

Quantum and quantum-inspired linear algebra (Tang, 2023) 학습일지

김태원

최초 작성 : 2023년 9월 4일

최근 편집 : 2023년 9월 4일

제 1 장

블록 인코딩 개요

해밀토니언 H 는 계의 전체 에너지에 대응하는 연산자이며, 해밀토니언 시뮬레이션은 1982년 파인만(Richard Feynman)이 고안한 양자정보학 문제다. 파인만의 요지는 해밀토니언 시뮬레이션이 계의 크기에 따라 지수적인(exponential) 증가를 보이니까 양자컴퓨터라는 물건이 필요할지도 모른다는 것이었다.

해밀토니언 시뮬레이션. H 를 m 개의 파울리(Pauli) 행렬로 구성한 해밀토니언이라고 하자. 다시 말해,

$$E_a \text{가 파울리 행렬들의 텐서곱일 때, } H = \sum_{a=1}^m \lambda_a E_a.$$

e^{-iHt} 에 근접하여 $\|U - e^{-iHt}\| \leq \epsilon$ 인 유니타리 U 를 구현하는 알고리즘을 찾아라.

여기서 (1) 파울리 행렬, (2) e^{-iHt} , (3) 유니타리 같은 용어가 낯설 수 있겠다. 우선 파울리 행렬의 정의에 유니타리의 정의가 필요하므로 유니타리 U 부터 정의한다.

정의 1.1. 복소 정방행렬 U 는 켈레전치 행렬 U^\dagger 가 U 의 역행렬이기도 할 때 유니타리다. 즉 항등행렬 I 에 대해 유니타리 행렬 U 는 다음과 같다.

$$U^\dagger U = U U^\dagger = U U^{-1} = I.$$

파울리 행렬은 유니타리 뿐만 아니라 에르미트(Hermitian), 거듭(involutory) 행렬로 정의되므로 에르미트와 거듭 행렬도 살핀다.

정의 1.2. 에르미트 행렬 H 는 켈레전치 H^\dagger 와 H 가 같은 복소 정방행렬이다. 즉

$$H = H^\dagger.$$

정의 1.3. 거듭행렬은 A 가 A 자신의 역행렬인 정방행렬이다. 즉

$$A^2 = I.$$

정의 1.4. 파울리 행렬은 에르미트, 유니타리, 거듭의 조건을 모두 만족하는 2×2 복소 행렬의 집합이며 아래 σ_i 를 원소로 지닌다.

$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

따라서 해밀토니언 H 는 상호작용하는 E_a 들의 합으로 볼 수 있고 이때 λ_a 는 그런 상호작용의 강도를 결정한다. 어떤 시간 t 에 상태 $|\alpha\rangle$ 가 주어진다고 하자. 시간이 $t = T$ 로 변화할 때 상태는 $|\alpha(T)\rangle$ 로 나타내는데 이는 $|\alpha\rangle$ 에 유니타리 (시간 변화) 연산자 U_1 를 적용한 것과 같다. 여기서

$$U_1 = e^{-iHT}$$

H 는 해밀토니언을 나타내고, T 는 시간을 나타낸다. 반면 해밀토니언 시뮬레이션에서는

$$\|U - e^{iHt}\| \leq \epsilon$$

이므로 구해야 하는 유니타리 U 는 해밀토니언 H 와 시간 T 에 대한 시간 변환 연산 U_i 에 근사하는 연산이다.

보통 이 문제의 답은 충분히 큰 r 에 대해 아래와 같은 트로터 Trotter 근사로 주어진다.

$$e^{-iHt} \approx (e^{-iE_1 t/r} e^{-iE_2 t/r} \dots e^{-iE_m t/r})^r.$$

하지만 이 해는 최적과는 거리가 멀다. 왜냐하면 위와 같은 근사는 양자회로의 게이트 개수에 대응하는 게이트 복잡도 gate complexity가 $\text{poly}(1/\epsilon)$ 만큼 요구되기 때문이다. 다시 말해 ϵ 의 역원에 대해 다항인 만큼 게이트들이 요구되기 때문이다. 개선된 알고리즘들은 저자 Ewin Tang가 제시하는 프레임워크를 따른다. 이 프레임워크는 다음과 같은 절차를 지닌다.

- (i) “블록-인코딩 block-encoding”이라는 양자 회로의 유형을 정의한다.
- (ii) 주어진 λ_a, E_a 에 대해 H 의 효율적인 블록-인코딩을 구성할 수 있다는 사실을 보인다.
- (iii) H 에 대한 블록-인코딩을 적게 사용하여 e^{-iHt} 의 근사에 대한 블록-인코딩을 취할 수 있다는 사실을 보인다.
- (iv) 이 블록-인코딩을 사용해 한 상태에 대해 근사를 내놓는다.

1.1 블록-인코딩

정의 1.5. 주어진 $A \in \mathbb{C}^{r \times c}$ 에 대해 $U \in \mathbb{C}^{d \times d}$ 는 U 가 $\mathcal{O}(Q)$ 게이트로 구현가능하고 아래 조건을

$$B_{L,1}^\dagger U B_{R,1} = A$$

항등 행렬의 첫 r 과 c 열인 $B_{L,1} \in \mathbb{C}^{d \times r}, B_{R,1} \in \mathbb{C}^{d \times c}$ 에 대해 만족하면 A 의 Q -블록 인코딩이라고 한다.

다시 말해, U 의 임의의 원소 \cdot 에 대해

$$U = \begin{pmatrix} A & \cdot \\ \cdot & \cdot \end{pmatrix}$$

인 경우다. 또한 $\Pi_L = B_{L,1} B_{L,1}^\dagger, \Pi_R = B_{R,1} B_{R,1}^\dagger$ 이 각각 $B_{L,1}$ 과 $B_{R,1}$ 의 생성에 대한 사영에 대응하도록 한다.

d, r, c 를 2의 지수승으로 자주 나타낼 예정인데 모든 것을 큐비트로 다루려는 목적이다. 이에 정의 1.5는 아래처럼 나타낼 수 있다.

$$(\langle 0|^{\otimes a_L} \otimes I) U (|0\rangle^{\otimes a_R} \otimes I) = A.$$