Quantum Information & Computation
Summary note

문진혁

January 14, 2026

Contents

Overview

해당 문서는 Quantum Information & Computation 을 공부하기 위해서 만들어 졌으며, 기본적인 순서는 IBM Quantum Information & Computation Course 를 따라갈 것이다.

해당 코스는 https://quantum.cloud.ibm.com/learning/en/courses 이며 해당 노트도 코스에 맞춰서 작성할 예정이다.

추가적인 내용과 미흡한 개념 같은 경우에는 추가로 양자계산과 양자정보(Nielsen Michael , Chuang, Isaac L.) 라는 책의 내용을 인용할 것이다.

Course 1. Basic of Quantum Information

Single Systems

Classical information

probability vector

- All entries are non negative real numbers (모든 entry는 음수가 아니어야 한다)
- The sum of the entries is 1. (모든 entry의 합은 항상 1이다)

Dirac notation

Σ를 classical state set이라고 한다면, 각 원소들의 위치에 대해서 다음 처럼 대응 시킬 수 있다.

$|a\rangle$ 은 column vector 이며, Σ에서 a 와 상응되는 벡터이다.

예시를 들면 $\{0,1\}$ 에서, $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ 라고 표현할수 있다.

그리고 위에서 예시로 든 vector를 standard basis vector라고 한다. 그리고 모든 vector들은 이 standard basis vector의 Linear combination으로 나타낼 수 있다.

추후에도 나오겠지만 해당 Dirac notation은 inner product와 outer product에 대해서도 비교적 간단하게 나타낼 수 있고, 각각이 의미하는 바에 대해서는 나중에 설명하게 된다. 간단하게 정리하면 outer product 형태는 해당 quantum Information에서 Operator와 같은 의미를 가진다.

Measure

어떤 확률 상태에서 system X를 측정한다면 어떻게 될지를 알아본다. classical state 에서는 여러 상태중에 하나가 측정되게 될것이다.

간단하게 생각해보면 주사위의 각 면이 나올 확률은 모두 1/6이 된다.

$$\frac{1}{6}|1\rangle + \frac{1}{6}|2\rangle + \frac{1}{6}|3\rangle + \frac{1}{6}|4\rangle + \frac{1}{6}|5\rangle + \frac{1}{6}|6\rangle$$

다음은 이 주사위의 각 면이 나올 확률을 probability vector로 나타낸 것이다. 보면 알겠지만 각 vector의 entry는 해당 상태가 나올 확률임을 알 수 있다.

Probabilistic operations

Probabilistic operation은 classical operator로, 다음과 같은 성질을 띄게 된다.

- All entries are nonnegative real numbers
- The entries in every column sum to 1 (각각의 column에서의 entry의 합은 1이다)
- 다음과 같은 형태가 예시이다. $\begin{pmatrix}1 & 1/2\\0 & 1/2\end{pmatrix}$

위에서 나온 operation은 stochastic matrix 라고도 불리며, 각 column의 row는 출력 확률을 나타낸다. 즉, 위의 예시는 다음 의미를 가진다. 현재 상태가 0인 경우에, 그대로이며, 만약 상태가 1이라면, 0.5의 확률로 bit flip이 일어난다는 뜻이다.

Composing operations

composing operation이란 여러개의 operations을 하나의 연산으로 묶는 것을 의미하며, 각 연산들은 matrix product로 이루어진다. 이때 먼저 한 연산이 나중 연산보다 오른쪽에 존재한다.

Classical Operation에서는 stochastic matrix 의 matrix product로 이루어지게 된다. 이때, product의 순서에 따라 결과값이 달라지게 되고, 이를 Not Commutative 하다고 한다.

Quantum information

지금까지 Classical Information을 알아봤다면 이제 Quantum State로 넘어가게 된다.

Quantum State도 Classical Information처럼 해당 System도 Column Vector 로 표현이 가능하고 다음과 같은 성질을 띄게 된다.

- The entries are complex numbers (각 Entry는 복소수이다)
- The sum of the absolute values squared of the entries must equal 1 (각 Entry의 절댓값의 제곱의 합은 항상 1이다)

고전 상태에서는 그냥 entry의 합이 1이였지만, 양자 상태에서는 절댓값의 제곱의 합이 1임이 다르기에 계산에 주의하여야 한다.

그리고 complex number로 구성된 vector의 Euclidean norm 표기 방법은 각 원소의 절댓값 제곱의 합에 루트를 씌운 형태이다. 이는 이후에 unit vector를 정의할때 꼭 필요하다.

$$\|\mathbf{v}\|_2 = \sqrt{\sum_{i=1}^{n} |v_i|^2}$$

dagger 고전 상태에서의 vector는 모두 real number entry이다. 하지만, 양자 상태에서의 vector는 complex number entry이므로, 만약 column vector를 row vector로 바꿀려면 transpose를 한 후에 켤레를 취해야한다. 이 일련의 과정을 †를 통해서 나타낸다.

$$\langle\psi| = |\psi\rangle^\dagger$$

Measuring quantum states

양자상태에서 측정을 하게 되면 고전 상태로 출력이 되게 된다. (양자역학에서 배우는 관측을 하면 값이 정해진다와 같은 맥락이다) 그리고 그 확률은 절댓값의 제곱과 같다.

이때 중요한 점은 복소수에서 절댓값의 제곱을 계산할때, 계산법을 혼동하면 안된다는 점이다. (이 점은 수학서적의 복소수 파트를 확인한다)

그리고 앞으로 이 요약노트에서는 $|0\rangle$을 측정하면 0이 나오고, $|1\rangle$을 측정하면 1이 나온다고 할것이다.

Unitary operations

이제부터 고전 상태와 양자상태의 큰 특징이 드러나는 operation들이 나오기 시작한다. 그중 가장 중요한 operation은 unitary operation 으로 다음과 같은 특징을 가진다.

- $U^\dagger U = \mathbf{I}, UU^\dagger$

하나 알수 있는건 unitary operation은 어떤 단위원 위에서 vector를 이동 시킨다. 이 말은 즉, $\|U\mathbf{v}\| = \|\mathbf{v}\|$ 임을 알 수 있다.

아까 위에서 나온 unitary의 특징을 보면 결국 U의 inverse matrix가 $U^\dagger$임을 알 수 있다. 즉 어떤 양자상태의 vector에 대해서 unitary operation을 취한 뒤에 다시 원래 상태로 즉 inverse matrix를 적용시킬 수 있다는 것을 알 수 있다.

Qubit unitary operations 이제 양자 상태에서 사용되는 기본적인 unitary operation을 설명한다.

- $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 은 bit flip gate로 $|0\rangle \to |1\rangle$ 같이 bit를 뒤집는다. (NOT GATE와 동일)
- $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ 은 bit를 뒤집지는 않지만 phase를 바꾸는 operation이다.
- $\sigma_y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 은 phase flip gate로 $|1\rangle \to -|1\rangle$ 와 같이 1인 경우의 phase를 뒤집는다.

- $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ 은 basis를 변환시키는 gate로 $|0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$ 처럼 작동한다. 이는 0과 1이 나올 확률을 절반으로 바꾸거나, 그 반대에서 사용하기도 하며, 나중에 bell state를 만들 때에도 사용한다.
- $P_\theta = \begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}$ 는 phase operation으로, θ 만큼 phase를 rotate 시킨다. 이때, 파생적으로 S 는 $\theta = \pi/2$ 일때이고, T 는 $\theta = \pi/4$ 일때이다.

Multiple Systems

이 단원부터는 두개 이상의 State를 다루게 된다.

Classical States

n개의 system이 있다면 우리는 n-tuple형태의 cartesian product 로 나타낼 수 있다.

- 해당 n-tuple형태를 간단히 string 형태로 표현이 가능하다.
- 해당 state sets의 순서는 lexicographical order를 따른다.
- 이 lexicographical order로 probabilistic states를 나타낼 수 있다.

Probabilistic states

위에서 나온 single system처럼 multiple system도 똑같이 probabilistic vector를 나타낼 수 있다. $\begin{pmatrix} 0.5 \\ 0 \\ 0 \\ 0.5 \end{pmatrix}$는 00 상태가 나올 확률이 0.5, 11 상태가 나올 확률이 0.5임을 나타낸다.

tensor Product

tensor product는 2개의 column vector를 하나의 vector로 만드는 연산이다. 다양한 표현방법이 있으며 여기에서는 생략한다.

Mesurements of probabilistic states

이 probabilistic state를 측정하는 방법은 위도 말했던 것처럼 각 상태의 entry가 해당 상태가 나올 확률이 된다. $\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle$은 측정 시에 00이 나올 확률은 .5 이고, 11이 나올 확률은 .5 임을 나타낸다.

그러면 만약 (X,Y)가 있는 probabilistic state에서 X를 측정하고, Y는 아무것도 하지 않는다면 어떤 일이 발생할까?

이에 대해서는 고등학교 수학에서 배운 조건부확률을 사용하면 되는데, X가 측정된 즉, X가 확정된 상태에서 Y=a일 확률을 구해주면 된다. 이는 전체 X=a,Y=b가 될 확률에서 X=a가 될 확률로 나누어주면 된다.

그럼 일단 tensor product로 이루어진 probabilistic state를 분리 시켜, X와 Y를 명확히 나누어준다. (Independent하기 때문에 가능하다) 그리고 X = a 이 나올 확률을 구해주고, 해당 $|a\rangle$ 와 tensor product된 부분을 해당 확률로 나누어 주면 된다.

Controlled-NOT

controlled not operation은 2 state 상태에서 사용이 가능하며, X가 1이면, Y는 NOT Operation 적용, X가 0이면 그대로 Y로 납두는 Operation이다.

이때 X는 control bit라 부르고, Y는 target bit라고 부른다.

Quantum states

Multiple system에서 quantum state vector는 column vector로 낱타내며, Cartesian product를 각각의 system에 대해서 한 형태이다.

$$\{0,1\} \times \{0,1\} = \{00, 01, 10, 11\}$$

Tensor product로 이루어진 quantum state vector도 quantum state vector인데, 이때 이 벡터의 상태는 product states 즉, 중첩된 상태라고 불린다. 그리고 이 상태는 독립적이므로, 각 system들은 서로에게 간섭하지 않는다.

이에 반하여, product 상태가 아닌 quantum state vector도 있다.

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

이 경우가 그런 경우인데, 증명은 contradiction을 사용하여 증명한다.

이러한 벡터들중 하나는 Bell states / Bell basis라고 불린다.

이런 것들은 모두 tensor product로 분해할수 없다는 특징을 가진다.

Measurements

quantum state에서의 측정은 원하는 상태의 bra 형태를 내적하여 나타낼 수 있고, 그 결과로 해당 상태가 나올 확률을 구할 수 있다.

만약 $a_1...a_n$이라는 상태가 나올 확률을 측정하고 싶다면, $|\langle a_1...a_n|\psi\rangle|^2$ 으로 확률을 구할 수 있다.

그러면 (X,Y) 가 있는 quantum state에서 X를 측정하고, Y는 가만히 두면 어떻게 될까?

여기에서 붕괴 (collapse)라는 개념이 나오게 되는데, 붕괴란 새로운 상태로 바뀌게 되는 것을 의미한다.

XY가 Tensor Product라면은 사실상 두 상태는 독립적이기 때문에 X가 측정이 되어도 Y는 상태가 바뀌지 않는다.

하지만 entangle 상태라면 두 상태는 얽혀있어서 X가 측정되는 순간 Y는 붕괴가 되어 새로운 확률을 얻게 된다. (조건부)

unitary operations

unitary operation들도 모두 tensor product를 통해서 multiple system operation으로 바뀔 수 있다.

대표적으로는 **SWAP GATE**가 있는데 (X,Y)의 한 상태를 (Y,X)로 교환 시키는 연산이다.

$$\text{SWAP} = \sum_{a,b\in\Sigma} |a\rangle\langle b| \otimes |b\rangle\langle a|, SWAP|\phi\otimes\psi\rangle = |\psi\otimes\phi\rangle$$

또한 이런 tensor product를 아용하여 controlled-U 라는 operation을 만들수 있다. 마찬가지로 control bit에 대해서 target bit가 U operation을 취하는 것이다. 기본적으로 controlled-NOT Operation도 해당 형태이다.

예시로는 controlled-SWAP opeation (on three qubits) 는 Fredkin operation이라고도 불리며, control bit에 따라 나머지 2개의 bit가 swap하는 형태이다.

다른 예시로는 controlled-controlled-NOT operation으로 Toffoli operation이라고도 불리며, 2개의 control bit를 가지고, 해당 비트가 모두 11 인 경우에 target bit가 NOT operation을 수행하는 형식이다.

Quantum Circuits

Quantum Circuit이란 qubits와 gate들이 연결된 모델을 의미 하며, 각 Operation들의 곱으로 이루어져있다.

이미 이전 chapter에서 여러가지 single gate, Controlled-NOT, Swap gate, Toffoligate, Fredkin gate 등 여러가지 operation을 알아보았고, 이제 이 operation들의 적절한 곱 연산을 통해 새로운 operation을 만들고, 각 qubit에 연결하여 Quantum Circuit을 만들어 볼 수 있다.

Projection Mesurements

Projection은 2가지 성질을 가지고 있다.

- $\Pi = \Pi^\dagger$ 이는 Hermitian 성질로, 항상 기댓값이 실수임을 나타낸다.
- $\Pi^2 = \Pi$ 이는 이미 Projection Measure을 했다면, 그 값은 여러번 연산을 적용해도 바뀌지 않는다는 것을 나타낸다.

모든 Projection matrix Π는 다음처럼 정의된다.

$$\Pi = \Sigma_{k=1}^{m} |\psi_k\rangle \langle\psi_k| , \sum \Pi_k = I$$

이때 사용되는 ψ_k는 orthonormal set이다.

그러면 이 projection을 사용하면 어떤일이 일어날까?

$|\psi\rangle$ 를 측정한다고 하면, outcome k는 다음 확률로 측정이 될것이다.

$$\Pr(outcome = k) = \| \Pi_k |\psi\rangle \|^2 = \langle\psi| \Pi_k |\psi\rangle$$

그리고 이렇게 측정된 시스템의 상태는 다음처럼 붕괴될 것이다.

$$\frac{\Pi_k |\psi\rangle}{\| \Pi_k |\psi\rangle \|}$$

또한 만약 2개의 시스템인경우 ,(X,Y) 인 경우에, X만 측정하고, Y는 아무것도 안했다고 한다면, 우리는 다음처럼 projective measurement를 표현해볼 수 있다. $|a\rangle \langle a| \otimes 1_Y$

그리고 모든 projective measurements는 unitary operation과 standared basis measurements를 사용하여 구현할 수 있다.

Irrelevance of global phases

$|\phi\rangle = \alpha|\psi\rangle, \quad |\alpha| = 1$ 을 만족하면, 둘의 phase가 다르다고 한다. 하지만 둘의 phase가 다르다고 해서 측정 확률이 달라진다거나 하지 않는다. 이 global phases는 측정이 되는 순간 의미가 없어지기 때문이다.

$$\Pr(a \mid |\phi\rangle) = |\langle a|\phi\rangle|^2 = |\langle a|e^{i\theta}|\psi\rangle|^2 = |e^{i\theta}|^2 |\langle a|\psi\rangle|^2 = |\langle a|\psi\rangle|^2$$

그래서 위상만 다른 두 벡터들은 결국 어떤 연산을 해도 같고, 양자정보에서는 각각의 벡터가 아닌 하나의 상태에 대한 동치류로 판단한다.

No - cloning theorem

이부분은 양자정보에서 중요한 파트 중 하나이다. 상태는 복제할수 없다는 의미이다. 임의의 양자 상태에서 $|\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$을 만족하는 Unitary 연산은 존재하지 않는다는 것이다. 이는 양자역학의 선형성과도 이루어지는 문제이다. 중첩 상태에서는 연산은 각 상태에서 각각 이루어지는 것이 아닌, 전체 상태에 대해서 일어나는 것이기 때문이다.

기저 상태에서는 CNOT 게이트를 얽힘을 이용하여 cloning과 같은 효과를 낼 수 있다. 이는 control bit와 target bit의 상관관계를 이용하여 상태를 정하는 것 뿐이다.

Discriminationg non-orthogonal states

고전 상태에서는 물체가 다른상태이면 구별이 가능하다. 예를 들면 동전과같은 경우이다. 하지만 양자역학에서는 직교상태가 아닌 이상 비직교 상태에서는 정확히 구별이 불가능하다. 그 이유는 비직교 상태에서는 이걸 구별할수 있는 measurement가 존재하지 않기 때문이다. 이미 비직교 상태는 예를 들면 두 직교성분을 가지고 있기 때문에, 측정을 하게 되면 100% 확률로 구별이 불가능하다.

Entanglement in Action

Quantum Teleportation

Alice는 Bob에게 어떤 qubit을 전송하고 싶어 한다. 이때 이 전송을 하기 위해서는 Alice는 Classical infromation만 전송이 가능하다. (No-Cloning theorem) 때문에 qubit 자체를 복사할수 없기 때문이다.

그래서 이 Teleportation을 하기 위해 Alice와 Bob은 공통적으로 e-bit을 공유함을 전제로 시작한다.

1. Alice는 controlled-NOT gate를 구현한다. (Q는 control, A (e-bit)은 target)
2. Alice는 Q에 Hadamard operation을 적용한다.
3. Alice는 A와 Q를 측정하고, outcome a,b를 얻게 된다.
4. Alice 는 a와 b를 Bob에게 보낸다.
5. Bob은 두개의 step을 수행하는데, 만약 a = 1이면 B (e-bit)에 X-Gate를 적용한다, 만약 b = 1이면 B에 Z게이트를 적용한다.

이 protocol을 통하면 최종적으로 Bob의 qubit B는 Q와 같은 상태를 지니게 된다.

그러면 이론적으로 매우 먼 거리에서도 서로 공통 e-bit를 가지고 있다면 teleportation이 가능하다. 하지만 이는 결국 고전적인 한계에 막히게 되는데, 외냐하면 어떻게 classic information인 a,b를 보낼 것인가이다.

superdense coding

Alice는 bob에게 2개의 classical bit을 전송하고 싶어한다. 그래서 Alice는 하나의 single qubit을 보낼것이고, Alice와 Bob은 e-bit을 공유한다.

1. Alice는 A(e-bit)에 b를 control로 가지는 Z gate와 a를 control로 가지는 x gate를 적용시킨 후, Bob에게 전송한다.
2. Bob은 A에 따라 B에 CNOT 연산을 하고, A는 H gate를 적용 시킨 후 측정을 하고, B도 측정을 한다.
3. B는 측정결과로 a를, A는 측정 결과로 b를 얻게 된다.

superdense coding도 마찬가지로 Alice의 qubit A를 Bob에게 전송시켜야 하기 때문에 고전적인 한계에 막히게 된다.