양자 컴퓨팅:
응용적 접근

제9 장 문제 :
양자 컴퓨팅 방법

1. 이 문제는 여러분이 어떻게 양자 컴퓨터를 이용하여 단일 큐비트의 기대값을 구할 수 있는지 안내해줍니다.
   a. 큐비트의 양자상태를 $|\psi\rangle$ 라고 합시다. 보른 규칙에 의해 $|0\rangle$ 상태를 측정할 확률 $p(0) = |\langle 0|\psi\rangle|^2$ 를 증명하십시오.
   b. 위와 비슷하게 $|1\rangle$ 상태를 측정할 확률 $p(1)$ 를 증명하십시오.
   c. 사영연산자(projector) $\Pi_0 = |0\rangle\langle 0|$ 와 $\Pi_1 = |1\rangle\langle 1|$ 를 정의해봅시다. 이때, $p(0) = \langle\psi|\Pi_0|\psi\rangle$ 이고 $p(1) = \langle\psi|\Pi_1|\psi\rangle$ 임을 보이십시오.
   d. $Z = \Pi_0 - \Pi_1$ 임을 증명하십시오.
   e. $\langle\psi|Z|\psi\rangle = p(0) - p(1)$ 임을 증명하십시오. 즉, Z-기저로 (여러번) 측정하면, 우리는 결과값의 빈도수의 차를 구함으로써 파울리 Z의 기대값을 추정할 수 있습니다.
   f. 이제 $\langle\psi|X|\psi\rangle$ 를 측정하고 싶다고 가정해봅시다. 계산 기저(computational basis, Z-기저)에서 측정하기 전 위의 단계에서 아다마르(Hadamard) 게이트를 더하여 이를 수행할수 있음을 보이십시오. 힌트: $HZH = X$

g. 위와 같은 아이디어를 $\langle\psi|Y|\psi\rangle$에도 적용할 수 있습니다. 어떠한 게이트(들)이 계산기저에서 측정하기 전에 수행되어야 할까요?

2. 문제 1에서 우리는 어떻게 단일 큐비트 기대값을 측정하는지 보았습니다. 이제 큐비트 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$가 주어졌을 때, $\alpha = 3/5$이고 $\beta = 4/5$라고 합시다.
   a. 해석적으로 $\langle X\rangle$, $\langle Y\rangle$ 및 $\langle Z\rangle$를 계산하십시오. 여기서 각진 괄호는 ψ에서의 기대값을 의미합니다.
   b. 양자 상태 $|\psi\rangle$를 준비하기 위한 양자 회로를 설계하십시오.
   c. $\langle X\rangle$를 추정하기 위한 양자 회로를 설계하십시오. 회로의 측정 횟수를 증가시킴으로써 어떻게 정확도(accuracy)를 향상시킬 수 있을까요?
   d. Y 및 Z에 대해서 c번 문제를 수행하십시오.

3. 여러 큐비트에서 정의된 해밀토니언의 경우, 우리는 $X \otimes Z$와 $Y \otimes Y \otimes Z$ 같은 연산자들의 기대값을 측정해야할 수 있습니다. 이러한 연산자를 우리는 일반화된 파울리 연산자(generalized Pauli operators)라고 부릅니다.
   a. 간단한 경우인 일반화된 파울리 연산자 $X \otimes Z$를 고려해봅시다. 문제 1을 통해 우리는 각 항의 기대값을 어떻게 계산하는지를 알았습니다. 이제 우리가 $H \otimes I$를 구현하고, Z기저에서 측정한 뒤, $p(00) - p(01) - p(10) + p(11)$를 계산하면 $\langle X \otimes Z\rangle$를 계산할 수 있음을 보이십시오. 여기서 $p(00)$란 두 큐비트를 측정할 때 비트열 00을 측정할 확률을 의미하며, 다른 경우도 이와 같습니다.
   b. 일반화된 파울리 연산자가 모든 유나타리에 대해 기저를 형성함을 증명하십시오. 문제 1-3을 종합하면, 어떠한 유니타리 행렬의 기대값도 (비록 효율적으로 할 수는 없을지라도) 추정할 수 있음을 보입니다.

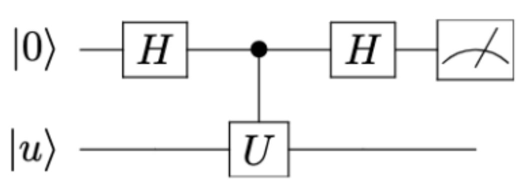
c. 다음의 단일 큐비트 유니타리들을 파울리 연산자들의 합으로 표현하십시오.
   i. H
   ii. S
   iii. T
   iv. $\theta = \pi/4$ 일 때 $R_Y(\theta)$

4. 유니타리 U의 기대값을 추정하기 위해 양자 위상 추정(quantum phase estimation, QPE) 알고리즘을 사용 해봅시다. 그리고 제어-U 게이트를 u 개 게이트들을 사용해 회로안에 구현할 수 있다고 해봅시다. 만일 n개 큐비트의 정밀도(precision)을 사용한다고 할 때, 그 회로에 얼마나 많은 총 게이트가 필요할까요? $1 \leq n \leq 10$ 에 대해 게이트의 수를 도식해보십시오.
5. 반복적 양자 위상 추정(iterative quantum phase estimation, IQPE)는 위상 추정 알고리즘을 더 적은 자원을 사용하게끔 수정한 알고리즘입니다. 위상추정에서 우리는 n 비트 길이의 고유값을 추정하기 위해 n 큐비트의 정밀도를 지닌 단일 회로를 사용합니다. 반복적 양자 위상 추정 알고리즘에서는, n비트 길이의 고유값을 추정하기 위해 한 개 큐비트 정밀도를 지닌 n개의 회로를 사용합니다. 다음의 세 개의 부분들에 대해, m개 큐비트에 대한 유니타리 U를 정의해봅시다.

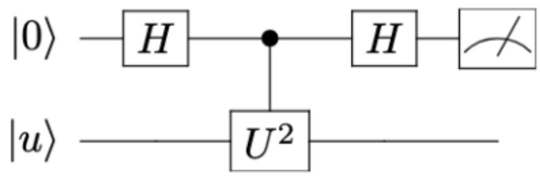
$$U|u\rangle = e^{2\pi i\phi}|u\rangle$$

나아가, ϕ 는 이진수 전개 $\phi = 0.\phi_1\phi_2\cdots\phi_n$, 즉 $\phi = \sum_{j=1}^{n}\phi_j 2^{-j}$ 로 표현된다고 가정합니다.

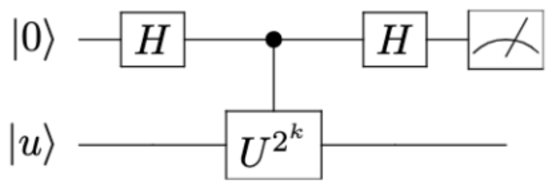
   a. 다음의 회로가 ϕ_1를 추정함을 보이십시오.



b. 다음의 회로가 ϕ_2 를 추정함을 보이십시오.



c. 다음의 회로가 를 추정함을 보이십시오.



d. 위와 같은 구조의 n개의 회로가 를 추정하기에 충분함을 보이시오.
e. 단일 회로에 필요한 게이트들의 최대수는 얼마입니까? 제어-U가 u개 게이트들로 구성된 1개의 회로에 구현될 수 있다고 가정해봅시다. 이 답과 4번 문제와 어떻게 비교되나요? 설명해보십시오.
f. 모든 n개 회로들에서 필요한 총 게이트의 수는 얼마입니까? 이 답과 4번 문제와 어떻게 비교되나요? 설명해보십시오.

6. 편향된 양자 난수 비트 발생기 알고리즘을 설계해보십시오. 이 알고리즘은 $|0\rangle$ 를 25%의 확률로 출력하고 $|1\rangle$ 를 75%의 확률로 출력합니다.
7. 고전 컴퓨터에서 난수를 어떻게 생성하는지 설명하십시오. 이러한 방식으로 생성된 비트열의 무작위성(randomness)를 어떻게 테스트할 수 있나요?
8. 양자 컴퓨터에 접근할 수 없다고 가정할 때 최소 2개 이상의 난수 생성 방식을 제안해 보십시오.

문헌 관련 문제들

1. 변분적 양자 인수분해(variational quantum factoring, https://arxiv.org/abs/1808.08927) 논문의 저자들은 소인수분해를 위한 근미래 양자 알고리즘입니다. 이 알고리즘은 이 장에서 논의한 QAOA의 (특히 인수 해밀토니안 H_f에 대한) 구현 으로 이해할 수

있습니다. 주어진 정수를 소인수분해 하기 위해 이 해밀토니안을 어떻게 구성할까요?

2. 낮은 깊이의 기울기 측정이 변분적 하이브리드 양자-고전 알고리즘의 수렴을 향상시킬 수 있다(Low-depth gradient measurements can improve convergence in variational hybrid quantum-classical algorithms, https://arxiv.org/abs/1901.05374) 논문에서는 다음의 함수 기울기(gradient)의 유한차이 근사를 설명합니다.

$$\frac{\partial f}{\partial \theta_i}(\theta) \approx \frac{1}{2\epsilon}(f(\theta + \epsilon \hat{e}_i) - f(\theta - \epsilon \hat{e}_i))$$

왜 이 공식이 $\frac{\partial f}{\partial \theta_i}(\theta) \approx (f(\theta+\epsilon\hat{e}_i) - f(\theta))/\epsilon$ 보다 더 선호될까요?

3. Harrow와 Napp는 기울기 및 비-기울기 오라클의 특별한 블랙박스 모델을 정의합니다. 실제 양자 컴퓨터와 이들 블랙박스 모델들이 어떤 면이 같고 다를까요?

4. 이 논문의 정리들이 기울기와 비-기울기 최적화의 경우를 어떻게 해결하나요? 그 가정들을 어떻게 이해할까요?

5. 고정된 제어 매개변수에 대하여 양자 근사 최적화 알고리즘의 목적 함수 값이 전형적인 예들에 집중한다.(For fixed control parameters the Quantum Approximate Optimization Algorithm’s objective function value concentrates for typical instances, https://arxiv.org/abs/1812.04170) 논문은 고정된 값 p에서 QAOA알고리즘의 3-정규 그래프 위에서 정의된 최대 컷(MaxCut)을 위한 비용함수의 기대값이 그래프가 크기만 하면 그래프에 독립적이라고 말합니다. 왜 그런지 설명해보십시오. 4-정규 그래프에 대해 고려하면 결과가 어떻게 달라질까요?