 한다. 그 중 보통 첫번째에 해당하는 상태 공간에 대한 공리를 먼저 보도록 하자.

⁶유클리드 공간 상에서 벡터의 종점이 원점과 떨어진 거리를 의미한다. 벡터는 당연하게도 유클리드 공간 상에 있지 않을 수도 있는데, 이 때는 그 노름을 유클리드 노름이라고 하지 않으며 구하는 방법도 좌표계에 따라 다르다.

⁷axiom은 공리로, 증명이 필요 없이 사실로 받아들이기로 한 명제이다. postulate는 가정에 가까운 것으로, 실험적 검증을 통해 참임이 드러난 명제이다. 모두 공리라는 의미로 쓰이지만, 물리학에서는 의미상의 이유로 postulate라는 말을 더 선호한다. 물론 둘 중 무엇을 사용해도 상관이 없다. 맥락을 전달하는 것이 가장 중요하겠다.

Axiom 2.1.1 (양자 상태)

각 양자계에는 그에 대응하는 상태 공간이 존재한다. 양자계의 한 상태는 이 상태 공간 상의 벡터이다. 상태 공간은 복소수체 \mathbb{C} 위에서 정의되는 벡터 공간이며, 에르미트 내적이 주어져야 한다. 물리적으로 유의미한 양자 상태는 에르미트 내적에 따른 크기가 1인 단위 벡터이다. 특히, 서로 구별 가능한 상태, 즉 상태 공간의 기본 상태들은 서로 직교(orthogonal)한다.

II.2. 에르미트 내적

먼저 n 차원 복소수 벡터 공간 V 를 생각하자.

$$V = \mathbb{C}^N \quad (2.3)$$

이 벡터 공간에 아래 두 개의 벡터가 있다고 하자.

$$\mathbf{u} = \begin{bmatrix} a_1 \\ \vdots \\ a_N \end{bmatrix}, \mathbf{v} = \begin{bmatrix} b_1 \\ \vdots \\ b_N \end{bmatrix} \quad (2.4)$$

$$\mathbf{u}, \mathbf{v} \in V$$

먼저, 두 벡터 \mathbf{u}, \mathbf{v} 에 대해 우리가 원래 알고 있는 내적 연산을 해 보자.

$$\mathbf{u} \cdot \mathbf{v} = \sum_{k=1}^N a_k b_k \quad (2.5)$$

그런데 내적을 이런 식으로 정의하면 조금의 문제가 있다. \mathbf{u} 가 아래와 같다고 하자.

$$\mathbf{u} = \begin{bmatrix} 1 \\ i \end{bmatrix} \quad (2.6)$$

그러면 \mathbf{u} 에 대해 자신과 내적하면

$$\mathbf{u} \cdot \mathbf{u} = 1^2 + i^2 = 1 + (-1) = 0 \quad (2.7)$$

과 같이 0이 된다.

자신과의 내적은 \mathbb{R}^N 상에서는 영벡터가 아닌 벡터에 대해 양수이며, 벡터의 크기에 관련이 있다는 특징이 있다. 그런데 여기서는 이 벡터가 0이 아님에도 자신과의 내적이 0이 되어버렸다. 이것은 이 벡터가 자기 자신에게 수직이라는 소리로도 들린다. 그렇게

좋은 상황은 아닌 것 같다. 그런데 이 문제를 해결할 방법이 있다. 바로 본래 내적 대신 에르미트 내적을 사용하면 된다. \mathbf{u}, \mathbf{v} 에 대한 에르미트 내적은 $\langle \mathbf{u}, \mathbf{v} \rangle$ 로 쓴다.

Definition 2.2.1 (에르미트 내적)

$\mathbf{u}, \mathbf{v} \in \mathbb{C}^N$ 에 대해 그 에르미트 내적(Hermitian scalar product) $\langle \mathbf{u}, \mathbf{v} \rangle$ 는

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{k=1}^N \bar{a}_k b_k \quad (2.8)$$

이런 식으로 내적을 정의하고 \mathbf{u} 를 다시 자기 자신과 내적해보면,

$$\langle \mathbf{u}, \mathbf{u} \rangle = \bar{1} \cdot 1 + \bar{i} \cdot i = 1 + (-i)i = 1 + 1 = 2 \quad (2.9)$$

이제 우리가 원하던 내적의 성질이 돌아왔고, \mathbf{u} 가 자기 자신에 수직인 벡터가 아니라는 것을 알 수 있다. 이제 자신에 대한 에르미트 내적 공식을 자명하게 알 수 있다.

$$\langle \mathbf{u}, \mathbf{u} \rangle = \sum_{k=1}^N \bar{a}_k a_k = \sum_{k=1}^N |a_k|^2 \quad (2.10)$$

이 값은 실수이며, 음수가 아니라는 것을 확인하자. 또, 당연한 이야기지만 실수에 대해서는 켈레복소수가 자기 자신이 되므로 기존의 내적 연산과 다를 것이 없다.

Theorem 2.2.2 (에르미트 내적의 성질)

복소 벡터 공간 V 상에서 에르미트 내적은

$$\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{C} \quad (2.11)$$

이며 반쌍선형이다. 즉, 아래를 만족한다.

1. $\langle u, v' + v'' \rangle = \langle u, v' \rangle + \langle u, v'' \rangle$
2. $\langle u' + u'', v \rangle = \langle u', v \rangle + \langle u'', v \rangle$
3. $\langle u, \lambda v \rangle = \lambda \langle u, v \rangle$
4. $\langle \lambda u, v \rangle = \bar{\lambda} \langle u, v \rangle, \quad \lambda \in \mathbb{C}$

교환법칙이 성립하지 않는다.

$$\langle v, u \rangle = \overline{\langle u, v \rangle} \quad (2.12)$$

이러한 관계를 에르미트 대칭(Hermitian symmetry)이라고도 한다.

양정(positive definite, 陽定) 형식이다.

$$u \neq 0 \Rightarrow \langle u, u \rangle > 0 \quad (2.13)$$

위 서술의 4번에서 보다시피 첫 번째 변수에 대해서는 완벽히 선형이 아니고 빠져 나올 때 켄레를 달고 나온다. 이런 것을 켄레 선형이라고 한다. 켄레 선형은 반만 선형인 것으로 보아서 반쌍선형(sesquilinear, 半雙線型)이라고 한다. 반쌍선형은 반만 쌍선형(bilinear)이라는 것인데, 굳이 따지자면 2 방향으로 선형인 것이 아니라 1.5 방향으로 선형이라는 뜻이 된다. 에르미트 내적이 반쌍선형이 되는 이유는 더할 때 앞에 곱해지는 계수에 켄레가 씌워지기 때문이라고 할 수 있다.

Exercise. 앞서 정의한 u, v 에 대해 $\langle u, v \rangle$ 가 [Theorem 2.2.2](#) 를 만족함을 증명해 보자.

이제 무한 차원 벡터 공간에서의 에르미트 내적에 대해서도 알아보자. V 를 구간 $[0, L]$ 에서 연속인 복소함수의 공간이라고 하자.

$$f : [0, L] \rightarrow \mathbb{C} \quad (2.14)$$

이때 두 함수의 에르미트 내적은

$$\langle f, g \rangle = \int_0^L \overline{f(x)} g(x) dx \quad (2.15)$$

이 된다.

함수 자신에 대한 에르미트 내적은 다음과 같이 되는 것도 알 수 있다.

$$\langle f, f \rangle = \int_0^L |f(x)|^2 dx \quad (2.16)$$

이 값 또한 $f(x) \neq 0$ 인 경우 0보다 크다.

II.3. 광자의 편광 상태

우선, 광자는 전자기파이다. 즉, 운동하며 전기장과 자기장을 만든다. 전기장 E 와 자기장 B 는 서로 직교하는 방향으로 동시에 진동한다.

광자가 z 방향으로 진행한다고 가정하자. 전기장 E 가 y 방향으로 진동할 때 광자가 수직 편광(vertical polarization)을 가졌다고 한다. 반대로, 전기장이 x 방향으로 진동한다면 수평 편광(horizontal polarization)을 가졌다고 한다.

그러므로 광자 한 개에 대해 편광 상태의 기저 상태는 두 개이다. $|\uparrow\rangle$ 를 수직 편광 상태로, $|\rightarrow\rangle$ 를 수평 편광 상태로 정의하자. 그러면 광자는 이 두 편광 상태만 가지느냐고 하면, 당연히 아니다. 수직 혹은 수평이 아니라 비스듬히 편광된 상태로 진행할 수도 있는 것이다.

$|\uparrow\rangle, |\rightarrow\rangle$ 를 두 개의 기저 벡터로 갖는 평면을 생각하자. 이것은 상태 벡터의 공간이므로 기저 상태의 선형 결합을 취함으로써 두 상태를 섞어서 모든 각도에 대한 편광 상태를 표현할 수 있을 것이다.

수평 편광에서 α 만큼 기울어진 편광 상태는 다음과 같이 표현할 수 있다.

$$|\psi\rangle = \cos \alpha |\uparrow\rangle + \sin \alpha |\rightarrow\rangle \quad (2.17)$$

그럼 이것으로 모든 편광 상태를 표현할 수 있는가?

아니다. 진동하는 전기장의 위상(phase)도 달라질 수 있다. θ 만큼 위상이 어긋났다고 생각하고 위상 변환(phase shift)을 해보자. $\theta \in [0, 2\pi]$ 에 대해 전기장을 위상 변환하면

$$e^{i\theta} |\uparrow\rangle \quad (2.18)$$

분명히 위상은 다른 상태지만, 전자기파를 한 점에서 측정할 때, 단순한 진폭 관측만으로는 위상 차이를 구별할 수 없다. 둘 다 진행하고 있는 전자기파일 뿐이다. 하지만 이걸

전자기파 하나만 보았을 때 이야기이고, 두 전자기파가 간섭할 경우, 상대적인 위상 차이가 실험적으로 관측 가능해진다. 극단적인 예시로, 만약 한 전자기파는 0, 다른 전자기파는 π 의 위상을 가지고 있다면 두 전자기파의 전기장과 자기장의 서로를 상쇄하여 진동이 완전히 사라질 것이다⁸.

서로 위상 차이가 있는 두 개의 전자기파의 편광 상태를 보자.

$$|\uparrow\rangle + e^{i\frac{\pi}{2}}|\rightarrow\rangle \quad (2.19)$$

앞의 전자기파는 수직 편광 상태이고, 뒤의 전자기파는 수평 편광된 채로 $\frac{\pi}{2}$ 만큼 위상이 어긋나 있다.

두 전자기파는 시간에 따라 공간을 통과해 진행하고 있다. 따라서 시간에 따라 z 축 위의 점을 바꿔보며 두 편광 상태의 합을 구해보면, 상태 공간에서 편광 상태 벡터가 반시계 방향으로 회전하는 것을 알 수 있다. 이런 상태를 원형 편광(circular polarization)이라고 한다. 이때, $e^{i\frac{\pi}{2}} = i$ 이므로 같은 상태를 이렇게도 표현할 수 있다.

$$|\uparrow\rangle + i|\rightarrow\rangle \quad (2.20)$$

같은 방법으로, 아래 상태는 시계 방향으로 회전하는 원형 편광 상태를 나타낸다.

$$|\uparrow\rangle - i|\rightarrow\rangle \quad (2.21)$$

편광의 원리는 3D 영화에 이용된다. 3D 영화를 찍을 때는 다른 각도에서 두 개의 카메라로 같은 장면을 찍는다. 이때 두 카메라는 각각 사람의 두 눈을 대신하는 역할을 한다. 사람은 두 눈으로 서로 다른 위치에서 시각 정보를 받아 뇌에서 처리함으로써 입체감을 느끼기 때문이다. 카메라 두 개로 영화를 찍는 건 어렵지 않다. 문제는 이것을 합쳐서 입체감 있게 관객에게 전달하는 것이다. 왼쪽 눈은 왼쪽 카메라의 영상을, 오른쪽 눈은 오른쪽 카메라로의 영상만을 받아야 한다. 이 과정은 편광된 빛과 편광 필터를 통해 구현된다. 예를 들어 수직 편광 필터는 수직으로 편광된 빛만을 통과시키고 수평 편광 빛은 차단한다. 이렇게 해 놓으면 두 개의 영상기로 두 개의 카메라의 영상을 각각 영상하고, 왼쪽 카메라의 영상은 수직 편광으로, 오른쪽 카메라의 영상은 수평 편광으로 내보낸 뒤, 관객이 편광 필터가 달린 안경을 써서 영상의 입체감을 느낄 수 있게 된다.

⁸이 원리는 다양한 물리학적 장치에 활용된다. 대표적인 예가 LIGO 중력파 관측소이다. 일종의 레이저 빛 시계 두 개를 서로 직교하도록 놓고 출발 지점에서 레이저 빔을 발사하면, 원래대로라면 광자가 동시에 출발했다가 반사되어 동시에 돌아와 위상이 같아야 한다. 그러나 중력파가 통과하면 중력파의 위상에 따라 공간이 늘어났거나 줄어들어 광자에 위상 차이가 발생한다. 출발 지점의 간섭계(interferometer)가 이 위상 차이를 측정하여 중력파를 감지할 수 있다. 이런 관측소를 지구 곳곳에 놓고 동시에 측정한 데이터를 합쳐보게 되면, 중력파의 근원 지점을 알 수 있게 된다.

그런데, 3D 영화관에서는 이런 방식을 사용하지 않는다. 수평, 수직 편광을 사용하게 되면 관객이 가만히 앉아서 스크린을 똑바로 바라보아야 영상이 선명하고 제대로 보이기 때문이다. 예를 들어 고개를 기울인다면, 필터도 같이 기울어져서 수평 편광과 수직 편광의 빛이 섞여서 들어오게 되어 흐리고 이상한 영상을 보게 될 수 있다. 이 문제를 해결하기 위해 실제로는 원형 편광된 빛을 사용한다. 한 개의 영사기는 왼쪽으로 회전하는 원형 편광을, 다른 영사기는 오른쪽으로 회전하는 원형 편광을 영사한다. 이때 안경의 편광 필터는 두 겹으로 되어 있어서, 원형 편광을 수직이나 수평 편광으로 변환하여 눈으로 보낸다. 이렇게 하면 고개를 기울여도 원형 편광에는 영향을 미치지 않고, 필터로 들어온 후 수직이나 수평 편광으로 변환되기 때문에 더 선명한 영상을 볼 수 있다.

3D 영화관에 갈 기회가 생긴다면, 3D 안경에 들어있는 안경알을 뽑아서 가지고 놀아보자. 두 안경알을 수평으로 겹치면 모든 빛이 통과하지만, 수직으로 겹치면 모든 빛이 막힐 것이다. 그 외에도, 비스듬히 기울여도 보고 (필터가 비닐인 경우) 구부려도 보자.

이제 광자의 일반적인 편광 상태를 살펴 보자. 이 상태 벡터는 종종 존스 벡터(Jones vector)로 불리기도 한다.

$$|\psi\rangle = a_1 e^{i\theta_1} |\uparrow\rangle + a_2 e^{i\theta_2} |\rightarrow\rangle$$

$$\text{s.t. } a_1, a_2 \in \mathbb{R}_+$$
(2.22)

그런데 $ae^{i\theta}$ 는 일반적으로 복소수를 나타내는 극형식 표현이므로 이것을 z 로 놓고 다음과 같이 쓸 수 있다.

$$|\psi\rangle = z_1 |\uparrow\rangle + z_2 |\rightarrow\rangle$$

$$\text{s.t. } z_1, z_2 \in \mathbb{C}$$
(2.23)

이때 양자역학의 공리에 따라 정규화⁹ 조건은

$$\langle\psi|\psi\rangle = 1 = |z_1|^2 + |z_2|^2$$
(2.24)

이 편광 상태 또한 큐비트의 상태로 해석할 수 있다. $|\uparrow\rangle$ 를 $|1\rangle$, $|\rightarrow\rangle$ 을 $|0\rangle$ 으로 보는 식으로 하면 된다.

II.4. 전자의 스핀 상태

다른 큐비트 구현의 예시로는 전자의 스핀이 있다.

⁹벡터의 크기가 1이 되도록 계수를 조정하는 것을 말한다. 정규화를 할 때는 크기 제곱의 합이 1이 된다는 것 외에도, 당연히 원본 벡터의 계수 가중치가 유지되도록 해야 한다.

전자의 스핀에는 두 가지 기본 상태가 존재한다.

$$\begin{aligned} |\uparrow\rangle &: \text{위 스핀} \\ |\downarrow\rangle &: \text{아래 스핀} \\ & (z\text{축 방향으로}) \end{aligned} \quad (2.25)$$

물리학적 관점에서는 과학적 정확성을 위해 $|\uparrow\rangle$ 를 $+\frac{1}{2}$, $|\downarrow\rangle$ 를 $-\frac{1}{2}$ 스핀이라고 할 수 있을 것이고, 수학적 관점에서는 계산의 편의성을 위해 $|\uparrow\rangle$ 를 $+1$, $|\downarrow\rangle$ 를 -1 로 볼 수 있을 것이다. 어차피 상태를 나타내는 데에는 큰 상관이 없으므로 아무거나 취해도 상관이 없다. 전자의 스핀 상태는 2차원 복소 벡터공간 상에 있으며, 기저 벡터로 $\{|\uparrow\rangle, |\downarrow\rangle\}$ 를 갖는다.

전자의 스핀이란 무엇인가? 스핀은 자기장을 만들며, 전자는 작은 자석이라고 볼 수 있다. 스핀 상태는 전자에 의해 유도된 자기장의 방향을 나타낸다고 할 수 있다. 원자에서, 전자가 짝을 이루는 것이 안정하다. 그러므로 하나의 오비탈 안에서 한 전자는 위 스핀, 다른 전자는 아래 스핀을 갖게 된다. 하지만 어떤 원자들은 오비탈 내에서 짝을 이루지 못하는 전자, 즉 홀전자가 있다. 원자가 홀전자를 가진다면 원자 전체가 전자 구름때문에 스핀을 가지게 된다.

일반적인 조건에서, 만약 홀전자가 있는 원자로 된 큰 물질의 덩어리가 있다면, 이 물질을 이루고 있는 서로 다른 원자들은 홀전자에 의해 서로 다른 스핀을 갖게 되고, 자기장은 서로에게 상쇄되어 사라지게 된다. 그래서 우리는 원자를 이루고 있는 전자의 스핀을 확인할 수 없다. 하지만, 이 물질을 자기장 안에 놓게 된다면 모든 홀전자의 스핀을 외부 자기장의 방향으로 고정시킬 수 있고, 어떤 물질(강자성체)에 대해서는 자기장을 제거해도 전자의 스핀 방향이 정렬된 채로 유지될 수 있다. 즉, 자석을 만든 것이다. 이런 예시로 양자역학이 실제로 작용하고 있음을 알 수 있다.

그런데, 모든 전자가 z 방향으로만 위와 아래 스핀을 가지지는 않을 것이다. x 나 y 방향에 대한 스핀은 어디갔는가?

일반적인 스핀 상태는 알다시피 아래와 같다.

$$\begin{aligned} z_1|\uparrow\rangle + z_2|\downarrow\rangle \\ \text{s.t. } z_1, z_2 \in \mathbb{C}, |z_1|^2 + |z_2|^2 = 1 \end{aligned} \quad (2.26)$$

z 방향이 아닌 방향에 대한 스핀을 알아보기 위해서는 파울리 행렬에 대해 알아야 한다.

파울리 행렬은 세 가지가 있다. $\sigma_1, \sigma_2, \sigma_3$ 은 각각 $\sigma_x, \sigma_y, \sigma_z$ 라고도 한다.

$$\begin{aligned}\sigma_1 &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ \sigma_2 &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ \sigma_3 &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\end{aligned}\tag{2.27}$$

파울리 행렬은 관측가능량(observable)의 예시이다. 관측가능량에 대해서는 다음 장에서 더 자세히 알아보도록 하겠다.

Definition 2.4.1 (고윳값과 고유벡터)

벡터공간 V 상의 어떤 선형변환(행렬) $A : V \rightarrow V$ 에 대하여 다음 식에 대해 0이 아닌 해 \mathbf{v} 가 존재하면 스칼라 $\lambda \in \mathbb{C}$ 는 A 의 고윳값(eigenvalue)이라고 한다.

$$A\mathbf{v} = \lambda\mathbf{v}\tag{2.28}$$

이때 해가 되는 벡터 \mathbf{v} 는 고윳값 λ 에 대응하는 고유벡터(eigenvector)이다.

즉, 선형변환 A 를 적용했을 때 방향은 바뀌지 않고 크기만 λ 배로 바뀌는 벡터가 고유벡터이다.

또, 주어진 고윳값 λ 에 대해

$$V_\lambda = \{\mathbf{v} \in V \mid A\mathbf{v} = \lambda\mathbf{v}\}\tag{2.29}$$

로 정의되는 부분공간, 즉 같은 고윳값에 속한 고유벡터의 모임을 고유공간(eigenspace)라고 한다.

x 방향 스핀 상태 $|\uparrow_x\rangle, |\downarrow_x\rangle$ 는 σ_x , y 방향 스핀 상태 $|\uparrow_y\rangle, |\downarrow_y\rangle$ 는 σ_y , z 방향 스핀 상태 $|\uparrow_z\rangle, |\downarrow_z\rangle$ 는 σ_z 의 고유벡터이다.

예를 들어 $|\uparrow_z\rangle$ 는 고윳값 1을 갖는 σ_z 의 고유벡터이고, $|\downarrow_z\rangle$ 는 -1 고유벡터이다. 여기서, 자명하게 $|\uparrow\rangle = |\uparrow_z\rangle, |\downarrow\rangle = |\downarrow_z\rangle$ 임을 확인하자.

기저벡터끼리 더하면 전체 행렬의 고유벡터가 되므로, $|\uparrow_z\rangle + |\downarrow_z\rangle$ 는 고윳값 1인 σ_x 의 고유벡터이고, 단위벡터가 되도록 정규화를 해주면 다음과 같다.

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}}|\uparrow_z\rangle + \frac{1}{\sqrt{2}}|\downarrow_z\rangle \quad (2.30)$$

또 $\sigma_x \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \end{bmatrix}$ 이므로

$$|\downarrow_x\rangle = \frac{1}{\sqrt{2}}|\uparrow_z\rangle - \frac{1}{\sqrt{2}}|\downarrow_z\rangle \quad (2.31)$$

임을 알 수 있다.

이런 식으로 우리는 큐비트를 물리적으로 구현할 방법을 찾은 것이다.

$$\begin{aligned} |\uparrow\rangle &= |1\rangle \\ |\downarrow\rangle &= |0\rangle \\ \psi &= z_0|0\rangle + z_1|1\rangle \end{aligned} \quad (2.32)$$

이로써 우리는 전자의 스핀 상태를 통해 단일 큐비트를 구현할 수 있게 되었다.

스핀은 MRI에 사용된다. MRI는 전자가 아니라 원자핵의 스핀을 이용한다. 원자핵은 여러 양성자와 중성자가 붙어 있는 것이므로 그 스핀은 2차원 상에 있는 전자의 스핀보다 큰 공간 상에 있다. 원자핵의 스핀 공간은 유한 차원이지만 어떤 원자냐에 따라 달라지는 것이다. 관측된 스핀값은 $\pm\frac{1}{2}$ 뿐이 아니라, $\frac{1}{3}, 2, 5$ 등등 여러 가지가 나올 수 있다.

어떤 원자인지 구별하려면, 예를 들어 탄소 원자를 마그네슘 원자와 구분하려면 어떻게 하는가? 스캔을 진행할 대상 환자를 간헐적이지만 매우 강한 자기장 속에 놓으면 핵자들은 모두 이 자기장 방향으로 정렬된다. 하지만 정렬된 상태는 안정하지 않으므로 일부 스핀이 뒤집어져 정렬을 푸는 과정이 일어나고, 그 과정에서 복사가 일어나게 된다. 그 복사의 에너지와 주파수 분포 등을 통해 정렬이 풀리기 전에 전체적으로 스핀 상태였는지 알 수 있다. 즉, 원자들이 각각 어떤 원자핵을 갖고 있는지 알 수 있다는 것이다.

이 기술이 처음 개발되었을 때 제안된 명칭은 NMR(Nuclear Magnetic Resonance, 핵자기 공명 분광법)였다. 하지만 사람들은 nuclear이 들어간 것은 방사능을 뿜는 것(nuclear decay), 핵폭탄에 관련된 것 등이라고 생각하여 매우 무서워했다. 하지만 실제로 이 과정에서 핵융합이나 핵분열, 치사량의 방사능 노출 등은 일어나지 않는다. 그래서 대중에게 이 사실을 입 아프게 교육하는 대신 그냥 이름을 MRI(Magnetic Resonance Imaging, 자기공명영상)로 바꾸었다.

II.5. 퍼텐셜 우물 속 입자

상태 공간에 대한 다른 예시는 그 공간의 차원이 무한인 경우이다. 이 주제는 양자 컴퓨팅과는 관련이 없지만 기본 지식으로 알아야 한다고 판단했다.

우선, 어떤 입자를 퍼텐셜 우물(potential well)에 가둔다고 하자. 입자가 특정 공간을 벗어나지 못하게 한다는 뜻이다. 간단하게, 1차원 퍼텐셜 우물의 구간을 $[0, L]$ 로 하자. 우리가 잡을 상태 공간 V 는 “파동함수”의 공간이다. 파동함수들은 $\psi : [0, L] \rightarrow \mathbb{C}$ 이고 해당 구간에서 연속인 함수이다.

이 공간 상의 두 파동함수 ψ, φ 에 대해 에르미트 내적은

$$\langle \psi, \varphi \rangle = \int_0^L \overline{\psi(x)} \varphi(x) dx \quad (2.33)$$

처럼 된다.

또, 입자가 구간 $[0, L]$ 에 갇혔으므로 $\psi(0) = \psi(L) = 0$ 이라고 놓아 파동이 양 끝에서 끝나도록 하자. 그런데, 이것이 물리량 무슨 상관인가?

그것에 대한 답은, 양자역학은 확률적이다. 이 경우에서, 입자를 $[0, L]$ 내의 구간 $[a, b]$ 에서 발견할 확률은 아래와 같이 주어지게 된다.

$$\int_a^b |\psi(x)|^2 dx \quad (2.34)$$

물론, 물리적 의미를 가지는 상태는 크기가 1이라는 조건을 가지므로 $|\psi|^2 = 1 = \langle \psi, \psi \rangle$ 이다. 그러므로 위 적분은 $[0, L]$ 에서 입자를 발견할 확률이 1이라는 것을 알려준다.

$$\langle \psi, \psi \rangle = \int_0^L |\psi(x)|^2 dx = 1 \quad (2.35)$$

이제 이 파동함수는 특별한 의미를 갖는다. $|\psi(x)|^2$ 은 확률 밀도를 나타내는 확률밀도함수(PDF, Probability Density Function)라는 것이다.

왜 그럴까? 그에 대한 답은 그냥 실험적으로 들어맞는다는 것이 증명되었기 때문이다. 또, 수학적으로도 확률 보존을 보장한다.

① $|\psi|^2$ 의 확률로서의 수학적 정당성

시간 의존 슈뢰딩거 방정식에서 $P = |\psi|^2$ 으로 두면 확률 보존을 보장한다.

$$i\hbar \frac{\partial \psi}{\partial t} = -\frac{\hbar^2}{2m} \frac{\partial^2 \psi}{\partial x^2} + V\psi \quad (2.36)$$

$P = \bar{\psi}\psi$ 에 대해 정리하면

$$\frac{\partial P}{\partial t} + \frac{\partial J}{\partial x} = 0 \quad (2.37)$$

이다. 여기서 J 는 확률 흐름 밀도(probability current)라고 하며,

$$J = -\frac{i\hbar}{2m} \left(\frac{\partial \psi}{\partial x} \bar{\psi} - \frac{\partial \bar{\psi}}{\partial x} \psi \right) \quad (2.38)$$

으로, 입자의 확률 밀도가 흐르는 정도를 나타낸다.

이런 것을 postulate(가정)이라고 하며, 막스 보른(Max Born, 1882 ~ 1970)이 정립한 규칙으로 보른 규칙(Born rule)이라고 한다. 보른 규칙에 파동함수의 진폭의 제곱이 PDF라는 것이 포함되어 있다.

이 상황에서 기본 상태들은 무엇일까? 이 공간의 기저벡터를 도출하기 위해서는 슈뢰딩거 방정식(Schrödinger equation)을 사용한다. 슈뢰딩거 방정식은 양자컴퓨팅 내부가 아닌 양자역학에서 다루는 내용이기 때문에, 여기서 따로 자세히 설명하지는 않는다.

파동함수로 ψ 를 갖는 입자는 다음 슈뢰딩거 방정식을 만족하면 에너지 E 를 갖는다.

$$-\frac{\hbar^2}{2m} \frac{\partial^2 \psi}{\partial x^2} = E\psi \quad (2.39)$$

이때 m 은 입자의 질량, $\hbar = \frac{h}{2\pi}$ 이며, \hbar 는 디랙 상수(Dirac constant) 또는 환산 플랑크 상수(reduced Planck constant)라고 한다.

슈뢰딩거 방정식은 파동방정식의 일종으로, 다시 쓰면

$$\frac{\partial^2 \psi}{\partial x^2} = -\lambda^2 \psi \quad (2.40)$$

이 파동방정식의 해는

$$\psi = a \cos \lambda x + b \sin \lambda x \quad (2.41)$$

이때 $\psi(0) = 0$ 이므로 $a = 0$ 이다. 이제 식이 선형이므로 b 를 없앨 수 있다¹⁰.

$$\psi = \sin \lambda x \quad (2.42)$$

$\psi(L) = 0$ 이므로

$$\sin \lambda L = 0 \Rightarrow \lambda L = \pi k, \lambda_k = \frac{\pi k}{L} \quad (2.43)$$

그런데 원래 방정식과 계수를 비교하여

$$\lambda_k^2 = \frac{2mE_k}{\hbar^2} \quad (2.44)$$

임을 알 수 있다(아랫첨자 k 는 k 에 대한 양이라는 뜻으로 임의로 붙인 것이다).

그러므로

$$\lambda_k^2 = \frac{\pi^2 k^2}{L^2} \quad (2.45)$$

이제

$$E_k = \frac{\pi^2 k^2 \hbar^2}{2mL^2} \quad (2.46)$$

로 입자들의 에너지 준위가 이산적이다.

파동함수는

$$\psi_k(x) = \sin \lambda_k x \quad (2.47)$$

로, 이것이 기저 함수들이 된다.

우리는 이로서 무한 차원 에르미트 공간과 서로 각각 직교하는 기저(정규직교 기저)들을 얻는다. 이제 일반 상태는 기저들의 중첩 또는 선형결합이며, 푸리에 급수로 전개할 수 있게 된다.

이번 장에서는 양자계의 상태에 대해 알아보았다. 다음 장에서는 관측가능량에 대해 알아보도록 하자.

¹⁰ $b\psi$ 가 해이면 ψ 도 해이기 때문이다.

III. 관측가능량

이번 장에서는 양자역학의 관측가능량에 대해 알아보겠다.

III.1. 자기 수반 연산자

상태 공간 V 는 에르미트 내적이 성립하는 복소 벡터공간이었다.

관측가능량(觀測可能量, observable)이란 V 상의 자기 수반(self-adjoint) 연산자 또는, 다른 말로 에르미트(Hermitian) 연산자이다. 직관적인 의미는 말 그대로 측정할 수 있는 양이라는 뜻이며, 가측량(可測量)이라고도 한다.

Definition 3.1.1 (자기 수반 연산자)

$A : V \rightarrow V$ 인 어떤 연산자 A 에 대해 다음이 성립하면 A 는 자기 수반 연산자(에르미트 연산자)이다.

$$\forall v, w \in V \quad \langle v | Aw \rangle = \langle Av | w \rangle \quad (3.1)$$

이때 아래가 성립한다.

$$A = A^\dagger \quad (3.2)$$

\mathbb{C}^N 상에서 다음과 같은 에르미트 내적을 보자.

$$\langle v | w \rangle = \bar{v}^T \cdot w \quad (3.3)$$

또, 다음 연산을 보자.

$$\begin{aligned} \langle v | Aw \rangle &= \bar{v}^T \cdot A \cdot w \\ \langle Av | w \rangle &= \overline{(Av)}^T \cdot w = \bar{v}^T \cdot \bar{A}^T \cdot w \end{aligned} \quad (3.4)$$

그러므로 [Definition 3.1.1](#) 에서 A 가 에르미트 연산자이라면 아래가 성립해야 한다.

$$A = \bar{A}^T = A^\dagger \quad (3.5)$$

이때 \bar{A}^T 를 A 의 켤레 전치(conjugate transpose) 또는 에르미트 전치(Hermitian transpose)라고 하며, A^\dagger 라고도 쓴다¹¹.

¹¹†는 단검을 본따 만든 기호로, 한국어로는 칼표라고 하며, A^\dagger 는 ‘A dagger’라고 읽는다. 수학에서는 켤레 전치를 A^* 로 쓰기도 한다.

Exercise. 연산자 A 에 대해 A 가 에르미트 연산자이라면 $A = \bar{A}^T$ 가 성립해야함을 엄밀히 증명하여라. v 의 기저를 i , w 의 기저를 j 로 놓으면 위 등식은 $a_{ij} = \bar{a}_{ji}$ 와 동치이다.

이 연산자 A 를 실수부와 허수부로 나누자. B 와 C 는 실수 행렬이다.

$$A = B + iC \quad (3.6)$$

A 가 에르미트 연산자라면

$$\begin{aligned} \bar{A}^T &= \overline{(B + iC)}^T \\ &= B^T - iC^T \\ &\stackrel{?}{=} B + iC \end{aligned} \quad (3.7)$$

여기서 $\stackrel{?}{=}$ 등호가 성립해야 한다. 그 조건은

$$B^T = B \wedge C^T = -C \quad (3.8)$$

그러므로 어떤 행렬의 실수부가 대칭(symmetric, 對稱)행렬이고 허수부가 비대칭(skew-symmetric, 非對稱)행렬이면 그 행렬은 자기 수반 행렬 또는 에르미트 행렬¹²이다.

한 가지 예시로 아래를 보자.

$$A = \begin{bmatrix} 2 & 1+i \\ 1-i & 3 \end{bmatrix} \quad (3.9)$$

이 행렬의 실수부를 취하면

$$\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} \quad (3.10)$$

으로 대칭이고, 허수부를 취하면

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad (3.11)$$

으로 비대칭이다.

¹²반대칭(antisymmetric, 反對稱)행렬이라고도 한다.

III.2. 자기 수반 연산자의 고윳값과 고유벡터

Definition 3.2.1 (에르미트 공간)

\mathbb{C} 상의 벡터공간 V 에 대해 그 공간 상에서 임의의 벡터의 내적이 에르미트 내적이 라면 이 공간을 에르미트 공간(Hermitian space)이라고 한다.

복소 벡터공간에 길이와 직교를 정의할 수 있도록 한 것이 에르미트 공간이며, 앞서 배운 에르미트 내적의 개념에서 기원한다.

Theorem 3.2.2 (자기 수반 연산자의 성질)

A 를 에르미트 공간 V 상의 자기 수반 연산자라고 하자. 이때 다음이 성립한다.

1. A 의 모든 고윳값은 실수이다.
2. 각 고윳값에 대응하는 고유벡터는 서로에 대해 직교한다.

Proof.

1. v 가 A 의 고유벡터라고 하자. 즉, $Av = \lambda v$ 이다.

$$\langle v | Av \rangle = \langle v | \lambda v \rangle = \lambda \langle v | v \rangle \quad (3.12)$$

이때 A 는 자기 수반 연산자이므로 다음도 성립한다.

$$\langle v | Av \rangle = \langle Av | v \rangle = \langle \lambda v | v \rangle = \bar{\lambda} \langle v | v \rangle \quad (3.13)$$

고윳값의 정의에 따라 $v \neq 0$ 이다. 즉, $\langle v | v \rangle \neq 0$ 이다. 이제 아래 등식

$$\lambda \langle v | v \rangle = \bar{\lambda} \langle v | v \rangle \quad (3.14)$$

에 의해 $\lambda = \bar{\lambda}$ 이므로 $\lambda \in \mathbb{R}$ 이다.

2. A 의 두 고유벡터 v, w 에 대해

$$\begin{aligned} Av &= \lambda v \\ Aw &= \mu w \\ \text{s.t. } \lambda &\neq \mu \wedge \lambda, \mu \in \mathbb{R} \end{aligned} \quad (3.15)$$

일 때,

$$\begin{aligned}
 \langle \mathbf{v} | A \mathbf{w} \rangle &= \langle \mathbf{v} | A \mu \mathbf{w} \rangle = \mu \langle \mathbf{v} | \mathbf{w} \rangle \\
 &= \langle A \mathbf{v} | \mathbf{w} \rangle = \langle \lambda \mathbf{v} | \mathbf{w} \rangle = \lambda \langle \mathbf{v} | \mathbf{w} \rangle \\
 \Rightarrow (\lambda - \mu) \langle \mathbf{v} | \mathbf{w} \rangle &= 0 \\
 \therefore \langle \mathbf{v} | \mathbf{w} \rangle &= 0 \quad \because \lambda \neq \mu
 \end{aligned} \tag{3.16}$$

이처럼 임의의 두 고유벡터 간 내적이 0이므로, 각 고유벡터는 대해 직교한다. \square

이해를 위해 빠르게 예시를 보자. 아래 연산자가 있다고 하자.

$$A = \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix} \tag{3.17}$$

이 행렬의 고유벡터는

$$\begin{aligned}
 \mathbf{v}_1 &= \begin{bmatrix} 1 \\ i \end{bmatrix} \\
 \mathbf{v}_2 &= \begin{bmatrix} 1 \\ -i \end{bmatrix}
 \end{aligned} \tag{3.18}$$

따라서

$$\begin{aligned}
 A \mathbf{v}_1 &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \lambda_1 = 0 \\
 A \mathbf{v}_2 &= \begin{bmatrix} 2 \\ -2i \end{bmatrix}, \quad \lambda_2 = 2
 \end{aligned} \tag{3.19}$$

A 의 실수부는 대칭이고 허수부는 비대칭이므로 A 는 자기 수반 행렬이다. 이때 고유벡터는 실수가 아니지만 고유값 λ_1, λ_2 는 모두 실수이다. 또, 두 고유벡터를 내적하면

$$\begin{aligned}
 \langle \mathbf{v}_1 | \mathbf{v}_2 \rangle &= \overline{\mathbf{v}_1}^T \mathbf{v}_2 \\
 &= [1 \quad -i] \begin{bmatrix} 1 \\ -i \end{bmatrix} = 1 - 1 = 0
 \end{aligned} \tag{3.20}$$

이므로 고유벡터끼리 직교한다는 것도 알 수 있다. 이로써 정리가 성립함을 확인해 볼 수 있었다.

III.3. 자기 수반 연산자의 스펙트럼 정리

Theorem 3.3.1 (자기 수반 연산자의 스펙트럼 정리)

유한차원 에르미트 공간 V 상의 자기 수반 연산자 A 는 대각화할 수 있다.

$V = \{v_1, \dots, v_N\}$ 에 직교하고 실수 곱셈값을 갖는 A 의 고유벡터가 존재한다.

$$\begin{aligned} Av_j &= \lambda_j v_j & \text{where } \lambda_j &\in \mathbb{R} \\ \langle v_j | v_k \rangle &= 0 & \text{if } j \neq k \end{aligned} \quad (3.21)$$

실수 자기 수반 행렬은 대칭행렬이다. 즉, 우리는 A 연산자의 행렬이 실수 대각행렬이 되도록 하는 V 의 직교 기저를 찾을 수 있다는 뜻이다.

자기 수반 연산자의 성질은 차원의 크기에 관련이 없었지만, 우리가 본 스펙트럼 정리는 유한차원에서만 성립한다는 것이다. 본 과정에서는 유한 차원에 대한 것만 필요하기 때문이다. 하지만 무한차원으로 일반화하여 확장한 스펙트럼 정리도 존재한다. 증명에 대한 것 등 자세한 것은 선형대수학에서 공부하자.

III.4. 브라-켓 표기법

브라-켓(bra-ket) 표기법 또는 디랙(Dirac)¹³ 표기법은 양자역학의 공리와 함께 양자역학을 공부할 때 상정하고 들어가는 것 중 하나로, 브라(bra, $\langle \cdot |$)와 켓(ket, $|\cdot\rangle$)을 이용해 벡터와 벡터 연산을 표기하는 방법이다. 이름은 뽀족괄호 $\langle \cdot \rangle$ 을 브라켓(bracket)이라고 하는 것에서 유래했다.

우리는 앞서 벡터의 내적을 이렇게 표기함을 배웠다.

$$\langle v, w \rangle \equiv \langle v | w \rangle = \bar{v}^T \cdot w \quad (3.22)$$

그런데 물리학자들은 이 표기를 반갈죽내서 사용하기로 했다.

$|w\rangle$ 는 우리가 관습적으로 사용하는 일반적인 열 벡터이다. $\langle v|$ 는 \bar{v}^T 로 행벡터이다.

자기 수반 연산자에서 다음이 성립했었다.

$$\langle v | Aw \rangle = \langle Av | w \rangle \quad (3.23)$$

이건 곧

¹³물리학자 폴 디랙(Paul Dirac, 1902 ~ 1984)의 이름을 땄다.

$$\bar{\mathbf{v}}^T \cdot A \cdot \mathbf{w} = (\overline{A\mathbf{v}})^T \cdot \mathbf{w} = \bar{\mathbf{v}}^T A^T \mathbf{w} \quad (3.24)$$

이라는 뜻이므로, 같은 연산에 대해 표기를 다음과 같이 하기도 한다.

$$\langle \mathbf{v} | A \mathbf{w} \rangle = \langle A \mathbf{v} | \mathbf{w} \rangle = \langle \mathbf{v} | A | \mathbf{w} \rangle \quad (3.25)$$

연산자 A 가 양 옆 아무데나 작용할 수 있다는 뜻이다.

III.5. 양자역학에서의 측정

양자계의 속성을 어떻게 측정하여, 물리적인 실험을 진행할 수 있는지 알아보자.

광자의 편광을 복기해 보자. 이 광자의 편광 상태를 어떻게 측정할 수 있을까? 레이저를 쏘서 광자 하나를 진행시킨다고 생각해 보자. 그 진로에는 수직 편광 필터가 놓여있다고 하자. 광자가 이 필터를 통과한다면, 수직 편광된 광자는 필터를 통과하고 수평 편광된 광자는 통과하지 못하고 튕겨나올 것이다. 그런데, 지난번에 광자는 수직이나 수평 편광 상태 이외의 상태들도 가진다고 했었다. 기본 상태가 아닌 상태도 가질 수 있다는 뜻이다.

광자가 α 의 각도로 편광되어 있다고 하자. 그렇다면 그 편광 상태는

$$\psi = \sin \alpha |\uparrow\rangle + \cos \alpha |\rightarrow\rangle \quad (3.26)$$

이제 이 광자가 수직 편광 필터로 들어가면 어떻게 될까? 결론적으로, 이 측정의 결과는 확률적이고, 가능한 결과는 두 가지가 있다.

- $\sin^2 \alpha$ 의 확률로 필터를 통과한다. 이때 광자는 수직 편광 상태가 된다.
- $\cos^2 \alpha$ 의 확률로 필터에서 튕겨나온다. 이때 광자는 수평 편광 상태가 된다.

중요한 것은, 정설로 받아들여지는 코펜하겐 해석에 의하면 광자는 필터에 들어가기 전에는 수직 편광 상태도 수평 편광 상태도 아니었다.

이 측정의 과정에는 두 가지 중요한 특징이 있다. 첫번째는 측정의 결과는 확률적이라는 것이다. 우리는 한 개의 광자로 측정의 결과를 예측할 수 없으며 그 결과는 상태의 확률에 의해 결정된다. 두번째는 측정은 양자계의 상태를 바꾼다는 것이다. 상태에 변화를 주지 않고 측정하는 것은 근본적으로 불가능하다.

이러한 특징들은 양자컴퓨팅을 매우 어렵게 만든다. 어떤 정보가 나올지 알 수 없으며, 그것을 알기 위해 측정을 하면 그 정보는 이미 변형되어서 전에는 어떤 정보가 저장되어 있었는지 알 수 없게 된다. 즉, 측정은 아껴서, 그리고 신중하게 사용해야 하는 것이다. 양

자 알고리즘의 경우, 알고리즘의 맨 마지막 부분에서 한 번만 측정하는 것이 일반적이다.

실제로는 광자 하나를 쏘기가 쉽지 않다. 그것보다는 레이저 빔을 쏘서 광자의 흐름을 만드는 것이 낫다. 그러면 우리는 수많은 측정 결과를 얻을 것이며, 큰수의 법칙에 따라 통계적 확률이 수학적 확률에 근접할 것이다. 여기서 갈라져 나오는 레이저 빔의 세기나 광자의 개수 등을 측정하여 편광 상태의 확률을 알아볼 수 있다.

이제 전자의 스핀을 측정하는 것에 대해 얘기해 보자. 전자의 스핀을 측정하는 방법으로 전자를 강한 자기장 속에 넣고(이 자기장은 연직 위 방향이라고 하자) 그곳에 전자 빔(음극선)을 쏘는 것이다. 그러면 빔이 자기장에 들어갈 때 두 갈래로 나뉘게 된다. 위로 갈라진 빔은 위쪽 스핀을, 아래로 갈라진 빔은 아래 스핀을 가진 전자로 이루어진다. 이때 상태는 다음과 같다.

$$\psi = a|\uparrow_z\rangle + b|\downarrow_z\rangle \quad (3.27)$$

아까와 비슷하게, 측정 결과는 다음과 같다.

- a^2 의 확률로 위쪽 스핀, 새로운 상태는 $|\uparrow_z\rangle$
- b^2 의 확률로 아래쪽 스핀, 새로운 상태는 $|\downarrow_z\rangle$

III.6. 양자역학적 측정의 공리

Axiom 3.6.1 (양자역학적 측정의 공리)

각 측정 실험에 대해 우리는 양자상태의 공간 V 상의 자기 수반 연산자인 관측가능량 A 를 할당할 수 있다. 스펙트럼 정리에 의해, A 는 고유공간을 갖는다. 이것을 분해했을 때 다음과 같다고 하자.

$$V = V_{\lambda_1} \oplus V_{\lambda_2} \oplus \dots \oplus V_{\lambda_k} \quad (3.28)$$

이때 λ_j 는 A 의 실수 고유값이고, V_{λ_j} 는 해당 고유값에 대응하는 고유공간들이다.

양자계 s 가 상태 $v \in V$ 에 있다고 하자. 이 상태 v 를 각 고유공간으로 분해하면 다음과 같다.

$$v = v_1 + \dots + v_k \quad \text{s.t. } v_j \in V_{\lambda_j}, Av_j = \lambda_j v_j \quad (3.29)$$

이 측정을 시행한다면 그 결과는 확률적인데, $|v_j|^2$ 의 확률로 값 λ_j 가 관측되며 양자상태는 상태 $\frac{v_j}{|v_j|}$ 로 붕괴한다. ◆

위 서술에서, 당연히 $|v| = 1$ 이고, 각 기저들은 서로에 대해 직교하므로, 피타고라스 정리의 확장을 생각하면 다음이 성립한다.

$$|v|^2 = |v_1|^2 + \dots + |v_k|^2 \quad (3.30)$$

전자의 스핀을 예로 들어보자. 스핀의 상태벡터는

$$\psi = a|\uparrow_z\rangle + b|\downarrow_z\rangle \quad \text{where } a, b \in \mathbb{C}, |\psi|^2 = |a|^2 + |b|^2 = 1 \quad (3.31)$$

라고 하자.

이때 관측가능량은

$$\frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (3.32)$$

이고, 고유벡터들은 기저벡터들로, 다음과 같다.

$$\begin{aligned} e_1 &= |\uparrow_z\rangle, \lambda_1 = \frac{1}{2} \\ e_2 &= |\downarrow_z\rangle, \lambda_2 = -\frac{1}{2} \end{aligned} \quad (3.33)$$

이 계에 대해 측정을 수행하면, 우리는 $|a|^2$ 의 확률로 스핀 $+\frac{1}{2}$ 를 관측하고, 계는 새로운 상태로 $|\uparrow_z\rangle$ 를 갖게 되며, $|b|^2$ 의 확률로 스핀 $-\frac{1}{2}$ 를 관측하고, 계는 새로운 상태로 $|\downarrow_z\rangle$ 를 갖게 된다.

III.7. 큐비트의 측정

n -큐비트의 양자상태는

$$\psi = \sum_{k=0}^{2^n-1} a_k |k\rangle \quad \text{s.t. } k \in \mathbb{Z} \quad (3.34)$$

였다. 여기서 k 는 10진수로 표현된 정수이다. 큐비트 상태로 작용할 때는 2진수로서의 의미를 갖는다.

양자컴퓨팅에서 우리는 한 가지 관측가능량만 필요한데, 그 관측가능량 A 는 다음을 만족해야 한다.

$$A|k\rangle = k|k\rangle \quad (3.35)$$

이해를 위해 몇 가지 계산 결과 예시를 주자면 아래와 같다.

$$\begin{aligned} A|000\rangle &= 0 \\ A|001\rangle &= |001\rangle \\ A|010\rangle &= 2|010\rangle \\ A|011\rangle &= 3|011\rangle \end{aligned} \quad (3.36)$$

측정의 결과로 우리는 값 k 를 $|a_k|^2$ 의 확률로 얻으며, 계의 새로운 상태는 $|k\rangle$ 가 된다. 이렇게 n -큐비트의 모든 비트를 읽어올 수 있다.

하지만 어떤 때는 특정 비트만 측정할 필요가 있을 때도 있다. 이런 것을 부분 측정이라고 한다. 예를 들어 3-큐비트의 첫 비트만 측정하겠다고 하자. 3-큐비트의 모든 기저 벡터는 2^3 가지로,

$$\begin{aligned} &|000\rangle, |001\rangle, |010\rangle, |011\rangle, \\ &|100\rangle, |101\rangle, |110\rangle, |111\rangle \end{aligned} \quad (3.37)$$

이다. 여기서 맨 앞 비트만 측정한다고 하면, 우리가 관측할 수 있는 값은 상태별로 각각

$$\begin{aligned} &0, 0, 0, 0, \\ &1, 1, 1, 1 \end{aligned} \quad (3.38)$$

이 된다.

이때 관측가능량 A 는 0이 4개, 1이 4개 있는 대각행렬이 된다.

$$A = \begin{bmatrix} 0 & & & & & & \\ & 0 & & & & & \\ & & 0 & & & & \\ & & & 0 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \\ & & & & & & & 1 \end{bmatrix} \quad (3.39)$$

또, 상태벡터는 다음과 같다.

$$\psi = a_0|000\rangle + a_1|001\rangle + \dots + a_7|111\rangle \quad (3.40)$$

여기서 우리는 벡터 공간을 측정값이 0인 것과 1인 것으로 나누어 볼 수 있다. 다음과 같이 생각하면,

$$\begin{aligned} &|000\rangle, |001\rangle, |010\rangle, |011\rangle : \lambda = 0 \\ &|100\rangle, |101\rangle, |110\rangle, |111\rangle : \lambda = 1 \end{aligned} \quad (3.41)$$

전체 벡터공간을 두 개의 부분적 고유공간으로 나누어 볼 수 있다.

$$V = V_0 \oplus V_1 \quad (3.42)$$

그러므로 상태벡터는

$$\begin{aligned} \psi &= \mathbf{v}_0 + \mathbf{v}_1 \\ \text{where } \mathbf{v}_0 &= a_0|000\rangle + \dots + a_3|011\rangle \\ \mathbf{v}_1 &= a_4|100\rangle + \dots + a_7|111\rangle \end{aligned} \quad (3.43)$$

이때 우리는 확률

$$|\mathbf{v}_0|^2 = \sum_{k=0}^3 |a_k|^2 \quad (3.44)$$

로 0을 관측하고 계는 새로운 상태로 $\frac{\mathbf{v}_0}{|\mathbf{v}_0|}$ 를 가진다.

또, 확률

$$|v_1|^2 = \sum_{k=4}^7 |a_k|^2 \quad (3.45)$$

로 1을 관측하고 새로운 상태는 $\frac{v_1}{|v_1|}$ 이 된다.

이렇게 n -큐비트의 상황에서 부분측정이 일어나는 예시를 알아보았다.

III.8. 퍼텐셜 우물에서 입자 물리량의 측정

이번 예시에서는 무한 차원 상태공간의 경우를 보고자 한다. 퍼텐셜 우물 속의 입자에 대해 이야기하자.

상태공간 V 의 파동함수 ψ 들은 $[0, L]$ 의 구간에서 정의되는 복소함수이다.

$$\psi : [0, L] \rightarrow \mathbb{C} \quad (3.46)$$

또,

$$\psi(0) = \psi(L) = 0 \quad (3.47)$$

이 함수들의 에르미트 내적은

$$\langle \psi, \varphi \rangle = \int_0^L \overline{\psi(x)} \varphi(x) dx \quad (3.48)$$

관측가능량으로는 운동량 연산자를 생각해 보자. 이 연산자 \hat{p} 의 식은 다음과 같다¹⁴.

$$\hat{p} = -i\hbar \frac{\partial}{\partial x} \quad (3.49)$$

이 연산자가 함수 ψ 에 작용한다면

$$\hat{p}\psi = -i\hbar \frac{\partial \psi}{\partial x} \quad (3.50)$$

처럼 된다는 뜻이다.

여기서 고유벡터는

$$\hat{p}\psi = \lambda\psi \quad (3.51)$$

¹⁴ \hat{p} 의 꼭지 ^은 hat이라고 하며, 말 그대로 모자 씌운 것과 비슷하다. 일반적으로 양자역학에서는 hat을 씌워 연산자라는 것을 표시한다. 본 문서에서는 편의를 위해 씌웠다가 안 씌웠다가 혼용하지만 씌우지 않을 경우 연산자라는 것을 명시한다.

이 식은 미분방정식이다.

$$\begin{aligned} -i\hbar \frac{\partial \psi}{\partial x} &= \lambda \psi \\ \frac{\partial \psi}{\partial x} &= \frac{\lambda i}{\hbar} \psi \end{aligned} \quad (3.52)$$

해를 쉽게 구할 수 있다.

$$\psi(x) = C \exp\left(-\frac{\lambda i}{\hbar} x\right) \quad (3.53)$$

여기서 C 는 정규화 상수이다.

이 고유함수들은 평면파로, 크기가 항상 1이기 때문에 앞서 정해둔 조건 $\psi(0) = \psi(L) = 0$ ¹⁵을 만족하지 않음을 확인할 수 있다. 이 때문에 일반적인 운동량 고유상태는 퍼텐셜 우물의 경계 조건을 만족하지 않는다.

지난번에 우리는 슈뢰딩거 방정식을 이용해 경계 조건을 만족하는 기본적인 해를 구해 보았다.

$$\psi = \sin \lambda_k x \quad (3.54)$$

이 사인 함수들은 지수 꼴로 나타낼 수 있다¹⁶.

$$\sin \lambda_k x = \frac{\exp(\lambda_k i x) - \exp(-\lambda_k i x)}{2i} \quad (3.55)$$

각 지수항은 \hat{p} 의 고유함수이다.

$$\begin{aligned} \hat{p} e^{i\lambda_k x} &= (+\hbar \lambda_k) e^{i\lambda_k x} \\ \hat{p} e^{-i\lambda_k x} &= (-\hbar \lambda_k) e^{-i\lambda_k x} \end{aligned} \quad (3.56)$$

즉 $\frac{1}{2}$ 의 확률로 운동량 $\hbar \lambda_k$, $\frac{1}{2}$ 의 확률로 운동량 $-\hbar \lambda_k$ 를 갖는다.

Exercise. 운동량 연산자 \hat{p} 가 자기 수반 연산자임을 보여라.

Solution. $\langle \psi | \hat{p} \phi \rangle = \langle \hat{p} \psi | \phi \rangle$ 임을 보이면 된다.

¹⁵이런 조건을 디리클레(Johann Dirichlet, 1805 ~ 1859) 경계 조건이라고 한다.

¹⁶왜인지 모르겠다면 오일러 공식 $e^{ix} = \cos x + i \sin x$ 으로 유도해 보아라. 다른 방법은 $\cosh x = \cos ix$, $\sinh x = \sin ix$ 라는 것을 이용하는 것이다.

$$\begin{aligned} \text{LHS} &= \int_0^L \overline{\psi(x)} \cdot i\hbar \varphi(x) dx \\ &= \cancel{i\hbar \overline{\psi} \varphi} \Big|_{x=0}^{x=L} - \int_0^L i\hbar \frac{d\overline{\psi}}{dx} \varphi(x) dx \end{aligned} \quad (3.57)$$

$$\because \psi(0) = \psi(L) = 0$$

이고

$$\begin{aligned} \text{RHS} &= \int_0^L i\hbar \overline{\psi(x)} \cdot \varphi(x) dx \\ &= - \int_0^L \hbar \frac{d\overline{\psi}}{dx} \varphi(x) dx \end{aligned} \quad (3.58)$$

따라서

$$\boxed{\hat{p} = \hat{p}^\dagger} \quad (3.59)$$

즉, \hat{p} 는 자기 수반 연산자이다.

■

주의할 것은, 엄밀하게 말하면 디리클레 경계 조건 하에서 정의한 운동량 연산자는 대칭이지만 일반적으로 자기 수반은 아니다.

또 하나 자연스럽게 측정할 수 있는 관측가능량은 위치이다. 위치연산자를 다음과 같다고 하자.

$$\hat{x} = x \quad (3.60)$$

$x \in \mathbb{R}$ 이므로,

$$\langle \psi | \hat{x} \varphi \rangle = \int_0^L \overline{\psi(x)} x \varphi(x) dx = \int_0^L x \overline{\psi(x)} \varphi(x) dx = \langle \hat{x} \psi | \varphi \rangle \quad (3.61)$$

와 같이 자명하게 자기 수반 연산자이다.

x 의 고유함수는 일반화 함수라고 하는 것들로, 델타함수(Dirac delta)라고 한다. 델타함수는 쉽게 말해 어떤 위치 $x = a$ 외에서는 그 값이 0인 함수를 말한다. a 에서의 값은 무한대라고 두는 것이 보통이다. 델타함수는 다음과 같은 성질이 있다.

$$\int_0^L \delta_a(x) \varphi(x) dx = \varphi(a) \quad (3.62)$$

즉 델타함수는 구간 $[0, L]$ 에서의 함수가 아니라, V 상의 선형 사상으로 보아야 한다¹⁷.

델타함수는 아래와 같은 성질도 가진다. 즉 \hat{x} 의 고유함수가 된다.

$$x\delta_a(x) = a\delta_a(x) \quad (3.63)$$

III.9. 두 물리량의 동시 측정

두 관측가능량에 대해, 그에 각각 대응하는 연산자 A, B 에 대해 아래가 성립하면 두 양을 동시에 측정할 수 있다.

$$A \cdot B = B \cdot A \quad (3.64)$$

이런 것을 가환(可換, commutable)이라고 하며, 두 연산자가 공통된 고유벡터 기저를 가지고 있다는 뜻과 같다.

특히, n -큐비트에 대해 그 기저 고유벡터가 모두 같으므로 모든 큐비트의 값을 동시에 측정할 수 있다.

전자의 스핀을 예시로 들어보자. 모든 방향으로 측정이 가능하므로, 각 방향의 관측가능량을 살펴보자. 먼저, x 방향으로의 측정 연산자는 아래와 같다.

$$\frac{1}{2}\sigma_1 = \frac{1}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (3.65)$$

y 방향으로의 연산자는

$$\frac{1}{2}\sigma_2 = \frac{1}{2} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad (3.66)$$

z 방향에 대응하는 관측가능량은

$$\frac{1}{2}\sigma_3 = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (3.67)$$

이때 $\sigma_1, \sigma_2, \sigma_3$ 은 파울리 행렬이다. 각 행렬은 자기 수반이다. 실수부는 대칭이고 허수부는 반대칭이기 때문이다. 하지만, 이 행렬들은 비가환이다($\sigma_j \sigma_k \neq \sigma_k \sigma_j$). 즉, 서로 다른 방향에 대한 전자의 스핀은 동시에 측정할 수 없다. 실험적으로 생각해 보자. 전자의 스핀

¹⁷델타함수는 일반적인 함수가 아니며, 일반화 함수(generalized function)이다.

을 측정하려면 전자를 강한 자기장 안에 넣어야 했었다. 그런데 상식적으로, 한 번에 두 방향의 자기장을 한꺼번에 걸 수 있는가? 물론 가능이야 하겠지만 자기장은 합성이 될 것이지 각각의 순수한 방향에 대한 측정 결과를 내놓지 못할 것이다.

비슷하게 퍼텐셜 우물 속 입자도 살펴보자. 우리는 두 관측가능량을 보았다.

$$\begin{aligned}\hat{p} &= -i\hbar \frac{\partial}{\partial x} \\ \hat{x} &= x\end{aligned}\tag{3.68}$$

이제 두 연산자의 곱을 보자.

$$\begin{aligned}\hat{p}\hat{x}(\psi) &= -i\hbar \frac{\partial}{\partial x}[x\psi(x)] \\ &= -i\hbar[\psi(x) + x\psi'(x)]\end{aligned}\tag{3.69}$$

또,

$$\hat{x}\hat{p}(\psi) = -i\hbar x\psi'(x)\tag{3.70}$$

그러므로 $\hat{p}\hat{x} \neq \hat{x}\hat{p}$ 이다. 즉, 퍼텐셜 우물 속 입자의 위치와 운동량을 동시에 측정할 수 없다. 우리가 살펴본 운동량 연산자와 위치 연산자는 우리가 앞서 상정한 퍼텐셜 우물의 디리클레 조건 외에서도 성립하므로, 일반적으로 입자의 위치와 운동량은 동시에 측정할 수 없다는 결론이 나온다. 이것은 하이젠베르크(Werner Heisenberg, 1901 ~ 1976)의 불확정성 원리(uncertainty principle)로 귀결된다.

Theorem 3.9.1 (불확정성 원리)

두 관측가능량 \hat{A}, \hat{B} 에 대해 다음이 성립한다.

$$\Delta A \Delta B \geq \left(\frac{1}{2}\right) |\langle [\hat{A}, \hat{B}] \rangle|\tag{3.71}$$

Proof. 먼저 다음을 상정한다. 아래 둘은 쉽게 증명 가능하므로 증명은 따로 하지 않는다.

- 에르미트 연산자의 기댓값은 실수이다.
- 반 에르미트 연산자¹⁸의 기댓값은 순허수이다.

이제 다음의 연산자를 약속하자.

¹⁸ $\hat{A}^\dagger = -\hat{A}$ 를 만족하는 연산자

$$\Delta\hat{A} = \hat{A} - \langle A \rangle \quad (3.72)$$

즉, 본래의 연산자에서 기댓값을 뺀 형태이다.

참고로

$$\begin{aligned} \langle (\Delta\hat{A})^2 \rangle &= \langle (\hat{A} - \langle A \rangle)^2 \rangle \\ &= \langle \hat{A}^2 - 2\hat{A}\langle A \rangle + \langle A \rangle^2 \rangle \\ &= \langle \hat{A}^2 \rangle - \langle A \rangle^2 \\ &= (\Delta A)^2 \end{aligned} \quad (3.73)$$

으로 분산이 된다. ΔA 는 표준편차이다¹⁹.

코시-슈바르츠 부등식에 의해 다음이 성립한다.

$$\langle |\alpha\rangle\langle\alpha| \rangle, \langle |\beta\rangle\langle\beta| \rangle \geq |\langle |\alpha\rangle\langle\beta| \rangle|^2 \quad (3.74)$$

이제 임의의 $|\xi\rangle$ 에 대해

$$\begin{aligned} |\alpha\rangle &= \Delta\hat{A}|\xi\rangle \\ |\beta\rangle &= \Delta\hat{B}|\xi\rangle \end{aligned} \quad (3.75)$$

라 놓자. 한편, $\Delta\hat{A}$ 는 쉽게 에르미트 연산자임을 보일 수 있어

$$\begin{aligned} \langle |\alpha\rangle\langle\alpha| \rangle &= \langle (\Delta\hat{A})^2 \rangle \langle |\beta\rangle\langle\beta| \rangle \\ &= \langle (\Delta\hat{B})^2 \rangle \langle |\alpha\rangle\langle\beta| \rangle \\ &= \langle \Delta\hat{A}\Delta\hat{B} \rangle \end{aligned} \quad (3.76)$$

가 되고, 다음을 얻는다.

$$\langle (\Delta\hat{A})^2 \rangle \langle (\Delta\hat{B})^2 \rangle \geq |\langle \Delta\hat{A}\Delta\hat{B} \rangle|^2 \quad (3.77)$$

위에서 논한 결과로 대치하면,

$$(\Delta A)^2 (\Delta B)^2 \geq |\langle \Delta\hat{A}\Delta\hat{B} \rangle|^2 \quad (3.78)$$

¹⁹경우에 따라 σ_A 와 같이 쓰기도 한다.

이제, 우변의 항을 구하는 것으로 귀결된다.

$$\Delta\hat{A}\Delta\hat{B} = \left(\frac{1}{2}\right)[\Delta\hat{A}, \Delta\hat{B}] + \left(\frac{1}{2}\right)\{\Delta\hat{A}, \Delta\hat{B}\} \quad (3.79)$$

으로 교환자와 반교환자의 합으로 구성할 수 있다.

한편, 여기서 $[\Delta\hat{A}, \Delta\hat{B}]$ 라는 연산자는 반 에르미트 연산자, $\{\Delta\hat{A}, \Delta\hat{B}\}$ 라는 연산자는 에르미트 연산자인데,

$$\langle\Delta\hat{A}\Delta\hat{B}\rangle = \left(\frac{1}{2}\right)\langle[\Delta\hat{A}, \Delta\hat{B}]\rangle + \left(\frac{1}{2}\right)\langle\{\Delta\hat{A}, \Delta\hat{B}\}\rangle \quad (3.80)$$

으로 쓸 수 있다.

위의 논의대로, 좌변의 1항은 실수가, 2항은 순허수가 나올 것이다. 이상에서

$$\begin{aligned} & |\langle\Delta\hat{A}\Delta\hat{B}\rangle|^2 \\ &= \left(\frac{1}{4}\right)|\langle[\Delta\hat{A}, \Delta\hat{B}]\rangle|^2 + \left(\frac{1}{4}\right)|\langle\{\Delta\hat{A}, \Delta\hat{B}\}\rangle|^2 \geq \left(\frac{1}{4}\right)|\langle[\Delta\hat{A}, \Delta\hat{B}]\rangle|^2 \end{aligned} \quad (3.81)$$

이상에서 다음의 결론을 얻는다.

$$\Delta A \Delta B \geq \left(\frac{1}{2}\right)|\langle[\Delta\hat{A}, \Delta\hat{B}]\rangle| \quad (3.82)$$

쉽게 $[\Delta\hat{A}, \Delta\hat{B}] = [\hat{A}, \hat{B}]$ 임을 증명 가능하므로 최종적으로

$$\boxed{\Delta A \Delta B \geq \left(\frac{1}{2}\right)|\langle[\hat{A}, \hat{B}]\rangle|} \quad (3.83)$$

□

특히, 위치와 운동량에 대해 둘은 정준교환자(canonical commutator)

$$[\hat{x}, \hat{p}] = i\hbar \quad (3.84)$$

이므로,

$$\Delta x \Delta p \geq \frac{\hbar}{2} \quad (3.85)$$

이 성립한다²⁰.

²⁰이 부분은 양자컴퓨팅이 아니라 양자역학의 영역이므로 이해가 안 된다면 넘어가도 된다.

IV. 유니터리 연산자

이번에는 양자계의 시간 변화(evolution)에 대해 알아보도록 하겠다.

IV.1. 양자계의 시간 변화와 유니터리 연산자

Definition 4.1.1 (유니터리 연산자)

닫힌 양자계의 시간 변화는 유니터리 연산자로 주어진다. V 를 양자계의 상태의 에르미트 공간이라고 하자. 수학적으로 V 는 에르미트 내적이 성립하는 복소벡터공간이다.

어떤 연산자 $U : V \rightarrow V$ 는 다음을 만족하면 유니터리(unitary) 연산자라고 한다.

$$\forall u, v \in V \quad \langle Uu | Uv \rangle = \langle u | v \rangle \quad (4.1)$$

유니터리 연산자의 조건은 아래와 같이 서술할 수도 있다.

$$U^\dagger U = I \quad (4.2)$$

이때 I 는 단위행렬이다.

이는 다음과 동치이다.

$$U^\dagger = U^{-1} \quad (4.3)$$

유니터리 연산자는 표준기저의 정규직교성(orthonormality)을 보존한다.

Definition 4.1.2 (표준기저)

어떤 벡터공간에서 가장 기본적인 방향을 나타내는 벡터의 집합을 표준기저 (standard basis)라고 한다.

예를 들어 3차원 실수 공간 \mathbb{R}^3 에서 표준기저는

$$\mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \mathbf{e}_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \quad (4.4)$$

과 같으며²¹, 각각 x, y, z 좌표축 방향과 일치한다. 이때 이 공간 상의 점 $P(2, 3, 1)$ 의 위치벡터 \mathbf{P} 는

$$\mathbf{P} = 2\mathbf{e}_1 + 3\mathbf{e}_2 + \mathbf{e}_3 \quad (4.5)$$

이 된다.

Definition 4.1.3 (정규직교기저)

정규직교기저(orthonormal basis)란 서로 직교(orthogonal)하면서 크기가 1로 정규화된(normalized) 벡터의 집합이다. 즉, 벡터 $\mathbf{u}_i, \mathbf{u}_j$ 에 대해 다음이 성립하면 두 벡터는 정규직교기저이다.

- 직교: $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$
- 정규화: $|\mathbf{u}_i| = |\mathbf{u}_j| = 1$

예를 들어 n 차원 표준기저도 정규직교기저이다.

정규직교기저의 내적은 다음과 같이 쉽게 계산할 수 있다²².

$$\langle \mathbf{u}_i, \mathbf{u}_j \rangle = \delta_{ij} \quad (4.6)$$

양자역학에서 상태벡터를 정규직교기저로 나타내면 계산이 매우 간단해진다는 장점이 있다.

간단히 설명해서, 표준기저에 대해서는

²¹물론 표기는 \mathbf{e}_x 로 하던 \hat{x} 로 하던 혼동만 되지 않으면 상관 없다.

²² δ_{ij} 는 크로네커 델타(Kronecker delta)라고 하며, $\delta_{ij} = \begin{cases} 1 & (i=j) \\ 0 & (i \neq j) \end{cases}$ 이다. 즉 두 매개변수가 같으면 1, 아니면 0을 반환하는 함수이다.

$$\langle e_i | e_j \rangle = \delta_{ij} \quad (4.7)$$

이 성립하는데, 여기에 U 가 작용해도 여전히

$$\langle Ue_i | Ue_j \rangle = \langle e_i | e_j \rangle = \delta_{ij} \quad (4.8)$$

이 성립하여 내적이 보존된다.

원래 표준기저는 정규직교기저이다. 즉 표준기저 $|e_i\rangle$ 의 집합 $\{|e_i\rangle\}$ 는 정규직교기저의 집합이다. 이때 U 가 작용한 벡터의 집합 $\{Ue_i\}$ 도 정규직교벡터의 집합이 된다는 뜻이다.

Exercise. $\forall u, v \in V = \mathbb{C}^N$ 에 대해

$$\langle u | v \rangle = u^\dagger v \quad (4.9)$$

이고

$$\langle Uu | Uv \rangle = (Uu)^\dagger Uv = u^\dagger U^\dagger Uv \quad (4.10)$$

이다. 이를 이용하여 유니터리 연산자의 정의 $U^\dagger U = I$ 를 유도하여라.

Solution.

$$\langle Uu | Uv \rangle = u^\dagger U^\dagger Uv = u^\dagger v \quad (4.11)$$

이므로 $\forall u, v \in V = \mathbb{C}^N$ 에 대해

$$u^\dagger (U^\dagger U)v = u^\dagger v = u^\dagger Iv \quad (4.12)$$

여야 한다.

즉,

$$\boxed{U^\dagger U = I} \quad (4.13)$$

■

$U^\dagger U = I$ 라는 것은 다음과도 동치이다.

$$U^\dagger = U^{-1} \quad (4.14)$$

IV.2. 유니터리 연산자의 고윳값과 고유벡터

Theorem 4.2.1 (유니터리 연산자의 고윳값과 고유벡터)

에르미트 벡터공간 V 상의 연산자 U 가 유니터리 연산자라고 하자. 이때 다음이 성립한다.

1. U 의 고윳값은 크기가 1인 복소수이다.
2. 서로 다른 고윳값에 대응하는 U 의 고유벡터는 서로에 대해 직교한다.

Proof.

1. $U\mathbf{v} = \lambda\mathbf{v}$ 라고 하자. 이때

$$\langle U\mathbf{v}|U\mathbf{v} \rangle = \langle \lambda\mathbf{v}|\lambda\mathbf{v} \rangle = \lambda\bar{\lambda}\langle \mathbf{v}|\mathbf{v} \rangle = |\lambda|^2\langle \mathbf{v}|\mathbf{v} \rangle = \langle \mathbf{v}|\mathbf{v} \rangle \quad (4.15)$$

그런데, $\mathbf{v} \neq 0$ 이라면 $\langle \mathbf{v}|\mathbf{v} \rangle \neq 0$ 이므로 $|\lambda| = 1$ 이다.

2. $U\mathbf{u} = \lambda\mathbf{u}, U\mathbf{w} = \mu\mathbf{w}$ 라고 하자. 그러면

$$\langle U\mathbf{u}|U\mathbf{w} \rangle = \langle \lambda\mathbf{u}|\mu\mathbf{w} \rangle = \lambda\bar{\mu}\langle \mathbf{u}|\mathbf{w} \rangle = \frac{\mu}{\lambda}\langle \mathbf{u}|\mathbf{w} \rangle \quad (4.16)$$

그런데, $\langle U\mathbf{u}|U\mathbf{w} \rangle = \langle \mathbf{u}|\mathbf{w} \rangle$ 이므로

$$\left(1 - \frac{\mu}{\lambda}\right)\langle \mathbf{u}|\mathbf{w} \rangle = 0 \quad (4.17)$$

이때 $\mu \neq \lambda$ 이면 $1 - \frac{\mu}{\lambda} \neq 0$ 이므로 $\langle \mathbf{u}|\mathbf{w} \rangle = 0$ 이다. \square

Theorem 4.2.2 (유니터리 연산자의 스펙트럼 정리)

유한차원 에르미트 공간 V 상의 유니터리 연산자 U 는 대각화 가능(diagonalizable)하다. U 는 크기가 1인 고윳값을 가진 고유벡터들로 이루어진 정규직교기저를 갖는다.

어떤 행렬 A 가 대각화 가능하다는 것은, 적절한 기저를 택하면 A 를 대각행렬로 표현할 수 있다는 뜻이다.

$$A = PDP^{-1} \quad (4.18)$$

이때 D 는 대각행렬, P 의 열벡터들은 A 의 고유벡터들, D 의 대각성분은 A 의 고윳값들이다. 즉, 대각화는 복잡한 행렬을 각 고윳값에 대응하는 축으로 분해하는 것과 같다.

유니터리 연산자가 대각화 가능한 고유벡터를 가지므로 유니터리 연산자는 대각화하면 이런 식으로 생겼다는 뜻이다.

$$U = \begin{bmatrix} e^{i\alpha_1} & & & \\ & e^{i\alpha_2} & & \\ & & \ddots & \\ & & & e^{i\alpha_N} \end{bmatrix} \quad (4.19)$$

$e^{i\alpha_i}$ 가 고윳값이므로, 만약 $|\lambda_i| = 1$ 이라면 λ_i 는 아래와 같이 쓸 수 있다.

$$\lambda_i = e^{i\alpha_i} = \cos \alpha_i + i \sin \alpha_i \quad \text{where } \alpha_i \in \mathbb{R} \quad (4.20)$$

λ_i 는 복소평면에서 편각 α_i 를 가지고 크기가 1인 벡터가 된다.

IV.3. 양자계의 시간변화

다시 양자계의 시간 변화로 돌아와 보자. 초기 상태 ψ_0 는 시간 $t = 0$ 일 때의 초기 상태라고 하자. 이때 이렇게 표현할 수 있다.

$$\psi(t) = U(t)\psi_0 \quad (4.21)$$

U 는 유니터리 변환의 모임이다. 계의 시간변화를 제어하기 위해서는 $U(t)$ 의 값들을 제어할 수 있다. 물리적으로는 계에 영향을 주는 자기장을 조작한다거나, 계에 레이저를 쏠 때 그 레이저의 세기나 파장을 조정할 수 있다. 즉 양자계의 시간변화는 다양하게 일어날 수 있다.

양자 계산의 일반적인 절차는 세 단계로 나뉜다.

1. 초기화(initialization)
2. 양자 알고리즘 적용
3. 측정

초기화는 초기 상태를 준비하는 단계이다. 이 벡터는 양자 알고리즘의 입력이다. 양자 알고리즘은 유니터리 연산자이다²³. 유니터리 연산자는 연산 적용 후에도 벡터의 내적을 보존하므로 크기를 보존한다²⁴. 측정 단계에서는 관측을 하여 확률적인 결과를 얻는다.

²³여러 연산자의 합성도 결국 하나의 연산자와 같다.

²⁴벡터의 크기는 자신과의 내적으로 표현되기 때문이다.

IV.4. 군론 기초

여기서 우리는 군론(group theory) 기초를 다지고 넘어갈 필요가 있다. 첫째로, 양자 알고리즘을 더 잘 이해하기 위함이고, 둘째로 암호학을 이해하기 위해 군론이 필요하기 때문이다. 군의 정의로 시작해보자.

Definition 4.4.1 (군)

군 G 는 이항연산이 주어진 집합으로, 연산과 그 연산의 대상이 되는 집합을 묶어 표현한다.

집합 G 의 이항연산을 $*$: $G \times G \rightarrow G$ 라고 할 때, $\forall a, b, c \in G$ 에 대해 $*$ 이 다음을 만족하면 $(G, *)$ 를 군이라고 한다.

1. 결합법칙

$$(a * b) * c = a * (b * c) \quad (4.22)$$

2. 항등원의 존재

$\exists e \in G$ 에 대해

$$a * e = a = e * a \quad (4.23)$$

가 성립하면 e 는 $*$ 의 항등원이고, 항등원의 존재는 유일하다. 따라서 이 원소를 $1, e, i$ 따위로 표기한다.

3. $a \in G$ 에 대해 $x \in G$ 가 존재하여

$$a * x = e = x * a \quad (4.24)$$

가 성립하면 x 는 $*$ 의 역원이고, 역원의 존재는 유일하다. 따라서 이 원소를 a^{-1} 로 표기한다.

Problem. 군 $(G, *)$ 의 항등원 e 와 역원 x 가 유일함을 보여라.

Solution.

1. 또 다른 항등원을 f 라고 하면

$$e = e * f = f \quad (4.25)$$

이므로 $e = f$ 이다. 즉, 항등원은 유일하다.

2. 또 다른 역원을 y 라고 하면

$$x = x * e = x * (a * y) = (x * a) * y = e * y = y \quad (4.26)$$

이므로 $x = y$ 이다. 즉, 역원은 유일하다.

아래는 흔하고 자주 등장하는 군의 예시이다.

Definition 4.4.2 (일반선형군)

$n \times n$ 실수 가역행렬들의 집합을 $GL(n, \mathbb{R})$ 또는 $GL_n(\mathbb{R})$ 이라 쓰고 n 차 일반선형군 (general linear group)이라고 한다.

$$GL_n(\mathbb{R}) := M_{n \times n}(\mathbb{R}) \setminus \{A \in M_{n \times n}(\mathbb{R}) \mid \det A = 0\} \quad (4.27)$$

$GL_n(\mathbb{C})$ 는 복소 가역행렬들의 집합이다. 행렬곱에 대해 그 항등원은 단위행렬 I 가 된다.

Definition 4.4.3 (특수선형군)

행렬식이 1인 $n \times n$ 실수 행렬들의 집합을 $SL(n, \mathbb{R})$ 또는 $SL_n(\mathbb{R})$ 이라고 쓰고 n 차 특수선형군(special linear degree)이라고 한다.

$$SL_n(\mathbb{R}) := \{A \in M_{n \times n}(\mathbb{R}) \mid \det A = 1\} \quad (4.28)$$

특수선형군에 속한 두 행렬 A, B 에 대해 $\det A = \det B = 1$ 이므로 $\det A \cdot \det B = \det AB = 1$ 이 된다. 마찬가지로 $SL_n(\mathbb{C})$ 는 행렬식이 1인 복소행렬들의 집합이다.

Definition 4.4.4 (유니터리 군)

$n \times n$ 유니터리 행렬들의 집합을 $U(n)$ 또는 U_n 이라고 쓰고 n 차 유니터리 군(unitary group)이라고 한다.

$$U_n := \{A \in M_{n \times n}(\mathbb{C}) \sim GL_n(\mathbb{C}) \mid A^\dagger A = I\} \quad (4.29)$$

Lemma 4.4.5 (유니터리 군과 일반선형군)

유니터리 군 U_n 은 일반선형군 $GL_n(\mathbb{C})$ 의 부분집합이자 부분군이다.

1. $I \in U_n \quad I^\dagger I = I$
2. $A, B \in U_n \Rightarrow A \cdot B \in U_n$

또, U_n 상의 모든 행렬은 가역이다. 다음을 확인하자.

$$(AB)^\dagger \cdot (AB) = A^\dagger B^\dagger AB = I \quad (4.30)$$

3. $X \in U_n \Rightarrow X^{-1} \in U_n$

Definition 4.4.6 (특수 유니터리 군)

행렬식이 1인 $n \times n$ 유니터리 행렬들의 집합을 $SU(n)$ 또는 SU_n 이라고 쓰고 n 차 특수 유니터리 군(special unitary group)이라고 한다.

$$\begin{aligned} SU_n &:= \{A \in M_{n \times n}(\mathbb{C}) \mid A^\dagger A = I \wedge \det A = 1\} \\ &= U_n \cap SL_n(\mathbb{C}) \end{aligned} \quad (4.31)$$

이상에서

$$SU_n \subset U_n \subset GL_n(\mathbb{C}) \quad (4.32)$$

유니터리 군은 양자 이론에서 다양한 부분을 차지하며, 한 가지 작은 예시로, 기본 입자의 표준 모형은 유니터리 군에서 기인한다. 기본입자를 표현하기 위해 아래와 같은 식을 쓴다.

$$U_1 \times SU_2 \times SU_3 \quad (4.33)$$

U_1 은 전자기력, SU_2 는 약한 핵력, SU_3 은 쿼크와 강한 핵력에 관련돼 있다.

V. 양자 얽힘

이번에는 양자 얽힘 현상에 대해 이야기해보겠다. 양자 컴퓨팅은 양자 얽힘 없이는 불가능할 정도로, 양자 얽힘은 양자 컴퓨팅에서 큰 부분을 차지한다.

V.1. 텐서곱

텐서 곱의 정의로부터 시작하겠다.

Definition 5.1.1 (텐서곱)

U 를 기저 $\{u_1, \dots, u_n\}$ 을 갖는 벡터공간, V 를 기저 $\{v_1, \dots, v_k\}$ 를 갖는 벡터공간이라고 하자. 이때 텐서곱 $U \otimes V$ 는

$$U \otimes V = \{u_i \otimes v_j \mid i = 1, \dots, n \wedge j = 1, \dots, k\} \quad (5.1)$$

이때 $\dim(U \otimes V) = \dim U \times \dim V$ 이다.

\otimes 기호는 u 와 v 를 엮어 합친 새로운 벡터를 만드는 역할 정도로 보면 된다. 수학적으로는 다음과 같이 정의된다.

$$\otimes : U \times V \rightarrow U \otimes V \quad (5.2)$$

즉 $u \in U, v \in V$ 일 때

$$(u, v) \mapsto u \otimes v \quad (5.3)$$

이때 \otimes 은 쌍선형으로, 쌍선형곱

$$\left(\sum_{i=1}^n a_i u_i \right) \otimes \left(\sum_{j=1}^k b_j v_j \right) = \sum_{i=1}^n \sum_{j=1}^k a_i b_j (u_i \otimes v_j) \quad (5.4)$$

이 성립한다.

V.2. 다중 양자계의 상태공간

텐서곱은 두 양자계를 결합해 볼 수 있게 한다.

Theorem 5.2.1 (상호작용하는 두 양자계의 합성 상태공간)

상태공간으로 각각 U, V 를 가지는 두 양자계가 있을 때, 두 계의 상태공간을 합성하여 하나로 본 상태공간은 $U \otimes V$ 이다.

이때 이 새로운 상태공간 $U \otimes V$ 에서의 내적은

$$\langle u_1 \otimes v_1 | u_2 \otimes v_2 \rangle = \langle u_1 | u_2 \rangle \cdot \langle v_1 | v_2 \rangle \quad (5.5)$$

이제 이것을 가지고 n -큐비트를 생각해 보자. 먼저, 단일 큐비트의 경우는 큐비트 상태공간 $B = \mathbb{C}^2$ 을 가지고, 기저는 $\{|0\rangle, |1\rangle\}$ 이다. 2-큐비트는 상태공간 $B \otimes B$ 를 가지고 기저는 $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$ 이다.

우리는 앞서 다주 큐비트를 간단히 줄여 나타내는 방법을 보았었다. 2-큐비트의 기저를 이 방법으로 표현하면 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 이 된다. 이 표현법에는 아래와 같은 정의가 내포되어 있다.

$$|a_1\rangle \otimes \dots \otimes |a_n\rangle = |a_1 \dots a_n\rangle \quad (5.6)$$

n -큐비트는 상태공간으로 $B_n = \underbrace{B \otimes B \otimes \dots \otimes B}_n$, 기저로는 $\left\{ \overbrace{|00\dots 0\rangle}^n, \dots, \overbrace{|11\dots 1\rangle}^n \right\}$ 를 갖는다.

이때 $\dim B_n = 2^n$ 이다.

예를 들어, 서로 상호작용하지 않는 두 입자가 각각 상태 $\psi_1 = a|0\rangle + b|1\rangle$ 과 $\psi_2 = c|0\rangle + d|1\rangle$ 을 가질 때, 합성된 상태는

$$\begin{aligned} \psi_1 \otimes \psi_2 &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \end{aligned} \quad (5.7)$$

Problem. 임의의 2-큐비트 상태는 $\psi_1 \otimes \psi_2$ 꼴로 분해될 수 있는가?

Solution. 없다. $z_1|00\rangle + z_2|01\rangle + z_3|10\rangle + z_4|11\rangle = \psi_1 \otimes \psi_2$ 이려면 $z_2z_3 = z_1z_4$ 이어야 하는데, 항상 그런 것은 아니기 때문이다. 예를 들어 흔하다고 할 수 있는 상태 $\psi = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ 은 $\psi_1 \otimes \psi_2$ 로 표현될 수 없다.

V.3. 양자 얽힘의 정의

Definition 5.3.1 (양자 얽힘)

어떤 양자계가 각각 상태공간 U, V 를 가지는 각각의 두 부분으로 되어 있다고 하자. 이때 이 다중 양자계의 상태 $\varphi \in U \otimes V$ 는 $\psi_1 \in U, \psi_2 \in V$ 에 대해 $\varphi \neq \psi_1 \otimes \psi_2$ 이면 얽혀 있다고 한다.

얽혀 있지 않은 상태는 상호작용하지 않는 입자들을 의미한다. 얽힌 상태는 자명하지 않은(nontrivial) 상호작용을 하는 입자들을 의미한다.

예를 들어 보자. 어떤 점에서 서로 반대방향으로 광자를 한 개씩 쏜다고 해보자. 한쪽 끝에는 관찰자 A, 다른쪽 끝에는 관찰자 B가 있다. 이때 이 광자의 편광 상태를 큐비트로 이용할 수 있다. 이 두 광자의 큐비트 상태를 하나로 합쳐 ψ 라고 하고, 현재 상태는 이렇다고 하자.

$$\psi = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \quad (5.8)$$

A가 자신에게 도달한 광자를 관측하면 한 쪽 광자만 보게 된다. A가 보는 광자를 첫째 큐비트라고 하겠다. 첫째 큐비트의 값은 50% 확률로 $|0\rangle$, 50% 확률로 $|1\rangle$ 이 된다. 그와 동시에, 상태벡터에 따라 둘째 큐비트의 상태도 정해지게 된다. 관측이 일어나면 상태가 하나로 정해지면서 붕괴하므로, A가 $|0\rangle$ 을 관측했다면 광자의 상태는 $|00\rangle$ 이 되고, $|1\rangle$ 을 관측했다면 상태는 $|11\rangle$ 이 된다. 이렇게 되면, A가 관측한 결과에 따라 B의 관측 결과가 확정적으로 정해지게 된다. 둘째 큐비트도 A가 관측한 첫째 큐비트에 따라 정해지기 때문이다.

즉, A와 B의 관측은 서로에 대해 종속되어 있는데, 둘은 모두 $|00\rangle$ 또는 $|11\rangle$ 을 관측하게 된다. 이게 무슨 일인가? 이것을 제대로 이해하기 위해서는 조건부 확률을 복습해야할 것이다.

Definition 5.3.2 (조건부 확률)

두 사건 A, B 에 대해 B 가 일어날 때 A 가 일어날 확률은

$$\Pr(A | B) = \frac{\Pr(A \cap B)}{\Pr(B)} \quad (5.9)$$

이러한 확률을 조건부 확률(conditional probability)라고 한다.

Definition 5.3.3 (사건의 독립)

두 사건 A, B 는 다음을 만족시키면 서로 독립이다.

$$\Pr(A \cap B) = \Pr(A) \Pr(B) \quad (5.10)$$

독립이란 두 사건이 서로가 일어날 확률에 영향을 주지 않는다는 뜻으로, 위 정의는 아래와 동치이다.

$$\Pr(A|B) = \Pr(A) \wedge \Pr(B|A) = \Pr(B) \quad (5.11)$$

이제 다시 아까 예시로 돌아가 보면, A 가 0을 관측했을 때 B 가 0을 관측할 확률은 1이지만, B 가 0을 관측할 확률은 0.5이다. 즉 두 사건은 독립이 아니다. 사건이 독립이 아니라면 종속이며, 이 종속 관계는 양자 얽힘에서 기인한다.

Problem. ψ_1, ψ_2 에 대해 얽힘이 없는 합성 큐비트 상태 $\psi_1 \otimes \psi_2$ 는 관측 사건이 서로 독립임을 보여라.

Solution.

$$\begin{aligned} \psi &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \\ \text{s.t. } |a|^2 + |b|^2 &= |c|^2 + |d|^2 = 1 \end{aligned} \quad (5.12)$$

예를 들어 A 가 0을 관측했을 때 B 가 0을 관측할 확률은

$$\Pr(A = 0 | B = 0) = \frac{\Pr(A = 0 \cap B = 0)}{\Pr(A = 0)} = \frac{|ac|^2}{|c|^2} = |a|^2 \quad (5.13)$$

이것은 $\Pr(B = 0)$ 과 같다. 따라서 두 사건은 독립이고 얽혀있지 않다. 다른 상황도 한 번 씩 해 보면 모두 서로 독립임을 알 수 있다.

정리하면, 상호작용하는 입자가 속한 다중 양자계의 상태를 측정하면 관측 사건이 서로 종속이며, 이때 개별 상태들은 얽혀 있게 된다. 관측 사건이 서로 독립이라면 개별 상태들은 얽힌 상태가 아니다. 즉 상태의 양자 얽힘 여부는 조건부 확률이라는 도구를 이용해 쉽게 확인할 수 있다.

V.4. EPR 역설

그런데 이런 현상은 비직관적이다. 이런 일이 실제로 일어날 수 있는가? 정보 전달이 빛보다 빠르게 되면 물리법칙에 모순이 아닌가? 상대성 이론에 모순되지는 않는가? A와 B는 (거의) 동시에 측정을 진행할 수 있다. 둘이 얼마나 많이 떨어져 있던 간에, A가 0을 관측하면 B도 0을 관측하게 되고, A가 1을 관측하게 되면 B도 1을 관측하게 된다. A가 측정을 하기 전에는 큐비트는 중첩되어 있는 상태이다. 즉 A도 B도 그 상태가 무엇인지 알지 못한다. 하지만 A가 측정을 하게 되면 그 결과가 반영되어 B에게 측정 결과에 대한 정보가 즉시 전달된다.

아인슈타인은 이것을 으스스한 원격 작용²⁵이라고 했다. 아인슈타인(Albert Einstein, 1879 ~ 1955), 포돌스키(Борис Подольский, 1896 ~ 1966), 로젠(Nathan Rosen, 1909 ~ 1995)은 1935년에 비국소(非局所)적²⁶ 양자 얽힘은 존재해서는 안 된다고 주장하는 내용의 논문을 발표했다. 이 내용은 주로 철학적인 논지를 들어, 광속보다 정보 전달이 빨리 가능한 으스스한 원격 작용이 일어나면 안 된다고 한 것이다.

이것은 아인슈타인이 틀린 말을 한 몇 안 되는 사례이다. 이 으스스한 원격 작용이라는 것이 여러 실험을 통해 확인되었기 때문이다. 그 중 가장 대표적인 실험은 2017년 중국이 양자 통신 위성 미시어스(Micius)을 발사하여 진행한 것이다. 위성은 우주에서 1200 km 이상 떨어진 지구의 두 관측소를 향해 각각 광자를 발사한 결과 거리가 멀어도 이러한 현상이 일어나는 것을 증명했다.

양자 얽힘은 사실 특수 상대성 이론과 상충하지 않는다. 두 관측은 어쨌든 한 게 안에서 이루어지는 것이며, A가 관측 결과를 임의로 조작하여 전달하는 것이 아니고 여전히 결과는 확률적이기 때문에 정보 전달이 광속으로 가능한 것이 아니다. B 입장에서는, A가 관측을 해서 내 관측 결과가 달라진 것인지, 그냥 자신이 관측한 결과가 이것인지도 알 수 없다. 다른 견해로는, 두 광자는 얽혀있기는 하나 두 광자 간 교환되는 정보는 없기 때

²⁵spooky action at a distance

²⁶공간적으로 분리된

문에 인과율을 위배하지 않는다는 주장도 있다. 억지로 끼워 맞추는 것처럼 보이긴 하나, 아직 특수 상대론은 그 입지를 지키고 있다²⁷.

V.5. 양자 얽힘과 양자 메모리 용량

양자 얽힘을 정보 이론의 관점에서 보자. 얽혀있지 않은 n -큐비트 상태는 두 상태의 곱으로 나타낼 수 있었다.

$$\psi = (a_1|0\rangle + b_1|1\rangle) \otimes \dots \otimes (a_n|0\rangle + b_n|1\rangle) \quad (5.14)$$

이 상태에 대한 정보를 고전적인 컴퓨터에 저장한다고 하자. 얼마나 많은 메모리가 필요할까? 각 상태에 대해 두 개의 복소수 계수가 있으므로 $2n$ 개의 복소수를 저장하면 될 것이다.

이제 일반적인 n -큐비트 상태를 생각해 보자. 이 일반적인 상태는 얽혀 있을 것이다.

$$\psi = \sum_{k=0}^{2^n-1} c_k |k\rangle \quad (5.15)$$

여기서는 2^n 개의 복소수를 저장해야 한다. 이로써 양자계에서는 전체는 그 부분의 합보다 크다는 것을 알 수 있다. 왜냐하면 전체는 그 부분의 합이 아니라 곱이기 때문이다. 큐비트는 각각 2 차원이고, 전체 상태공간의 차원은 $2n$ 차원이 아니라 2^n 차원일 것이다.

고전 컴퓨터에서는, 메모리를 n 배로 늘리면 저장할 수 있는 정보의 양도 n 배가 된다. 하지만 양자 컴퓨터에서는 상태를 합성할 때 공간을 더하지 않고 곱하므로, 메모리가 n 배로 늘면 저장할 수 있는 정보의 양은 전체의 n 제곱이 되며 기하급수적으로 증가한다.

²⁷만약 이런 식으로 일이 계속되어 특수 상대론의 반례가 나온다면 현대 물리학 전체가 무너질 수도 있기 때문에, 과학자들은 최대한 특수 상대론을 건드리고 싶지 않아 한다.

VI. 양자 암호학