Quantum Computing

Vaughn Sohn

November 19, 2024

Contents

Chapter 1

Quantum Algorithms

Lecture 9

1.1 Introduction

7 Oct. 10:30

이번 챕터에서 우리는 *Quantum Algorithm*에 대해 다루고자한다. Quantum algorithm은 quantum circuit이나 quantum computer에서 구현되는 알고리즘을 지칭한다. Classical computer가 어려운 문제를 해결하기 위하여 만들어진 것처럼, quantum algorithm에 대해서 공부하고 새로운 방식을 고안하는 것은 quantum computer의 동작방식과 quantum computer의 한계를 분석하기 위한 중요한 과제이다. Quantum computer라는 개념이 등장하고 나서부터 지금까지 많은 종류의 quantum algorithm들이 고안되어 왔다. 이번 강의에서 다루고자하는 quantum algorithm은 다음과 같다.

- Elementary quantum algorithms
- Hamiltonian simulations
- Quantum Fourier transform
- Phase estimation
- Quantum search algorithm (Grover search algorithm)
- Amplitude amplification / estimation algorithms
- HHL algorithm

1.2 Elementary quantum algorithms using quantum parallelism

Quantum mechanics만의 특징을 이용할 수 있는 quantum computer는 *Quantum parallelism*이라는 특성을 가진다. 이는 quantum computer가 특정 oracle; function $f(x)$에 대하여 동시에 여러개의 입력에 대한 결과를 병렬적으로 얻을 수 있다는 의미이다. 고전적인 개념인 $f(x)$를 quantum computer에서 실행하기 위해서는, quantum computer의 연산단위인 *unitary operator*로 함수를 표현해야하는 필요가 있다.

먼저, 간단한 one-bit boolean function $f : \{0,1\} \to \{0,1\}$를 생각해보자. 직관적으로, 이 함수에 대응되는 operator는 다음과 같이 설계할 수 있다. 이 operator는 $f(0) = 1$이라면, $U_f |0\rangle = |1\rangle$처럼 동작하도록 quantum gate들을 이용하여 구현된다.

$$|x\rangle \xrightarrow{U_f} |f(x)\rangle$$

그러나 이러한 방식으로 operator를 설계하게 되면, *non-invertible* 함수 $f(x)$에 대한 operator는 더이상 unitary 조건을 만족하지 못한다. 따라서 이 문제를 해결하기 위하여 control을 수행하는 추가적인 input qubit을 추가하여 unitary operator가 되도록 설계한다.

Definition 1.2.1 (Unitary oracle). 함수 f에 대한 unitary operator U_f는 다음과 같이 정의된다.

$$|x\rangle |y\rangle \xrightarrow{U_f} |x\rangle |y \oplus f(x)\rangle$$

$|x\rangle$는 f의 입력으로 사용되는 **oracle qubit**이며, $|y\rangle$는 1일때는 $f(x)$의 결과를 flip 시키고 0일 때는 $f(x)$의 결과를 반환하는 역할을 수행한다. 그럼 이렇게 설계한 unitary operator에 *superposition state*를 $|x\rangle$로 제공하면 결과적으로 우리는 다음과 같은 two-qubit state를 얻게 된다.

$$|+\rangle|y\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2}}(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle)$$

즉, one-bit boolean function에서 가능한 모든 입력 0, 1에 대한 출력을 U_f를 한 번 호출함으로써 얻게 된 것이다! Classical computer에서 병렬연산은 서로 다른 컴퓨팅 자원을 사용할 뿐, f를 여러번 호출해야 하는 사실은 변하지 않지만, quantum computer에서의 병렬연산은 실제로 f를 한 번 호출하여 모든 연산을 수행할 수 있다.

이렇게 어떤 함수 f에 대응되는 unitary operator를 설계하는 것은 n-bit boolean function에 대해서 쉽게 일반화할 수 있다. n-bit boolean function $f : \{0,1\}^n \to \{0,1\}$에 대응되는 unitary operator는 Definition 1.2.1을 이용하여 쉽게 설계할 수 있으며, 더 나아가 n-qubit에 대한 superposition state를 입력으로 제공하면 다음 결과를 얻게된다.

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle \to \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

이 회로를 이용하면 한 번의 연산만으로 2^n개의 입력에 대한 출력을 동시에 얻을 수 있다. 그러나 한 가지 주의해야할 점은, 우리가 결과를 측정하는 순간 여러개의 superposition output은 사라지고 확률에 따라서 단 하나의 결과만을 얻을 수 있다는 사실이다. 따라서 이러한 quantum parallelism만의 독특한 특징을 잘 활용하여 효과적인 연산을 수행할 수 있도록 알고리즘을 설계하는 것이 중요하다.

이 강의에서는 parallelism의 장점을 활용하는 대표적인 알고리즘들(e.g., Deutsch's algorithm, Deutsch-Josza algorithm, Simon's algorithm, and Bernstein-Vazirani algorithm)에 대해 소개한다.

1.2.1 Deutsch's algorithm

Deutsch's algorithm은 주어진 one-bit boolean function f이 **balance**인지 **constant**인지를 판단하는 문제를 해결한다.[1] Classical computer가 이 문제를 해결하기 위해서는 두 함숫값 $f(0), f(1)$을 비교하기 위해서 반드시 2번의 함수 호출이 필요하다. 그러나, 지금부터 우리는 quantum computer는 **단 한번**의 gate call만으로 이 문제를 해결할 수 있음을 보이고자한다.

1. input state : 우리는 다음과 같은 state를 input으로 제공한다.

$$|\psi\rangle = |0\rangle|1\rangle$$

2. apply Hadamard gates on both qubits : H gate를 가하면, 다음과 같은 상태로 변화한다.

$$|\psi\rangle = |+\rangle|-\rangle$$

3. apply U_f : operator를 통과한 state는 다음과 같다.[2]

$$\begin{aligned}|\psi\rangle &= U_f\left(\frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle)\right)\\ &= \frac{1}{2}(|0, f(0)\rangle|1, f(1)\rangle - |0, 1\oplus f(0)\rangle - |1, 1\oplus f(1)\rangle)\\ &= \frac{1}{2}\Big(|0\rangle(-1)^{f(0)}(|0\rangle - |1\rangle) + |1\rangle(-1)^{f(1)}(|0\rangle - |1\rangle)\Big)\\ &= \frac{1}{2}\sum_{x\in\{0,1\}}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)\end{aligned}$$

따라서 각 case에 대해 state는 다음의 2가지 모습을 띄게 된다.

$$|\psi\rangle = \begin{cases}\pm|+\rangle|-\rangle & \text{if } f(0) = f(1)\\ \pm|-\rangle|-\rangle & \text{if } f(0)\neq f(1)\end{cases}$$

[1] constant: $f(0) = f(1)$, balance: $f(0)\neq f(1)$

[2] $|f(x)\rangle - |1\oplus f(x)\rangle$는 $f(x)$의 값에 따라서, $|0\rangle - |1\rangle$ $(f(x) = 0)$ 또는 $|1\rangle - |0\rangle$ $(f(x) = 1)$이 된다.

4. apply again Hadamard gates on oracle qubit : 마지막으로 oracle qubit에 H gate를 가하면, f의 종류에 따라서 다음과 같은 상태가 된다.

$$|\psi\rangle = \begin{cases} \pm|0\rangle|-\rangle & \text{if } f(0) = f(1) \\ \pm|1\rangle|-\rangle & \text{if } f(0) \neq f(1) \end{cases}$$

따라서, oracle qubit을 측정하면, 100%의 확률로 0 또는 1의 값을 얻게될 것이며, 그 값에 따라서 우리는 f가 balance인지 constant인지를 다음 규칙에 따라서 쉽게 판단할 수 있다. □

$$|\psi\rangle = \begin{cases} constant & \text{if } q_o = 0 \\ balance & \text{if } q_o = 1 \end{cases}$$

Deutsch's algorithm은 classical algorithm보다 quantum algorithm 알고리즘이 더 효과적임을 보인 첫 번째 알고리즘이다. 하지만, 그 효과는 단지 2번의 호출을 1번으로 줄일 뿐이다. 따라서 지금부터 더 효과적인 알고리즘들에 대해서 소개하고자한다.

Lecture 10

1.2.2 Deutsch-Jozsa algorithm

14 Oct. 10:30

Deutsch-Jozsa algorithm은 간단히 말하자면, one-bit boolean function에 대한 문제인 Deutsch-Jozsa algorithm을 n-bit boolean function에 대한 문제로 일반화한 것이다. 즉, n-bit boolean function $f : \{0,1\}^n \to \{0,1\}$이 **constant**인지 **balanced**인지를 판단하는 문제를 해결하는 알고리즘이다.[3] 마찬가지로 classical computer가 이 문제를 해결하기 위해서는 최대 $2^{n-1}+1$개의 function value를 비교해야하기 때문에 $2^{n-1}+1$번의 함수 호출을 필요로한다. 그러나, 지금부터 이런문제를 해결하려고 할 때도, quantum computer는 **단 한번**의 gate call만으로 이 문제를 해결할 수 있음을 보일 것이다.

1. input state : 우리는 다음과 같은 state를 input으로 제공한다. $\{0,1\}^n$의 가능한 모든 input을 나타내기 위하여, oracle qubit은 n개의 qubit으로 구성된다.

$$|\psi\rangle = |0\rangle^{\otimes n}|1\rangle$$

2. apply Hadamard gates on both qubits: 이때, $|+\rangle^{\otimes n}$은 가능한 모든 2^n개의 n-bit string들의 superposition이기 때문에, 다음과 같이 표현할 수 있다.

$$\begin{aligned} |\psi\rangle &= |+\rangle^{\otimes n}|-\rangle \\ &= \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

3. apply U_f : operator를 통과한 state는 다음과 같다. (Deutsch's algorithm의 표현을 이용하자)

$$\begin{aligned} |\psi\rangle &= U_f \frac{1}{\sqrt{2^{n+1}}}\Big(\sum_{x\in\{0,1\}^n} |x\rangle(|0\rangle - |1\rangle)\Big) \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \end{aligned}$$

4. apply again Hadamard gates on oracle qubit : H gate를 임의의 n-qubit computational basis에 가한 결과는 다음과 같다. 이는 single qubit에 대한 동작을 n-qubit에 대해 *독립적*으로 적용한 결과이다.

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}|z\rangle \tag{1.1}$$

이를 이용하여 H gate를 적용한 state를 표현하면, 다음과 같다.

$$|\psi\rangle = \frac{1}{2^n} \sum_{x,z\in\{0,1\}^n} (-1)^{f(x)+x\cdot z}|z\rangle|-\rangle$$

[3] 여기서 말하는 balanced는 2^n개의 input중에서 2^{n-1}개의 input에 대한 결과가 0이고, 나머지 2^{n-1}개의 input에 대한 결과가 1인 경우를 의미한다.

만약 $f(x)$가 constant function이라면, $\forall x$에 대해서 $f(x)$의 값은 항상 동일하기 때문에, $(-1)^{f(x)}$의 값이 $+1$, 또는 -1이라는 constant가 되어 다음과 같이 나타낼 수 있다.

$$|\psi\rangle = \pm\frac{1}{2^n}\sum_{x,z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle\,|-\rangle$$

$z = 0^n$인 경우를 가정해보자. 이는 x가 어떤 값이 되던지간에 $x\cdot z$ [4]의 값이 0이 되기 때문에, 다음과 같이 표현할 수 있게 된다. $|0\rangle^{\otimes n}$의 amplitude의 square norm이 1이기 때문에, 100% 확률로 0^n을 측정할 수 있다.

$$\pm\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot 0^n}|0\rangle^{\otimes n}\,|-\rangle = \pm\frac{1}{2^n}2^n\,|0\rangle^{\otimes n}\,|-\rangle = \boxed{\pm\,|0\rangle^{\otimes n}\,|-\rangle}$$

반면, $f(x)$가 balance function이라면, $f(x)$의 값이 0인 경우와 1인 경우가 정확히 1/2씩 나타나기 때문에, 각 항들이 소거되면서 $z = 0^n$에 대한 amplitude가 0이 된다.

$$\Big(\frac{1}{2^n}2^{n-1}|0\rangle^{\otimes n}\,|-\rangle\Big) + \Big(-\frac{1}{2^n}2^{n-1}|0\rangle^{\otimes n}\,|-\rangle\Big) = \boxed{0\,|0\rangle^{\otimes n}\,|-\rangle}$$

따라서, oracle qubit을 측정한 결과가 0^n인지 확인하여, f가 constant인지 balanced인지를 알 수 있다. □

$$|\psi\rangle = \begin{cases} constant & \text{if } q_o = 0^n \\ balance & \text{if } q_o \neq 0^n \end{cases}$$

1.3 Hamiltonian simulations

Hamiltonian simulation은 quantum computer가 고안된 핵심적인 이유 중 하나이다. 리처드 파인만의 말을 인용하자면 자연, 그중에서도 특히 미시세계는 고전역학을 따르지 않기때문에, quantum mechanical을 따르는 simulation이 필요하다.

> **Note.** *Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.*

Hamiltonian simulation은 간단히 말해 quantum state의 time evolution을 구하는 것이다. Schrödinger equation에 의하면, initial state $|\psi(0)\rangle$의 시간 t에 대한 time evolution은 다음과 같이 주어진다.

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

이 방정식을 곧바로 해결하여 문제를 풀 수도 있지만, Hamiltonian matrix의 크기가 exponential하게 증가하기 때문에 이를 classical algorithm으로 효과적으로 해결하기는 어렵다.

1.3.1 Solution of Hamiltonian simulations

우리는 k-local Hamiltonian을 이용하여 Hamiltonian simulation 문제를 해결하고자 한다.

Definition 1.3.1. k-local[a] Hamiltonian은 주어진 H가 n-qubit system에서 **최대 k개의 system**에 대해서만 동작하는 H_i들의 합으로 표현되는 Hamiltonian이다. (이때 L은 n에 대해 polynomial이다.)

$$H = \sum_{i=1}^{L} H_i$$

[a] 여기서 local은 geometrically local이 아니라 단순히 system의 '개수'를 나타내기 위해 사용된다.

Example. 예를 들어, 다음과 같이 정의되는 Hamiltonian은 2개의 system (2, 4)에 대해서만 동작한다.

$$H_i = I_1 \otimes Z_2 \otimes I_3 \otimes X_4 \otimes I_\perp$$

[4] $x\cdot z = x_1z_1 + x_2z_2 + \cdots + x_nz_n \mod 2$

Hamiltonian이 k-local Hamiltonian이라고 가정할 때, 이를 이용하여 어떻게 문제를 해결할 수 있을까? 그 아이디어는 단순하다. e^{-iHt}를 계산하는 것은 어렵지만, e^{-iH_it}는 최대 $k << n$ subsystem에만 작용하기에 더 단순하며, 그 단순성 덕분에 quantum circuit을 사용하여 시뮬레이션 하기 쉽다.

만약, $[H_j, H_k] = 0$[5]이 성립한다면 $e^{-iHt} = e^{-i\sum H_j t} = \prod e^{-iH_j t}$[6]가 성립하기 때문에, 각각의 H_i에 대한 time evolution을 독립적으로 계산한 결과를 곱하여 전체 time evolution을 쉽게 구할 수 있다. 그러나 일반적으로 $[H_j, H_k] = 0$은 성립하지 않기 때문에, 우리는 Trotter formula를 이용한다.

Theorem 1.3.1 (Trotter formula). Hermitian operator H_j, H_k에 대하여, 어떤 t에 대해서도 다음이 성립한다.[a]

$$e^{i(H_j+H_k)t} = \lim_{m\to\infty}\left(e^{iH_jt/m}e^{iH_kt/m}\right)^m$$

이는 H_j, H_k가 not-commute라 하더라도 항상 성립한다.

[a] 직관적으로, 주어진 time t 대신에, 매우 짧은 시간간격인 t/m에 대한 time evolution을 m번 반복하여 t에 대한 time evolution을 근사할 수 있다는 것을 의미한다.

따라서 $L = 2$인 k-local Hamiltonian $H = H_1 + H_2$에 대해, Hamiltonian simulation을 수행하는 propagator $\tilde{U}(t) = e^{-iH_1t}e^{-iH_2t}$를 시간에 대해서 미분하면, 다음과 같이 전개할 수 있다. (with initial condition $\tilde{U}(0) = I$)

- Eq. (1.3): H_1, H_2는 matrix라서 순서를 바꿀 수 없기에, 다른 항을 더하여 항을 정리하고 다시 뺀다.
- Eq. (1.4): commutator를 사용하여 항을 정리한다.

$$\begin{aligned}
i\frac{d\tilde{U}(t)}{dt} &= H_1e^{-iH_1t}e^{-iH_2t} + e^{-iH_1t}H_2e^{-iH_2t} && (1.2)\\
&= (H_1+H_2)\,e^{-iH_1t}e^{-iH_2t} + e^{-iH_1t}H_2e^{-iH_2t} - H_2e^{-iH_1t}e^{-iH_2t} && (1.3)\\
&= He^{-iH_1t}e^{-iH_2t} + \left[e^{-iH_1t}, H_2\right]e^{-iH_2t} && (1.4)\\
&= H\tilde{U}(t) + \left[e^{-iH_1t}, H_2\right]e^{-iH_2t} && (1.5)
\end{aligned}$$

미분 방정식에 대한 Duhamel's formula [7]를 이용하면, $\tilde{U}(t)$를 다음과 같이 구할 수 있다.

$$\tilde{U}(t) = U(t) - i\int_0^t e^{-iH(t-s)}\left[e^{-iH_1s}, H_2\right]e^{-iH_2s}ds \tag{1.6}$$

1.3.2 Performance

그렇다면, 이제 실제 Hamiltonian에 대한 time evolution $U(t) = e^{-iHt}$와 Trotter formula를 이용하여 근사한 $\tilde{U}(t)$의 error가 어떻게 bound 되는지 분석해보자. Eq. (1.6)의 항을 이항시키면, 두 operator의 차이에 대한 norm의 upper bound를 구할 수 있다. [8]

$$\|\tilde{U}(t) - U(t)\| = \left\|-i\int_0^t e^{-iH(t-s)}\left[e^{-iH_1s}, H_2\right]e^{-iH_2s}ds\right\| \le \int_0^t \left\|\left[e^{-iH_1s}, H_2\right]\right\| ds \tag{1.7}$$

이때, norm은 다음과 같이 정의된다.

Definition 1.3.2.

$$\|A\| \triangleq \max_{|\psi\rangle}\|A|\psi\rangle\|_2 = \max_{|v\rangle\neq 0}\frac{\|A|v\rangle\|_2}{\||v\rangle\|_2}$$

이제 이 norm이 적절한 error rate ϵ에 의하여 bound됨을 보임으로써, 이 Hamiltonian simulation을 실제로 활용할 수 있을지 분석할 수 있다.

[5] $[H_j, H_k] = H_jH_k - H_kH_j$
[6] 지수함수의 성질이 성립하기 위해서 필요한 조건. 실수들은 항상 commutative하기 때문에 이 성질이 자명하게 정립되었던 것
[7] See https://en.wikipedia.org/wiki/Duhamel%27s_principle
[8] e^{-iH_it}는 unitary operator이기 때문에 norm을 변화시키지 않기 때문에 무시해도 된다.

이를 위하여 다음과 같은 새로운 연산자를 가정하자.

$$G(t) \triangleq [e^{-iH_1t}, H_2]e^{iH_1t} = e^{-iH_1t}H_2e^{iH_1t} - H_2, \text{ with } G(0) = 0 \tag{1.8}$$

이 연산자에 대하여 $\tilde{U}(t)$처럼 시간에 대한 도함수를 구하면 다음과 같고,

$$i\frac{d}{dt}G(t) = e^{-iH_1t}\,[H_1, H_2]\,e^{iH_1t}$$

양변을 t에 대해서 적분하면 다음과 같다.

$$G(t) = G(0) - i\int_0^t e^{-iH_1s}\,[H_1, H_2]\,e^{iH_1s}ds$$

norm을 취하고 *triangle inequality*를 이용하면, $\|G(t)\|$에 대한 upper bound를 얻는다.

$$\|G(t)\| = \left\|-i\int_0^t e^{-iH_1s}\,[H_1, H_2]\,e^{iH_1s}ds\right\| \le \int_0^t \|\,[H_1, H_2]\,\|ds = t\|\,[H_1, H_2]\,\| \tag{1.9}$$

이때, $G(t)$의 norm은 자기자신의 정의 (1.8)에 의하여 다음 관계가 성립하게 된다.

$$\left\|\left[e^{-iH_1t}, H_2\right]\right\| = \|G(t)\| \le t\,\|[H_1, H_2]\|$$

따라서 이를 Eq. (1.7)에 대입하면, 다음을 얻는다.

$$\|\tilde{U}(t) - U(t)\| \le \int_0^t \underbrace{\left\|\left[e^{-iH_1s}, H_2\right]\right\|}_{s\|[H_1,H_2]\|} ds \le \int_0^t s\,\|[H_1, H_2]\|\,ds$$

$\|[H_1, H_2]\|$는 s에 관계없는 상수이기 때문에, 다음과 같이 정리할 수 있으며,

$$\|\tilde{U}(t) - U(t)\| \le \frac{t^2}{2}\,\|[H_1, H_2]\|$$

commutator를 전개한 뒤, triangle inequality와 norm의 성질[9]을 이용하면 다음과 같이 전개할 수 있다.

$$\begin{aligned}\|\tilde{U}(t) - U(t)\| \le \frac{t^2}{2}\,\|[H_1, H_2]\| &= \frac{t^2}{2}\,\|H_1H_2 + (-H_2H_1)\| \le \frac{t^2}{2}(\|H_1H_2\| + \|H_2H_1\|) \\ &\le \frac{t^2}{2}2\|H_1\|\|H_2\| \le t^2\max\{\|H_1\|, \|H_2\|\}^2\end{aligned}$$

정리하면, 다음과 같다.

$$\|\tilde{U}(t) - U(t)\| = \|U(t) - \tilde{U}(t)\| \le t^2\max\{\|H_1\|, \|H_2\|\}^2 \tag{1.10}$$

따라서 시간간격 Δt에 대한 error는 다음과 같이 bound된다.

$$\left\|e^{-iH\Delta t} - \left(e^{-iH_1\Delta t}e^{-iH_2\Delta t}\right)\right\| \le (\Delta t)^2\max\{\|H_1\|, \|H_2\|\}^2 \tag{1.11}$$

Trotter formula에 의하여 시간간격 $\Delta t = t/m$에 대하여 m단계 근사의 오차는 Δt에 대한 단일 단계 오차의 누적으로 생각할 수 있기 때문에, 다음을 얻는다.

$$\left\|e^{-iHt} - \left(e^{-iH_1\Delta t}e^{-iH_2\Delta t}\right)^m\right\| \le m\frac{t^2}{m^2}\max\left\{\|H_1\|, \|H_2\|\right\}^2 = \frac{t^2}{m}\max\left\{\|H_1\|, \|H_2\|\right\}^2$$

이 bound를 사용하면, 우리가 원하는 target error rate ϵ을 달성하기 위해서 필요한 m의 값을 $m = O(t^2\epsilon^{-1})$으로 결정할 수 있다.[10]

이 과정을 더 많은 term을 가지는 k-local Hamiltonian에 대해서 일반화할 수 있다.

$$\left\|e^{-i\sum_{i=1}^L H_i\Delta t} - \prod_{j=1}^L e^{-iH_i\Delta t}\right\| = O\left(\frac{t^2}{L}\sum_{i<j}\|[H_i, H_j]\|\right).$$

[9] $\|AB\| \le \|A\|\|B\|$

[10] $\max\{\|H_1\|, \|H_2\|\}^2$ (i.e., $\|H_i\|$)의 값은 상수라서 무시하였다.

$\Delta t = t/m$로 가정하면 다음을 얻는다.

$$\left\| e^{-i\sum_{i=1}^{L} H_i t} - \left(\prod_{j=1}^{L} e^{-iH_i \Delta t} \right)^m \right\| = O\left(\frac{m\Delta t^2}{L} \sum_{i<j} \|[H_i, H_j]\| \right) = O\left(\frac{t^2}{mL} \sum_{i<j} \|[H_i, H_j]\| \right)$$

이때, $\|H_i\| = O(1)$이므로 $\sum \|[H_i, H_j]\| = L^2$이 되어 다음과 같이 bound된다.

$$\left\| e^{-i\sum_{i=1}^{L} H_i t} - \left(\prod_{j=1}^{L} e^{-iH_i \Delta t} \right)^m \right\| = O\left(\frac{Lt^2}{m} \right).$$

$m = O(Lt^2\epsilon^{-1})$로 설정하게되면 우리는 항상 target error rate ϵ을 upper bound로 가지는 근사 operator $\tilde{U}(t)$를 구성할 수 있고 이를 이용하여 simulation 할 수 있다. 따라서, 이 solution은 주어진 k-local Hamiltonian에 대하여, time t에 대한 quadratic overhead (i.e., error)를 가지고 simulation을 할 수 있음을 보여준다. 즉, simulation time이 증가하더라도 error rate은 polynomial하게 증가하게 된다. □

반면, 2nd-Trotter formula를 이용하여 표현할 수도 있다.

$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2} e^{iB\Delta t} e^{iA\Delta t/2} + O\left((\Delta t)^3\right)$$

이를 이용하면, time t에 대하여 error는 다음과 같이 표현된다.

$$\left\| e^{-i(A+B)t} - \prod_{i=1}^{m} e^{-iA\Delta t/2} e^{-iB\Delta t} e^{-iA\Delta t/2} \right\| = O\left(m(\Delta t)^3\right) = O\left(t^3/m^2\right)$$

즉, $m = O(t^{3/2}\epsilon^{1/2})$으로 설정하면, target error rate ϵ을 달성할 수 있으며 이는 1st-Trotter formula를 사용한 simulation보다 더 효율적이다.[11] 2nd-Trotter 방법을 L개의 term을 갖는 Hamiltonian에 대하여 일반화하면 m은 다음과 같다.

$$m = O\left(\frac{\left(\sum_{j=1}^{L} \|H_j\| t\right)^{3/2}}{\epsilon^{1/2}} \right)$$

더 나아가 pth order Trotter formula를 사용하면, m은 다음과 같다.

$$m = O\left(\frac{\left(\sum_{j=1}^{L} \|H_j\| t\right)^{1+1/p}}{\epsilon^{1/p}} \right)$$

Hamiltonian simulation을 위하여 다양한 연구들이 현재까지도 진행되고 있으며, 대표적인 알고리즘들은 다음을 참고하라.

- Higher-order product formula [Chi+21]
- Linear combination of unitary (LCU) [BCK15]
- Quantum signal processing (*optimal*) [Haa19]

Lecture 11

1.4 Quantum Fourier transform

16 Oct. 10:30

1.4.1 Quantum Fourier transform

Quantum Fourier transform은 Shor algorithm이나 HHL algorithm과 같은 다양한 quantum algorithm에서 사용되는 중요한 알고리즘이다. QFT에 대해서 소개하기에 앞서, 먼저 classical Fourier transform에 대해서 간단히 알아보자.

[11] time t에 대한 3/2 overhead

Definition 1.4.1 (Discrete Fourier transform). Discrete Fourier transform은 vector $\mathbf{x} \in \mathbb{C}^N$을 입력으로 받아서, 다음과 같이 정의되는 연산을 수행하여 output vector $\mathbf{y} \in \mathbb{C}^N$으로 변환하는 과정이다.[a]

$$y_k \triangleq \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$$

[a] $\mathbf{x} = x_0 \cdots x_{N-1}$, $\mathbf{y} = y_0 \cdots y_{N-1}$

Definition 1.4.2 (Quantum Fourier transform). Quantum Fourier transform은 DFT와 유사하게, quantum state vector $|x\rangle = |x_0 \cdots x_{N-1}\rangle$을 입력으로 받아서, output quantum state vector $|y\rangle = |y_0 \cdots y_{N-1}\rangle$으로 변환하는 과정이다. 단, DFT와는 다르게 **computational basis** $\{|0\rangle, \cdots, |N-1\rangle\}$에 대한 변환만이 정의되어 있다.

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle.$$

따라서 임의의 state vector $|x\rangle$의 transform은 변환된 basis vector $|k\rangle$들의 linear combination으로 표현하게 된다.

$$\sum_{j=0}^{N-1} x_j |j\rangle \to \sum_{j=0}^{N-1} x_j \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle = \sum_{k=0}^{N-1} y_k |k\rangle,$$

이때, y_k는 다음과 같다.[a]

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}.$$

[a] DFT와 똑같다.

즉, QFT가 하는일은 basis $\{|k\rangle\}$에 대한 linear combination으로 표현된 벡터 $|x\rangle$를 다른 basis $\{|j\rangle\}$에 대한 linear combination으로 나타내는 *basis transform*이다.[12]

이제 QFT가 어떻게 구현되는지 알아보자. $|j\rangle$에 대한 변환을 수행하는 QFT의 circuit은 다음과 같다.

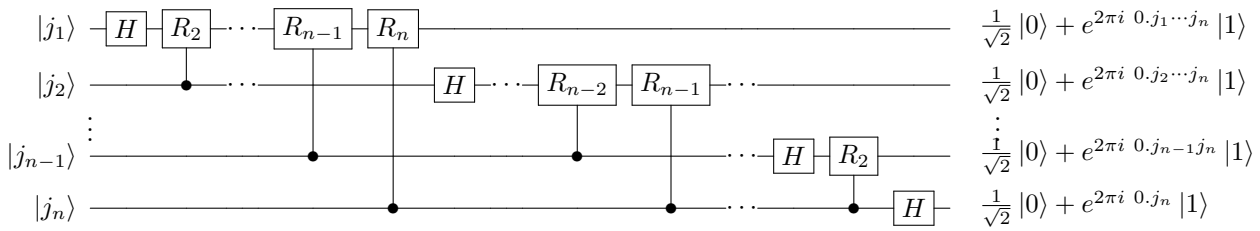


Figure 1.1: QFT circuit

QFT가 n-qubit system에 대해서 computational basis를 변환시킬 때, 우리는 computational basis를 나타내기 위하여 binary representation을 도입하고자한다. 어떤 $|j\rangle \in \{|0\rangle, \cdots, |2^n - 1\rangle\}$에 대한 binary representation은 다음과 같다. ($N = 2^n$)

$$j = j_1 j_2 \ldots j_n = j_1 2^{n-1} + \cdots + j_n 2^0 = \sum_{k=1}^{n} j_k 2^{n-k}.$$

또한, 소수도 다음과 같은 binary representation으로 표현할 수 있다.

$$0.j_l j_{l+1} \cdots j_m = j_l/2 + j_{l+1}/2^2 + \cdots + j_m/2^{m-l+1} = \sum_{k=l}^{m} j_k/2^{k-l+1}$$

[12] $\{|k\rangle\}$ basis에서의 amplitude는 x_i이며, $\{|j\rangle\}$ basis에서의 amplitude는 y_i이다.

Binary representation을 이용하면 QFT의 연산을 다음과 같이 분석할 수 있다.

- Eq. (1.12): Definition 1.4.2에 따라, $|j\rangle$에 대한 QFT는 다음과 같이 표현된다.
- Eq. (1.13): $k = \sum k_l 2^{n-l}$이므로 $k/2^n = \sum k_l 2^{-l}$이다.
- Eq. (1.14): $e^{a+b} = e^a e^b$, 그리고 $|k\rangle$가 n-qubit에 대해 tensor product로 표현됨을 이용한다.
- Eq. (1.15): 표현 단순화. ($\sum_{k_1,k_2,\cdots,k_n\in\{0,1\}}$ 을 $\sum_{k_l\in\{0,1\}}$로 표현)
- Eq. (1.16): (1) $k_l = 0$, then $e^{2\pi i j k_l 2^{-l}} = e^0$. (2) $k_l = 1$, then $e^{2\pi i j k_l 2^{-l}} = e^{2\pi i j 2^{-l}}$
- Eq. (1.17): 모든 tensor product들을 전개한뒤 fraction을 binary representation으로 표현한다.

$$|j\rangle \to \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle \tag{1.12}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1, \ldots, k_n\rangle \tag{1.13}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \tag{1.14}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \tag{1.15}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle\right] \tag{1.16}$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle\right)}{2^{n/2}} \tag{1.17}$$

즉, $|j\rangle$의 각 qubit $|j_i\rangle$에 대해 독립적으로 특정 gate U를 적용하여 $|0\rangle + e^{2\pi i 0.j_i \cdots j_n}$가 되도록 quantum circuit을 설계하면, 그 결과가 QFT에 해당한다는 사실을 알아냈다.

$$U|j_i\rangle \to |0\rangle + e^{2\pi i 0.j_i \cdots j_n}|1\rangle$$

본격적으로 quantum circuit을 만들기 위해서 rotation operator R_k를 다음과 같이 정의하자. 이렇게 정의한 operator는 $|0\rangle$에 대해서는 아무것도 수행하지 않지만, $|1\rangle$에 대해서는 phase $e^{2\pi i/2^k}$를 적용한다.

$$R_k \triangleq \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

Fig. 1.1의 연산을 단계별로 따라가보자.

1. input state : 다음과 같은 input state로 시작한다. 이는 computational basis state중 하나이다.

$$|\psi\rangle = |j_1, \cdots, j_n\rangle$$

2. apply Hadamard gate on the first qubit : 첫 번째 qubit; $|j_1\rangle$에 H를 적용하면, 다음을 얻는다. [13]

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{j_1}|1\rangle)|j_2, \cdots, j_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)|j_2, \cdots, j_n\rangle$$

3. apply controlled-R_2 gate with the first qubit as the *target* and the second qubit as *control*.

$$|\psi\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)|j_2, \cdots, j_n\rangle & \text{if } j_2 = 0, \\ \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.01} e^{2\pi i 0.j_1}|1\rangle\right)|j_2, \cdots, j_n\rangle & \text{if } j_2 = 1 \end{cases}$$
$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right)|j_2, \cdots, j_n\rangle.$$

[13] 이때, $e^{i\pi} = e^{2i\pi\frac{1}{2}} = -1$ 그리고 $e^0 = e^{2i\pi\frac{0}{2}} = 1$라는 사실을 이용한다.

4. apply controlled-R_k gate consequently : 3번의 과정을 control qubit을 하나씩 증가시키면서 반복한다. 이때, control qubit의 순서가 i번째라면, R_i gate를 적용해야한다.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)|j_2, \cdots, j_n\rangle$$

5. apply controlled-R_k gate consequently with other *target state* : 3-4번 과정을 다른 control qubit에 대해서 반복한다.

   예를 들어, second qubit을 target qubit으로서 가정하면, 다음과 같은 state를 얻게된다.

$$|\psi\rangle = \frac{1}{\sqrt{2}^2}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 j_3 \cdots j_n}|1\rangle\right)|j_3, \cdots, j_n\rangle$$

   일반화하면, j번째 qubit에 대해, $k(j<k)$번째 qubit을 control qubit으로 controlled-R_{k-j} gate를 차례대로 적용하는 과정을 반복한다.

6. n번째 qubit까지 이 과정을 수행하면 최종적으로 다음 state를 얻게된다.

$$|\psi\rangle = \frac{1}{\sqrt{2}^n}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 j_3 \cdots j_n}|1\rangle\right)\cdot\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)$$

7. 따라서 SWAP gate를 적용하여 qubit의 순서를 반대로 뒤집으면, 우리가 구하고자하는 QFT의 결과 (see Eq. (1.17))를 얻을 수 있다. □

따라서 우리는 1번의 QFT circuit을 수행하는 것으로 n개의 data에 대한 QFT결과를 동시에 얻을 수 있다. (단, 관측하면 확률에 따라 하나의 결과만 얻게 된다.)

1.4.2 Performance

그렇다면, QFT가 가지는 gate complexity가 얼마인지 분석해보자. 알고리즘에 따라 첫 번째 qubit에 대해서 1개의 H-gate, 그리고 $(n-1)$개의 controlled rotation gate를 필요로한다. 두 번째 qubit에 대해서는 1개의 H-gate, 그리고 $(n-2)$개의 controlled rotation gate를 필요로한다. 따라서 n개의 qubit에 대해 모두 필요한 gate의 개수는 다음과 같다.[14]

$$n + n - 1 + \cdots + 1 = \frac{n(n+1)}{2} = \Theta(n^2)$$

Some Remarks

- QFT는 exponential speed-up을 달성하는 것처럼 보이지만, 실제로는 값을 관측하게 되면 하나의 데이터에 대한 결과만 얻을 수 있다.
- 또한, input state $|j\rangle$를 준비하는 과정도 효과적이지 못하다.
- 따라서 QFT을 활용하여 알고리즘을 설계하는 것은 쉽지 않다.

1.5 Phase estimation

1.5.1 Phase estimation

QFT를 활용하는 중요한 알고리즘 중 하나가 바로 *phase estimation*이다. phase estimation이 해결하고자 하는 문제에 대해서 먼저 소개한다. 다음의 관계를 만족하는 unitary operator U에 대해, 우리가 알고 있는 것은 오직 eigenvector인 $|u\rangle$이고 eigenvalue는 알지 못한다고 하자.

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

Phase estimation의 목적은 eigenvalue에 대한 phase $\varphi \in [0,1)$를 구하는 것이다.

Eigenvector를 알고있을 때, eigenvalue를 구하는 문제에는 다양한 활용이 존재한다. 예를 들어, 주어진 Hamiltonian에 대해 ground state의 energy를 추정하는 상황을 가정하자. k-local Hamiltonian $\hat{H}$와 ground state $|\psi_0\rangle$에 대해 다음이 성립한다.

$$\hat{H}|\psi_0\rangle = E_0|\psi_0\rangle$$

따라서, 우리가 E_0를 estimate하기를 원한다는 것은 $\hat{H}$에 대한 eigenvector $|\psi_0\rangle$이 알려져있을 때 eigenvalue를 구하는 것을 의미하며, 이는 phase estimation으로 해결할 수 있는 문제이다.[15]

[14] qubit의 순서를 바꾸기 위해 필요한 SWAP gate에 대한 gate complexity는 $O(n)$이므로 무시할 수 있다.

[15] $\hat{H}$를 unitary operator $\hat{U} = e^{-i\hat{H}t}$로 구성하면, $\hat{U}$에서 eigenvalue는 e^{-iE_0t}가 된다. (with matrix exponential)

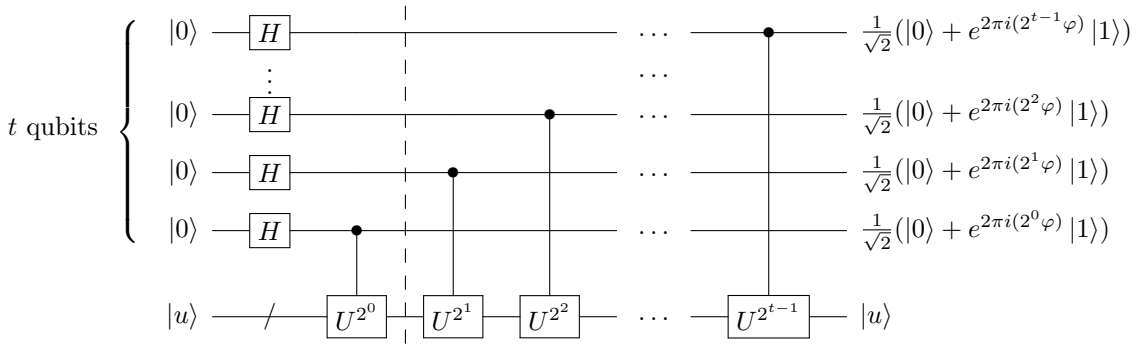


Figure 1.2: QPE circuit (first step)

Phase estimation을 설계하기 위해, 우리는 먼저 다음과 같은 oracle들을 가지고 있다고 가정한다.

- eigenvector $|u\rangle$를 준비시킬 수 있는 oracle
- controlled-U^{2^j} operation을 수행할 수 있는 oracle

Phase estimation algorithm은 크게 2가지 step으로 구성되는데, 첫 번째 step은 Fig. 1.2와 같이 구성되어 controlled-U operation을 차례대로 수행하는 과정이다. 두 번째 step은 첫 번째 register에 대해 *inverse QFT*를 수행하는 것이다. 각 step별로 어떻게 연산이 이루어지는지 따라가보자.

먼저 Fig. 1.2의 연산은 다음 단계를 따른다.

1. input state : phase estimation이 사용하는 2개의 register들을 각각 다음과 같이 초기화한다.[16]

$$|\psi\rangle = \left|0^{\otimes t}\right\rangle |u\rangle$$

2. apply H-gate : 첫 번째 register에 대해 H-gate를 적용하면 다음과 같은 state를 얻게된다.

$$|\psi\rangle = \frac{1}{\sqrt{2}^t}(|0\rangle + |1\rangle)^{\otimes t} |u\rangle$$

3. apply controlled-U operation : 두 번째 register를 *target*으로 하고, 첫 번째 register의 각 qubit을 *control*로 하여 controlled-U operation을 가하는 과정을 control qubit을 바꿔가면서 수행한다.

   예를 들어, t번째 qubit을 control qubit으로 하여 controlled-U^{2^0}를 가하면, 다음의 상태를 얻는다.[17]

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{2}^t}(|0\rangle + |1\rangle)^{\otimes t-1}(|0\rangle |u\rangle + |1\rangle e^{2\pi i(2^0\varphi)} |u\rangle) \\ &= \frac{1}{\sqrt{2}^t}(|0\rangle + |1\rangle)^{\otimes t-1}(|0\rangle + e^{2\pi i(2^0\varphi)} |1\rangle) |u\rangle\end{aligned}$$

일반화하여, j번째 qubit을 target qubit으로 하여 두 번째 레지스터에 controlled-U^{t-j} gate를 가하는 과정을 t개의 qubit에 대해서 모두 수행하면 얻게되는 최종 state는 다음과 같다.

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 2^0\varphi}|1\rangle\right) = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle. \tag{1.18}$$

이렇게 얻은 state는 QFT를 $|N\psi\rangle$에 대해서 적용한 result state와 동일하다. (put $j = N\varphi$, $N = 2^t$) 따라서, φ의 값을 얻기 위하여 Eq. (1.18)에 inverse QFT를 수행하여 $N\varphi$를 구할 수 있다.

앞에서 우리는 $\varphi \in [0,1)$이라고 가정하였으므로, $\varphi = 0.\varphi_1\varphi_2\cdots\varphi_t = \sum_{k=1}^{t}\varphi_k/2^k$이라는 binary representation으로 표현할 수 있다. 따라서 inverse QFT 결과로 얻는 $N\varphi$는 다음과 같다.

$$N\varphi = 2^t\sum_{k=1}^{t}\varphi_k/2^k = \sum_{k=1}^{t}\varphi_k 2^{t-k} = \varphi_1\varphi_2\cdots\varphi_t$$

[16] 첫 번째 register의 qubit 개수 t는 QPE의 accuracy, success probability를 결정한다.

[17] target qubit은 $|u\rangle$이지만, U^{2^0}s는 phase만 변화시키기 때문에, control qubit에 대해 phase term을 옮겨서 표현할 수 있다.

즉, 최종적으로 QPE를 진행하면 φ의 binary representation에서 소수점 아래 자릿수를 값으로 갖는 t개의 qubit을 얻게되며, 각 qubit의 값은 0 또는 1이므로 computational basis에서 측정하게되면 φ의 근사값을 얻을 수 있다. □

Lecture 12

1.5.2 Performance

28 Oct. 10:30

앞에서 우리는 phase φ가 t개의 소수점 아랫수로 표현될 수 있는 값이라는 가정을 했었다. 그러나, $\varphi = 0.\varphi_1\varphi_2\cdots\varphi_t\varphi_{t+1}\cdots$ 처럼 $t+1$개 이상의 소수점 아랫자리수를 가지게 되면, QPE를 사용하여 얻은 결과 $\tilde{\varphi}$는 실제값의 근사치가 된다. 즉, error가 발생하게 된다.

error를 분석하기 위해서, t개의 qubit로 나타낼 수 있는 이진수 표현중에서 가장 φ와 가까운 φ보다 크지 않은 수를 만드는 정수를 b라고 하자. ($b/2^t = 0.b_1\cdots b_2$)

$$b = \underset{0\le b\le 2^t-1}{\arg\min}\ \varphi - b/2^t, \qquad (b/2^t \le \varphi) \tag{1.19}$$

우리는 이제 QPE의 측정 결과가 b와 가까우며, 따라서 φ를 높은 확률로 추정할 수 있음을 보이고자한다. Eq. (1.18)에 IQFT를 적용한 결과는 다음과 같다.

$$\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle \xrightarrow{\text{IQFT}} \frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{2\pi i\varphi k}\underbrace{e^{-2\pi ilk/2^t}|l\rangle}_{|k\rangle} = \frac{1}{2^t}\sum_{k,l=0}^{2^t-1}\left(e^{2\pi i\left(\varphi - l/2^t\right)}\right)^k|l\rangle.$$

만약 $\varphi = l/2^t$라면, $e^{2\pi i(\varphi - l/2^t)} = 1$이 2^t개의 항에 대해서 더해지기 때문에, $|l\rangle$의 amplitude가 1이되어서 100% 확률로 $|l\rangle = |N\varphi\rangle$를 관측한다. 그러나 φ가 $l/2^t$와 *유사*하다면, 다른 항들도 관측될 확률을 가질 수 있고 이것이 바로 error를 발생시키는 원인이 된다.

Definition 1.5.1 (Inverse Quantum Fourier transform)**.** Inverse QFT는 fourier basis $|k\rangle$에 대하여, 다음 변환을 수행한다.[a]

$$|k\rangle \to \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{-2\pi ijk/N}|j\rangle$$

[a] phase를 소거하기 위해 phase가 음수이다.

다른 항이 관측될 확률을 분석하기 위해서, α_l을 $|(b+l) \mod 2^t\rangle$ state에 대한 amplitude라고 하자. 등비급수 공식을 사용하여 나타내면 다음과 같다. ($\delta = \varphi - b/2^t$) (See Eq. (1.19))

$$\alpha_l \triangleq \frac{1}{2^t}\sum_{k=0}^{2^t-1}\left(e^{2\pi i\left(\varphi-(b+l)/2^t\right)}\right)^k = \frac{1}{2^t}\left(\frac{1-e^{2\pi i\left(2^t\varphi-(b+l)\right)}}{1-e^{2\pi i(\varphi-(b+l)/2^t)}}\right) = \frac{1}{2^t}\left(\frac{1-e^{2\pi i\left(2^t\delta-l\right)}}{1-e^{2\pi i(\delta-l/2^t)}}\right)$$

이때, a_l은 $b+l \mod 2$ 연산에 의해 결정되기 때문에, 서로 다른 l에 대해서 동일한 α_l을 정의할 수 없도록 l은 $-2^{t-1} < l \le 2^{t-1}$ 범위로 제한된다.

이제 QPE의 측정 결과가 m이라고 가정하자. 우리는 m과 b의 차이 $|m-b|$가 β보다 클 확률을 계산하고자한다. 이는 우리가 허용할 수 있는 error β보다 더 큰 error가 발생할 *failure probability*를 의미한다.

$$\Pr(|m-b| > \beta) = \sum_{\beta\le|l|}|\alpha_l|^2 = \sum_{-2^{t-1}<l\le-(\beta+1)}|\alpha_l|^2 + \sum_{\beta+1\le l\le 2^{t-1}}|\alpha_1|^2 \tag{1.20}$$

이때, $|1-e^{i\theta}|$에 대한 다음의 2가지 bound를 적용하여 확률을 계산할 수 있다.

- $|1-e^{i\theta}| \ge \frac{2|\theta|}{\pi}$, for $(-\pi \le \theta \le \pi)$
- $|1-e^{i\theta}| \le 2$, for any $\theta \in \mathbb{R}$.

l의 범위에 대한 제한 덕분에, $-\pi \le 2\pi(\delta - l/2^t) \le \pi$ 조건 만족하여 $|\alpha_l|$의 upper bound를 구할 수 있다.

$$|\alpha_l| = \left|\frac{1}{2^t}\left(\frac{1-e^{2\pi i\left(2^t\delta-l\right)}}{1-e^{2\pi i(\delta-l/2^t)}}\right)\right| \le \frac{2}{2^t|1-e^{2\pi i(\delta-l/2^t)}|} \le \frac{1}{2^{t+1}\left(\delta-l/2^t\right)} = \frac{1}{2}\left(\frac{1}{2^t\delta-l}\right) \tag{1.21}$$

따라서 Eq. (1.20)에 Eq. (1.21)을 대입하면, 다음의 upper bound를 얻는다.

$$\Pr(|m-b|>\beta) \leq \frac{1}{4}\left[\sum_{-2^{t-1}<l\leq-(\beta+1)} \frac{1}{(l-2^t\delta)^2} + \sum_{\beta+1\leq l\leq 2^{t-1}} \frac{1}{(l-2^t\delta)^2}\right] \tag{1.22}$$

$0 \leq 2^t\delta \leq 1$을 이용하여 간략히 표현하면, 다음을 얻는다.

- Eq. (1.23) : upper bound를 구하기 위해서 각 항의 값이 최대가 되도록 하는 $2^t\delta$를 대입한다.[18]
- Eq. (1.24) : 첫 번째 항을 보면 l^2에 대해서 연산하고 있기 때문에 l의 범위를 음수에서 양수로 바꾸어도 된다.
- Eq. (1.25) : 두 항의 하나로 나타낸 뒤[19], 합을 적분으로 근사한다.

따라서 정리하자면, QPE의 failure probability는 β에 대해 $\frac{1}{2(\beta-1)}$로 bound 된다.

$$\Pr(|m-b|>\beta) \leq \frac{1}{4}\left[\sum_{-2^{t-1}<l\leq-(\beta+1)} \frac{1}{l^2} + \sum_{\beta+1\leq l\leq 2^{t-1}} \frac{1}{(l-1)^2}\right] \tag{1.23}$$

$$= \frac{1}{4}\left[\sum_{\beta+1\leq l<2^{t-1}} \frac{1}{l^2} + \sum_{\beta+1\leq l\leq 2^{t-1}} \frac{1}{(l-1)^2}\right] \tag{1.24}$$

$$\leq \frac{1}{2}\sum_{l=\beta}^{2^{t-1}-1} \frac{1}{l^2} \leq \frac{1}{2}\int_{\beta-1}^{2^{t-1}-1} \frac{1}{l^2}dl \leq \frac{1}{2(\beta-1)}. \tag{1.25}$$

만약 우리가 φ를 정확도 2^{-n}으로 추정하기를 원한다면,[20] $\beta = 2^{t-n}-1$으로 선택한다. 이때, t는 QPE에 사용하는 qubit의 개수이다. ($p=t-n$) 그럼 이 β에 대해, failure probability는 $1/2(2^{t-n}-2) = 1/2(2^p-2)$로 bound되기 때문에, QPE의 정확도는 적어도 $1-1/(2(2^p-1))$ 이상이다.

따라서, n bits로 표현된 φ를 success probability가 $1-\delta$ 이상이 되도록 QPE를 수행하기 위해서는, 첫 번째 레지스터의 개수 t를 다음과 같이 결정해야한다.

$$t = n + \left\lceil \log\left(2+\frac{1}{2\delta}\right)\right\rceil$$

또한, 앞에서 우리는 eigenvector의 state $|u\rangle$로 준비할 수 있는 oracle을 가정했다. 그러나, 실제 상황에서는 이것이 불가능할 수도 있다. 만약 우리가 다른 state $|\psi\rangle$를 $|u\rangle$ 대신에 사용했다고 하자. $|\psi\rangle$는 eigenbasis에 대해 다음과 같은 linear combination으로 표현된다.

$$|\psi\rangle = \sum_u c_u|u\rangle$$

각 eigenstate의 eigenvalue가 $e^{2\pi i\varphi_u}$라면, $|\psi\rangle$에 대해 phase estimation을 수행한 결과는 다음과 같이 각각의 eiganstate에 대해 phase estimation을 수행한 결과들의 superposition state가 될 것이다.

$$\left|0^{\otimes n}\right\rangle|\psi\rangle \xrightarrow{\text{QPE}} \sum_u c_u\left|\varphi_u\right\rangle|u\rangle,$$

따라서 이러한 output state를 측정하게 되면, probability $|c_u|^2$에 따라서 랜덤하게 어떤 eigenstate $|u\rangle$에 대한 phase $|\varphi_u\rangle$를 얻게된다. 즉, 우리가 실제로 얻고자하는 eigenstate $|u\rangle$에 대한 amplitude c_u가 충분히 크다면, QPE를 여러번 반복하여 우리가 원하는 eigenvalue를 얻을 수 있다.

마지막으로, QPE의 resource requirement를 분석해보자.

- (space complexity) accuracy ϵ을 달성할 probability가 $1-\delta$가 되도록 필요한 qubit의 개수 :

$$t = \log(1/\epsilon) + \left\lceil \log\left(2+\frac{1}{2\delta}\right)\right\rceil = O\left(\log\frac{1}{\delta\epsilon}\right).$$

[18] 첫 번째 항은 l이 음수이기 때문에 $2^t\delta$가 0이 되도록하고, 두 번째 항은 l이 양수이기 때문에 $2^t\delta$가 1이 되도록한다.
[19] using $\frac{1}{l^2}+\frac{1}{(l-1)^2} \leq \frac{2}{l^2}$.
[20] n-bit 이진수에서 n번째 자릿수 이하에서 발생하는 차이값

- (time complexity)
  - (step 1) QPE를 실행하기 위해서는 controlled unitary를 2^t번 가해야하므로, gate complexity를 qubit의 개수 t에 대해서 표현하면 $O(1/(\delta\epsilon))$이 된다.
  - (step 2) t개의 qubit에 대해 IQFT를 가하기 때문에 IQFT의 complexity는 $\Theta(t^2)$이 된다.

  따라서 QPE의 total time complexity는 다음과 같다.

$$O\left(\frac{1}{\delta\epsilon}\right) + \Theta\left(\left(\log\frac{1}{\delta\epsilon}\right)^2\right)$$

Lecture 13

1.6 Applications of phase estimation

30 Oct. 10:30

1.6.1 Ground state energy estimation

앞에서 phase estimation의 대표적인 예시로 사용했던 ground state energy estimation에 대해 조금 더 자세히 살펴보자. H가 다음의 eigendecomposition을 가지는 Hamiltonian operator라고 하자.[21]

$$H\left|\psi_j\right\rangle = \lambda_j\left|\psi_j\right\rangle, \qquad (\text{suppose } 0 < \lambda_0 < \lambda_1 \leq \cdots \leq \lambda_{N-1} < \frac{1}{2})$$

우리가 ground state $|\psi_0\rangle$의 정확한 state를 알고있다면, QPE를 적용해서 높은 확률로 ground state energy를 추정할 수 있다. 반면, 다음과 같은 eigenstate의 approximation state를 이용한다고 하자.

$$|\psi\rangle = \sum_{k\in\{0,\cdots,N-1\}} c_k\left|\psi_k\right\rangle$$

이 state를 관측했을 때, ground state를 얻을 확률은 $p_0 = |\langle\psi|\psi_0\rangle|^2$ 이고, p_0이 충분히 크다면 QPE를 여러번 반복하여 ground state energy를 추정할 수 있다. (Poly)

Ground state energy estimation은 ϵ의 정확도로 ground state energy λ_0를 추정하고자한다. ($\epsilon < \lambda_0$) 이 문제는 quantum many-body physics, quantum chemistry, optimization 등 많은 분야에서 중요한 문제이다. 일반적으로, QPE를 활용하기 위해서 Hamiltonian에 대한 unitary operation을 이용할 수 있다고 가정한다.

$$U = e^{2\pi iH}$$

이 unitary에 대해 ground state energy는 phase에 위치하게 되며, 따라서 QPE를 적용할 수 있다.

$$U\left|\psi_0\right\rangle = e^{2\pi i\lambda_0}\left|\psi_0\right\rangle.$$

1.6.2 Order-finding algorithm

Prerequisite: Uncomputation

먼저, order-finding algorithm을 설명하기 전에 uncomputation technique에 대해 먼저 이야기해보자. Classical circuit f에 대응되는 quantum circuit O_f를 구성하는 과정을 *uncomputation*이라고 한다.[22]

$$O_f|x,b\rangle = |x, b\oplus f(x)\rangle$$

구체적으로 uncomputation 과정을 어떻게 수행하는지 단계별로 살펴보자.

1. classical circuit을 *reversible*하도록 n개의 ancilla qubit을 추가한다. ($g(x)$는 임의의 garbage 값)

$$\tilde{O}_f|x\rangle\left|0^n\right\rangle|b\rangle \to |g(x)\rangle|f(x)\rangle|b\rangle$$

2. $|b\rangle$와 ancilla qubit에 대해 controlled-X gate를 적용한다.

$$|g(x)\rangle C(X)|f(x)\rangle|b\rangle \to |g(x)\rangle|f(x)\rangle|b\oplus f(x)\rangle$$

3. $O_f^\dagger$를 적용하고 ancilla qubit을 무시하면, $O_f = \tilde{O}_f^\dagger C(X)\tilde{O}_f$는 우리가 원하는 연산을 수행한다.

$$\tilde{O}_f^{-\dagger}|g(x)\rangle|f(x)\rangle|b\oplus f(x)\rangle \to |x\rangle\underbrace{\left|0^n\right\rangle}_{ancilla}|b\oplus f(x)\rangle$$

[21] 다음 가정은 non-degenerate case; 중복된 고윳값이 없는 상태를 다룬다는 것을 의미한다.
[22] Deutsch's algorithm에서 사용했던 oracle과 동일한 개념이다.

Order-finding

이제 order-finding problem이 무엇인지 소개하려고 한다. order-finding problem은 다음과 같이 표현된다.[표]

- `input`: integer (x, N), $(x < N,\ \gcd(x, N) = 1)$
- `output`: the order of $x \mod N$, r.

Definition 1.6.1 (Order). 다음을 만족하는 가장 작은 양의 정수 r을 *order of x modulo N*이라고 한다.

$$x^r \equiv 1 \mod N$$

Classical algorithm으로 이 문제를 input의 크기 L에 대하여 polynomial time에 해결할 수 있는 방법은 현재까지 없다고 알려져있다. 이때 L은 N과 N보다 작은 수 x를 표현하는데 필요한 bit의 개수를 의미하기 때문에 $L \triangleq \lceil \log N \rceil$ 이다.

Quantum algorithm으로 이 문제를 해결하기 위해서 우리는 *phase estimation*을 활용한다. Phase estimation을 적용하기 위해서는 unitary operator U와 그에 대응되는 eigenvector $|u\rangle$, eigenvalue φ의 형태로 문제를 정의해야한다. 따라서 이를 위해 computational basis $|y\rangle \in \{|0\rangle, \cdots |2^L - 1\rangle\}$에 대하여 다음과 같이 동작하는 unitary를 정의하자.

$$U|y\rangle \triangleq \begin{cases} |xy \mod N\rangle & 0 \le y < N, \\ |y\rangle & N \le y < 2^L \end{cases}$$

이 unitary는 N보다 큰 basis들의 subspace에 대해서는 identity matrix처럼 행동하지만, 그보다 작은 subspace에 대해서는 주어진 input x에 대해 $xy \mod N$ 연산 결과가 되도록 만든다. 이렇게 정의한 unitary가 정말로 valid한지를 확인하기 위해 subspace에 대해 작용하는 unitary $|U\rangle$가 valid한지를 확인해보자.

$$\langle y|\tilde{U}^\dagger \tilde{U}|y'\rangle = \langle xy \mod N | xy' \mod N\rangle = \langle y|y'\rangle$$

연산 전후 norm을 보존하기 때문에 우리가 정의한 unitary는 valid하다.[23] □

이제 다음과 같이 정의한 state가 U의 eigenvector임을 보인다면, phase estimation을 통해 어떤 임의의 eigenvector에 대해서도 항상 eigenvalue r을 얻을 수 있다는 사실을 입증할 수 있다.

$$|u_s\rangle \triangleq \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i s k}{r}\right) |x^k \mod N\rangle$$

어떤 정수 $0 \le s \le r-1$에 대해서도 $|u_s\rangle$가 eigenvector임을 보이기 위해 definition을 이용하자.

- Eq. (1.26) : $x^k \mod N$은 modulo 연산 때문에 항상 그 결과가 $\{0, \cdots, N-1\}$ 범위에 존재하여 unitary operation이 $|x^{k+1} \mod N\rangle$으로 state를 변화시킨다.
- Eq. (1.27) : $k = k+1$로 재정의하면, sigma의 적용 범위가 $[0, r-1]$에서 $[1, r]$로 변화하지만, modulo N 연산 때문에 연산 범위를 동일하게 생각할 수 있다.
- Eq. (1.29) : 따라서 U를 $|u_s\rangle$에 적용한 결과는 단순히 $|u_s\rangle$에 phase $e^{2\pi i s/r}$을 가한 결과와 동일하므로 $|u_s\rangle$는 U의 eigenvector이다. □

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i s k}{r}\right) |x^{k+1} \mod N\rangle \tag{1.26}$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i s (k-1)}{r}\right) |x^k \mod N\rangle \tag{1.27}$$

$$= \frac{1}{\sqrt{r}} exp\left(\frac{2\pi i s}{r}\right) \sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i s k}{r}\right) |x^k \mod N\rangle \tag{1.28}$$

$$= \exp\left(\frac{2\pi i s}{r}\right) |u_s\rangle . \tag{1.29}$$

따라서, 어떤 s에 대해서도 phase estimation을 적용하면 s/r을 얻을 수 있다.

[23] 또는 $\gcd(x, N) = 1$이라면, modulo N에서 x의 역원은 **항상** 존재한다는 성질을 활용해서 증명할 수도 있다.

단, phase estimation을 수행하기 위해서는 아직 2가지의 요소가 더 필요하다.

- 다음 연산을 구현하는 방법 (t개의 qubit를 이용할 때)

$$|z\rangle U^{z_t 2^{t-1}} \cdots U^{z_1 2^0} |y\rangle = |z\rangle |x^z y \mod N\rangle .$$

- U의 eigenvector $|u_s\rangle$를 r[24]없이 준비하는 방법.

(1) 의 구현은 앞에서 설명한 *uncomputation* 기법을 활용하여 생각할 수 있다. 다음 gate는 $f(z) = x^z \mod N$을 수행하는 classical function을 quantum circuit으로 구현한 것이다.[25]

$$|z\rangle|y\rangle|0\rangle \xrightarrow{\tilde{O}_f} |z\rangle|y\rangle |x^z \mod N\rangle \tag{1.30}$$

만약 $f(z) = x^z \mod N$을 계산하는 classical circuit이 있다면, uncomputation을 사용하여 Eq. (1.30)과 같은 연산을 quantum computer에서도 수행할 수 있다. *modular exponentiation*[26]에 의하여, $f(z) = x^z \mod N$은 다음과 같이 계산할 수 있다. ($z = z_t z_{t-1} \cdots z_1$)

$$x^z \mod N = (x^{z_t 2^{t-1}} \mod N)(x^{z_{t-1} 2^{t-2}} \mod N) \cdots (x^{z_1 2^0} \mod N)$$

따라서 이 아이디어를 이용하여 uncomputation 과정을 적용하면 다음의 circuit을 만들 수 있다.

1. *modular exponentiation*을 사용하면, Eq. (1.30)을 다음과 같이 계산할 수 있다.

$$|z\rangle|y\rangle|0\rangle \xrightarrow{\tilde{O}_f} |z\rangle|y\rangle|(x^{z_t 2^{t-1}} \mod N)(x^{z_{t-1} 2^{t-2}} \mod N) \cdots (x^{z_1 2^0} \mod N)\rangle$$

2. $|q_3\rangle$과 ancilla qubit $|q_2\rangle$을 곱한다. ($|q_1 q_2 q_3\rangle$)

$$|z\rangle|y\rangle |x^z \mod N\rangle \to |z\rangle |x^z y \mod N\rangle |x^z \mod N\rangle$$

3. inverse operation $\tilde{O}_f^\dagger$를 취한다.

$$|z\rangle |x^z y \mod N\rangle |x^z \mod N\rangle \xrightarrow{\tilde{O}_f^\dagger} |z\rangle|x^z y \mod N\rangle|0\rangle$$

$|q_3\rangle$을 무시하면, $O_f = \tilde{O}_f^\dagger U \tilde{O}_f$는 우리가 원하는 연산을 수행한다. 만약 $|x^z y \mod N\rangle$을 나타내기 위해서 사용하는 qubit의 개수가 L개라면, 이 연산의 time complexity는 $O(L^3)$이다.

- QPE에 사용하는 qubit의 개수 t는 다음과 같이 설정된다.[27]

$$t = 2L + 1 + \lceil \log(2 + 1/(2\delta)) \rceil = O(L)$$

- $0 \le j < t$ 범위의 모든 j에 대해 이를 계산해야하므로, $O(t)$번 연산을 수행한다.
- 매 단계마다, $x^z y \bmod y$ 값을 갱신하기 위해서 이전 단계까지의 누적 계산 결과 $x^{z_1 2^0} \cdots x^{x_i 2^{i-1}}$에 이번 단계에 얻은 결과인 $x^{x_{i+1} 2^i}$를 곱한 뒤 mod$N$을 취한다.
  - L bit 수의 곱셈 연산의 complexity: $O(L^2)$
  - mod$N$ 연산의 complexity: $O(L^2)$

반면, (2) 를 구현하는 것은 조금 더 까다롭다. 이 문제를 해결하기 위해서 $|u_s\rangle$들의 superposition state를 대신 입력으로 제공하는 방법을 사용할 수 있다. 만약 r개의 qubit를 이용하여 $|u_s\rangle$를 준비한다고 가정하면, superposition state는 다음과 같이 정리할 수 있다.[28]

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{r} \sum_{s,k=0}^{r-1} \exp\left[-\frac{2\pi i s k}{r}\right] |x^k \bmod N\rangle = \sum_{k=0}^{r-1} \delta_{k0} |x^k \bmod N\rangle = |1\rangle.$$

따라서 $|1\rangle$을 입력으로 사용하면, 확률에 따라서 임의의 s에 대해 $\varphi \approx s/r$를 적어도 $(1-\delta)/r$확률로 $2L+1$ bit 정확도를 달성할 수 있다.

[24] eigenvector의 정의에 이미 우리가 얻고자하는 값인 r이 들어있다
[25] $0 \oplus f(z)$
[26] $ab \mod N = (a \mod N)(b \mod N)$
[27] 우리가 조절할 수 있는 parameter인 L에 의해, QPE의 accuracy가 조절된다.
[28] complex exponential의 orthogonality에 의하여, $\sum_{s=0}^{r-1} e^{(2\pi i s/r)(k-0)} = \begin{cases} 0, & \text{for } k \neq 0 \\ r, & \text{for } k = 0 \end{cases}$

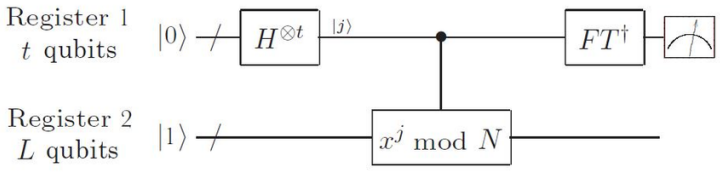


Figure 1.3: Order-finding algorithm [Dha15]

The continued fraction expansion

우리가 앞의 알고리즘을 통해서 얻은 결과는 s/r이다. 따라서 이 결과로부터 r의 값을 얻어내는 추가적인 후처리가 필요하다. 우리가 얻은 $\varphi \approx s/r$은 임의의 $2L+1$ bit 소수이므로 임의의 실수이지만, 실제로 우리가 얻고자 하는 값은 s/r은 분명히 *유리수*이다. 이 특징을 활용하기 위해 continued fraction이라는 개념을 도입한다. continued fraction은 주어진 실수를 연분수 형태로 표현한 것이다.[29]

$$[a_0, \ldots, a_M] \triangleq a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$$

주어진 convergent를 연분수 형태로 변환하는 알고리즘을 *continued fraction algorithm*이라고 한다.

Theorem 1.6.1. s/r이 유리수이고, φ가 QPE로 얻은 근사값일 때 두 값의 차이가 다음과 같은 upper bound를 만족한다면, continued fraction algorithm을 적용하여 얻은 결과가 바로 s/r이다.

$$\left|\frac{s}{r} - \varphi\right| \leq \frac{1}{2r^2}$$

Order-finding problem에서는 $(1-\delta)/r$의 높은확률로 $2L+1$ bit 정확도를 달성하기에, 다음을 만족한다.

$$\left|\frac{s}{r} - \varphi\right| \leq \frac{1}{2^{2L+1}} \leq \frac{1}{2r^2}$$

따라서 continued fraction algorithm을 적용할 수 있으므로, $O(L^3)$의 time complexity로 s/r을 구할 수 있고 $\gcd(s, r) = 1$[30]이라면 r을 구할 수 있다.

Performance

Order-finding algorithm의 정확도를 분석하기 위해서, 이 알고리즘이 실패하는 경우를 분석해보자.

- QPE가 실패하는 경우 : 아주 작은 확률 ϵ로 실패할 수 있다. 이 경우 qubit의 개수를 늘려서 QPE의 정확도를 높히거나 QPE를 여러번 반복하여 각 outcome의 확률을 비교하여 해결할 수 있다.
- $\gcd(s, r) \neq 1$인 s를 얻는 경우 : $0 \leq s < r-1$ 범위에서 두 수가 서로소일 확률은 매우 높기 때문에, 알고리즘을 $2\log N$번 반복하면 이 문제를 해결할 수 있다.

마지막으로 Order-finding algorithm의 circuit이 필요로하는 자원을 분석해보자.

- $O(L)$: Register 1에 H 변환을 가하는데 필요한 circuit의 개수
- $O(L^2)$: IQFT를 적용하는데 필요한 circuit의 개수
- $O(L^3)$: Controlled unitary; modular exponentiation에 필요한 circuit의 개수
- $O(L^3)$: continued fraction algorithm이 사용하는 time complexity
- $O(\log N)$: 오류가 발생했을 때, 다시 알고리즘을 실행하는 횟수

[29] 이때 $[a_0, \cdots, a_M]$을 Mth convergent라고 한다.
[30] 만약 두 수 사이에 공약수가 존재하면, continued fraction algorithm이 반환하는 값이 통분한 값이 된다

1.6.3 Shor's algorithm: factoring

이제 마지막으로 그 유명한 Shor's algorithm에 소개하고자 한다. Classical computer에서 polynomial time에 해결하는 효과적인 알고리즘이 아직 존재하지 않는 *factoring*을 quantum computer를 사용하여 효율적으로 수행할 수 있다는 사실을 보여주는 중요한 알고리즘이다.

Prime factorization problem은 다음과 같이 정의된다.

- `input`: natural number N
- `output`: list of prime numbers $\{p_1, p_2, \ldots, p_k\}$ such that $N = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$

이를 해결하는 Shor's algorithm은 다음과 같다.

1. **if** N이 짝수라면, *return* 2
2. **if** N이 prime p에 대해서 $N = p^k$라면, *return* p[31]
3. $1 \leq x \leq N-1$ 범위에서 랜덤하게 x를 선택한다.
   (a) **if** $\gcd(N, x) > 1$[32], *return* $\gcd(N, x)$
   (b) **else**, order-finding algorithm을 사용하여 order r을 찾는다.
4. **if** r이 홀수라면, *goto* step 3.
5. **else**,
   (a) 다음을 계산한다.
   $$x^r - 1 \equiv (x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \mod N$$
   (b) 계산 결과로부터 얻은 2개의 항에 대해, 다음의 조건들을 확인한다.
      i. **if** $N | x^{r/2} - 1$, *error*[33]
      ii. **elif** $N | x^{r/2} + 1$, *goto* step 3.
      iii. **neither**, N이 $(x^{r/2} - 1)(x^{r/2} + 1)$을 동시에 나눌 수 없으므로 각각의 항이 N의 인수를 포함하고 있다는 의미이다.
      return $\boxed{\gcd(N, x^{r/2} + 1),\ \gcd(N, x^{r/2} + 1)}$

Shor's algorithm이 성공하기 위해서는 order-finding algorithm으로 얻은 r이 짝수여야하며, **neither** case에 포함되어야한다. 정수론의 개념들을 도입하면, 성공확률은 1/2이상임을 증명할 수 있으며, 여기에서는 증명을 생략한다.

Lecture 14

1.7 Applications of the QFT

4 Nov. 10:30

이번 section에서는 QFT를 활용하는 문제들에 대해서 소개하고자 한다. QFT를 활용하여 효과적으로 해결할 수 있는 문제들은 모두 *Hidden subgroup problem*으로 일반화할 수 있다.

1.7.1 Period-finding

Hidden subgroup problem을 소개하기 전에, 먼저 hidden subgroup problem의 특수한 경우들에 대해 이야기하고자 한다. 첫 번째로 소개하는 문제는 *period-finding problem*이다.

- `input`: period function f such that $f(x) = f(x + r)$ for some *unknown* integer r, $(0 < r < 2^L)$
- `output`: least integer $r > 0$ such that $f(x) = f(x + r)$

주어진 period function은 uncomputation을 사용하여 다음과 같은 unitary operator로 표현할 수 있다.

$$U_f |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$$

[31] 이를 판단하는 효과적인 classical algorithm이 존재
[32] using Euclidean algorithm
[33] order r이 이를 만족하는 가장 작은 수이기 때문에 이런 경우는 일어나지 않는다.

이 U_f가 주어지면, 다음의 과정을 따라서 period r을 찾을 수 있다.

1. input state : $|0\rangle|0\rangle$으로 state를 초기화한다.[34]

$$|\psi\rangle = |0\rangle|0\rangle$$

2. apply H gate on 1st register

$$|\psi\rangle = \frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle|0\rangle$$

3. apply U_f : $|y\rangle = |0\rangle$이므로 2nd register에 $f(x)$가 저장된다.

$$|\psi\rangle = \frac{1}{\sqrt{2^t}}\sum_{x=0}^{2^t-1}|x\rangle|f(x)\rangle$$

4. apply QFT on **2nd** register
   QFT를 사용하여 함수 $f(x)$를 표현하면, 다음과 같다. (See Definition. 1.4.2)

$$f(x) \to \frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}e^{2\pi i l x/r}|\hat{f}(l)\rangle, \qquad |\hat{f}(l)\rangle \triangleq \frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}e^{-2\pi i l x/r}|f(x)\rangle$$

   따라서 이를 이용하면, state를 다음과 같이 표현할 수 있다.

$$|\psi\rangle = \frac{1}{\sqrt{r2^t}}\sum_{l=0}^{r-1}\sum_{x=0}^{2^t-1}e^{2\pi i l x/r}|x\rangle|\hat{f}(l)\rangle$$

5. apply IQFT on **1st** register[35]

$$|\psi\rangle = \frac{1}{\sqrt{r2^t}}\sum_{l=0}^{r-1}\sum_{x,y=0}^{2^t-1}e^{2\pi i l x/r}e^{-2\pi i x y/2^t}|y\rangle|\hat{f}(l)\rangle = \frac{1}{\sqrt{r2^t}}\sum_{l=0}^{r-1}\sum_{x,y=0}^{2^t-1}e^{(2\pi i x)(l/r-y/2^t)}|y\rangle|\hat{f}(l)\rangle \quad (1.31)$$

   final state의 coefficient를 분석하기 위해 r이 2^t를 나누는가에 대한 cases를 분석할 수 있다.

- $r \nmid 2^t$: 일반적으로는 r이 2^t를 나누지 않는 경우가 더 많다.[36] 그러나 이 경우에도 최종 outcome이 높은 확률로 nl이 된다.
- $r \mid 2^t$: $nr = 2^t$가 되게 만드는 positive integer가 존재한다. 따라서 이를 이용하면 state가 다음과 같이 단순화 된다. (Eq. (1.31)에 $r = 2^t/n$ 대입)[37]

$$\frac{1}{2^t}\sum_{x,y=0}^{2^t-1}e^{(2\pi i x/2^t)(nl-y)}|y\rangle = \sum_{y=0}^{2^t-1}\delta_{y,nl}|y\rangle = |nl\rangle = \frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}|nl\rangle|\hat{f}(l)\rangle$$

   따라서 1st register를 측정한 결과를 2^t로 나누면 $nl/2^t = l/r$이므로 r을 구할 수 있다. □

1.7.2 Discrete logarithm

이번에 소개하려는 문제는 *Discrete logarithm problem*; 이산 로그 문제이다. 이 문제는 다과 같이 정의된다.

- `input`: $x \in G$, 이때 $G = \langle g\rangle$는 g로부터 만들어지는 cyclic group[38][39]이다.
- `output`: minimum α such that $g^\alpha = x$ (or equivalently, $\alpha = \log_g x$)

[34] (1st register)함숫값을 저장하기 위해 $t = O(L + \log(1/\epsilon))$개의 qubit, (2nd register)ancilla qubit
[35] 2nd register가 x, l간의 QFT를 이용했다면, 1st register는 l이 아닌 다른 변수 y에 대해 IQFT를 수행하게 된다.
[36] 2^t의 약수; 2의 거듭제곱이 아닌 이상 나눌 수 없음
[37] $nl - y$에 대해, complex exponential의 orthogonality를 사용하여 정리한다.
[38] See https://en.wikipedia.org/wiki/Cyclic_group
[39] 대표적인 cyclic group으로 modular multiplication이 있다.

다음은 다양한 cyclic group들의 discrete log에 대한 예시이다.

- (Property of logarithm) For any $G = \langle g \rangle, \log_g 1 = 0$,
- For $G = \mathbb{Z}_7^\times, \log_3 2 = 2$,
- For $G = \mathbb{Z}_{541}^\times, \log_{126} 282 = 101$.

이 문제를 해결하기 위해, Discrete logarithm problem을 *period finding* problem의 형태로 변환할 수 있다. 먼저 다음 integer function f를 가정하자. 여기서 $\gcd(a, N) = 1$이며, modulo N에서 a order가 r이라고 하자.

$$f(x_1, x_2) = a^{sx_1 + x_2} \bmod N$$

이렇게 정의한 함수는 어떤 l에 대해 $(l, -ls)$라는 period를 가진다.

$$f(x_1 + l, x_2 - ls) = a^{sx_1 + sl + x_2 - ls} \mod N \equiv a^{sx_1 + x_2} \mod N = f(x_1, x_2)$$

Uncomputation을 사용하면 이 f에 대응되는 unitary를 구성할 수 있다.

$$U |x_1\rangle |x_2\rangle |y\rangle = |x_1\rangle |x_2\rangle |y \oplus f(x)\rangle$$

우리는 discrete logarithm problem을 다시 다음과 같이 표현할 수 있다.[40]

- `input`: $b \in \mathbb{Z}_N^\times$ such that $b \equiv a^s \mod N$, $a \in \mathbb{Z}$
- `output`: integer s

따라서 period function f를 이용하면 문제를 해결할 수 있다.

1. input state : 3개의 register를 사용한다.

$$|\psi\rangle = |0\rangle |0\rangle |0\rangle$$

2. apply H-gate on 1st and 2nd register

$$|\psi\rangle = \frac{1}{2^t} \sum_{x_1, x_2 = 0}^{2^t - 1} |x_1\rangle |x_2\rangle |0\rangle$$

3. apply U_f : $f(x_1, x_2)$를 3rd register에 저장한다.

$$|\psi\rangle = \frac{1}{2^t} \sum_{x_1, x_2 = 0}^{2^t - 1} |x_1\rangle |x_2\rangle |f(x_1, x_2)\rangle$$

4. apply QFT on 3rd register
   QFT를 사용하여 함수 $f(x_1, x_2)$를 표현하면 다음과 같다. (See Definition. 1.4.2)

$$|f(x_1, x_2)\rangle \to \frac{1}{r} \sum_{l_1, l_2 = 0}^{r-1} e^{2\pi i (l_1 x_1 + l_2 x_2)/r} |\hat{f}(l_1, l_2)\rangle$$

$$|\hat{f}(l_1, l_2)\rangle \triangleq \frac{1}{r} \sum_{x_1, x_2 = 0}^{r-1} e^{-2\pi i (l_1 x_1 + l_2 x_2)/r} |f(x_1, x_2)\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i l_2 j / r} |f(0, j)\rangle$$

   따라서 이를 이용하면, state를 다음과 같이 표현할 수 있다.[41]

$$\begin{aligned} |\psi\rangle &= \frac{1}{2^t \sqrt{r}} \sum_{l_2 = 0}^{r-1} \sum_{x_1, x_2 = 0}^{2^t - 1} e^{2\pi i (s l_2 x_1 + l_2 x_2)/r} |x_1\rangle |x_2\rangle |\hat{f}(s l_2, l_2)\rangle \\ &= \frac{1}{2^t \sqrt{r}} \sum_{l_2 = 0}^{r-1} \left[\sum_{x_1 = 0}^{2^t - 1} e^{2\pi i (s l_2 x_1)/r} |x_1\rangle \right] \left[\sum_{x_2 = 0}^{2^t - 1} e^{2\pi i (l_2 x_2)/r} |x_2\rangle \right] |\hat{f}(s l_2, l_2)\rangle \end{aligned}$$

[40] a가 g, s가 α에 대응된다.
[41] put $l_1 = l_2, l_2 = s l_2$

5. apply IQFT on 1st and 2nd register

$$|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{l_2=0}^{r-1} |sl_2/r\rangle \, |l_2/r\rangle \, |\hat{f}\,(sl_2, l_2)\rangle$$

따라서 1st, 2nd register를 측정하면 각각 sl/r, 그리고 l/r이라는 값을 얻게 되는데, $sl/r \times r/l = s$이므로 s를 구할 수 있다. □

1.7.3 Hidden subgroup problem

이제 Hidden subgroup problem에 대해 이야기할 시간이 찾아왔다.[42]

Definition 1.7.1 (Hidden subgroup problem). Let f be a function from finitely generated group G to some finite set X. s.t. f is constant on the cosets of a subgroup K, and distinct on each coset.[a][b]

$$f : G \to X \quad \longrightarrow \quad U_f \, |g\rangle \, |h\rangle = |g\rangle \, |h \oplus f(g)\rangle \quad (\text{for } g \in G, h \in X)$$

Find a generating set for K.

[a] K가 주어졌을 때, coset은 G의 원소에 대해서 $gK = \{gk : k \in K\}$로 정의된다.
[b] 같은 coset이라면 f의 값은 매우 동일하지만, 서로 다른 coset에 속한다면 f의 값은 서로 다르다.

앞에서 우리가 다루었던 order-finding problem, period-finding, discrete logarithm과 같은 문제들이 Hidden subgroup problem의 특수한 예시이다. 예를 들어, order-finding problem이 왜 Hidden subgroup problem으로 표현될 수 있는지 알아보자. Hidden subgroup problem에서 각각을 다음과 같이 정의하자.

- $G = \mathbb{Z}$
- $K = r\mathbb{Z}$
- (coset) $K_g = \{rg\}$ for $g \in \mathbb{Z}$ (e.g., $K_1 = \{\cdots, -2, -1, 0 \cdots, 1, 2\}, K_3 = \{\cdots, -6, -3, 0 \cdots, 3, 6\}$)
- $f(k) = a^k \mod N$

이때, (1) $f(k) = f(k+r)$의 주기를 가지고 (2) $0 \le k \le r-1$ 범위에서 각각의 $f(k)$의 값은 모두 구분된다. 이 두 가지 성질은 f가 동일한 coset에 속하는 원소들에 대해서 constant하고, 서로 다른 coset에 속한 원소들에 대해서는 distinct한 값을 가지는 것을 의미한다. 따라서 order-finding problem은 Hidden subgroup problem의 특수한 경우로 생각할 수 있다.

G가 finite abelian group[43]이라면, QFT를 적용하여 Hidden subgroup problem을 해결할 수 있다. 그러나, non-abelian group에 대해서는 아직 이 문제를 효과적으로 푸는 방법이 알려지지 않았다. (non-abelian group에 대한 대표적인 문제가 바로 *Graph isomorphism*)

1.8 Quantum search algorithms

1.8.1 Grover operator

1.8.2 Grover search algorithm

1.8.3 Performance

Lecture 15

6 Nov. 10:30

[42] See https://en.wikipedia.org/wiki/Hidden_subgroup_problem
[43] 교환법칙이 성립하는 군

1.8.4 Example: Classical circuit-SAT problem

1.8.5 Amplitude amplification

1.9 Amplitude estimation algorithm (Quantum counting)

1.10 HHL (Harrow–Hassidim–Lloyd) algorithm

Lecture 16

1.11 Optimality of the quantum search algorithm

8 Nov. 17:00

Chapter 2

Introduction to Computational Complexity

Lecture 16

2.1 Introduction

8 Nov. 17:00

Lecture 17

2.2 The class NP: Reducibility and completeness

11 Nov. 17:00

2.2.1 P and NP problems

2.2.2 Reducibility and NP-completeness

2.2.3 Boolean formula and Cook-Levin theorem

2.3 Quantum complexity

2.3.1 Probabilistic algorithms

2.3.2 Quantum algorithms

2.3.3 BQP vs PSPACE

Appendix

Appendix A

Useful Environments for the Note

A.1 Useful Environment

We now see some common environment you'll need to complete your note.

Definition A.1.1 (Natural number)**.** We denote the set of *natural numbers* as $\mathbb{N}$.

Lemma A.1.1 (Useful lemma)**.** Given the axioms of natural numbers $\mathbb{N}$, we have

$$0 \neq 1.$$

An obvious proof. Obvious. ■

Proposition A.1.1 (Useful proposition)**.** From Lemma A.1.1, we have

$$0 < 1.$$

Exercise. Prove that $1 < 2$.

Answer. We note the following.

> **Note.** We have Proposition A.1.1! We can use it iteratively!
>
> With the help of Lemma A.1.1, this holds trivially. ⊛

Example. We now can have $a < b$ for $a < b$!

Proof. Iteratively apply the exercise we did above. ⊛

Remark. We see that Proposition A.1.1 is really powerful. We now give an immediate application of it.

Theorem A.1.1 (Mass-energy equivalence)**.** Given Proposition A.1.1, we then have

$$E = mc^2.$$

Proof. The blank left for me is too small,[a] hence we put the proof in appendix. ■

[a] https://en.wikipedia.org/wiki/Richard_Feynman

From Theorem A.1.1, we then have the following.

Corollary A.1.1 (Riemann hypothesis)**.** The real part of every nontrivial zero of the Riemann zeta function is $\frac{1}{2}$, where the Riemann zeta function is just

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots .$$

Proof. The proof should be trivial, we left it to you. ■

TODO mark

As previously seen. We see that Lemma A.1.1 is really helpful in the proof!

Internal Link

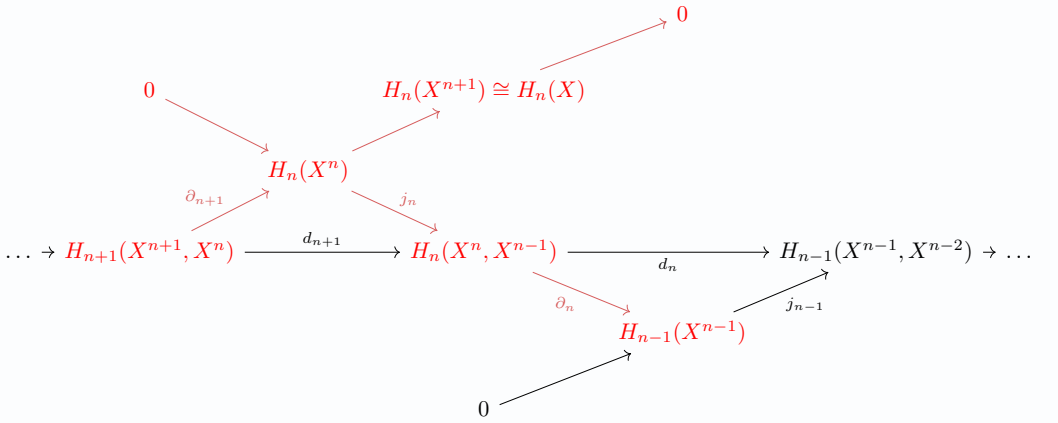
You should see all the common usages of internal links. Additionally, we can use citations as citation [NC01], which just link to the reference page!

A.2 Commutative Diagram

We can use the package `tikz-cd` to draw some commutative diagram.

Example. The cellular homology agrees with singular homology.

Proof. The following commutative diagram shows everything.



⊛

A.3 Fancy Stuffs

With this header, you can achieve some cool things. For example, we can have multiple definitions under a parent environment, while maintains the numbering of definition. This is achieved by `definition*` environment with `definition` inside. For example, we can have the following.

Definition. We have the following number system.

Definition A.3.1 (Rational number)**.** The set of *rational number*, denote as $\mathbb{Q}$.

Definition A.3.2 (Real number)**.** The set of *real number*, denote as $\mathbb{R}$.

Definition A.3.3 (Complex number)**.** The set of *complex number*, denote as $\mathbb{C}$.

Note. And indeed, we can still reference them correctly. For instance, we can use rational numbers to define real numbers and then further use it to define complex numbers.

Furthermore, we can completely control the name of our environments. We already saw we can name definition, lemma, proposition, corollary and theorem environment. In fact, we can also name remark, note, example and proof as follows.

Example (Interesting Example). We note that $1 \neq 2$!

Note (Important note). As a consequence, $2 \neq 3$ also.

Remark (Easy observation). We see that from here, we easily have the following theorem.

Theorem A.3.1 (Lebesgue Differentiation Theorem). Let $f \in L^1$, then

$$\lim_{r \to 0} \frac{1}{m(B(x,r))} \int_{B(x,r)} |f(y) - f(x)| \, \mathrm{d}y = 0$$

for a.e. x.

An obvious proof of Theorem A.3.1. Obvious. ■

As we can see, specifically for the `proof` environment, we allow `autoref` and `hyperref`. One can actually allow all example, note and remark environment's name to use reference, but I think that is overkilled. But this can be achieved by modify the header in an obvious way.[1]

[1] This time I mean it!

Bibliography

[BCK15] Dominic W Berry, Andrew M Childs, and Robin Kothari. "Hamiltonian simulation with nearly optimal dependence on all parameters". In: *arXiv preprint arXiv:1501.01715* (2015).

[Chi+21] Andrew M Childs et al. "Theory of trotter error with commutator scaling". In: *Physical Review X* 11.1 (2021), p. 011020.

[Dha15] Sayandip Dhara. *Quantum Order Finding and Factorization*. July 2015. DOI: 10.13140/RG.2.1.4954.9925.

[Haa19] Jeongwan Haah. "Product decomposition of periodic functions in quantum signal processing". In: *Quantum* 3 (2019), p. 190.

[NC01] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Vol. 2. Cambridge university press Cambridge, 2001.