Quantum Algorithms (Childs) 학습일지

김태원

2023년 10월 9일

차 례

서문

본고는 양자 알고리즘 강의록이다. 우선 양자 정보 기초 과정을 수강한 대학원생이 대상이다. 이들 기초 과정은 보통 쇼어의 인수분해 알고리즘 (1994) 혹은 그로버의 탐색 알고리즘 (1996) 같은 양자 알고리즘 분야의 초창기 돌파구를 다룬다. 본고는 지난 25년간 개발된 양자 알고리즘 여럿을 탐구하여 양자컴퓨팅에 이보다 많은 것이 존재한다는 사실을 보인다.

이 강의록은 양자 알고리즘 분야의 몇 가지 주요 주제를 여섯 부분으로 나눠 다룬다.

- I편에서는 양자 회로를 다룬다. 특히 양자 알고리즘을 주어진 보편 양자 회로 집합으로 나타내는 문제를 다룬다.

제 1 장

기초

1장은 양자계산에 대한 배경 지식을 일별한다. 우리는 이들 주제를 아주 높은 수준으로 다루는데, 강의록을 이해하기 위해 알아야 하는 내용의 감을 잡기 위해서다. 이들 주제가 낯설다면, 양자계산에 대한 교재를 통해 보충할 수 있다. Nielsen과 Chuang [3], Kitaev, Shen, Vyalvi [2], Kaye, Laflamme, Mosca [1]의 교재를 참고하라.

1.1 양자 데이터

양자컴퓨터는 계산을 수행하기 위해 정보의 양자역학적인 표현을 사용하는 장치다. 정보는 양자 비트, 복소벡터공간상의 ℓ_2-정규화된 벡터로 나타낼 수 있는 상태로 저장된다. 이를테면 우리는 n 큐비트의 상태를 아래처럼 작성할 수 있으며

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x |x\rangle \tag{1.1}$$

여기서 $a_x \in \mathbb{C}$는 $\sum_x |a_x|^2 = 1$을 만족한다. 우리는 상태의 기저 $|\psi\rangle$를 계산 기저라고 부른다.

더 추상적인 형식으로 데이터를 저장하는 것이 양자 상태라고 받아들이는 편이 종종 유용하다. 이를테면 군 G가 주어질 때, 군 원소 $g \in G$에 대응하는 기저 상태에 대해 $|g\rangle$라고 쓰고

$$|\phi\rangle = \sum_{g\in G} b_g |g\rangle \tag{1.2}$$

라고 군에 대한 임의의 중첩을 나타낸다. 우리는 비트 문자열로 군 원소를 나타내는 효율적인 표준 방식이 존재한다고 가정하겠다. 보통 이런 표현을 명시적으로 보일 필요는 없다.

양자 컴퓨터가 상태 $|\psi\rangle$와 상태 $|\phi\rangle$를 저장한다면, 총 상태는 이들 두 상태의 텐서곱으로 주어진다. 이를 $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle\,|\phi\rangle = |\psi, \phi\rangle$라고 나타낸다.

제 I 편

양자 회로

제 2 장

선형대수

2.1 스펙트럼 이론

스펙트럼spectral 이론은 선형 연산자의 구조를 파악하기 위한 개념이다. 벡터공간 V에 대해 아래와 같은 선형변환이 존재하여 자기 자신과 곱할 수도 있고 제곱이나 다항식을 취할 수도 있다고 하자.

$$A : V \to V$$

스펙트럼 이론은 연산자를 작은 부분으로 나눠 각 부분을 따로 분석하자는 발상이다. 아래와 같은 식이 있다고 하자.

$$x_{n+1} = Ax_n, \quad n = 0, 1, 2, \ldots,$$

여기서 $A : V \to V$는 선형변환이고 x_n은 시간 n상의 계가 지니는 상태다. 초기 상태 x_0이 주어질 때 시간 n상의 상태 x_n을 알고자 한다거나 x_n의 장기간 행태를 분석하고자 할 수 있다. 물론 $x_n = A^n x_0$이다. 하지만 n이 조금만 커져도 $A^n x_0$을 계산하기 어렵다. 이에 대한 도구가 바로 고윳값*eigenvalues*과 고유벡터다. 스칼라 λ가 존재하여 아래를 만족한다고 하자.

$$Ax_0 = \lambda x_0$$

그렇다면 아래가 성립하며 λ는 스칼라이기에 계산이 어렵지 않다.

$$A^n x_0 = \lambda^n x_0$$

정의 2.1. 스칼라 λ는 0이 아닌 벡터 $v \in V$가 존재하여 아래를 만족하는 경우

$$Av = \lambda v$$

연산자 $A : V \to V$의 고윳값이라고 하며 v는 A의 고유벡터라고 한다.

λ가 고윳값이라는 사실을 안다면 고유벡터를 어렵지 않게 찾을 수 있다. 그냥 아래

를 풀면 된다.

$$Ax = \lambda x$$
$$\Leftrightarrow (A - \lambda I)x = 0$$

정의 2.2. A의 스펙트럼 $\sigma(A)$는 A의 모든 고윳값의 집합이다.

제 3 장

기초

3.1 양자 데이터

큐비트는 복소벡터공간상의 ℓ_2-정규화 벡터로 나타낼 수 있는 상태다. 이를테면 n 큐비트의 상태는 아래처럼 적는다.

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle$$

이때 ℓ_2-정규화 벡터란 $a_x \in \mathbb{C}$가 아래를 만족한다는 뜻이다.

$$\sum_x |a_x|^2 = 1$$

상태 $|x\rangle$의 기저를 계산기저*computational basis*라고 부른다고 한다. 군 G에 대해 $g \in G$에 대응하는 기저 상태를 $|g\rangle$라고 나타내고, 군에 대한 임의의 중첩은 아래처럼 나타낸다.

$$|\phi\rangle = \sum_{g \in G} b_g |g\rangle$$

양자컴퓨터가 상태 $|\psi\rangle$와 $|\phi\rangle$를 저장할 때 총 상태는 이들 두 상태의 텐서곱으로 아래처럼 나타낼 수 있다.

3.2 양자 회로

양자 상태에 대해 가할 수 있는 연산은 정규화된 상태에서 정규화된 상태로 사상하는 것이 있다. 이를 유니타리 연산자 U라고 부르고 U는 아래를 만족한다.

$$UU^\dagger = U^\dagger U = I$$

3.3 보편 게이트 집합

원리상 n 큐비트에 대한 유니타리 연산은 모두 하나 혹은 두 개의 큐비트로 구성된 게이트만으로 구현할 수 있다. 따라서 이들 하나 혹은 두 개의 큐비트로 구성된 게이트의 집합은 보편적이라고 한다.

회로는 유니타리 연산에 적절하게 근사해야 한다. 게이트 $U_1, U_2, \ldots, U_t$로 구성된 회로는 아래를 만족하는 경우 U에 정밀도 ϵ으로 근사한다.

$$\|U - U_t \cdots U_2 U_1\| \leq \epsilon$$

여기서 $\|\cdot\|$은 노름 가운데 하나로 $\|U - V\|$가 작을 때 U를 V와 구분하기 어려워야 한다는 조건을 지닌다. 이런 노름 가운데 하나로 스펙트럼spectral 노름을 꼽을 수 있다.

$$\|A\| := \max_{|\phi\rangle} \frac{\|A|\psi\rangle\|}{\||\psi\rangle\|}$$

여기서 $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$는 $|\psi\rangle$의 2-노름을 나타낸다. 스펙트럼 노름은 A의 최대 특잇값singular value으로 볼 수 있다. 벡터를 최대한 늘릴 수 있는 행렬로 생각하면 된다.

참고 문헌

[1] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An Introduction to Quantum Computing.* Oxford University Press, 2006.

[2] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation.* American Mathematical Society, USA, 2002.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.