

Introduction to Quantum Information Science
학습일지

김태원

최초 작성 : 2023년 8월 29일

최근 편집 : 2023년 9월 2일

차 례

차 례	2
제 1 장 기초	3
제 2 장 얹힘	10
제 3 장 결레 코딩	16

제 1 장

기초

파인만Richard Feynman이 말하길 이중슬릿double slit 실험으로 양자역학을 전부 요약할 수 있다.

두 개의 슬릿slit을 지닌 벽에 광자photons를 하나씩 쏜다고 하자. 두 슬릿 모두 열릴 때 광자가 특정 구간에 부딪히는 확률을 P , 1번 슬릿만 열릴 때 광자가 특정 구간에 부딪히는 확률을 P_1 , 2번 슬릿만 열릴 때 광자가 특정 구간에 부딪히는 확률을 P_2 라고 하자. 확률론에 따르면 당연히 $P = P_1 + P_2$ 다. 그런데 실험 결과에 따르면 $P \neq P_1 + P_2$ 다. 다시 말해 자연스러운 확률론은 자연의 현상을 설명하지 못한다.

고전적인 확률론이 자연을 충분히 설명하지 못하는데도 자연스러워 보이는 이유는 **결어긋남decoherence**이라는 현상에서 비롯한다. 이를테면 상자를 열었을 때 슈뢰딩거의 고양이는 생과 사의 중첩superposition으로 나타나지 않는다. 고양이가 제 환경과 끊임없이 상호작용하기 때문이다. 고양이와 환경 간의 상호작용은 고양이 계system의 정보를 누설하는 반면 양자 중첩은 입자나 입자들의 군이 환경과 고립isolated 될 때 일어난다.

똑똑한 물리학자들이 이중슬릿 같은 실험을 통해 관찰한 바, 자연은 고전적인 확률 $P \in [0, 1]$ 가 아니라 어떤 파동함수를 따른다. 그리고 이런 파동함수를 포착하는 개념이 바로 **진폭amplitude** $\alpha \in \mathbb{C}$ 다. 양자역학에서 확률은 진폭을 사용해 **보른 규칙Born Rule**으로 정의된다. 보른 규칙은 양자계의 파동함수를 아우르는 슈뢰딩거 방정식의 해를 해석할 수 있는 유일한 방법으로 1926년 보른Max Born이 제시한 공리다.

$$P = |\alpha|^2 = \text{Real}(\alpha)^2 + \text{Imaginary}(\alpha)^2 \quad (1.1)$$

진폭으로 이중슬릿 실험을 다시 확인하겠다. 두 슬릿 모두 열릴 때 광자가 특정 구간에 부딪히는 진폭을 α , 1번 슬릿만 열릴 때 광자가 특정 구간에 부딪히는 진폭을 α_1 , 2번 슬릿만 열릴 때 광자가 특정 구간에 부딪히는 진폭을 α_2 라고 하자. 이때 등식 $\alpha = \alpha_1 + \alpha_2$

는 모순을 유도하지 않는다. $\alpha_1 = a_1 + b_1 i, \alpha_2 = a_2 + b_2 i$ 에 대해

$$\begin{aligned}
 \alpha &= \alpha_1 + \alpha_2 \\
 \Rightarrow P &= |\alpha|^2 \quad [\text{보른 규칙}] \\
 &= |\alpha_1 + \alpha_2|^2 \\
 &= \text{Re}(\alpha_1 + \alpha_2)^2 + \text{Im}(\alpha_1 + \alpha_2)^2 \\
 &= (a_1 + a_2)^2 + (b_1 + b_2)^2 \\
 &= (a_1^2 + 2a_1 a_2 + a_2^2) + (b_1^2 + 2b_1 b_2 + b_2^2) \\
 &= (a_1^2 + b_1^2) + (a_2^2 + b_2^2) + 2(a_1 a_2 + b_1 b_2) \\
 &= \text{Re}(\alpha_1)^2 + \text{Im}(\alpha_1)^2 + \text{Re}(\alpha_2)^2 + \text{Im}(\alpha_2)^2 + \overline{\alpha_1} \alpha_2 + \alpha_1 \overline{\alpha_2} \\
 &= |\alpha_1|^2 + |\alpha_2|^2 + \overline{\alpha_1} \alpha_2 + \alpha_1 \overline{\alpha_2}
 \end{aligned}$$

복소수 진폭 α 가 음수일 수 있으므로 아래 상황이 가능하기 때문이다.

$$\alpha_1 := \frac{1}{2}, \alpha_2 := -\frac{1}{2} \Rightarrow \begin{cases} |\alpha_1|^2 = \frac{1}{4}, |\alpha_2|^2 = \frac{1}{4} \\ |\alpha = \alpha_1 + \alpha_2|^2 = 0 \end{cases}$$

이처럼 두 상태의 진폭은 서로 소거할 수 있다. **간섭**interference이라는 현상이다. 간섭은 간단한 선형대수학으로 설명된다. 우선 2-노름_{norm} $\alpha^2 + \beta^2 = 1$ 을 충족하는 벡터 (α, β) 가 원을 형성한다는 사실에 주목한다. 2-노름을 유클리드 노름Euclidean norm이라고 부르

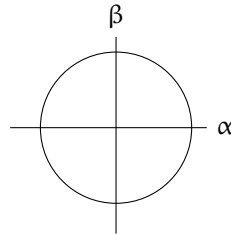


그림 1.1: 유클리드 노름

기도 한다. 원은 임의의 α, β 에 대해 형성되기에 어느 유클리드 노름 단위 벡터를 다른 유클리드 노름 단위 벡터로 사상하는maps to 행렬 혹은 변환이 존재한다. 바로 **유니타리 행렬**unitary matrix이다. 또한 여기서 ‘유클리드 노름 단위 벡터’가 바로 **큐비트**qubit다.

물리학자들은 디랙Paul Dirac이 도입한 브라-켓bra-ket 표기법으로 큐비트를 나타낸다.

켓ket $|\psi\rangle$ 과 브라bra $\langle\psi|$ 는 아래와 같다.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \langle\psi| = \bar{\alpha}\langle 0| + \bar{\beta}\langle 1| = (\bar{\alpha} \quad \bar{\beta})$$

이에 유클리드 노름 $\|\psi\|^2$ 가 자연스럽게 정의될 수 있다.

$$\|\psi\|^2 = (\bar{\alpha} \quad \bar{\beta}) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\alpha|^2 + |\beta|^2$$

내적 $\langle\psi|\phi\rangle$ 는 아래 성질을 만족한다.

$$\begin{aligned} \langle\psi|\phi\rangle &= (\bar{\alpha}_1 \quad \bar{\beta}_1) \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \\ &= \bar{\alpha}_1\alpha_2 + \bar{\beta}_1\beta_2 \\ &= \overline{\alpha_1\alpha_2} + \overline{\beta_1\beta_2} \\ &= (\overline{\alpha_2} \quad \overline{\beta_2}) \begin{pmatrix} \bar{\alpha}_1 \\ \bar{\beta}_1 \end{pmatrix} = \overline{\langle\phi|\psi\rangle} \end{aligned}$$

여기서 α 는 $|0\rangle$ 이라는 결과에 대한 진폭이고 β 는 $|1\rangle$ 이라는 결과에 대한 진폭이다. 따라서 상태 $|\psi\rangle$ 에서 상태 $|\phi\rangle$ 에 이르는 확률 $P(|\phi\rangle)$ 에 대해 보른 규칙을 다시 서술할 수 있다.

$$P(|\phi\rangle) = |\langle\psi|\phi\rangle|^2$$

이에 행렬을 45° 즉 $\frac{\pi}{4}$ 만큼 회전하며 노름을 보존하는 아래 같은 유니타리 행렬이 있다고 하자.

$$\begin{pmatrix} \cos \frac{\pi}{4} & -\sin \frac{\pi}{4} \\ \sin \frac{\pi}{4} & \cos \frac{\pi}{4} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

$|0\rangle$ 를 위 유니타리 행렬로 변환한다.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad (1.2)$$

$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ 을 다시 위 유니타리 행렬로 변환한다.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

즉 무작위 상태 $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ 에 위 유니타리 행렬과 같은 무작위 연산을 적용하면 $|1\rangle$ 이라는 결과가 결정론적(deterministic)으로 나온다. 여기 무작위 연산을 다시 적용하여 나타난 무작위 상태 $-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ 에 무작위 연산을 또다시 적용하면 $|0\rangle$ 이라는 결과가 결정론적으로 나온다. 이것이 앞서 언급한 **간섭** 개념의 선형대수학적 바탕이다.

여기서 $|0\rangle$ 이라는 결과를 결정론적으로 도출하는 유니타리 행렬이 $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ 이라는 사실에 주목한다. 이 사실을 **경로** path가 두 개 존재하여 한 경로는 음의 진폭 $-\frac{1}{\sqrt{2}}$ 를 지니고 다른 경로는 양의 진폭 $\frac{1}{\sqrt{2}}$ 을 지녀 두 경로는 **파괴적 간섭** destructive interference 관계에 놓인다고 표현한다. 반면 $|1\rangle$ 이라는 결과를 결정론적으로 도출하는 경로는 모두 양의 진폭 $\frac{1}{\sqrt{2}}$ 을 지녀 **구성적 간섭** constructive interference 관계다.

이제 그림 1.1상의 원을 다시 그린다. 여기서 $\{|+\rangle, |-\rangle\}$ 는 아다마르 기저(Hadamard basis)

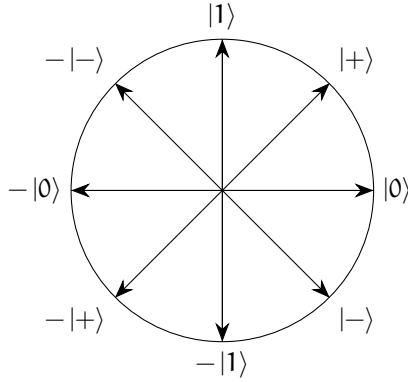


그림 1.2: 직교 행렬

라고 하며 45° 회전 유니타리 변환 과정 1.2에서 이미 봤다.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

아다마르 기저는 **아다마르 게이트**¹ $H: \{|0\rangle, |1\rangle\} \rightarrow \{|+\rangle, |-\rangle\}$ 를 형성한다. 이를테면 $|0\rangle$ 에 H를 적용한 결과는 아래와 같다.

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = |+\rangle$$

그림 1.2에서 확인할 수 있는 사실은 $\frac{\pi}{4}$ 회전과 반사만으로 여덟 가지 상태를 나타낼 수 있다는 것과 원의 방정식에 의해 유니타리 변환이 유클리드 노름을 보존한다는 것이다.

¹유니타리 변환을 게이트라고 부르기도 한다.

가령 임의의 유니타리 행렬 U 의 복소전치행렬 U^\dagger 를 U 로 변환하면 항등행렬 I 가 나온다.

$$\langle \psi | \psi \rangle = (|\psi\rangle)^\dagger |\psi\rangle = (U|\psi\rangle)^\dagger U|\psi\rangle = \langle \psi | U^\dagger U | \psi \rangle \iff \forall |\psi\rangle, U^\dagger U = I$$

유니타리 변환은 선형변환이기도 해서 $U(c|0\rangle) = cU|0\rangle$ 이 임의의 상수 c 에 대해 성립할 수 있다. 여기서 c 가 어떤 θ 에 대해 오일러 공식 $e^{i\theta} = \cos\theta + i\sin\theta$ ²를 만족하면 **전역위상** **global phase**이라고 한다. 다만 $|\psi\rangle$ 와 $e^{i\theta}|\psi\rangle$ 가 물리적으로 구분될 수 없기에 전역위상은 관찰불가능하다. 전역위상이 관찰가능하다는 말은 큐비트와 같은 양자계에 어떤 스칼라를 곱해서 우주 전체를 살짝 옮길 수 있다는 소리와 같다. 이에 반해 관찰 가능한 것은 바로 **상대위상** **relative phase**이다. 가령 $|+\rangle$ 와 $|-\rangle$ 라는 두 상태 간에는 상대위상차이가 관측될 수 있는데, $|-\rangle$ 에서 $|+\rangle$ 에 이르는 일련의 유니타리 연산들이 존재하기 때문이다.

관찰 혹은 측정 **measurement**과 유니타리 연산 간에 차이가 존재하는 셈이다. 유니타리 변환이 (그 복소전치행렬로 인해) 가역 **invertible**이고 결정론적이며 (복소수 행렬이기에 모든 a 에 대해 \sqrt{a} 를 내놓을 수 있어서) 연속적인 반면, 측정은 비가역 **irreversible**이고 확률론적, 비연속적이다. 이처럼 판이한 유니타리 변환과 측정을 이어주는 것이 바로 유클리드 노름이다. 유니타리 변환은 유클리드 노름을 보존하고 측정은 유클리드 노름으로 결정되는 확률을 제공한다. 그리고 이에 따른 연속과 비연속, 결정론과 확률론의 상호작용을 소진하는 사고실험이 바로 튜링의 역설 혹은 **양자 제논 효과**다.

$|0\rangle$ 이나 $|1\rangle$ 로 설정된 큐비트가 있다고 하겠다. 이 큐비트에 유니타리 변환을 전혀 사용하지 않으면서 상태를 바꿀 수 있을까? 아주 작은 ϵ 에 대해 $\{|0\rangle, |1\rangle\}$ 에서 ϵ 만큼 회전한 기저는 아래처럼 측정할 수 있다.

$$\begin{aligned} |0\rangle &\mapsto |v\rangle = \cos\epsilon |0\rangle + \sin\epsilon |1\rangle & |1\rangle &\mapsto |w\rangle = -\sin\epsilon |0\rangle + \cos\epsilon |1\rangle \\ \Rightarrow P(|v\rangle) &= |\langle 0|v\rangle|^2 & P(|w\rangle) &= |\langle 1|w\rangle|^2 \\ &= \left| \begin{pmatrix} 1, 0 \end{pmatrix} \begin{pmatrix} \cos\epsilon \\ \sin\epsilon \end{pmatrix} \right|^2 & &= \left| \begin{pmatrix} 0, 1 \end{pmatrix} \begin{pmatrix} -\sin\epsilon \\ \cos\epsilon \end{pmatrix} \right|^2 \\ &= |\cos\epsilon|^2 \approx \left(1 - \frac{\epsilon^2}{2}\right)^2 & &= |\cos\epsilon|^2 \approx \left(1 - \frac{\epsilon^2}{2}\right)^2 \\ &= 1 - \epsilon^2 + \frac{\epsilon^4}{4} \approx 1 - \epsilon^2 & &= 1 - \epsilon^2 + \frac{\epsilon^4}{4} \approx 1 - \epsilon^2 \end{aligned}$$

큐비트가 ϵ 만큼 회전할 수 있는 확률은 ϵ 이 감소할수록 증가³한다. 그러니 이 절차를

²오일러 공식은 슈뢰딩거 방정식을 비롯해 양자역학에서 중요한 파동-삼각함수를 지수함수로 변환할 수 있도록 하며, 복소평면에서 일정한 속도로 원운동하는 물체의 위치 방정식으로 정의된다.

³근사값의 유도에 관해서는 **작은 각도 근사**를 참고하라.

대략 $\frac{1}{\epsilon}$ 번 반복하며 매번 ϵ 만큼 회전하면, $|0\rangle$ 을 아주 천천히 $|1\rangle$ 로 옮길 수 있다. 이 과정이 성공하지 않을 확률은 $1 - (1 - \epsilon^2) = \epsilon^2$ 에 $\frac{1}{\epsilon}$ 을 곱한 ϵ 이다. 그리고 ϵ 은 가정에 의해 극미량이다. 따라서 유니타리 변환이 없더라도 아주 높은 확률로 상태를 바꿀 수 있다.

그런데 이게 무슨 소리인가? 비유하자면, 홍길동의 $|미혼\rangle$ 상태를 $|기혼\rangle$ 상태로 바꾸는 유니타리 변환 수준의 깔끔한 방법은 당장 김철수와 서류상 혼인신고하는 것이다. 이 방법은 지금 어렵다고 할 때, 홍길동이 김철수를 1년간 그냥 지켜보다가 어느 날 갑자기 프로포즈하는 쪽보다는 홍길동이 1년을 $\frac{1}{\epsilon}$ 정도로 아주 잘게 나눠 ϵ 만큼의 애정 표현을 반복하는 쪽의 결혼 확률이 더 높을 것이다.

다음 예는 **엘리추르-바이드만 폭탄** Elitzur-Vaidman Bomb 으로, 양자 공항이 배경이다. 화물에 폭탄이 존재하는 것 같은데, 폭탄이 있다면 화물을 여는 순간 폭발할 것이 분명하다. 폭탄이 폭발할 확률을 최소화할 수 있을까?

우선 $|0\rangle$ 을 초기 상태로 둔다. 화물 확인이라는 행동은 회전 R_ϵ 으로 정의한다.

$$R_\epsilon = \begin{pmatrix} \cos \epsilon & -\sin \epsilon \\ \sin \epsilon & \cos \epsilon \end{pmatrix}$$

폭탄이 없다면, 그대로 $\cos \epsilon |0\rangle + \sin \epsilon |1\rangle$ 이다. 폭탄이 있다면, 폭탄은 $\{|0\rangle, |1\rangle\}$ 을 기저로 측정된다. 다시 말해 회전-확인 결과 $|0\rangle$ 이라면 폭탄이 폭발하지 않은 것이다. 그리고 결과가 $|1\rangle$ 이라면 폭탄이 폭발한 것이다.

초기 상태 $|0\rangle$ 에 대해 화물을 한 번 확인- R_ϵ 한 결과는 $\cos \epsilon |0\rangle + \sin \epsilon |1\rangle$ 이다. 폭탄이 존재할 때, 폭탄이 폭발할 확률 $P(1)$ 은 $\cos \theta |0\rangle + \sin \epsilon |1\rangle$ 이 $|1\rangle$ 로 관측될 확률과 같다.

$$\begin{aligned} P(1) &= |\langle b|1\rangle|^2 \\ &= \left| \begin{pmatrix} \cos \epsilon & \sin \epsilon \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right|^2 \\ &= |\sin \epsilon|^2 \approx \epsilon^2 \end{aligned}$$

따라서 이 과정을 대략 $\frac{\pi}{2\epsilon}$ 번⁴ 반복하며 매번 R_ϵ 을 적용하면, 존재하는 폭탄이 터지는 확률은 $\frac{\pi}{2\epsilon} \epsilon^2 = \frac{\pi}{2} \epsilon$ 에 불과하다. 따라서 양자 공항에서는 대단히 높은 확률로 폭탄이 폭발하지 않는다.

⁴여기서 $\frac{\pi}{2\epsilon}$ 은 90° 보다 아주 약간 작은 각도로, 그림 1.2의 원에서 ‘ $|1\rangle$ ’ 직전에 해당한다.

양자 회로

그림 1.3은 $|1\rangle$ 로 초기 상태를 설정한 다음 두 아다마르 게이트를 적용하여 표준기저 $\{|0\rangle, \dots, |N-1\rangle\}$ 상의 측정으로 종결하는 양자회로다. 양자회로는 여러 큐비트에 대한 연산을 표기할 수도 있다. 그림 1.4는 이중 큐비트 게이트 U 에 대해 첫 번째 큐비트로 아다마르 게이트를 적용한 다음 두 큐비트를 모두 측정하는 양자회로다.

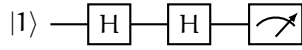


그림 1.3: 양자 회로 예제

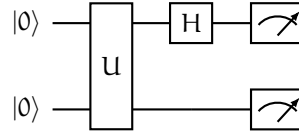


그림 1.4: 이중 양자 회로 예제

그림 1.5 좌측의 양자회로는 제어_{controlled} 게이트를 사용한다. 첫 줄에 놓인 $\bullet - \oplus$ 는 제어 NOT 혹은 CNOT 게이트를 나타내고 이는 첫 비트 혹은 제어 큐비트가 $|1\rangle$ 이면 두 번째 큐비트를 반전_{flip}한다. 그 다음 줄에 놓인 $\bullet - U$ 는 임의의 U 에 대해 제어 U 게이트를 나타내며 제어 큐비트가 $|1\rangle$ 이면 U 를 적용한다. 마지막 줄은 우측 도면과 같다.

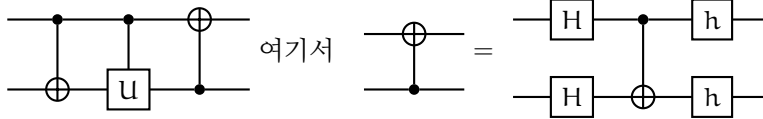


그림 1.5: 제어 양자 회로 예제

제 2 장

얽힘

두 개의 큐비트로 $|\psi\rangle$ 를 구성할 때

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

각 결과는 보른 규칙 1.1에 의해 아래 확률을 지닌다.

$$\begin{aligned} P(|00\rangle) &= |\alpha|^2 & P(|01\rangle) &= |\beta|^2 \\ P(|10\rangle) &= |\gamma|^2 & P(|11\rangle) &= |\delta|^2 \end{aligned}$$

그리고 첫 번째 큐비트가 $|0\rangle$ 이라는 정보에 대해 두 번째 큐비트는 아래 같은 중첩으로 주어진다.

$$|0\rangle \otimes \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2}} = \begin{bmatrix} \alpha \\ \beta \\ 0 \\ 0 \end{bmatrix} \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2}} \quad (2.1)$$

여기서 $\sqrt{|\alpha|^2 + |\beta|^2}$ 로 나누는 과정을 정규화normalization라고 부른다. 노름화라고 이해할 수도 있는데 왜냐하면 α 와 β 서로만 있어도 유클리드 노름의 조건을 유지하도록 보조하는 과정이기 때문이다.

$$\left| \frac{\alpha}{\sqrt{|\alpha|^2 + |\beta|^2}} \right|^2 + \left| \frac{\beta}{\sqrt{|\alpha|^2 + |\beta|^2}} \right|^2 = \frac{|\alpha|^2 + |\beta|^2}{|\alpha|^2 + |\beta|^2} = 1$$

중첩 2.1은 **부분측정규칙**partial measurement rule이라고 부르는 양자역학의 기본 규칙이다. 1장에서 다룬 양자역학 기초와 부분측정규칙만으로 학부 수준 양자정보학은 전부

유도할 수 있다. 부분측정규칙의 용례로는 얽힘을 뽑을 수 있다.

첫 큐비트에 아무것도 하지 않고 두 번째 큐비트에 NOT 게이트를 적용¹하는 게이트가 있다.

$$\begin{array}{c} \begin{array}{cccc} & 00 & 01 & 10 & 11 \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

이 게이트를 텐서곱^{tensor product}으로 나타낼 수도 있다.

$$I \otimes \text{NOT} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

감으로 텐서곱이 어떤 연산인지 파악하길 바란다. 핵심은 “두 번째 큐비트에 NOT 게이트를 적용”과 같은 표현의 뜻이다. “첫 번째 큐비트에 아다마르 게이트를 적용하고 두 번째 큐비트에 다시 아다마르 게이트를 적용하라”는 말은 텐서곱으로는 $H \otimes H$ 와 같으며 게이트로는 아래와 같다.

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{array}{c} \begin{array}{cccc} & 00 & 01 & 10 & 11 \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \end{array}$$

여기서 00이라는 첨자를 지니는 첫 번째 행이 구성되는 방식을 $H \otimes H|00\rangle = |++\rangle$ 이라는 텐서곱으로 생각할 수 있다. 마찬가지로 01이라는 첨자를 지니는 두 번째 행이 구성되는 방식을 $H \otimes H|01\rangle = |+-\rangle$ 이라는 텐서곱으로 받아들일 수 있다.

$$|+-\rangle = |+\rangle \otimes |-\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \frac{1}{2} \begin{array}{c} \begin{array}{c} 01 \\ \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} \end{array} \end{array}$$

¹가령 $|a0\rangle$ 에 대해 $|a\rangle$ 는 가만히 놔두고 두 번째 큐비트만 반전하여 $|a1\rangle$ 을 출력하는 식이다. 또한 행렬 주변의 첨자 00, 01, 10, 11은 행에서 입력을 나타내고 열에서 출력을 나타낸다. 가령 CNOT 게이트는 11이라는 입력에 대해 10을 출력한다.

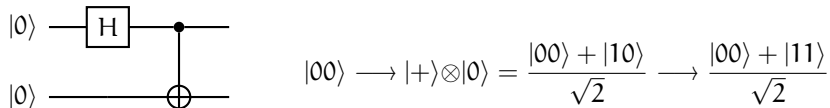
이처럼 2-큐비트 유니터리를 1-큐비트 유니터리의 텐서곱으로 구성할 수 있다. 다만 CNOT 게이트는 예외다. 첫 번째 큐비트가 0이면 두 번째 큐비트를 놔두고 첫 번째 큐비트가 1이면 두 번째 큐비트를 반전하는 CNOT 게이트는 이렇게 생겼다.

$$\begin{array}{cc} & \begin{matrix} 00 & 01 & 10 & 11 \end{matrix} \\ \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

다시 말해 CNOT은 한 큐비트가 다른 큐비트한테 영향을 미치는 게이트다. CNOT의 이런 성질을 사용하는 특이한 상태가 있다. 바로 **벨 쌍** Bell Pair 혹은 **EPR 쌍** 혹은 **싱글렛** singlet이다.

$$(\text{CNOT})(H \otimes I) \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \rightarrow \text{CNOT} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

CNOT의 첫 큐비트와 두 번째 큐비트를 텐서곱으로 분해할 수 없으므로 벨 쌍 또한 첫 큐비트와 두 번째 큐비트의 상태가 텐서곱으로 분해되지 않는다. 이런 상태를 **얽힘** entanglement 혹은 **순수 상태**라고 부른다. EPR 쌍은 이름만 무려 세 개인 만큼 중요한 상태이기 때문에 회로와 브라켓도 기억해 둔다.



$$|00\rangle \rightarrow |+\rangle \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}} \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

그림 2.1: EPR 쌍

얽힘은 양자역학을 구성하는 수학의 필연적인 귀결이다. 또한 얽힘은 (EPR 쌍에서 ‘E’에 해당하는) 아인슈타인이 양자역학에 신경질을 부린 이유다.

달에는 철수가 있고 지구에는 영희가 있다고 하자. 철수와 영희는 입자의 쌍에 얽힘을 부여할 수 있다. EPR 쌍 $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ 로 상태를 설정하는 것이다. 그리고 철수가 입자의 상태를 측정한 바로 그때 철수는 영희가 관측할 상태가 $|0\rangle$ 인지 $|1\rangle$ 인지 알 수 있다.

여타 물리학자와 다르게 아인슈타인은 이 이야기가 아주 거슬렸다. 1935년, 아인슈타인, 포돌스키 Boris Podolsky, 로젠 Nathan Rosen은 이 문제를 확대하는 논문을 발표한다. 이 논문은 철수가 $\{|0\rangle, |1\rangle\}$ 이 아니라 $\{|+\rangle, |1\rangle\}$ 을 기저로 측정하면 어떻게 되냐고 묻는다.

이 물음은 철수가 자신의 큐비트에 아다마르 게이트를 적용한 다음 $\{|0\rangle, |1\rangle\}$ 을 기저로 측정하는 상황을 통해 나타낼 수 있다.

$$(H \otimes I) \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) = \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2}$$

부분측정규칙 2.1에 의해 철수가 $|0\rangle$ 을 보면 영희의 큐비트는 아래처럼 붕괴하고²

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

철수가 $|1\rangle$ 을 보면 영희의 큐비트는 아래처럼 붕괴한다.

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

아인슈타인, 포돌스키, 로젠은 이게 왜 거슬렸는가? 철수가 $\{|0\rangle, |1\rangle\}$ 을 기저로 EPR 상태를 측정하면 영희가 $|0\rangle$ 이나 $|1\rangle$ 을 보고, 철수가 $\{|+\rangle, |-\rangle\}$ 를 기저로 측정하면 영희가 $|+\rangle$ 이나 $|-\rangle$ 을 보는데, 이런 통신communication이 즉각적으로 혹은 바로 그때 이루어진다는 사실 때문이었다. 따라서 빛보다 빠른 의사소통이 존재한다는 말인데, 이는 얽힘이라는 양자역학적 현상이 상대성이론을 근본부터 전면 부인하다는 소리다.

다행히 이들을 화해시킬 수 있다. 순수상태 뿐만 아니라 **혼합상태**mixed states도 논의에 끌어들이는 방법이다. 혼합상태란 양자 상태 $|\psi\rangle$ 에 대한 확률 p_i 의 분포 $\{p_i, |\psi_i\rangle\}$ 이다. 핵심은 바로 상이한 확률분포를 지니는 순수상태들을 정확히 서로 같은 혼합상태로 나타낼 수 있다는 사실에 달렸다.

우선 **밀도행렬**density matrix이라는 도구를 쥔다. 혼합상태 $\{p_i, |\psi_i\rangle\}$ 에 대한 밀도행렬 표현은 아래처럼 주어진다.

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| \quad (2.2)$$

여기서 $|\psi_i\rangle \langle \psi_i|$ 는 **외적**을 나타낸다.

$$\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} \begin{bmatrix} \overline{\alpha_0} & \overline{\alpha_1} & \cdots & \overline{\alpha_{N-1}} \end{bmatrix} = \begin{bmatrix} |\alpha_0|^2 & & & \\ & \ddots & \alpha_i \overline{\alpha_j} & \\ & & \ddots & \\ \alpha_j \overline{\alpha_i} & & & \ddots \\ & & & & |\alpha_{N-1}|^2 \end{bmatrix}$$

보시다시피 혼합상태의 밀도행렬 ρ 는 ρ 자신과 켤레 전치 ρ^\dagger 가 같은 에르미트 행렬Hermitian

² $\frac{1}{\sqrt{2}}$ 는 $\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2}$ 로 정규화하는 값이다.

*matrix*이다. 따라서 표준 기저에 대한 외적은 아래와 같고

$$|0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

균등하게 섞으면 아래와 같으며

$$\frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} = \frac{I}{2}$$

$\{|+\rangle, |-\rangle\}$ 에 대해서는 아래와 같다.

$$|+\rangle\langle +| = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \quad |-\rangle\langle -| = \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \Rightarrow \frac{|+\rangle\langle +| + |-\rangle\langle -|}{2} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} = \frac{I}{2}$$

서로 다른 중첩을 지닌 두 기저에 대해 밀도행렬이 일치한다. 임의의 기저에 대해서도 마찬가지라는 사실도 쉽게 확인할 수 있다. 따라서 철수가 EPR 쌍에서 기저를 바꿔도 영희 측에서는 상태의 밀도행렬 표현이 유지되는데, 밀도행렬은 확률을 표현하기 때문이다. ρ 를 기저 $\{|0\rangle, \dots, |N-1\rangle\}$ 상에서 측정하면 $|i\rangle$ 가 출력되며 확률 $P(|i\rangle) = \rho_{ii} = \langle i|\rho|i\rangle$ 가 잇따른다. 말이 어려우니 예를 들면, 아래 M 은 밀도행렬일 수 없다.

$$\begin{aligned} M &= \begin{bmatrix} \frac{1}{2} & -10 \\ -10 & \frac{1}{2} \end{bmatrix} \\ \Rightarrow \langle +|M|+\rangle &= \begin{bmatrix} -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} & -10 \\ -10 & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \\ &= \begin{bmatrix} -\frac{1}{2\sqrt{2}} & \frac{10}{\sqrt{2}} \\ \frac{10}{\sqrt{2}} & -\frac{1}{2\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = -\frac{1}{4} + 5 + 5 - \frac{1}{4} = \frac{19}{2} \end{aligned}$$

밀도행렬 $\frac{I}{2}$ 로 예를 들면, 임의의 기저 $\{|v\rangle, |w\rangle\}$ 에 대한 확률은 아래와 같다.

$$\langle v|\frac{I}{2}|v\rangle = \frac{1}{2} \langle v|v\rangle = \frac{1}{2}, \quad \langle w|\frac{I}{2}|w\rangle = \frac{1}{2} \langle w|w\rangle = \frac{1}{2}$$

이처럼 균등하게 기저들이 혼합된 밀도행렬을 **최대혼합상태** Maximally Mixed State라고 부른다. 최대혼합상태는 말 그대로 최대이기 때문에 철수든 영희든 똑같은 최대혼합상태다. 따라서 실상 철수와 영희 간에는 통신이 이루어지지 않았다. 이를 **무통신정리** No-Communication theorem이라고 한다.

한편 계의 순수상태에서 계의 혼합된 상태로 추적해 나감(tracing out) 수 있다. 큐비트

두 개의 순수상태에 대해, 철수한테 첫 번째 큐비트를 주고 영희한테 두 번째 큐비트를 준다고 하겠다.

$$\frac{|00\rangle + |01\rangle + |10\rangle}{\sqrt{3}}$$

이때 영희가 계산해야 하는 밀도행렬을 **축소밀도행렬** reduced density matrix 혹은 **국소밀도행렬** local density matrix이라고 부른다. 국소밀도행렬을 계산하기 위해 우선 철수 쪽으로 가서 직교 기저를 골라, 위 상태를 아래처럼 다시 나타낸다.

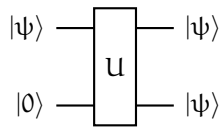
$$\frac{\sqrt{2}}{\sqrt{3}}|0\rangle|+\rangle + \frac{1}{\sqrt{3}}|1\rangle|0\rangle$$

보른 규칙에 의해 $P(|0+\rangle) = \frac{2}{3}$, $P(|10\rangle) = \frac{1}{3}$ 이므로 영희의 밀도행렬은 아래와 같다.

$$\frac{2}{3}|+\rangle\langle+| + \frac{1}{3}|0\rangle\langle 0| = \frac{2}{3}\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} + \frac{1}{3}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} \end{bmatrix}$$

정리하면 철수가 빛보다 빠르게 통신할 수 없는 이유는 영희가 큐비트의 상태가 어느 기저에 있는지 확실하게 알 수 없기 때문이다. 그런데 이때 영희가 자신의 큐비트에 대해 복사본_{copy}을 무한히 지닐 수 있다면, 사본 가운데 하나는 철수가 측정한 기저를 따를 수밖에 없다. 따라서 빛보다 빠른 통신이 가능하겠지만, 이런 복사는 불가능하다. 앞서 언급하기도 했지만 무통신정리를 위배한다는 것이 하나의 이유다.

그래도 한 번 시도해 볼 수 있다. 큐비트 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 에 대해 $|\psi\rangle$ 하나와 더미 큐비트 하나를 입력 삼아 $|\psi\rangle$ 두 개를 출력하는 양자회로다. 다시 말해 $|\psi\rangle$ 의 사본을 만든다.



여기서 U는 아래 변환을 구현해야 한다.

$$\begin{aligned} & (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \\ \rightarrow & (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ = & \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle \end{aligned}$$

이런 변환-복사가 불가능한 이유는 α^2 를 통해 알 수 있듯이 애초에 이 변환이 선형적이지 않고, 따라서 유니타리 변환일 수 없기 때문이다. 따라서 **복사불능정리**No-Cloning Theorem³가 성립한다. 이 정리 하나에 기초해서 양자화폐와 양자암호라는 분야가 탄생할 만큼 복사불능정리는 대단히 강력하다.

³CNOT 같은 게이트가 큐비트를 복사하는 것처럼 보일 수 있지만, CNOT은 오직 입력 상태가 $|0\rangle$ 이나 $|1\rangle$ 일 때만 복사하는 것으로, 이때는 고전적인 정보가 복사된다. 즉, 임의의 정규직교 기저에 대해 자신의 입력 상태가 기저 벡터라는 정보를 안다면, 기저 벡터를 복사할 수 있다.

제 3 장

켈레 코딩

와이즈너Steven Weisner와 베넷Charles Bennett은 대학교에서 처음 만났다. 둘은 친구였다. 둘은 다른 대학원으로 진학했다. 연락은 끊지 않았다. 와이즈너가 베넷의 집으로 자주 놀러갔다. 1960년대 후반에서 1970년대 초반쯤 와이즈너는 베넷이랑 양자역학으로 만든 지폐에 관해 이야기했다. 이 지폐는 절대 위조할 수 없다. 자연이 허락하지 않는다.

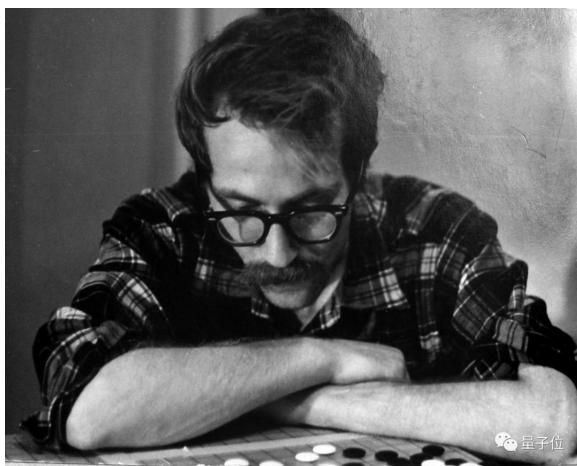


그림 3.1: 젊은 날의 와이즈너

와이즈너는 이 이야기를 「켈레 코딩」Conjugate Coding이라는 논문으로 정리해 유명한 정보이론 저널에 투고했다. 저널은 「켈레 코딩」을 거절했다. 정보학자들이 물리학자의 어투를 낯설게 여긴 탓이다. 와이즈너는 머지 않아 학계를 떠났다. 그리고 베유Simon Weil처럼 육체 노동의 가치를 찬미하며 건설 노동자로 여생을 보냈다.

하지만 베넷은 와이즈의 이야기를 잊지 않았다. 계속 이야기하고 다녔다. 그러다 몬트리올 출신 암호학자 브라사르Gilles Brassard가 재밌게 들었다. 베넷과 브라사르는 상이한 배경에도 불구하고 미친듯이 이야기를 나눴다. 그리고 1982년 「양자 암호학, 혹은

복제 불가능한 지하철 승차권」Quantum Cryptography, or Unforgeable Subway Tokens이라는 논문을 내놓았다. 이 논문이 이론 업적 가운데 하나는 바로 「켈레 코딩」을 1983년 ACM 뉴스레터에 신도록 유도한 것이다.

「켈레 코딩」에 따르면 해커는 어느 미지의 큐비트와 동일한 양자 상태의 두 번째 큐비트를 생산할 수 없다. 또 위조할 수 없는 화폐가 존재할 수 있다. 양자 상태는 복사 불가능하기 때문이다. 다시 말해 양자정보라는 분야는 커녕 ‘큐비트’라는 말조차 없던 시절 복사불능정리를 당연하게 받아들이고 양자화폐와 양자암호라는 응용 분야를 개척한 10쪽 짜리 논문이 바로 「켈레 코딩」이다.

양자은행이 존재하여 양자지폐를 찍어낸다고 하겠다. 각 양자지폐는 고전적인 일련번호 $s \in \{0, 1\}^n$ 와 양자 상태 $|\psi_{f(s)}\rangle$ 를 지닌다. 이때 $|\psi_{f(s)}\rangle$ 상의 큐비트들은 얽혀있지 않고 각각 아래 네 상태 가운데 하나다.

$$|\psi_{00}\rangle = |0\rangle, |\psi_{01}\rangle = |1\rangle, |\psi_{10}\rangle = |+\rangle, |\psi_{11}\rangle = |-\rangle$$

양자은행에는 초거대 데이터베이스가 존재하여 각 양자지폐에 대해 일련번호 S 와 양자지폐가 지녀야 하는 큐비트에 대해 그 기저를 부호화한 문자열 $f(s)$ 를 저장한다. 문제는 양자지폐를 어떻게 검증verify하느냐는 것이다.

우선 양자지폐를 양자은행에 갖다준다. 양자은행은 일련번호로 양자지폐를 검증한다. 그리고 양자지폐 속 각 큐비트를 앞서 부호화한 기저로 측정한다. 큐비트가 $|0\rangle$ 혹은 $|1\rangle$ 이어야 할 때 측정은 $\{|0\rangle, |1\rangle\}$ 을 기저로 이루어진다. 이제 각 측정에 대해 예상한 결과가 나오는지 확인하면 끝이다. 위조범이 각 큐비트가 요구하는 기저를 모른다면 무작위로 기저를 찍을 테다. n 번 찍을 때 이게 먹힐 확률은 $(\frac{1}{2})^n$ 이다.

그러나 바로 이게 문제다. 양자지폐를 사용하려고 할 때마다 양자은행의 검증이 필요하다면 애초에 양자지폐를 사용할 이유가 없다. 거래 과정상 은행의 개입을 요구하지 않는다는 현금의 최대 장점이 쏙 빠진 셈이다.

그리하여 **공개키**public-key를 도입할 수도 있겠다. 모든 사람이 공개키로 양자지폐를 검증할 수 있도록 허락하고 개인키를 지닌 양자은행만 양자지폐를 생산할 수 있도록 제한하는 방법이다. 물론 위조범이 엄청난 계산 능력을 지녀서 그냥 있을 수 있는 양자상태를 다 때려박으면 공개키 검증 절차를 통과하는 양자 상태를 찾아낼 수도 있다. 이론적으로 따져도 나쁜 상황이다.

이에 1984년 베넷과 브라사드는 **양자 키 분배**quantum key distribution를 고안한다. 베넷과 브라사드가 1984년 발표한 방법이라 **BB84 프로토콜**이라고 부른다. 지난 장에서 만난 철수와 영희를 이제 (암호학의 전통에 따라) 앨리스와 밥이라고 부르겠다. BB84의 골자는 공유 기밀 지식을 엿듣든 말든 상관 없다는 것이다.

- (i) 앨리스가 문자열의 쌍 $x, y \in \{0, 1\}^n$ 를 무작위로 고른다. 가령 x 가 010...010이고 y 가 111...110일 수 있다.

- (ii) 앨리스는 n 개의 큐비트로 구성된 양자 상태 $|\psi\rangle$ 를 생성한다. 여기서 앨리스는 y 의 비트를 사용해 큐비트를 부호화할 기저를 결정한다. 0에는 $\{|0\rangle, |1\rangle\}$, 1에는 $\{|+\rangle, |-\rangle\}$ 같은 식이다. 가령 $y = 111 \dots 110$ 에 대해 첫 번째, 두 번째, 세 번째 큐비트는 $\{|+\rangle, |-\rangle\}$ 을 기저로 부호화하고 마지막 큐비트는 $\{|0\rangle, |1\rangle\}$ 을 기저로 부호화한다.
- (iii) 앨리스는 밥에게 양자 상태 $|\psi\rangle$ 를 보낸다. $|\psi\rangle$ 만으로는 $|\psi\rangle$ 상의 각 큐비트가 무엇을 기저로 지니는지 알 수 없다.
- (iv) 밥은 $\{0, 1\}^n$ 에서 무작위로 문자열 y' 을 고른다. 가령 $y' = 001 \dots 100$ 일 때
- (v) 밥은 y' 의 비트를 사용해 앨리스가 보낸 $|\psi\rangle$ 의 각 큐비트를 측정할 기저를 결정한다. 이에 측정 결과가 나타나겠다. 측정 결과를 문자열 x' 에 $|0\rangle$ 이나 $|+\rangle$ 에 대해 0을, $|1\rangle$ 이나 $|-\rangle$ 에 대해 1을 기록하는 식이다.
- (vi) 이제 앨리스와 밥은 양자 상태 $|\psi\rangle$ 의 부호화와 측정에 대해 사용한 기저를 공유한다. 문자열 y 와 y' 를 공유하는 것이다. 그리고 앨리스와 밥은 자신들이 같은 기저를 고르지 않은 x 와 x' 의 비트를 전부 버린다. 이게 대략 절반의 비트일 것이다. 이제 x 와 x' 로 남은 것이 공유된 비밀키다.

염탐자 이브가 있다고 하자. 이브는 앨리스와 밥이 전송하는 큐비트를 관찰한다. 하지만 이브가 큐비트를 측정하려고 할 때마다 밥이 수신하는 큐비트를 본질적으로 바꿔 버린다. 물론 이브가 $|0\rangle$ 이나 $|1\rangle$ 을 측정하고 큐비트가 $\{|0\rangle, |1\rangle\}$ 기저상에 준비되어 있다면 큐비트가 변하지는 않겠다.