Commun. Korean Math. Soc. **18** (2003), No. 2, pp. 193–205

초청논문

양자 계산 알고리즘

지동표

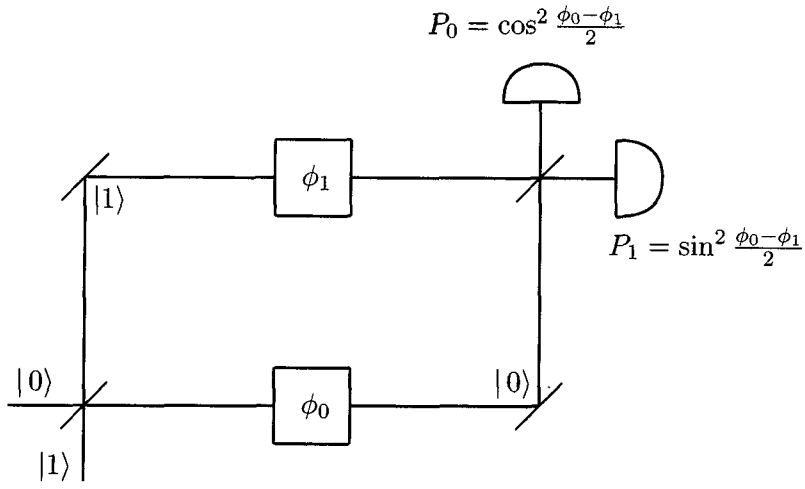
요 약. 본 해설 논문에서 선형대수에 기반을 두고 있는 양자 계산 알고리즘 몇 가지를 설명하고자 한다. 선형대수의 기초적 지식만 있으면 누구든지 할 수 있는 분야이다.

제 1 절 서 론

양자 계산은 중첩 상태(superposition)와 양자 간섭(quantum interference), 양자 얽힘(quantum entanglement) 등의 세 가지 양자 현상에 기초하고 있다. 이러한 효과는 고전적인 방법으로는 풀기 어려운 몇 가지 문제를 경이적으로 빠른 시간 안에 해결하게 해준다. 양자 얽힘은 주어진 자료를 다입자(multi-particle)의 중첩 상태로 부호화할 수 있게 해주며, 양자 간섭은 다입자의 중첩 상태를 적절한 방법으로 조절하여 입력에 해당하는 초기 상태를 출력에 해당하는 마지막 상태로 변화하게 해준다. 단입자의 간섭 현상과는 달리, 다입자의 양자 간섭 현상은 어떠한 고전 물리학으로 설명될 수 없으며, 양자 역학의 고유한 성질 중 하나로써 보여질 수 있다. 이러한 양자 간섭 현상은 double-slit 실험이라고 부르는 아주 간단한 실험으로부터 볼 수 있는데, 이 실험은 (그림 1)에서 볼 수 있는 Mach-Zehnder 간섭계(interferometry)를 사용하여 현대적으로 재해석될 수 있다.

광자와 같은 입자는 광선 분산기(beam splitter) **BS1** 에서 또 다른 광선 분산기 **BS2** 가 있는 두 개의 다른 경로를 통해서 확률적으로 전달된다. 여기에서 두번째 광선 분산기의 역할은 두 개의 탐지기 중 하나에 그 입자를 전달하는 것이다. 두 개의 광선 분산기 간의 경로 위에 위상 변환기(phase shifter) **PS** 가 있다. 아래 경로는 $|0\rangle$ 상태이고, 위의

Received March 17, 2003.
2000 Mathematics Subject Classification: 81Vxx.
Key words and phrases: 양자계산 알고리즘, 푸리에 변환, 소인수 분해.



(그림 1) 두 개의 위상변환기(phase shifter)로 구성된 Mach-Zehnder 간섭계(interferometer): 간섭형태는 간섭계의 서로 다른위상변환 사이의 차이에 의한다.

경로는 $|1\rangle$ 상태였다면, 다음과 같은 일련의 변환을 보여준다.

$$
\begin{aligned}
|0\rangle &\xrightarrow{\text{BS1}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&\xrightarrow{\text{PS}} \frac{1}{\sqrt{2}}(e^{i\phi_0}|0\rangle + e^{i\phi_1}|1\rangle) \\
&= e^{i\frac{\phi_0+\phi_1}{2}} \frac{1}{\sqrt{2}} \left(e^{i\frac{\phi_0-\phi_1}{2}}|0\rangle + e^{-i\frac{\phi_0-\phi_1}{2}}|1\rangle \right) \qquad (1) \\
&\xrightarrow{\text{BS2}} e^{i\frac{\phi_0+\phi_1}{2}} \left(\cos\frac{\phi_0-\phi_1}{2}|0\rangle + \sin\frac{\phi_0-\phi_1}{2}|1\rangle \right).
\end{aligned}
$$

이 실험에서 세 가지의 중요한 성분들의 역할은 분명하다. 첫 번째 빛살 가르개는 가능한 경로에 중첩인 상태를 준비해주고, 위상 변환기는 서로 다른 경로에 양자 위상을 조절해 준다. 그리고 마지막으로 두 번째 빛살 가르개는 모든 경로를 결합시켜주는 역할을 한다. 이와 같은 간섭계의 패러다임을 양자 알고리즘에서도 볼 수 있다: Walsh-Hadamard 변환 혹은 양자 Fourier 변환으로 계산 경로의 중첩 상태를 준비하고, 적절한 위상 변환을 통한 함수 값 계산 후, 다시 Walsh-Hadamard 변환이나 양자 Fourier 변환을 사용하여 계산 경로를 모은다. 구체적인 알고리즘의 설명에 들어가기 전에, 다음과 같은 양자계산에 사용되는 몇 가지 기본적인 작용소와 양자 병렬처리(quantum parallelism)를 소개하는 것

이 필요하다. 먼저, 양자 컴퓨터에서 함수를 계산하기 위해서는 두 개의 양자 레지스터를 준비해야 한다. 첫 번째 레지스터는 입력 데이터를 저장하는 것이고, 두 번째 레지스터는 출력 데이터를 저장하는 것이다. 준비된 두 개의 레지스터를 이용하여 함수의 값을 계산하려면 유니타리 작용소인 함수 계산 작용소(function evaluation operator)

$$U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y + f(x)\rangle \tag{2}$$

를 사용한다. 이 함수 계산 작용소 U_f는 함수 값을 하나하나 계산하는 것이 아니라 중첩된 상태로 모든 입력에 대한 함수 값을 한번에 계산할 수 있다. 그러기 위해서 다음의 유니타리 작용소를 도입한다. Walsh-Hadamard 변환

$$W : |x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \tag{3}$$

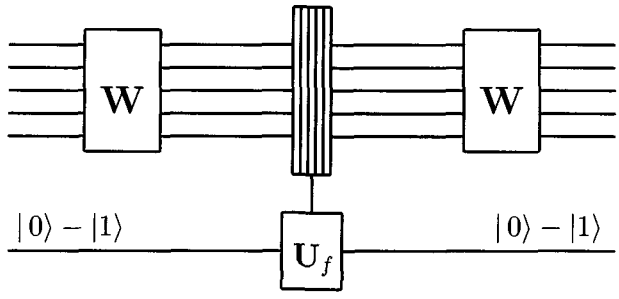
을 사용하면 수식 (4)에서 보는 바와 같이, 단지 하나의 상태를 이용하여 모든 입력 값의 중첩상태를 준비할 수 있고, 여기에 함수 계산 작용소를 단지 한번 작용함으로써 모든 함수 값을 계산할 수 있다. 이것이 바로 자연스러운 양자 병렬처리(quantum parallelism)이다.

$$|0^n\rangle \otimes |0\rangle \xrightarrow{W^n \otimes I} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} |i\rangle \otimes |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} |i\rangle \otimes |f(i)\rangle. \tag{4}$$

이러한 양자 병렬처리를 사용하여 그 함수 값에 대해서 입력 값에 의존하는 임의의 연산을 취하여 계산된 모든 출력 값을 하나의 상태에 담을 수는 있지만, 어떠한 양자 측정도 그 모든 계산된 값을 전부 추출할 수는 없다. 하지만, Deutsch-Jozsa 문제에서 보여지는 함수의 특정한 성질이나, Shor의 소인수분해 알고리즘에서 중요한 역할을 하고 있는 함수의 주기와 같은 함수의 광역적인 성질에 대한 정보를 얻어낼 수 있는 방법이 존재한다. 바로 이점이 양자 계산의 중요한 특징 중 하나이며 양자 컴퓨터가 고전 컴퓨터에 비하여 월등한 계산 능력을 가지는 이유 중 하나이다. 이제 이러한 양자 컴퓨터의 놀라운 계산능력을 보여주는 몇 가지 알고리즘에 대해서 구체적으로 살펴보도록 하자.

제 2 절 Deutsch-Jozsa 알고리즘

양자 컴퓨터를 사용하면 고전 계산보다 월등히 빠르게 해결할 수 있는 문제가 처음으로 소개된 것은 1985년 Deutsch에 의해서 였다 [1]. 그 문제는 함수 $f : \mathbf{Z}_2 \to \mathbf{Z}_2$ 가 상수함수 인지 상수함수가 아닌지를 판정하는 문제인데, 이것은 함수 f의 특정한 함수 값을 묻는 문제가 아니고 함수 자체의 성질을 결정하는 문제이기 때문에, 고전적으로는 이 판



(그림 2) Deutsch-Jozsa 알고리즘의 회로

정을 위해서 함수 값 $f(0)$ 와 $f(1)$ 모두를 계산해야 한다. 그러나, 양자 계산에서는 단 한번의 함수 값 계산으로 이 문제를 해결할 수 있다. 이 문제는 1992 년에 Deutsch와 Jozsa [2]에 의해서 일반화 되었는데, 그것은 다음과 같다. 부울 함수 $f : \mathbf{Z}_{2^n} \to \mathbf{Z}_2$ 가 상수함수 이거나 균형함수($f^{-1}(0) = f^{-1}(1)$ 인 함수) 둘 중의 하나로 주어져 있다고 가정했을 때, 주어진 함수 f 가 상수함수 인지 균형함수인지를 판별하고자 한다. 앞선 문제와 마찬가지로 고전적으로는, 최악의 경우, $2^{n-1}+1$ 번 함수 값을 계산해야 함수를 판정할 수 있다. 그러나, 양자 계산을 이용하면, 단 한번의 함수 값 계산으로 정확하게 그 함수를 결정할 수 있다. 이러한 Deutsch-Jozsa 알고리즘의 구체적인 설명은 다음과 같으며, 이 알고리즘의 회로는 (그림 2)에서 보여진다.

$$
\begin{aligned}
|0^n\rangle \otimes |1\rangle \quad &\xrightarrow{W^{n+1}} \quad \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&\xrightarrow{U_f} \quad \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad (5) \\
&\xrightarrow{W^n \otimes I} \quad \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).
\end{aligned}
$$

이제 수식 (5)의 마지막 상태에서 다음의 합

$$
\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} \qquad (6)
$$

을 계산해보면, 함수 f 가 상수함수인 경우에는 $y \neq 0$ 일 때이며, 함수 f 가 균형함수인 경우에는 $y = 0$ 일 때 0 이 됨을 알 수 있다. 따라서, 앞 부분의 레지스터를 측정했을 때, 0 이 관측되었다면 f 는 상수함수 이

며, 0 아닌 것이 관측되었다면 균형함수임을 단 한번 함수 값을 계산함으로써 결정할 수 있다.

이 Deutsch-Jozsa 문제와 알고리즘은 부울함수인 f 를 두 개 이상의 값을 갖는 함수로 확장하여 다시 두 가지로 일반화될 수 있는데, 균형함수를 균등균형함수(evenly balanced function)라는 개념을 도입하여 확장하는 일반화 [3]와 균등분포함수(evenly distributed function)를 사용하는 일반화가 있다 [4]. 전자의 경우에, 균등균형함수는 함수 값의 절반이 parity 0 을, 나머지 반이 parity 1 을 갖는 경우를 의미하기 때문에 단순히 주어진 함수에 parity 함수를 합성하면, 본래의 Deutsch-Jozsa 문제와 동일하게 해결될 수 있다. 그리고, 후자의 경우에, 균등분포함수는 함수 값의 분포가 주기적이고, 각각의 함수 값의 역상에 해당하는 원소의 개수가 동일한 함수를 의미한다. 이 경우 본래의 Deutsch-Jozsa 알고리즘을 약간 수정하면 이 문제를 해결할 수 있는 알고리즘을 다음과 같이 만들 수 있으며 이 알고리즘의 회로는 (그림 3)과 같다.

$$
\begin{aligned}
|0^n\rangle \otimes |\Psi\rangle &\xrightarrow{W^n \otimes I} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |\Psi\rangle \\
&\xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} e^{\frac{2\pi i f(x)}{M}} |x\rangle \otimes |\Psi\rangle \\
&\xrightarrow{W^n \otimes I} \sum_{y=0}^{2^n-1} \left(\frac{1}{2^n} \sum_{x=0}^{2^n-1} e^{\frac{2\pi i f(x)}{M}} (-1)^{x \cdot y} \right) |y\rangle \otimes |\Psi\rangle.
\end{aligned} \tag{7}
$$

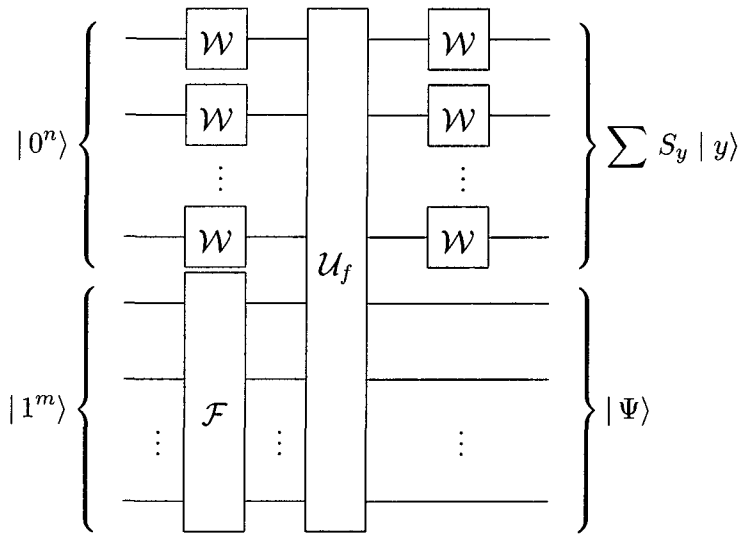
여기에서 주어진 함수는 $f : \mathbf{Z}_{2^n} \to \mathbf{Z}_M$ 이고, $|\Psi\rangle = \frac{1}{\sqrt{M}} \sum_{v=0}^{M-1} e^{-\frac{v}{M}} |v\rangle$ 이다. $\mathcal{F}$ 를 양자 Fourier 변환이라고 하면, $|\Psi\rangle = \mathcal{F}|1^m\rangle$ 이라고 할 수 있다.

수식 (7)의 마지막 상태의 괄호 안에 있는 합을

$$
S_y = \frac{1}{2^n} \sum_{x=0}^{2^n-1} e^{\frac{2\pi i f(x)}{M}} (-1)^{x \cdot y} \tag{8}
$$

라 하면, 함수 f 가 상수함수이면 S_y 가 y 가 0 이 아닐 때, 0 이 되며, f 가 균등분포함수이면 S_0 가 0 이 된다. 따라서 Deutsch-Jozsa 알고리즘과 마찬가지로 단 한번의 함수 값 계산으로 두 종류의 함수를 판정할 수 있다.

이러한 놀라운 계산 능력에도 불구하고, 이러한 문제들은 작은 오류를 감안한다면 이론적으로는 양자 컴퓨터가 아닌 고전적인 확률 컴퓨터에서도 효율적으로 풀려질 수 있다. 이러한 문제들과는 달리, 어떠한 고전적인 방법보다도 양자 컴퓨터에서 훨씬 더 효율적으로 문제를 해결할



(그림 3) 균등분포함수를 사용하여 일반화된 Deutsch-Jozsa 알고리즘의 회로

수 있는 대표적인 알고리즘인 Shor의 소인수분해 알고리즘과 Grover의 자료검색 알고리즘을 이후의 절에서 소개할 것이다.

제 3 절 Shor의 소인수분해 알고리즘

Shor에 의해서 1994년에 고안된 소인수분해 알고리즘은 양자 Fourier 변환

$$\mathcal{F} : |x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle \tag{9}$$

의 성질을 이용한 것이다 [5]. 이 알고리즘은 주어진 N 에 대하여 $N^2 < 2^n < 2N^2$ 을 만족하는 n 을 선택하고 N 보다 작은 임의의 수 y 를 선택하는 것으로부터 시작된다. 구체적인 소인수분해 알고리즘은 다음과 같다.

$$\begin{aligned} |0^n\rangle \otimes |0\rangle &\xrightarrow{\mathcal{F}\otimes I} \frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^n-1} |a\rangle \otimes |0\rangle \\ &\xrightarrow{U_{F_N}} \frac{1}{\sqrt{2^n}} \sum_{a=0}^{2^n-1} |a\rangle \otimes |y^a (\mathrm{mod} N)\rangle. \end{aligned} \tag{10}$$

여기에서 $F_N(x) = y^x (\mathrm{mod} N)$ 이다. 위의 식 (10)에서 마지막 상태의 두 번째 레지스터를 측정하여 z 를 얻었다면 0 부터 A (r 이 $\mathbf{Z}_N{}^*$ 에서 y 의 차수일 때 A 는 $(2^n-1)/r$ 보다 작은 정수 중 가장 큰 정수) 까지의 정수 j 에 대하여 $z \equiv y^{jr+l} (\mathrm{mod} N)$ 되는 가장 작은 정수 l 이 존재한다. 이제 두 번째 레지스터를 버리면, 첫 번째 레지스터의 상태는 다음과 같이 된다.

$$|\phi_l\rangle = \frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |jr+l\rangle = \sum_{a=0}^{2^n-1} f(a)|a\rangle. \tag{11}$$

여기에서 $f(a)$ 는 $r|(a-l)$ 이면 $\frac{1}{\sqrt{A+1}}$ 을, 그렇지 않다면 0 을 값으로 갖는 함수이다. 수식 (11)의 상태에 다시 양자 Fourier 변환을 취하면 그 상태는 다음과 같이 변한다.

$$\frac{1}{\sqrt{2^n}} \sum_{c=0}^{2^n-1} \sum_{a=0}^{2^n-1} e^{2\pi i \frac{ac}{2^n}} f(a)|c\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i \frac{lj}{r}} \left| \frac{2^n}{r} j \right\rangle. \tag{12}$$

이 상태를 관측하여 c 를 얻는다면 c 는 0 과 r 사이의 적당한 s 에 대하여 $\frac{s2^n}{r}$ 이 되고, 이 s 와 r 에 대하여 $\frac{s}{r} = \frac{c}{2^n}$ 이라는 식을 얻게 되는데, s 와 r 의 최대공약수가 1 이라면 이 식은 기약분수로 쓸 수 있다. 이 때, s 와 r 의 최대공약수가 1 일 확률은 $\frac{1}{\log N}$ 보다 크다. 일반적으로 식 (12)에서 c 를 관측할 확률은 다음과 같다.

$$\left| \frac{1}{2^n(A+1)} \sum_{j=0}^{A} e^{2\pi i \frac{rc}{2^n} j} \right|^2. \tag{13}$$

$|rc(\mathrm{mod} 2)|$ 이 $r/2$ 보다 작거나 같은 c 들의 집합을 C 라 하면, C 에 있는 각각의 c 에 대해서

$$|2^n c' - rc| \leq \frac{r}{2} \tag{14}$$

이 되는 c' 은 유일하게 존재한다. 따라서 C 는 정확하게 r 개의 원소를 가지고, c 와 c' 사이에는 일대일 대응관계가 있으므로 c' 을 얻을 확률은 c 를 얻을 확률과 같다. 그러므로, 다음과 같은 부등식을 얻을 수 있다.

$$\Pr(c') = \Pr(c) \geq \frac{4}{\pi^2 r}. \tag{15}$$

부등식 (14)를 다시 정리하면 다음과 같다.

$$\left| \frac{c}{2^n} - \frac{c'}{r} \right| \leq \frac{1}{2^{n+1}} \leq \frac{1}{2N^2} \leq \frac{1}{2r^2}. \tag{16}$$

여기에서 c'/r 은 $c/2^n$ 의 연분수(continued fraction) 전개로 볼 수 있으므로, c' 과 r 의 최대공약수가 1 이라면 우리는 r 의 값을 얻을 수 있다. 따라서 부등식 (15)를 이용하면 다음과 같은 부등식을 얻을 수 있다.

$$\Pr(c \in C \text{ and } \gcd(c', r) = 1) \geq \frac{4\phi(r)}{\pi^2 r} \geq \frac{4}{\pi^2 \log N}. \tag{17}$$

그러므로, 부등식 (17)에 있는 확률로, 주어진 N 의 약수를 구할 수 있다.

이제 소인수분해 알고리즘의 효율성에 대해서 알아보도록 한다. 어떤 알고리즘이 $1-\varepsilon$ 의 확률을 가지고 성공적으로 일을 수행한다고 하면, ε 은 입력값 N 과 독립적이므로, 그 알고리즘을 k 번 반복해서 성공률을 $1-\varepsilon^k$ 으로 높일 수 있다. 따라서 반복횟수를 충분히 크게 정함으로써 성공률을 임의로 1 에 가깝게 할 수 있다. 이 Shor의 소인수분해 알고리즘도 마찬가지여서, 이 효율적인 확률론적 알고리즘을 $O((\log N)^2)$ 번 반복하면 높은 성공률을 가진 알고리즘을 얻을 수 있다.

제 4 절 Grover의 자료검색 알고리즘

Shor 의 소인수분해 알고리즘과 더불어 양자 알고리즘의 우수성을 보여주는 또 다른 알고리즘이 바로 1996년에 Grover에 의해서 고안된 자료검색(database search) 알고리즘이다 [6].

이제 간단한 한가지 예 (4 개의 자료중에서 검색하고자 하는 자료의 수는 1 개인 경우) 를 통하여, Grover 의 자료검색 알고리즘에 대해 알아보기로 하겠다. 이러한 경우에, 고전적으로는 평균적으로 2 번, 최악의 경우 4 번까지 질의(query)가 필요하다. 그러나, 이 알고리즘에 의하면 단 한번의 질의로 원하는 자료를 얻을 수 있다. 구체적인 알고리즘에 대해서 살펴보도록 한다. 먼저 다음과 같은 상태를 준비한다.

$$|s\rangle = \frac{1}{2}\sum_{x=0}^{3} |x\rangle. \tag{18}$$

수식 (18)과 같이 준비되어 있는 상태는 $|0\rangle$ 상태에 Walsh-Hadamard 변환을 취함으로써 쉽게 얻을 수 있다. 0 부터 3 사이에 있는 어떤 값 w 를 모른다고 할지라도, 상태 $|w\rangle$ 가 기저 중 하나이므로 다음과 같은 식이 만족하는 것은 알 수 있다.

$$|\langle w|s\rangle| = \frac{1}{2} = \sin 30^\circ. \tag{19}$$

위 식 (19)로 부터, 기하학적으로 $|s\rangle$ 는 $|w\rangle$ 에 수직인 축으로부터 30도 만큼 떨어져 있음을 알 수 있다. 양자 오라클(quantum oracle)로부터 작용하는 변환 U_w 를 $I - 2|w\rangle\langle w|$, 그리고 U_s 를 $2|w\rangle\langle w| - I$ 라 하고, Grover 반복(iteration) R_{grov} 를 $U_s U_w$ 라고 하자. U_w 는 상태 $|w\rangle$ 의 부

호를 반대로 해주며 $|w\rangle$ 를 제외한 다른 어떠한 기저 상태에 대해서도 영향을 주지 않는다. 그리고, U_s 는 상태 $|s\rangle$ 와 직교하는 벡터의 부호를 반대로 해주며 $|s\rangle$ 는 그대로 보존한다. 따라서 Grover 반복 R_{grov} 라는 변환은, 기하학적으로 $|s\rangle$ 와 $|w\rangle$ 로부터 생성되는 평면에서의 60도 회전 변환임을 알 수 있다. 그러므로, 상태 $|s\rangle$ 에 Grover 반복 R_{grov} 을 한 번 취하면, $R_{\text{grov}}|s\rangle$ 와 $|w\rangle$ 는 같은 직선 상에 놓이게 되고, 따라서 그 상태를 측정하면 확률 1 로 $|w\rangle$ 를 관측할 수 있게 되는 것이다.

Grover 반복은 또 다른 방법으로 설명할 수 있는데, 그것은 "평균에 대한 반전(inversion)"으로 이해하는 것이다. 일반적인 상태는 다음과 같이 주어진다.

$$|\psi\rangle = \sum_{x=0}^{3} a_x |x\rangle. \tag{20}$$

그러면, 식 (20)의 상태와 $|s\rangle$ 와의 내적은 다음과 같이 된다.

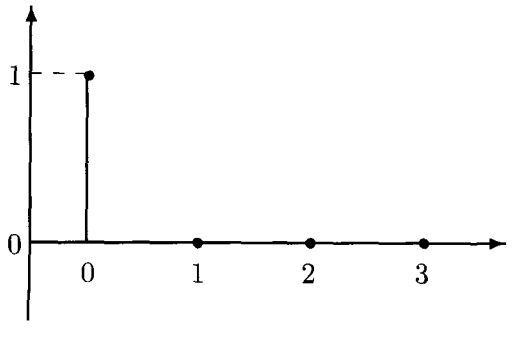
$$\langle s|\psi\rangle = \frac{1}{2}\sum_{x=0}^{3} a_x = 2\langle a\rangle. \tag{21}$$

여기에서 $\langle a\rangle$ 는 이 상태의 진폭(amplitude)의 평균값이다. 식 (20)의 상태에 U_s 를 취하면 다음과 같은 식을 얻을 수 있다.

$$U_s|\psi\rangle = \sum_{x=0}^{3} (2\langle a\rangle - a_x)|x\rangle. \tag{22}$$

수식 (21)로 부터 U_s 는 진폭(amplitude)에 대해서만 보면 $a_x - \langle a\rangle$ 를 $\langle a\rangle - a_x$ 로 변환해 준다는 것을 알 수 있다. 따라서, U_s 는 어떤 상태에 대한 각각의 진폭(amplitude)을 그것들의 평균에 대해 반전(inversion)시키는 역할을 한다는 것을 알 수 있다. 이에 따른 알고리즘을 간단히 그림과 함께 설명하면 다음과 같다.

여기에서 우리가 찾고 싶은 자료 w 를 1 이라고 가정한다.

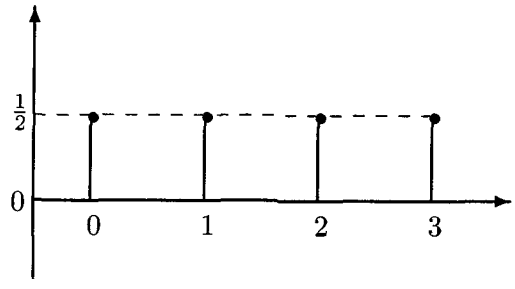


(그림 4) 초기상태 $|0\rangle$

먼저 (그림 4)와 같이 $|0\rangle$ 상태를 준비한다.

그리고 나서 $|0\rangle$ 상태에 Walsh-Hadamard 변환을 취한다. Walsh-Hadamard 변환을 $|0\rangle$ 상태(state)에 작용시키면, (그림 5)에서 보는 바와 같이 다음의 상태로 변한다.

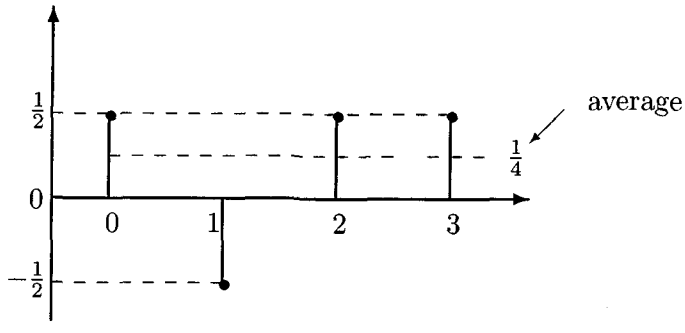
$$|s\rangle = \frac{1}{2}\sum_{x=0}^{3}|x\rangle. \tag{23}$$



(그림 5) Walsh-Hadamard 변환 후의 상태

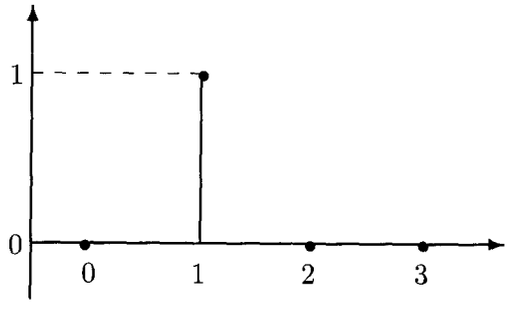
이러한 상태에 양자 오라클(quantum oracle)로부터 조건적으로 위상(phase)을 변환해주는 유니타리 작용소 U_w - 조건부위상변환(conditional phase transform) - 을 취해주면, 양자 오라클에 의해서 계산된 함수를 f_w 라 할 때, 즉, f_w 가 w 에 대해서만 함수 값이 1 이고 나머지에 대해서는 함수 값이 0 인 함수일 때, (그림 6) 에서와 같이 변환되는 상태는 다음과 같이 된다.

$$\frac{1}{2}\sum_{x=0}^{3}(-1)^{f_w(x)}|x\rangle. \tag{24}$$



(그림 6) 변환 U_w를 취한 후의 상태

마지막으로, 평균에 대한 반전을 나타내주는 유니타리 변환 U_s - 위상 확산 변환(phase diffusion transform) - 을 작용시키면, (그림 7)에서와 같이 원하는 $|w\rangle$ 상태만 남게 된다. 따라서, 이 상태를 서로 수직인 $|0\rangle$과 $|1\rangle$, $|2\rangle$, $|3\rangle$ 상태를 관측할 수 있는 측정을 사용하면 확률 1 로 원하는 상태를 관측할 수 있게 되는 것이다.



(그림 7) 변환 U_s를 취한 후의 상태

이러한 Grover 의 자료 검색 알고리즘은 검색하고자 하는 자료의 수가 전체 자료의 1/4 이상일 때, 단 한번의 질의만으로 원하는 자료를 확률 1 로 검색할 수 있는 알고리즘으로 일반화될 수 있다 [7]. 이 일반화된 자료 검색 알고리즘의 자세한 설명은 다음과 같다.

우선 $N = 2^n$ 이라고 가정하자. 그리고, H_N 을 기저 $B_N = \{|e_1\rangle, |e_2\rangle, \cdots, |e_N\rangle\}$ 에 의해서 생성된 N 차원 Hilbert 공간이라 하고, H_m 을 $B_m = \{|e_{j_1}\rangle, |e_{j_2}\rangle, \cdots, |e_{j_m}\rangle\}$ 을 기저로 갖는 H_N 의 m 차원 부분공간이라 하자.

$F : \mathbf{Z}_N \to \mathbf{Z}_2$ 를 오라클에 의해서 계산되는 부울 함수라고 하면, 임의의 실수 γ 에 대하여 H_m 위에서의 조건부 γ-위상 변환 $S^{H_m}_{F,\gamma} : H_m \to H_m$ 을 다음과 같이 정의할 수 있다. 임의의 $k = 1, 2, \cdots, m$ 에 대하여

$$S^{H_m}_{F,\gamma}|e_{j_k}\rangle = (e^{i\gamma})^{F(e_{j_k})}|e_{j_k}\rangle. \tag{25}$$

$F_l(e_{j_k}) = \delta_{j_k j_l}$ 일 때, 간단히 $S^{H_m}_{F_l,\gamma}$ 를 $S^{H_m}_{l,\gamma}$ 이라고 표기할 것이다.

임의의 실수 β 에 대하여 H_m 위에서의 β-위상 확산 변환 $D^{H_m}_{l,\beta}$ 을 다음과 같이 정의한다.

$|e_j\rangle, |e_k\rangle \in B_m$ 이며 $j \neq k$ 일 때는 $\langle e_j|D^{H_m}_{l,\beta}|e_k\rangle = \frac{e^{i\beta}-1}{m}$ 이고, $|e_j\rangle, |e_k\rangle \in B_m$ 이며 $j = k$ 인 경우에는 $\langle e_j|D^{H_m}_{l,\beta}|e_k\rangle = 1 + \frac{e^{i\beta}-1}{m}$ 으로 정의하며 나머지인 경우에는 δ_{jk} 로 정의한다.

이 두 변환으로부터 (β,γ)-위상의 일반화된 Grover 작용소 $G^{H_m}_{F,\beta,\gamma}$: $H_N \to H_N$ 를

$$G^{H_m}_{F,\beta,\gamma} = D^{H_m}_{\beta} : H_N \to H_N \tag{26}$$

이라고 정의한다.

이 일반화된 Grover 작용소 $G^{H_m}_{F,\beta,\gamma}$ 를 사용하면, 전체 자료 N 개 중에서 원하는 자료 t 개가 있고, t 가 $N/4$ 에서 N 까지의 수라고 할 때, $\beta = \gamma = \cos^{-1}(1 - \frac{N}{2t})$ 으로 놓으면, 본래의 Grover의 자료검색 알고리즘과 마찬가지로, 단 한번의 질의로 원하는 자료를 검색할 수 있다.

제 5 절 결 론

지금까지 현재 잘 알려져 있는 몇 가지 양자 알고리즘과 그 일반화에 대해서 알아보았다. 여기에서 소개된 양자 알고리즘은 그에 대한 분석과 더불어 그 알고리즘의 새로운 해석이 시도되기도 하였다. 특히, Shor의 소인수분해 알고리즘은 소인수분해 문제나 이산로그 문제의 어려움에 의거하고 있는 공개키 암호체계에 큰 영향을 미칠 수 있고, Grover의 자료검색 알고리즘은 DES와 같은 비밀키 암호체계에 위협을 가할 수 있다. 따라서 양자 알고리즘의 개발은 현대 사회에 지대한 영향력을 행사할 수 있는 능력을 가지고 있으며, 아직은 유치한 단계일지라도 그 알고리즘에 대 한 구현 또한 급속도로 진전되고 있다.

앞서 소개한 양자 알고리즘뿐만 아니라 이것들을 응용한 여러 가지 알고리즘이 많은 연구진에 의해서 개발되고 실험되고 있다. 이것은, 양자 알고리즘이란 분야가 다른 양자 계산 분야와 마찬가지로, 양자 컴퓨터의 우수한 능력을 과시하는, 계속되는 시도가 있다는 것을 보여주는 하나의 예라고 볼 수 있으며, 그러한 사실로부터, 또 다른 놀라운 계산 능력을 보여주는 새로운 알고리즘의 개발을 기대해보는 것도 그리 무리한 일은 아니라고 생각된다.

참고 문헌

[1] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society. London. Series A **400** (1985), 96–117.

[2] D. Deutsch and R. Jozsa, *Rapid solution of problems by quantum computation*, Proceedings of the Royal Society. London. Series A **439** (1992), 553–558.

[3] R. Cleve, A. Ekert, C. Macciavello, and M. Mosca, *Quantum algorithms revisited*, Proceedings of the Royal Society. London. Series A **454** (1998), 339–354.

[4] D. P. Chi, J. Kim and S. Lee, *Initialization-free generalized Deutsch-Jozsa algorithm*, Journal of Physics A: Math. Gen. **34** (2001), 5251–5258.

[5] P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science (Piscataway, NJ), IEEE Computer Society Press, pp. 124-134, 1994; SIAM Journal of Computing **26** (1997), 1484–1509.

[6] L. K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings of the 28th Annual ACM Symposium on Theory of Computing (New York), ACM, pp. 212-219, 1996; Physical Review Letters **79** (1997), 325–328.

[7] D. P. Chi and J. Kim, *Quantum database search by a single query*, Proceedings of First NASA International Conference on Quantum Computing and Quantum Communication (Palm Springs, CA), Lecture Notes in Computer Science, Springer-Verlag **1509**, pp. 148-151, 1999; Chaos, Solitons and Fractals **10** (1999), 1689–1693.

[8] R. Cleve, A. Ekert, L. Henderson, C. Macciavello, and M. Mosca, *On quantum algorithms*, quant-ph/9903061, 1999.

[9] J. Kim, S. Lee and D. P. Chi, *Quantum Functional Oracles*, Journal of Physics A: Math. Gen. **35** (2002), 6911–6917.

서울대학교 자연과학대학 수리과학부
서울시 관악구 신림동 산 56-1
151-747
E-mail: dpchi@math.snu.ac.kr