

응용물리연구실심화실습3 (PHY3075)

2024년 11월 4주차

응용물리학과 2022006971 이민성

Entanglement in action

번역

- 서론

이번 강의에서는 세 가지 근본적으로 중요한 예시를 살펴보겠습니다. 첫 번째 두 가지는 텔레포테이션과 슈퍼덴스 코딩 프로토콜로, 주로 송신자와 수신자 간의 정보 전송과 관련이 있습니다. 세 번째 예시는 CHSH 게임이라는 추상적인 게임으로, 양자 정보에서 비국소성이라고 불리는 현상을 설명합니다. (CHSH 게임은 항상 게임으로 설명되지는 않습니다. 종종 실험으로 설명되며, 특히 벨 테스트의 예시로 언급되고 CHSH 부등식이라고도 불립니다.)

텔레포테이션, 슈퍼덴스 코딩, CHSH 게임은 단순히 양자 정보가 어떻게 작동하는지를 설명하는 예시들에 그치지 않습니다. 이들은 양자 정보의 기초를 이루는 중요한 개념들이며, 세 가지 모두 얽힘(entanglement)이라는 개념이 중요한 역할을 합니다. 따라서 이번 강의는 얽힘이 실제로 어떻게 작용하는지, 그리고 얽힘이 왜 그렇게 흥미롭고 중요한 개념인지를 탐구할 첫 번째 기회입니다.

이제 예시들에 들어가기 전에, 세 가지 예시와 관련된 몇 가지 기본적인 주제를 다루고자 합니다.

앨리스와 밥

앨리스(Alice)와 밥(Bob)은 정보의 교환과 관련된 시스템, 프로토콜, 게임 및 기타 상호작용에서 사용되는 가상의 인물 또는 대리인의 전통적인 이름입니다. 이 이름들은 일반적으로 인간을 지칭하지만, 실제 인간을 의미하는 것은 아니며, 복잡한 계산을 수행하는 대리인일 수도 있습니다.

이 이름들은 1970년대 암호학 분야에서 처음 사용되었지만, 이후 그 사용이 더 널리 퍼졌습니다. 간단히 말하면, '앨리스'와 '밥'은 A와 B로 시작하는 일반적인 이름들이며, 이는 편리하게도 앨리스를 '그녀'로, 밥을 '그'로 지칭하는 데에도 유용합니다.

기본적으로 앨리스와 밥은 서로 다른 위치에 있다고 상상합니다. 그들의 목표와 행동은 그들이 등장하는 맥락에 따라 달라질 수 있습니다. 예를 들어, 정보 전송의 경우, 앨리스는 송신자를, 밥은 수신자를 의미할 수 있습니다. 일반적으로 앨리스와 밥은 협력하는 관계에 있으며, 이는 다양한 상황에서 흔히 볼 수 있는 모습입니다. 하지만 때로는 그들이 경쟁 관계에 있거나 목표가 일치하지 않거나 협조적이지 않은 경우도 있을 수 있습니다. 이런 점들은 해당 상황에서 명확히 정의되어야 합니다.

필요에 따라 찰리(Charlie)와 다이앤(Diane)과 같은 추가적인 캐릭터를 도입할 수도 있습니다. 또한, 도청을 하는 악의적인 인물인 이브(Eve)나, 해를 끼치려는 인물인 말로리(Mallory)와 같은 다른 인물들을 나타낼 때도 이 이름들이 사용됩니다.

앨리스와 밥은 이번 강의에서 다룰 세 가지 예시 모두에 등장하며, 앞으로의 강의에서도 자주 등장할 것입니다.

얽힘을 자원으로서

이번 강의에서는 Lesson 2에서 다룬 두 큐비트의 얽힌 양자 상태를 다시 한 번 살펴보겠습니다:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle. \quad (1)$$

이 상태는 네 개의 벨 상태 중 하나로, 얽힌 양자 상태의 전형적인 예시로 자주 언급됩니다.

우리는 또한 두 비트의 확률적 상태 예시를 접했습니다:

$$\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle. \quad (2)$$

이는 어느 정도, 얽힌 양자 상태 (1)와 유사하다고 할 수 있습니다. 이 상태는 두 비트가 상관 관계를 가지지만 얽힘 상태는 아닙니다. 얽힘(entanglement)은 본질적으로 양자 현상으로, 정의상 비고전적인 양자 상관관계를 의미합니다.

불행히도, 얽힘을 비고전적인 양자 상관관계로 정의하는 것은 직관적으로 만족스럽지 않습니다. 왜냐하면 얽힘을 정의하는 방식이 그것이 무엇이 아닌지를 기준으로 하기 때문입니다. 아마도 이 점이 바로 얽힘이 정확히 무엇인지, 그리고 그것이 특별한 이유를 직관적으로 설명하기 어려운 이유일 수 있습니다.

얽힘에 대한 일반적인 설명은 종종 두 상태 (1)과 (2)의 차이를 의미 있는 방식으로 구분하지 못합니다. 예를 들어, 얽힌 두 큐비트 중 하나를 측정하면 다른 큐비트의 상태가 즉시 영향을 받는다고거나, 두 큐비트의 상태를 별개로 설명할 수 없다는 식의 설명이 종종 나옵니다. 이런 설명들은 틀린 것은 아니지만, 왜 (2)의 비얽힘 확률적 상태에 대해서도 똑같이 적용되지 않는지 그 이유를 명확히 설명할 수 없습니다. 상태 (2)에서 나타나는 두 비트는 서로 밀접하게 연결되어 있으며, 각 비트는 문자 그대로 다른 비트에 대한 완벽한 기억을 가집니다. 그럼에도 불구하고 이 상태는 얽힘 상태가 아닙니다.

얽힘이 특별한 이유, 그리고 양자 상태 (1)이 확률적 상태 (2)와 어떻게 다른지를 설명하는 한 가지 방법은, 얽힘을 통해 무엇을 할 수 있는지, 또는 얽힘으로 인해 우리가 무엇을 경험할 수 있는지를 설명하는 것입니다. 이 강의에서 다룰 세 가지 예시는 바로 이런 특징을 가지고 있으며, 상태 (1)을 사용해서 할 수 있는 일들은 (2)와 같은 고전적으로 상관된 상태에서는 할 수 없는 일들입니다.

실제로, 양자 정보와 계산의 연구에서 얽힘은 다양한 작업을 수행할 수 있는 자원으로 간주됩니다. 이렇게 할 때, 상태 (1)은 하나의 얽힘 단위로 간주되며, 우리는 이를 e-bit이라고 부릅니다. ("e"는 "entangled" 또는 "entanglement"의 약자입니다. 상태 (1)은 두 큐비트의 상태이지만, 이 상태가 나타내는 얽힘의 양은 하나의 e-bit입니다.)

참고로, 확률적 상태 (2)도 하나의 자원으로 간주할 수 있습니다. 이는 하나의 공유된 무작위 비트를 나타내며, 예를 들어 암호화에서 매우 유용할 수 있습니다. 누군가와 비밀 키(또는 비밀 키의 일부)로 사용할 무작위 비트를 공유하면, 그 비트는 다른 사람이 알 수 없기 때문에 암호화에서 중요한 역할을 할 수 있습니다. 그러나 이번 강의에서는 얽힘에 초점을 맞추고, 얽힘을 통해 할 수 있는 몇 가지 작업을 다루겠습니다.

용어에 대한 설명을 추가하자면, 앨리스와 밥이 e-bit을 공유한다고 할 때, 이는 앨리스가 큐비트 A를 가지고 있고, 밥이 큐비트 B를 가지고 있으며, 함께 큐비트 쌍 (A, B)가 상태 (1)에 있다는 것을 의미합니다. 물론 큐비트의 이름은 다른 것으로 선택할 수 있지만, 이번 강의에서는 명확성을 위해 이러한 이름을 사용하겠습니다.

정리

이번 강의에서는 얽힘(entanglement)의 역할을 설명하기 위해 세 가지 중요한 예시를 다룹니다: 텔레포테이션, 슈퍼덴스 코딩, CHSH 게임. 이들은 모두 얽힘을 활용한 중요한 개념들로, 양자 정보에서 중요한 역할을 합니다. 각 예시는 얽힘이 실제로 어떻게 작용하는지, 그리고 그것이 왜 중요한지 이해하는 데 도움을 줍니다.

앨리스와 밥

앨리스와 밥은 정보 교환과 관련된 시스템에서 흔히 등장하는 가상의 인물로, 이들은 암호학 및 양자 정보 이론에서 자주 사용됩니다. 예를 들어, 앨리스는 송신자를, 밥은 수신자를 의미할 수 있습니다.

얽힘을 자원으로서

강의에서는 두 큐비트의 얽힌 양자 상태를 다시 살펴봅니다. 이 상태는 벨 상태 중 하나로, 얽힌 상태의 전형적인 예시로 자주 언급됩니다. 얽힘은 양자 상관관계를 의미하며, 이는 고전적인 확률적 상태와 구분됩니다. 예를 들어, 두 비트가 상관 관계를 가지지만 얽힌 상태는 아니며, 얽힘은 비고전적인 양자 상관관계를 의미합니다.

얽힘의 특성

얽힘은 두 상태가 서로 독립적으로 설명될 수 없는 상태를 의미합니다. 예를 들어, 얽힌 상태에서는 한 큐비트를 측정하면 다른 큐비트의 상태도 즉시 영향을 받지만, 확률적 상태에서는 그런 현상이 발생하지 않습니다. 얽힘은 양자 정보와 계산의 중요한 자원으로, 특정 작업을 수행할 수 있게 해줍니다. 이 상태는 "e-bit"이라고 불리며, 하나의 얽힘 단위를 나타냅니다.

e-bit과 공유된 무작위 비트

확률적 상태는 암호화에서 유용한 공유된 무작위 비트를 나타내며, 얽힘 상태는 e-bit이라는 양자 자원으로 간주됩니다. 이 강의에서는 얽힘을 중심으로 몇 가지 중요한 작업을 다루게 됩니다.