교육학석사 학위논문

IBM QX를 활용한
양자 알고리즘 교육 프로그램 개발

- Grover 알고리즘을 중심으로 -

2023년 2월

서울대학교 대학원

수학교육과

류 건

IBM QX를 활용한
양자 알고리즘 교육 프로그램 개발

- Grover 알고리즘을 중심으로 -

지도교수 윤 상 균

이 논문을 교육학석사 학위논문으로 제출함
2023년 2월

서울대학교 대학원
수학교육과
류 건

류건의 석사 학위논문을 인준함
2023년 2월

위 원 장 조 정 효 (인)

부위원장 이 훈 희 (인)

위 원 윤 상 균 (인)

국문초록

앞으로 학생들이 살아갈 시대는 양자 컴퓨터에 의해 기존의 과학 기술의 난제가 해결되고, 새로운 응용 산업 및 연구 분야가 출범하는 시대이다. 따라서 미래 교육은 양자 컴퓨터에 대해 전문성을 갖춘 창의·융합 인재 양성에 주목해야할 것으로 보인다.

본 연구의 목적은 교수학적 변환을 통해 Grover 알고리즘의 수학적 엄격함을 낮추고, 중등교육 기관 학생들을 대상으로 공학적 도구 기반의 <양자 알고리즘> 교육 프로그램을 개발하는 것이다. 이를 위해 현 Grover 알고리즘의 내용 체계를 정립하였고, 정의 유형과 정의 수준을 분석하여 공학 통합 교육 환경 내에서 학교수학 수준의 가르칠 지식을 선언함으로써 재구조화된 Grover 알고리즘의 내용 체계를 제안하였다. 또한 Grover 알고리즘의 작동 원리의 이해를 성취 기준으로 하는 과제를 개발하고, 그에 따른 교수·학습 과정을 설계하였다. 최종적으로는 2022년 서울대학교 사범대학 부설 시흥영재교육원 고등학생 2학년을 대상으로 본 연구에서 개발한 <양자 알고리즘> 교육 프로그램 적용하였고, 해당 과정을 평가 및 분석 함으로써 수정·보완하였다.

본 연구는 미래 사회에 대비하기 위한 수학 교과 신설의 필요성이 강조되고 있는 현재, 학교수학의 도입을 목적으로 한 새로운 수학 교과의 가능성을 제시하였다는 점에서 그 의의를 갖는다. 한편 본 연구에서 개발한 교육 프로그램은 학습자들이 의사소통 및 추론 역량을 함양할 수 있다는 점에서 교육적 의의를 갖는다. 또한 코딩을 수반하지 않는다는 점과 교수·학습 과정에 대한 해설이 상세히 제시되어 있다는 점으로부터 교사들에 대한 접근성이 높다는 의의를 갖는다.

주요어 : Grover 알고리즘, IBM QX, 교육 프로그램, 교수학적 변환
학　번 : 2021-21157

목 차

표 목 차

그 림 목 차

제 1 장 서론

고전 컴퓨터[1]는 정보 처리의 기본 단위로 2진 숫자(binary digit) 비트(bit)를 사용하고, 양자 컴퓨터는 정보 처리의 기본 단위로 2차원 복소 벡터공간의 기저 벡터(basis vector) 큐비트(qubit)를 사용한다. 고전 컴퓨터가 비트를 이용하여 정보를 한 번에 한 가지씩만 표현할 수 있는 것에 비해, 양자 컴퓨터는 큐비트를 이용하여 단일 정보를 표현하는 것에서 더 나아가 중첩된 정보를 표현할 수 있다. 이러한 몇 가지 특성으로부터 양자 컴퓨터는 많은 양의 계산을 병렬적으로 처리할 수 있고, 특정 문제에 대해서는 선형적으로 연산을 처리하는 고전 컴퓨터보다 극적인 효율성을 보인다(McMahon, 2008, p. 197).[2] 양자 컴퓨터는 이와 같이 연산 처리 시간을 획기적으로 단축시킬 수 있다는 가능성으로부터 큰 관심을 끌었다. 특히, 큰 소수들의 곱으로 주어진 수를 효율적으로 분해할 수 있는 Shor 알고리즘이 현대의 인터넷 통신과 상거래의 표준인 RSA 암호체계에 큰 위협이 된다는 점으로부터 지대한 관심을 끌었던 것을 예로 들 수 있다(김영훈 & 허재성, 2020, p. 115).

앞으로의 양자 컴퓨터는 특정 문제에 대해서 미래에 성능이 가장 뛰어날 것으로 예상되는 슈퍼컴퓨터[3]조차 능가할 것으로 예상되며, 이에 따라 기존의 과학 기술 난제를 해결하고 새로운 응용 산업 및 연구 분야가 출범할 것으로 예상된다. 이에 발맞춰 세계 주요국은 국가 차원의 투자와 함께 양자 컴퓨터 개발에 대한 육성 정책 수립과 전략적 R&D를 추진하고 있다(이준 & 이상민, 2019, pp. 2-7). 따라서 미래 교육은 양자

---

1) 본 연구에서 '고전 컴퓨터'라는 용어는 양자 컴퓨터 이전 세대의 디지털 컴퓨터에 한정하여 사용한다.

2) Google(2019)은 53-큐비트 수준의 양자 컴퓨터 칩 시커모어(sycamore)를 발표하면서 기존의 슈퍼컴퓨터로 해결하는 데 1만년 걸릴 과제를 약 200초 만에 풀 수 있다고 밝혔다(국방과 기술, 2021).

3) 국가슈퍼컴퓨팅센터에 따르면, 통상적으로 연산 처리 속도가 세계 500위 이내에 해당하는 컴퓨터를 슈퍼컴퓨터로 정의한다.

컴퓨터에 대해 전문성을 갖춘 창의·융합 인재 양성에 더욱 주목해야할 것으로 보인다.

양자 컴퓨터의 개발은 인공지능, 양자소자, 양자계측 등 첨단 과학기술에 힘입어 상당히 가속화되고 있으나[4], 상용화까지는 아직 많은 시간이 필요한 것으로 보인다. 그러나 오늘날 주요 선도 기업들은 서로 독립적으로 개발한 자사의 양자 컴퓨터를 제한된 차원 하에서 클라우드 기반으로 제공하기 시작했으며, 중소기업의 경우 이러한 서비스를 이용하여 차별화된 응용 프로그램을 적극적으로 개발하고 있다(pp. 13-14). 이에 따라 국내에서도 양자 알고리즘을 이용한 특정 문제의 접근 및 해결, 양자 자원 평가 등 다양한 맥락에서 클라우드 기반 양자 컴퓨터와 관련된 많은 연구들이 이루어져 왔다(e.g., 김범일 외, 2020; 김범일 외, 2021; 김정민 & 허준, 2020; 김창준 외 2020a, 2020b; 문현승 외 2019; 민건식 & 허준 2020a, 2020b; 서영진 외, 2018; 서영진 & 허준, 2020; 손일권 외, 2019; 송경주 외, 2021; 신용재 & 허준, 2021; 윤진호 & 문봉교, 2019; 장경배, 김현준 외, 2021; 장경배, 김현지 외, 2021; 조윤호 & 허준, 2020; 하진영 외, 2018; 하진영 외, 2019). 한편 교육부(2017a)는 교과의 특성에 맞는 다양한 학습이 이루어질 수 있도록 교수·학습의 전 과정에서 적절한 교육 기자재를 활용하여 학습 효과를 높일 것을 강조하고 있으며, 이를 위해 다양한 공학적 도구와 교구의 확보를 강조한 바 있다(p. 147). 그러나 클라우드 기반 양자 컴퓨터의 교육적 활용 가능성을 살펴보는 연구는 미흡한 실정이다.

Steen(1988)은 수학을 패턴(pattern)의 과학으로 설명한다. 즉 Steen에 따르면, 수학은 패턴들 사이의 관계이며 수학의 응용은 패턴을 이용하여 자연적인 현상이나 수학적인 현상을 설명하고 예상하는 것이다(류희찬 & 이지요, 1993, p. 75에서 재인용). 이러한 패턴은 시각화를 함의하므로 그동안 수학교육에서 시각화는 중요시되어 왔다(고상숙 & 홍석만 2002a, 2002b; 류희찬 & 이지요, 1993). 수학적 개념의 시각화는 새로운 개념의

4) 1997년 IBM사에서 2-큐비트 수준의 양자 컴퓨터를 출시한 지 20년이 채 지나지 않은 2011년에 D-Wave 사는 128-큐비트 수준의 양자 컴퓨터를 출시하였다.

발견과 이해를 위해 수학적 이미지를 형성하고 활용하는 과정으로서(이상구 외, 2014), 수학 개념의 직관적인 인지에 대한 본질적인 요소로 작용한다. 한편 양자 컴퓨팅은 컴퓨터 공학(computer science)뿐만 아니라 해석학(analysis)과 선형대수학(linear algebra), 더 넓게는 정수론(number theory), 함수해석학(functional analysis), 확률론(probability theory), 군론(group theory) 등 다양한 수학 분야로부터 유래되었다(Scherer, 2019, p. vii). 즉 양자 계산 이론은 엄밀한 수학적 구조 아래에서 기술되며, 이로부터 시각화는 <양자 알고리즘> 교육에서도 중요시되어야 할 요소임을 알 수 있다.

지금까지 진술한 맥락을 고려하였을 때, 본 연구자는 공학적 도구의 부재를 안고 있던 <양자 알고리즘> 교육에서 클라우드 기반 양자 컴퓨터의 교육적 활용 가능성은 어떠하며, 이에 의한 시각화는 어떻게 제공되어야 하는지에 대해서 고찰해볼 필요성이 있다고 생각하였다. 이를 위해 본 연구에서는 'Grover 알고리즘'을 중심 소재로 선정하였는데, 그 이유는 다음과 같다. 첫째, Grover 알고리즘은 비정형 데이터베이스로부터 특정 객체에 접근할 수 있는 검색 알고리즘(search algorithm)으로 광범위한 응용성을 갖고 있다. 둘째, Grover 알고리즘은 양자 계산의 실용성에 대해 많은 관심을 일으킨 양자 알고리즘 중 하나로(p. 313), 특정 문제에 대해서 고전 컴퓨터보다 훨씬 적은 연산으로 극적인 효율성을 보여주는 양자 컴퓨터의 강점을 잘 보여준다. 셋째, Grover 알고리즘은 학문을 위한 수학 지식 수준에서 엄밀하게 기술되지만, 기하학적인 관점에서 그 작동 원리를 해석할 수 있어 중등교육 기관 학생들에게 도입할 수 있는 여지가 있다.

이상의 맥락에서 본 연구의 목적은 Grover 알고리즘의 수학적 엄격함을 낮추고, 중등교육 기관 학생들을 대상으로 한 공학적 도구 기반의 <양자 알고리즘> 교육 프로그램을 개발하는 것이다. 이를 위해 교수학적 변환을 거쳐 Grover 알고리즘의 내용 체계를 재구조화하고, Grover 알고리즘의 작동 원리에 대한 이해를 성취 기준으로 하는 클라우드 양자 컴퓨터 기반의 과제와 수업을 설계하고자 한다.

제 2 장 이론적 배경

제 1 절 교수학적 변환

학문수학[5]과 학교수학[6] 사이의 차이는 일반적으로 학문수학에서 출발하여 그것의 내용들이 교육적인 목적에 의해 어떻게 변형될 수 있을지에 대하여 하향식(top-down) 관점에서 논의된다(Dreher et al., 2018). 대표적으로 Chevallard(1985)의 교수학적 변환론은 교육을 목적으로 하지 않는 학문수학의 내용 지식을 어떻게 학교 교육과정 내의 지식으로 재구성할 수 있을지에 관한 논의의 기반을 제공하였다(강완, 1991; 이경화, 1996). 교수학적 변환 과정에서는 필연적으로 내용 요소의 축소가 포함되며, 학문적 지식의 세부적인 내용들은 의도적으로 생략되고 수학적인 엄격함의 수준은 낮아진다(Dreher et al., 2018). 따라서 이러한 변환 과정에서는 해당 내용 지식이 여전히 '지적으로 정직한'(Bruner, 1960, p. 33) 방식으로 가르쳐질 수 있도록 '수학적 지식의 파손성'(Brousseau & Otte, 1991, p. 11)에 주의를 기울여야 한다(류건 외, 2022).

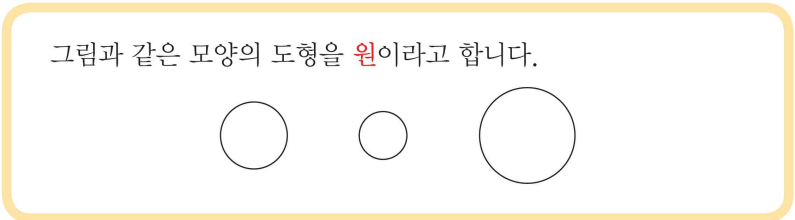
추상성과 논리성을 내포하는 수학 지식은 교사의 교수·학습 의도에 따라 본래의 의미가 파손되기 쉽다. 황혜정(2019)의 연구에 따르면, 이러한 지식의 파손성은 '환경의 재조성'과 '지식의 선언'을 통해 방지할 수 있다. 환경의 재조성은 교수학적 변화의 전 과정을 설명하는 것으로 교과서의 구성, 수업의 상황 및 설정 등을 뜻하며, 교사로 하여금 과거의 수학자와 현재의 학생간의 간격을 줄이기 위함이다. 지식의 선언은 사전 분석을 통해 교사가 가르칠 내용을 구성하고 선택하는 과정을 뜻하며, 학생들에게 보다 충실한 의미의 내용과 지식을 가르칠 것을 제안하기 위

5) 본 논문에서 '학문수학'이라는 용어는 고등교육 기관(대학, 대학원 등)에서 가르치고 행해지는 순수 수학 혹은 응용 수학을 의미한다.
6) 중등교육 기관(중학교, 고등학교)에서 가르치고 행해지는 수학을 의미한다.

함이다. 본 연구에서는 지적으로 정직한 방식으로 교수학적 변환이 이루어질 수 있도록 중심 소재의 핵심 내용 요소에 대한 정의 유형과 정의 수준을 분석하여 중등교육 기관 학생들을 대상으로 가르칠 지식을 선언하고, 재조성된 환경으로 공학적 도구의 구비가 마련된 공학 통합 교육 환경을 가정하였다. 이에 따라 본 절에서는 정의 유형과 정의 수준, 그리고 공학적 도구를 활용한 교육에 관한 선행연구들을 살펴본다.

1. 정의 유형과 정의 수준

학교수학에서 용어와 기호를 정의하는 방식은 학문수학에서 사용되는 정의 방식을 학교수학에 적절한 형태로 변형한 일종의 교수학적 변환으로 볼 수 있다(우정호 & 조영미, 2001; 조영미, 2001; 2002; 김선희 외, 2016). 학문수학에서 사용되는 정의 방식은 형식적이고 엄밀한 방법이다. 여기서 '엄밀함'은 수학적 개념의 본질을 간결한 표현을 통해 분석적으로 정의함을 말한다. 반면에 학교수학에서 사용하는 정의 방식은 학습자들이 학문으로서의 수학을 보다 쉽게 익힐 수 있도록 변형한 것으로써, 학문수학의 정의 방식보다 덜 엄밀하며 때로는 전혀 엄밀하지 않을 수 있다(조영미, 2001, pp. 3-4). 예컨대 <유클리드 원론>에서는 '어떤 선으로 둘러싸인 평면 도형에 있어서, 한 점에서 직선들을 그었을 때 그 도형의 내부에 놓이는 부분들이 모두 서로 같은 도형'으로 정의되는 원을 초등학교 2학년 1학기 수학 교과서에서는 [그림 Ⅱ-1]과 같이 시각적인 특성에 의존하여 원의 그림을 지시함으로써 정의한다(교육부, 2017b, p. 30).



[그림 Ⅱ-1] 초등학교 수학 교과서에서의 원의 정의

교육부는 교사용 지도서를 통해 초등학교 2학년 1학기에서는 '한 점에서 같은 거리에 있는 점들의 모임'이라는 원의 개념적 정의는 배우지 않는다고 명시하고 있으며(2017d, p. 203), 원 모양의 물건을 본뜨거나 모양자를 이용하여 학생들로 하여금 원의 특징을 시각적으로 이해할 수 있게 지도하도록 안내하고 있다(2017c, p.150). 이러한 교수·학습 방안은 학문을 위한 수학에는 적절하지 않지만, 교육을 염두에 둘 때 인지 수준이 낮은 학습자에게는 유용한 방안이다.

1.1. 정의 유형

Ginther(1964)는 학교수학에서 용어를 얼마나 엄밀하게 사용하고 있는지를 분석하고자 일반 논리학을 참조하여 학교수학의 정의 유형을 내포적(connotative), 외연적(denotative), 동의적(synonymical)의 세 범주로 구분하고, 다시 각 범주 내에서 하위 유형을 설정한 바 있다. 조영미(2001)는 일반 논리학에 따른 Ginther의 구분이 수학적인 특성을 온전히 포착하기에는 비교적 단순함을 지적하며(p. 26), 각 범주가 학교수학에서 제시하고 있는 수학적 정의의 특성을 보다 잘 반영할 수 있도록 구분을 세분화하였다. 여기서는 조영미가 설정한 정의 유형의 분석 틀을 살펴본다.

첫 번째로 내포적 정의는 정의 대상의 성질을 기술하여 정의하는 방식으로, 일정한 조건을 제시하고 있는 정의이다. 내포적 정의는 다시 조건의 제시 방식에 따라 필요충분조건으로서의 내포와 필요조건 또는 충분조건으로서의 내포로 구분된다. 이는 학문으로서의 수학에서 사용하는 정의 방식과 가장 유사한 것으로, 수학적 엄밀성을 가장 잘 보장하는 방식이다. 이와 같은 내포적 정의에 해당하는 정의 방법으로는 논리적, 발생적, 관계적, 조작적, 공리적 정의 등이 있다. 논리적 정의는 (최근)류와 종차에 의한 정의이고, 발생적 정의는 어떤 개념의 발생 조건 또는 과정을 사용하는 정의이며, 관계적 정의는 관계로 이루어진 어떤 체계 내에서 정의하려는 사물이 차지하는 위치를 사용하는 정의이다. 조작적 정의는 한 개념이 관찰되는 사태를 정의의 한 부분으로 포함시키는 정의이

고, 공리적 정의는 대상을 직접적으로 기술하지 않으면서 그 대상이 갖추어야 할 조건을 제시하는 정의이다. 두 번째로 외연적 정의는 정의 대상을 완전하게 규정하지 않고 개념에 속하는 일부의 예들을 사용하여 정의하는 방식으로, 개념에 포괄되는 대상 전체로서 개념을 기술하는 정의이다. 외연적 정의는 다시 대상을 지시하는 방식과 대상의 전체 또는 부분을 열거하는 방식으로 구분된다. 세 번째로 동의적 정의는 정의 대상의 동의어를 사용 또는 대체하여 정의하는 방식으로, 피정의항과 유사한 의미를 지닌 용어를 사용하는 정의이다. 이와 같은 동의적 정의에는 학습자에게 친숙하거나 이해하기 쉬운 언어를 사용하는 방법과 사전식 방법, 그리고 축약과 기호화가 포함된다. 외연적 정의와 동의적 정의는 내포적 정의에 비해 학문을 위한 수학의 정의 특성으로부터 벗어나 논리적으로 불완전하다고 볼 수 있으나, 심리적인 적합성을 지닐 수 있어 학교수학에서 적극적으로 사용된다(pp. 26-35).

조영미(2001)는 Ginther의 분석 틀을 참조한 이상의 구분을 기반으로 학교수학에서 제시하고 있는 정의 방식의 특징을 추출하고자 초·중·고의 수학 교과서에서 나타나는 정의의 문장 형태를 조사 및 분류함으로써 각 범주의 하위 유형을 추출하고, 그에 대한 예를 <표 Ⅱ-1>과 같이 제시하였다(pp. 55-60).

<표 Ⅱ-1> 학교수학의 정의 유형 분석 틀

정의 유형	유형 코드	하위 유형	예시
내포적	C1	U인 V를 X라고 한다.	• 그 내용이 참인지 거짓인지 판별할 수 있는 문장을 명제라고 한다.
	C2	…일 때, U인 V를 X라고 한다.	• 어떤 문제에서 주어진 집합에 포함된 부분집합만 다룰 때, 그 주어진 집합을 전체집합이라 한다.
	C3	1) U인 V, 곧 U'인 V를 X라고 한다. 2) V가 U일 때, 곧 U'인 V를 X라고 한다.	• 약수를 2개만 갖는 자연수, 곧 1보다 큰 자연수 중에서 1과 그 수 자시만을 약수로 가지는 자연수를 소수라 한다. • 자연수 a가 자연수 b로 나누어 떨어질 때, 곧 $a=b\times$(자연수)의 꼴로 나타낼 수 있을 때, b를 a의 약수, a를 b의 배수라고 한다.

	C4	… 이다. U인 V를 X라고 한다.	• 평균을 구할 때 대략의 평균을 미리 가정하여 각 변량의 차에 대한 평균을 구하면 편리하다. 이때 미리 가정한 대략의 평균을 가평균이라 한다.
	C5	V가 U일 때, V를 X라고 한다.	• a가 집합 A의 원소일 때, a는 A에 속한다고 한다.
	C6	U일 때, V를 X라고 한다.	• 오차의 절댓값이 어떤 값 이하라고 할 때, 그 값을 주어진 근사값에 대한 오차의 한계라고 한다.
	C7	U이다. 이때(여기서) V를 X라고 한다.	• 앞쪽의 물음에서 등식 $x+3=7$은 x에 4를 대입하면 참이 되지만 4이외의 값을 대입하면 거짓이 된다. 이와 같이 x의 값에 따라 참이 되기도 하고, 거짓이 되기도 하는 등식을 방정식이라 하며, 이때 x를 미지수라고 한다.
외연적	D1	…[한가지 예]인 V를 X라고 한다.	• 이러한 [그림]을 벤 다이어그램이라고 한다.
	D2	…[예들을 열거]인 V를 X라고 한다.	• ±1, ±2, …과 같은 수를 양의 정수라고 한다.
	D3	… 에서 ~[예]를 X라고 한다.	• 두 직선 l, m과 한 직선 n이 만날 때 생기는 8개의 각 중에서 $\angle a$와 $\angle e$, $\angle a$와 $\angle e$, $\angle a$와 $\angle e$, $\angle a$와 $\angle e$를 각각 서로 동위각이라 한다.
	D4	… 이다. 이때, ~[예] ~를 X라고 한다.	• 점 P를 P$(-3, 2)$와 같이 나타낸다. 여기서 -3을 점 P의 x 좌표, 2를 점 P의 y 좌표라 한다.
	D5	…[부분집합을 열거]를 X라고 한다.	• 좌변과 우변을 통틀어 양변이라고 한다.
	D6	…[지시하는 경우]를 X라고 한다.	• [그림]을 정사면체라 한다.
	D7	…[예시적 언어를 사용]를 X라고 한다.	• 5의 오른쪽에 쓴 2, 3, 4, …을 5의 거듭제곱의 지수라고 한다.
동의적	S1	보다 친숙하고 알기 쉬운 말을 사용하여 정의한다.	• 이와 같이 집합 A의 원소 a에 집합 B의 원소 b가 맺어졌다면 a에 b가 대응된다고 한다.
	S2	말을 기호로 바꾼 정의이다.	• 이와 같이 두 집합 A, B에서 A와 B의 원소 전체로 이루어진 집합을 A와 B의 합집합이라 하며, 기호 A$\cup$B로 나타낸다.
	S3	기호 읽는 법을 알려주는 정의이다.	• 오진법의 수 243을 십진법의 수와 구별하여 $243_{(5)}$와 같이 쓰고, 오진법의 수 2, 4, 3이라고 읽는다.
	S4	정의항을 압축하여 정의한다.	• 양의 유리수를 간단히 양수라고 한다.
	S5	정의항을 대체하여 정의한다.	• 일반적으로 자연수 a, b, c에 대하여 $a=b\times c$로 나타내어질 때, a의 약수 b와 c를 a의 인수라고도 한다.

1.2. 정의 수준

조영미(2001)의 연구에 따르면, 초, 중, 고의 순서로 내포적 정의 방식의 빈도는 증가하고 외연적 정의 방식의 빈도는 감소한다. 이는 학년이 올라갈수록 류에 유의하면서 관점을 변화시켜 엄밀해지는 방향으로 재정의하는 학교수학의 특징에 기인한다(pp. 122-123). 조영미는 이와 같이 엄밀하지는 않지만 학교수학에 필연적으로 존재하는 정의의 양태를 수용하여 van Hiele의 기하 학습 수준과 Freudenthal의 수학적 언어 수준을 바탕으로 학교수학에 제시된 기하 영역의 정의 수준을 탐색하였다. 여기서는 조영미가 설정한 정의 수준에 대한 분석 틀을 살펴본다.

Freudenthal(1978)에 따르면, 수학 학습 과정에서는 단계별 언어 수준이 발견되며 수학적 상징이나 기호에는 많은 수학적 의미가 압축되어 있으므로 교수학적 변환을 거쳐 학습자들의 심리적 수준에 맞는 언어로 용어를 정의하고 개념을 설명해야 한다. 학습 과정에서 발달된 수학적 언어 수준은 특별한 이유가 없다면 다시 낮출 필요가 없지만, 그 수준은 주어진 상황에 가장 적합한 것으로 계속 바뀔 수 있다(여미주 & 권혁진, 2012). 한편 교수·학습 과정에서 교사가 사용하는 수학적 언어도 다양하게 나타날 수 있고, 교사의 언어 선택에 따라 학습자들의 이해 수준 역시 상이할 수 있다. 따라서 교사는 학생들이 도달해야 할 목표와 자신의 전달 방식을 세밀하게 분석하여 적절한 수학적 언어를 선택할 수 있어야 한다(황혜정 외, 2019b, p.187). Freudenthal의 수학적 언어 수준은 다음과 같다(p.186).

- 구체적 언어 수준. 일상적 예나, '이것', '저것' 등과 같은 지시적 언어를 사용하는 수준
- 관계적 언어 수준. 여러 대상과의 상대적인 관계를 이용하여 설명하는 수준
- 관습적 언어 수준[규약적인 변수의 도입 수준]. 관계적 언어가 더 유연하게 기능하며, 수학적 대상을 나타내는 상징을 도입하는 수준
- 함수적 언어 수준. 적절한 함수를 도입하여 사용하는 수준

van Hiele의 기하 학습 수준 이론은 자신들이 연역적 증명을 통해 형식적 추론을 지도함에 있어 학생들이 기하 학습에 어려움을 느낀다는 점을 흥미롭게 관찰하고, 그 원인을 밝혀내려고 노력하는 가운데 제시되었다. van Hiele의 기하 학습 수준은 다음과 같다(우정호, 2011, p. 435; 황혜정 외, 2019a, pp. 302-304).

- 제0수준(시각적 수준). 대상을 형이라는 인식 수단에 의해 파악하는 단계
- 제1수준(기술적/분석적 수준). 정리 수단이었던 형이 연구의 대상이 되어 도형의 성질에 대한 비형식적인 분석을 통해 도형을 파악하는 단계
- 제2수준(관계적/추상적 수준). 국소적인 논리 관계를 파악하는 이론 수준으로 도형의 성질과 도형 사이의 관계가 연구의 대상이 되고 명제가 정리 수단이 되는 단계
- 제3수준(형식적 연역 수준). 명제가 연구의 대상이 되며 명제 사이의 논리적 관계가 정리 수단으로 등장하여 공리, 정의, 정리, 증명의 의미와 역할을 이해하며 전체 기하의 연역 체계를 파악하는 단계
- 제4수준(엄밀한 수학적 수준). 논리적 법칙의 본질을 통하는 수준으로 기하학 체계 그 자체가 연구의 대상이 되어 여러 가지 공리 체계를 비교하고, Hilbert 기하학의 형식적 엄밀성을 파악하는 단계

이들에 따르면 수학적 사고 활동은 경험의 세계를 조직하는 것으로, 사고 수준 간의 비약이 이루어지는 불연속성의 특징을 갖는다. 즉, 한 수준에서 경험을 정리하는 수단이 새롭게 경험의 대상으로 의식되어 그것을 조직하는 활동이 이루어지게 되면서 그다음 수준으로의 비약을 하게 되는 과정을 반복하게 된다는 것이다(우정호, 2011, p. 434). 그렇기에 학습자들이 수학적 사고를 재발명하도록 한다는 것은 사고 수준 간의 비약이 가능하도록 적절한 교수학적 조취를 취해가면서 점진적으로 안내해가는 것을 의미한다(황혜정 외, 2019a, p. 301). 이는 “수학은 인간의 정신적 활동이며, 수학화 과정은 현상과 본질의 교대 작용에 의해 수준의 상승이 이루어지면서 조직화・구조화되는 불연속 과정”이라고 한 Freudenthal의 주장과 일맥상통한다고 볼 수 있다(황혜정 & 김수진, 2019).

조영미(2001)는 수준 간의 위계를 탐색하는데 유용한 Freudenthal의

수학적 언어 수준을 바탕으로 학교수학에 제시된 기하 영역의 정의 수준과 그에 대한 예를 <표 Ⅱ-2>와 같이 제시하였다(pp. 125-159).

<표 Ⅱ-2> 학교수학의 정의 수준 분석 틀

수준	설명	예시
제0수준	(전수학적 수준) 용어를 정의하는 데 수학적 성격의 의미보다는 일상적 의미를 대응시키는 단계	• 상자모양을 직육면체라 한다. • 원을 그릴 때 침이 꽂혔던 점을 원의 중심이라 한다.
제1수준	(기술적 수준) 용어를 정의하는 데 성질이나 관계를 기술하는 성격의 문장을 사용하는 단계 ① 1a수준 : 시각적 특성이, 기술된 성질과 관계가 동시에 사용되어 정의되는 단계 ② 1b수준 : 제0수준의 특성은 나타나지 않고 순전히 기술된 성질과 관계만으로 정의하는 단계	[1a수준] • 두 반지름과 원의 한 부분으로 둘러싸인 부채 모양의 도형을 부채꼴이라 한다. [1b수준] • 면이 모두 정사각형인 직육면체를 정육면체라 한다.
제2수준	(대상 기호를 사용하는 수준) 용어를 정의하는 데 본격적으로 대상을 나타내는 문자 기호가 사용되는 단계 ① 2a수준 : 문자 기호가 부분적으로 사용되는 단계 ② 2b수준 : 문자 기호가 전체적으로 사용되는 단계	[2a수준] • 원 O 위의 두 점 A, B를 이은 선분을 현이라고 한다. [2b수준] • 접선 l이 원 O와 만나는 한 점 M을 접점이라고 한다.
제3수준	(관계 기호를 사용하는 수준) 정의항에 기호화한 관계적 표현이 사용되는 단계 ① 3a수준 : 제2수준에 해당하는 표현과 관계 기호 표현이 함께 사용되는 단계 ② 3b수준 : 제2수준에 해당하는 표현과 관계 기호 표현이 함께 사용되지 않는 단계	[3a수준] • 선분 AM과 선분 MB의 길이가 같을 때, 이것을 $\overline{AM}=\overline{MB}$와 같이 나타내며, 점 M을 선분 AB의 중점이라 한다. [3b수준] • 점 P가 선분 AB 위에 있고 AP : BP = $m:n$ 일 때, 점 P는 선분 AB를 $m:n$으로 내분한다고 한다. 이때 점 P를 선분 AB의 내분점이라고 한다. (단, $m>0$, $n>0$)
제4수준	(함수적 언어를 사용하는 수준) 용어를 정의하는 데 함수적 언어를 사용하는 단계	• 좌표평면 위의 점 P(x, y)를 점 P′$(x+a, y+b)$로 대응시키는 함수 $T:(x, y)\mapsto(x+a, y+b)$를 평행이동이라 한다.

해당 분석 틀에서 조영미는 구체적 언어 수준 보다 더 하위 수준인 제0수준을 설정하였는데, 이는 van Hiele의 기하 학습 수준의 시각적 수준을 참조한 것이다. 또한 van Hiele의 기하 학습 수준의 기술적/분석적

수준을 자신의 제1수준을 설정하는데 이용하였으며, 규약적인 변수를 도입하여 사용하는 관습적 언어 수준을 대상 기호를 사용하는 제2수준과 관계 기호를 사용하는 제3수준으로 구분하여 함수적 언어 수준에 해당하는 제4수준까지 총 다섯 가지의 수준을 설정하였다.

2. 공학적 도구를 활용한 교육

앞으로 학생들이 살아갈 제4차 산업혁명 시대는 초연결성, 초지능성, 예측 가능성을 특징으로, 사물 인터넷(Internet of Things, IoT), 빅 데이터(big data), 인공지능(Artificial Intelligence, AI) 등의 첨단 정보통신기술(Information and Communication Technologies, ICT)에 의해 다양한 영역 간의 융합이 이루어지는 시대이다(이상구 외, 2018). 이에 대해 세계경제포럼(World Economic Forum, WEF)에서는 복합 문제에 대한 인지 능력과 해결 능력을 가진 인재 양성에 대한 요구가 높아질 것으로 전망하였다(김진하, 2016). 또한 교육부는 2015 개정 교육과정 총론을 통해 창의·융합형 인재의 양성을 비전으로 제시하였으며, 2022 개정 교육과정 총론 주요사항[시안]을 통해 변동성, 불확실성, 복잡성을 특징으로 갖는 미래사회에 학습자들이 적절히 대응할 수 있도록 최적화된 맞춤형 교육으로서의 디지털 기반 교수·학습의 혁신을 강조하였다.

이러한 시대적 요구에 발맞춰 수학 교과에서 공학적 도구의 활용은 지속적으로 강조되어 왔다. 미국의 NCTM[7](2000)는 학교수학의 원리로 공학의 원리를 제시하면서 “학교수학을 위한 교수·학습에서 공학적 도구의 활용은 필수적이며, 이는 수학의 응용 및 활용의 범위를 크게 확장시켜 학습자들의 수학 학습 능력을 향상시킨다”고 명시하고 있다. 또한 교육부(2015)는 수학 교과를 통해 함양해야할 역량 중의 하나로 정보 처리 역량을 제시하였다. 정보 처리 역량은 다양한 자료와 정보를 수집, 정리, 분석, 활용하고, 적절한 도구를 선택하여 정보와 자료를 효과적으로 처리하는 능력을 말하며, 공학적 도구를 활용한 지도 하에서 학습자들로

7) 수학교사협의회(National Council of Teachers of Mathematics)

하여금 수학적 개념과 전략을 탐구하고 문제를 해결함으로써 함양된다(박래성 외, 2019). 마찬가지로 PISA[8] 2012에서 제시하고 있는 수학 소양의 정의에는 수학적 도구의 사용이 포함되어 있으며, 디지털 장비, 소프트웨어, 계산 도구 등 다양한 공학적 도구를 수학적 도구로 설명하고 있다(조지민 외, 2011, p. 14).

교수·학습에 있어서 공학적 도구의 활용이 강조됨에 따라 이에 관한 연구들이 상세히 이루어진 바 있다. 특히, 국내에서는 공학적 도구를 접목한 교육 자료의 개발과 함께 다양한 맥락에서의 그 역할에 주목해 왔다(e.g., 공민숙 & 강윤수, 2014; 김향숙, 2001; 류희찬 & 이지효, 1993; 이상구 외 2014; 임현정 & 고상숙, 2016; 장종욱 & 김화선, 2004; 주순종 & 김응환, 2009). 이들의 연구에 따르면, 공학적 도구는 학습자들의 흥미를 유발하여 수학 활동에 적극적으로 참여하게 함으로써 탐구 활동을 활발하게 한다. 또한 공학적 도구는 서로 다른 표상 간의 연결을 가능하게 함으로써 학습자들이 겪는 인신론적 어려움을 완화해주며(양성현 & 강옥기, 2011; 양성현, 2021; 이상희 외, 2012), 자신이 탐구한 내용을 반성하게 함으로써 창의성 신장에 기여한다(우정호, 2011, pp. 479-480).

2.1. 시각화

테크놀로지와 교육을 연구한 여러 연구자들(Fischbein, 1987; Laborde, 1993; Schwartz, 1989; Yershalmy & Chazan, 1990)은 공학적 도구를 활용한 교수·학습으로부터 얻을 수 있는 가장 중요한 이점 중의 하나로 시각화를 말한다. 수학적 개념의 시각화는 새로운 개념의 발견과 이해를 위해 수학적 이미지를 형성하고 활용하는 과정이다. 그렇기에 정적인 그림에 그래픽과 애니메이션을 이용하여 동적인 시각화를 보태는 것은 학습자들이 수학적 개념을 인지적으로 구조화하는 데 도움을 준다(이상구 외, 2014). 예컨대 프로그램에서 발생한 오류를 시각적으로 수정하는 과정은 학습자 자신의 수학적 사고와 그것의 절차적 형태를 다시 한 번 프

8) 국제 학업성취도 평가 연구(Programme for International Student Assessment)

로그램으로 변형하게 함으로써 반성의 기회를 제공하고, 이는 더 높은 사고 수준으로의 발달을 모색하는 반영적 추상화 활동에 기여한다(신동선 & 류희찬, 1998, pp. 5-6). Aless & Trollip(1985)에 따르면, 교수·학습에서 그래픽과 애니메이션에 의한 시각화의 활용이 학습자들에게 제공하는 근본적인 기능에는 다음과 같은 세 가지가 포함된다(이중권, 2015, p. 11에서 재인용).

- 정보 표현으로서의 기능을 한다. 즉, 언어나 숫자를 대신해서 학습자에게 정보를 쉽게 전달하는 수단이 된다.
- 유추에 의한 설명과 기억보조로서의 기능을 한다. 즉, 수학 학습에서 유추에 의한 설명으로 학습자들이 어떤 개념을 정확히 파악하고, 기억할 수 있도록 도와준다.
- 교과서 내용에 대한 요약 및 암시로서의 기능을 한다. 즉, 학생들에게 학습 내용을 요약해 보여주거나 암시함으로써, 학생들의 호기심을 자극하고 목표에 집중하도록 한다.

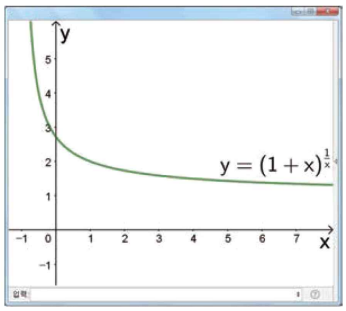
프로그래밍과 알고리즘 교육에서도 공학적 도구를 이용한 시각화는 교수·학습의 효과를 높이는 데 있어 중추적인 요소로, 이에 관한 연구들이 상세히 이루어진 바 있다. 오연재 외(2012)와 오경숙 외(2011)의 연구에서는 알고리즘 시각화 시스템의 적용 집단과 비적용 집단의 비교를 통해 학습자들의 학업성취도 및 흥미도, 집중도, 이해도 등을 향상시키는 데 있어 시각화를 이용한 알고리즘 교육의 효용성을 확인하였다. 오경숙 외(2009)는 수학적 사고 능력을 필요로 하는 알고리즘을 학습하는 데 있어 이론만으로는 알고리즘을 이해하는 데 한계가 있음을 지적하며 시각화 프로그램을 활용한 알고리즘 교육 시스템을 개발하였고, 그래픽 및 애니메이션을 통해 학습자들에게 효과적인 이해 체계를 제공해주어야 함을 강조하였다. 정인기(2004)는 비주얼 프로그래밍으로 대변되는 현 패러다임에 맞게 자료 구조 및 알고리즘 과목 역시 변화해야 함을 강조하며, 기존의 정렬 프로그래밍 교육 자료가 부분적인 시각화만을 제공했던 것과 달리 각 단계를 온전히 시각화할 수 있는 교육용 도구를 개발하였다.

2.2. 수학적 정당화

수학에서의 증명의 성격과 역할이 무엇인지에 관하여 다양한 해석과 관점들이 존재하지만(CadwalladerOlsker, 2011), 적어도 증명 자체가 형식적인 논증을 거쳐 결론에 이르는 일련의 절차라는 점에 있어서는 보편적인 합의가 이루어져 있다. 한편 수학적 정당화는 이와 같이 엄밀한 증명뿐만 아니라, 어떤 추측을 참으로 인정하게 하는 다양한 방법을 포괄하는 과정으로 볼 수 있다(이동근 외 2017; 홍영석 & 손홍찬, 2021). 실제로 다양한 형태의 수학적 정당화를 제시하고 있는 연구들(Balacheff, 1987; Harel & Sowder, 1998; Knuth & Eliott, 1998; Samandeni, 1984)에서도 엄밀한 증명 외에 명제의 타당성을 입증할 수 있는 직관적인 접근을 인정하고 있는 것을 확인할 수 있다.

공학적 도구는 새로운 수학적 사실을 발견하고 이를 정당화할 수 있는 기회를 제공한다(손홍찬, 2011). 이는 시각화 자료가 Fischbein(1987)이 제시한 직관의 인지적 특성인 자명성, 내재적 확실성, 고집성, 강제성, 이론적 성격, 외삽성, 전체성을 내포하고 있는 것(문광호 & 우정호, 1999)에 기인한다. 이로부터 공학적 도구는 교육과정 내에서 엄밀한 정당화 과정을 제시할 수 없는 경우, 직관적인 접근을 통해 해당 요소를 도입하는 데 이용할 수 있다. 예컨대 학문수학 수준에서 엄밀하게 정당화되는 극한 $\lim_{x\to 0}(1+x)^{1/x}$의 존재성은 학교수학 수준에서 [그림 Ⅱ-2](김원경 외, 2019, p. 52)와 같이 공학적 도구를 통해 정당화된다(류건 외, 2022).

x	(1+x)^(1/x)
0.1	2.5937424601
0.01	2.7048138294
0.001	2.7169239322
0.0001	2.7181459268
0.00001	2.7182682372
0.000001	2.7182804692
-0.000001	2.7182831877
-0.00001	2.7182954200
-0.0001	2.7184177550
-0.001	2.7196422164
-0.01	2.7319990264
-0.1	2.8679719908



[그림 Ⅱ-2] 학교수학에서의 극한 $\lim_{x\to 0}(1+x)^{1/x}$의 존재성의 정당화

제 2 절 양자 계산 이론

본 절에서는 <양자 알고리즘> 교육 프로그램 개발에 밑바탕이 되는 양자 계산 이론에 대해서 살펴본다. 양자 계산 이론의 모든 측면을 다루는 것은 본 연구의 범위를 벗어나므로, 여기서는 Grover 알고리즘의 작동 원리를 이해하는데 필요한 내용 요소로 그 범위를 제한하였다. 보다 자세히는 Grover 알고리즘의 수학적 구조를 이해하는 데 필요한 양자 비트와 텐서 곱 그리고 양자 측정에 대한 내용을 개관하고, 그다음 Grover 알고리즘을 구현하는 과정에서 필요한 양자 게이트와 양자 회로에 대한 내용을 개관한다.

1. 양자 비트와 텐서 곱

고전적 정보[9] 처리 기본 단위는 어떤 질문에 대한 답을 '예' 또는 '아니오'로 표현하는 비트(bit)이다. 이때 비트는 두 가지 대답을 각각 0, 1과 동일시하여 이진수(binary digit)로 표현한다. 유사한 방식으로 양자 계산(quantum computing)의 정보 처리 기본 단위를 정의할 수 있는데, 이를 양자 비트(quantum bit)라고 하고, 줄여서 큐비트(qubit)라 한다. 큐비트는 비트와 마찬가지로 두 가지 상태 중 하나가 될 수 있고, 이때 두 가지 상태 각각을 기호 $|0\rangle$, $|1\rangle$로 표현한다. 큐비트는 비트가 단일 상태에만 있을 수 있는 것에 비해 보다 일반적인 중첩 상태(superposition state)에도 있을 수 있다. 여기서 중첩 상태는 큐비트의 두 상태 $|0\rangle$과 $|1\rangle$의 확률적 결합을 말한다. 즉 상태 $|\psi\rangle$가 중첩 상태에 있다고 하면, 이는 두 복소수 α, β에 대하여

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

9) 본 연구에서 '고전적 정보'라는 용어는 고전 컴퓨터에서 이루어지는 전통적인 정보 처리 및 연산 방식을 의미한다.

로 나타낼 수 있다. 그러나 측정(measurement) 후의 큐비트에서는 중첩 상태를 확인할 수 없다. 한편 $|\psi\rangle$는 $|0\rangle$, $|1\rangle$ 중 하나로만 측정되는데, 식 2.1에서 α, β를 각각 $|0\rangle$, $|1\rangle$의 확률 진폭(probability amplitude)이라 한다. 즉, $|\alpha|^2 = \alpha \cdot \alpha^*$는 $|\psi\rangle$가 0으로 측정될 확률이고, $|\beta|^2 = \beta \cdot \beta^*$는 $|\psi\rangle$가 1로 측정될 확률이다. 이때, 확률의 합은 1이어야 하므로 두 계수 α, β는 다음과 같은 관계를 만족한다.

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.2}$$

보다 일반적으로 아래의 식 2.3을 만족하는 상태 $|\psi_1\rangle$, $|\psi_2\rangle$, …, $|\psi_n\rangle$와 복소수 c_1, c_2, …, c_n에 대하여 $c_1|\psi_1\rangle + c_2|\psi_2\rangle + \cdots + c_n|\psi_n\rangle$을 중첩 상태라 한다. 여기서 해당 선형결합 역시 상태가 되는 것을 '중첩의 원리(superposition principle)'라 한다.

$$\| c_1\psi_1 + c_2\psi_2 + \cdots + c_n\psi_n \| = 1 \tag{2.3}$$

고전 정보 처리 과정에서 흔히 접할 수 있는 000, 001, 010, 100, 110, 101, 011, 111을 데카르트 곱(Cartesian product)으로 주어지는 3 - 비트 공간 $\{0, 1\} \times \{0, 1\} \times \{0, 1\}$의 원소로 생각할 수 있는 것처럼 양자 정보 처리 과정에서도 다입자 상태를 n - 큐비트 공간의 원소로 이해할 수 있다. 양자계(quantum system)에서 합성계(composite system)는 여러 힐베르트 공간(Hilbert space)을 부분계(sub-system)를 포함하는 힐베르트 공간으로 이해할 수 있다. 이 과정을 기술하기 위한 수학적 도구가 텐서 곱(tensor product)이다. 예를 들어 텐서 곱을 기호를 $\otimes$로 표기할 때, 차원이 각각 n_1, n_2인 두 힐베르트 공간을 $\mathcal{H}_1$, $\mathcal{H}_2$에 대하여 $\mathcal{H}_1$, $\mathcal{H}_2$를 부분계로 포함하는 힐베르트 공간 $\mathcal{H}$는

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \tag{2.4}$$

로 나타낼 수 있고, 이때 $\mathcal{H}$의 차원은 $\dim(\mathcal{H})=n_1 \cdot n_2$가 된다. 또한 힐베르트 공간 $\mathcal{H}$에 속한 상태 벡터는 두 힐베르트 공간 $\mathcal{H}_1$, $\mathcal{H}_2$에 속한 벡터의 텐서 곱의 선형결합으로 나타낼 수 있다. 여기서 텐서 곱은 다음과 같은 자연스러운 성질들을 만족한다.

$$(\mu_1+\mu_2)\otimes\psi=\mu_1\otimes\psi+\mu_2\otimes\psi \ (\mu_1,\ \mu_2\in\mathcal{H}_1,\ \psi\in\mathcal{H}_2) \tag{2.5}$$

$$\mu\otimes(\psi_1+\psi_2)=\mu\otimes\psi_1+\mu\otimes\psi_2 \ (\mu\in\mathcal{H}_1,\ \psi_1,\ \psi_2\in\mathcal{H}_2) \tag{2.6}$$

$$(\lambda\mu)\otimes\psi=\mu\otimes(\lambda\psi) \ (\mu\in\mathcal{H}_1,\ \psi\in\mathcal{H}_2,\ \lambda\in\mathbb{C}) \tag{2.7}$$

지금까지의 논의는 양자계 내의 고전계(classical system)를 살펴보면 보다 명시적으로 이해할 수 있다. 양자계 내의 고전계는 다양한 형태로 존재할 수 있으나, 가장 자연스러운 방식은 고전 정보 처리 과정에서 1-비트의 상태 0과 1을 각각 열벡터

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix},\ |1\rangle=\begin{bmatrix}0\\1\end{bmatrix} \tag{2.8}$$

과 동일시하여 2차원 복소벡터공간 $\mathbb{C}^2$를 1-큐비트 공간으로 이해하는 것이다.[10] 이때, $\mathbb{C}^2$ 내의 두 벡터 $|\mu\rangle=\begin{bmatrix}a\\b\end{bmatrix}$, $|\psi\rangle=\begin{bmatrix}c\\d\end{bmatrix}$의 텐서 곱은

$$|\mu\rangle\otimes|\psi\rangle=\begin{bmatrix}a\\b\end{bmatrix}\otimes\begin{bmatrix}c\\d\end{bmatrix}=\begin{bmatrix}a\begin{bmatrix}c\\d\end{bmatrix}\\b\begin{bmatrix}c\\d\end{bmatrix}\end{bmatrix}=\begin{bmatrix}ac\\ad\\bc\\bd\end{bmatrix} \tag{2.9}$$

---

10) 양자 계산 이론에서 열벡터를 $|\cdot\rangle$로, 이에 대응하는 에르미트 켤레 전치벡터(Hermitian conjugate transpose vector)를 $\langle\cdot|$로 표기하는 방법을 '브라-켓 표기법(bra-ket notation)'이라고 한다. 이때 열벡터 $|\cdot\rangle$를 켓 벡터(ket vector), 행벡터 $\langle\cdot|$를 브라 벡터(bra vector)라고 읽는다.

와 같이 정의할 수 있다. 또한 두 행벡터 $\langle 0| = [1 \quad 0]$, $\langle 1| = [0 \quad 1]$에 대하여 1-비트의 상태 0과 1을 각각

$$\begin{aligned} |0\rangle\langle 0| &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} [1 \quad 0] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \\ |1\rangle\langle 1| &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} [0 \quad 1] = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \tag{2.10}$$

과 동일시하여 복소행렬공간 $M_2(\mathbb{C})$를 1-큐비트 공간으로 이해할 수 있다. 이때 $M_2(\mathbb{C})$ 내의 두 행렬 $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$의 텐서 곱은

$$\begin{aligned} A \otimes B &= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ &= \begin{bmatrix} a_{11} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{bmatrix} \\ &= \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix} \end{aligned} \tag{2.11}$$

와 같이 정의할 수 있다. 한편 식 2.9와 식 2.11과 같은 연산 규칙은 텐서 곱의 자연스러운 성질들(식 2.5 ~ 식 1.7)을 모두 만족한다.

2. 양자 측정

연산 시스템은 특정 순간에 필요한 정보를 얻을 수 있어야 하기 때문에 양자 측정(quantum measurment)은 양자 계산 이론에 밑바탕이 되는

요소이다. 물리량을 측정 할 때 양자역학을 이용하면 측정 가능한 값과 그 측정 확률을 알아낼 수 있다. 이때 측정 이후의 계가 어떤 상태가 되는지도 중요한 주제이다. 고전계에서는 측정이 어떠한 영향도 끼치지 않지만, 양자계에서는 불가역적인 영향을 끼친다(McMahon, 2008, p. 121). 앞에서 언급한 특정 상태에 대한 확률 진폭의 제곱을 해당 값의 측정 확률을 취하는 것은 사영 측정(projective measurement)[11] 모델에서 흔히 말하는 'Born의 규칙(Born's rule)'에 해당한다. 여기서는 보다 일반적인 양자 측정 모델에 대해서 살펴본다.

양자 측정은 $M_{m,n}(\mathbb{C})$에 속하면서 식 2.12과 같은 조건을 만족하는 측정 연산자들의 모임 $\{M_1, M_2, \cdots, M_k\}$으로 주어진다.

$$\sum_{i=1}^{k} M_k^{\dagger} M_k = \mathrm{Id}_n \tag{2.12}$$

이때 $1, 2, \cdots, k$는 상태 $|\psi\rangle$가 주어졌을 때 측정의 결과로서 얻을 수 있는 측정값들이며, 여기서 $b \in \{1, 2, \cdots, k\}$를 얻을 확률은 식 2.13과 같이 주어진다.

$$\mathbb{P}(b) = \| M_b|\psi\rangle \|^2 = \langle\psi| M_b^{\dagger} M_b|\psi\rangle \tag{2.13}$$

앞서 언급했듯이 여기서 기억해야하는 중요한 사실은 양자 측정을 통해 측정값 b를 확률적으로 얻어냄과 동시에 계의 상태 $|\psi\rangle$는 식 2.14와 같이 변한다는 것이다. 이때 $|\psi'\rangle$는 상태 $|\psi\rangle$가 $|b\rangle$로 사영된 것과 같다.

$$|\psi'\rangle = \frac{M_b|\psi\rangle}{\sqrt{\langle\psi| M_b^{\dagger} M_b|\psi\rangle}} \tag{2.14}$$

11) 사영 연산자들의 모임을 양자 측정으로 하는 사영 측정 모델은 물리학자이자 수학자인 John von Neumann이 최초로 설명한 모델로서 'von Neumann 측정'이라고도 한다(p. 123).

한편 양자계를 밀도 연산자(density operator)[12] ρ로 기술했을 경우, $b \in \{1, 2, \cdots, k\}$를 얻을 확률은 식 2.15와 같이 나타낼 수 있다.

$$\mathbb{P}(b) = tr\left(\rho M_b^{*} M_b\right) \tag{2.15}$$

또한 측정값 b를 확률적으로 얻어냄과 동시에 변화된 계의 상태는 식 2.16으로 나타낼 수 있다.

$$\rho' = \frac{M_b \rho M_b^{\dagger}}{tr\left(\rho M_b^{\dagger} M_b\right)} \tag{2.16}$$

3. 양자 게이트와 양자 회로

고전 컴퓨터의 최하단에는 비트 단위의 정보를 가공하거나 처리하기 위한 논리 게이트(logic gate)와 논리 게이트들을 연결한 디지털 회로(digital circuit)가 존재한다. 양자 컴퓨터에서도 이에 상응하는 개념으로서 양자 게이트(quantum gate)와 양자 회로(quantum circuit)가 존재한다. 양자 게이트는 유니터리 변환(unitary transformation)으로 유니터리 행렬(unitary matrix)로 기술될 수 있다.[13] 이때 유니터리 행렬은 다음과 같은 성질을 만족하는 행렬을 의미한다.

$$UU^{\dagger} = U^{\dagger}U = \mathrm{Id} \tag{2.17}$$

---

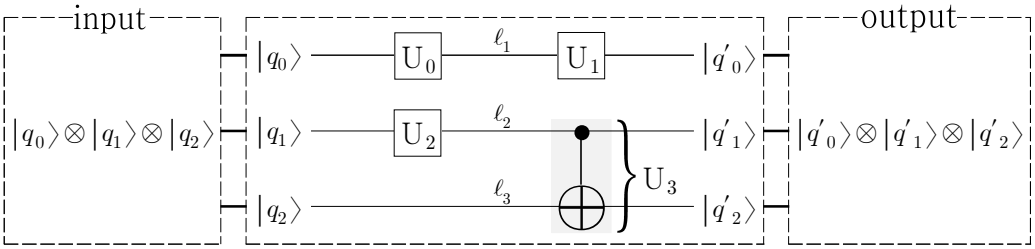
12) 밀도 연산자 ρ는 $\rho^{*} = \rho$, $\rho \geq 0$, $Tr(\rho) = 1$을 만족하는 연산자로, 순수 상태(pure state)와 혼합 상태(mixed state) 모두를 포함하는 양자계를 기술하기 위한 도구이다(Scherer, 2019, pp. 43-44).

13) 양자계의 양자 게이트가 노름(norm)을 보존하는 유니터리 변환이어야 하는 이유는 계의 파동 함수(wave function)의 노름이 1이어야 하기 때문이다(Lala, 2019, p. 103). 여기서 파동 함수는 힐베르트 공간 내의 벡터 $|\psi\rangle$로, 양자계의 상태에 대한 모든 정보를 담고 있는 복소 함수를 뜻한다.

한편 조금 더 복잡한 계산을 수행하기 위해 양자 게이트들을 연결한 것을 양자 회로라 한다. 즉, 양자 회로는 양자 게이트들의 합성으로 볼 수 있다(김영훈 & 허재성, p. 95).

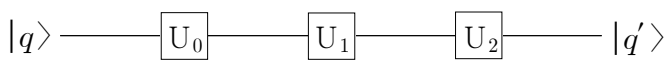
3.1. 양자 회로도와 연산

양자 회로도(quantum circuit diagram)는 [그림 Ⅱ-3]과 같이 양자 게이트와 양자선(quantum wire)을 나타내는 다이어그램(양자 게이트 - $\boxed{U_0}$, $\boxed{U_1}$, $\boxed{U_2}$, $\boxed{U_3}$; 양자선 - ℓ_1, ℓ_2, ℓ_3)을 이용하여 가시화할 수 있다. 일반적으로 양자 회로도는 입력 큐비트를 좌측에 위치시키고, 이에 작용하는 양자 게이트들을 전선에 연속적으로 배열함으로써 작성한다.



[그림 Ⅱ-3] 가시화된 양자 회로의 예

양자 회로도에서의 연산은 수행 방식에 따라 직렬 연산과 병렬 연산으로 구분할 수 있다. 먼저 직렬 연산은 순차적으로 수행되는 연산으로, 첫 번째로 작용하는 양자 게이트를 입력 큐비트의 우측에 두고 그다음으로 작용하는 양자 게이트들을 차례대로 위치시킴으로써 표현한다. 예를 들어, [그림 Ⅱ-4]는 세 개의 양자 게이트 U_0, U_1, U_2가 입력 큐비트 $|q\rangle$에 차례대로 작용하여 큐비트 $|q'\rangle$을 출력하고 있는 회로도이다.

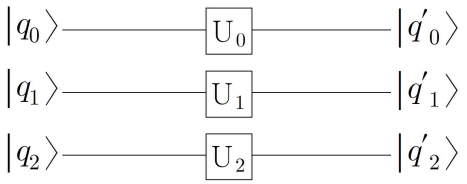


[그림 Ⅱ-4] 양자 회로도에서 직렬 연산의 예

이러한 직렬 연산의 행렬 표현은 각각의 양자 게이트에 대응되는 연산자 행렬들을 입력 큐비트에 역순으로 곱함으로써 나타낼 수 있다. 즉, [그림 Ⅱ-4]의 행렬 표현은 다음과 같다.

$$|q'\rangle = U_2 U_1 U_0 |q\rangle \tag{2.18}$$

반면에 병렬 연산은 동시에 수행되는 연산으로, 여러 개의 양자선을 통해 텐서 곱을 표현함으로써 나타낸다. 예를 들어, [그림Ⅱ-5]는 세 개의 양자 게이트 U_0, U_1, U_2가 입력 큐비트 $|q_0\rangle \otimes |q_1\rangle \otimes |q_2\rangle$에 동시에 작용하여 큐비트 $|q'_0\rangle \otimes |q'_1\rangle \otimes |q'_2\rangle$를 출력하고 있는 회로도이다.



[그림 Ⅱ-5] 양자 회로도에서 병렬 연산의 예

이러한 병렬 연산의 행렬 표현은 각각의 양자 게이트에 대응되는 연산자 행렬들의 텐서 곱을 입력 큐비트에 곱함으로써 나타낼 수 있다. 즉, [그림 Ⅱ-5]의 행렬 표현은 다음과 같다.[14]

$$|q'_0\rangle \otimes |q'_1\rangle \otimes |q'_2\rangle = (U_0 \otimes U_1 \otimes U_2)(|q_0\rangle \otimes |q_1\rangle \otimes |q_2\rangle) \tag{2.19}$$

3.2. 여러 가지 양자 게이트

양자 게이트는 n겹(n-fold) 힐베르트 공간 $\mathcal{H}^{\otimes n}$에서 $\mathcal{H}^{\otimes n}$로의 유니터

14) 텐서 곱 상태 $|x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{n-1}\rangle$는 간단하게 $|x_0 x_1 \cdots x_{n-1}\rangle$로 표현할 수 있다. 즉, 식 2.19는 $|q'_0 q'_1 q'_2\rangle = (U_0 \otimes U_1 \otimes U_2)|q_0 q_1 q_2\rangle$로 나타낼 수 있다.

리 변환으로 정의되며, $\mathcal{H}^{\otimes n}$의 계산 기저(computational basis)에 의해 유니터리 행렬로 기술된다.[15] 예를 들어, $\mathcal{H}(\cong\mathbb{C}^2)$에서 $\mathcal{H}$로의 유니터리 변환으로 정의되는 단일 큐비트 게이트(single-qubit gate)는 $\mathcal{H}$의 계산 기저 $\{|0\rangle, |1\rangle\}$ 하에서 2×2 유니터리 행렬로 기술된다. 유사하게 $\mathcal{H}^{\otimes2}$ $(\cong\mathbb{C}^4)$에서 $\mathcal{H}^{\otimes2}$로의 유니터리 변환으로 정의되는 2-큐비트 게이트는 $\mathcal{H}^{\otimes2}$의 계산 기저 $\{|0\rangle^2, |1\rangle^2, |2\rangle^2, |3\rangle^2\}=\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$[16] 하에서 4×4 유니터리 행렬로 기술된다.

한편 양자 컴퓨터에서 수행되는 모든 계산은 측정 이전의 상태로 되돌릴 수 있고, 이는 입력에 상관없이 임의의 시작 지점으로 되돌아갈 수 있는 것을 의미한다. 실제로 유니터리 행렬로 기술되는 모든 양자 게이트는 식 2.17로부터 되돌릴 수 있는 계산(reversible computation)이다. 이러한 양자 계산의 가역성은 고전 AND 게이트와 같이 비가역성을 지닌 논리 연산과 대비된다(Moran, 2019, pp. 84-85).

여기서는 본 연구의 교육 프로그램에서 설계된 프로젝트 과제를 해결하는데 필요한 단일 큐비트 게이트와 다중 큐비트 게이트(multi-qubit gate)에 대해서 알아본다. 해당 양자 게이트들은 자기 자신의 직렬 연산에 의해 되돌려지는 양자 게이트이다.

가. 단일 큐비트 게이트(X 게이트, Z 게이트, 아다마르 게이트)

X 게이트는 1-큐비트에 작용하는 단일 큐비트 게이트로, $\mathbb{C}^2$의 계산

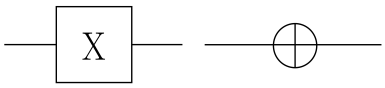
---

15) 여기서 $\mathcal{H}^{\otimes n}$는 $\mathcal{H}$를 n번 텐서 곱한 $\underbrace{\mathcal{H}\otimes\mathcal{H}\otimes\cdots\otimes\mathcal{H}}_{n\text{개}}$을 표기한 기호이다. 이때 $x\in\{0, 1, \cdots, 2^n-1\}$에 대하여 $|x\rangle=|x_{n-1}\rangle\otimes|x_{n-2}\rangle\otimes\cdots\otimes|x_0\rangle$로 표현되는 $\mathcal{H}^{\otimes n}$의 정규직교기저(orthonormal basis)를 $\mathcal{H}^{\otimes n}$의 계산 기저라 한다(Scherer, 2019, p. 87).

16) 기호 $|x_k\rangle^n$ $(k=0, 1, \cdots, n-1)$는 n겹 힐베르트 공간 $\mathcal{H}^{\otimes n}$의 모든 계산 기저를 $|00\cdots0\rangle$, $|00\cdots1\rangle$, $\cdots$, $|11\cdots1\rangle$와 같이 차례대로 나열하였을 때, 0번째 계산 기저 $|00\cdots0\rangle$로부터 k번째 계산 기저를 의미한다. 즉, $|0\rangle^2=|00\rangle$, $|1\rangle^2=|01\rangle$, $|2\rangle^2=|10\rangle$, $|3\rangle^2=|11\rangle^2$이 성립한다.

기저 하에서 <표 Ⅱ-3>의 (3)과 같은 2×2 유니터리 행렬로 기술되며, 양자 회로도에서는 (4)와 같은 심볼로 표현된다.

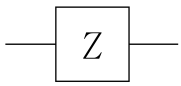
<표 Ⅱ-3> X 게이트의 연산자, 연산 결과, 행렬 표현, 심볼

(1) 연산자	(2) 연산 결과	(3) 행렬 표현	(4) 심볼
X	• $\|0\rangle \mapsto \|1\rangle$ • $\|1\rangle \mapsto \|0\rangle$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	

X 게이트는 고전 컴퓨터의 NOT 게이트에 대응되는 양자 게이트로 양자 NOT 게이트라고도 불린다. 실제로 X 게이트는 <표 Ⅱ-3>의 (2)와 같이 $|0\rangle$을 $|1\rangle$, $|1\rangle$을 $|0\rangle$으로 전환시켜 고전 NOT 게이트와 동일한 연산을 수행한다. 즉 입력 큐비트들을 서로 전환시키는데, 이와 같은 연산 결과로부터 X 게이트를 비트 전환 게이트(bit flip gate)라고도 부른다.

Z 게이트는 1-큐비트에 작용하는 단일 큐비트 게이트로, $\mathbb{C}^2$의 계산 기저 하에서 <표 Ⅱ-4>의 (3)과 같은 2×2 유니터리 행렬로 기술되며, 양자 회로도에서는 (4)와 같은 심볼로 표현된다.[17]

<표 Ⅱ-4> Z 게이트의 연산자, 연산 결과, 행렬 표현, 심볼

(1) 연산자	(2) 연산 결과	(3) 행렬 표현	(4) 심볼
Z	• $\|0\rangle \mapsto \|0\rangle$ • $\|1\rangle \mapsto -\|1\rangle$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	

17) Pauli는 전자 스핀을 다루기 위해 세 가지의 2×2 복소 행렬을 고안한 바 있다(Lala, 2019, p. 104). 본 절에서 설명하는 X 게이트와 Z 게이트는 각각 기호 σ_x, σ_z로 표현되는 파울리 X 행렬(Pauli X matrix)과 파울리 Z 행렬(Pauli Z matrix)에 대응된다. 때문에 양자 계산에 관한 문헌에서는 X 게이트와 Z 게이트의 연산자로 σ_x와 σ_z를 사용하기도 하는데, 파울리 행렬의 기호보다는 X와 Z를 사용하는 것이 일반적이다(Scherer, 2019, p. 171). 본 논문에서도 X 게이트와 Z 게이트의 연산자로 'X'와 'Z'를 사용한다.

Z 게이트는 $x \in \{0, 1\}$에 대하여 입력 큐비트 $|x\rangle$를 $(-1)^x|x\rangle$로 사상한다. 즉, <표 Ⅱ-4>의 (2)와 같이 입력 큐비트가 $|0\rangle$인 경우에는 $|0\rangle$을 그대로 출력하고, $|1\rangle$인 경우에는 $-|1\rangle$을 출력한다. 이러한 연산 동작 때문에 Z 게이트를 위상 전환 게이트(phase flip gate)라고도 부른다.

아다마르 게이트(Hadamard gate)는 1-큐비트에 작용하는 단일 큐비트 게이트로 $\mathbb{C}^2$의 계산 기저 하에서 <표 Ⅱ-5>의 (3)과 같은 2×2 유니터리 행렬로 기술되며, 양자 회로도에서는 (4)와 같은 심볼로 표현된다.

<표 Ⅱ-5> 아다마르 게이트의 연산자, 연산 결과, 행렬 표현, 심볼

(1) 연산자	(2) 연산 결과	(3) 행렬 표현	(4) 심볼
H	• $\|0\rangle \mapsto \|+\rangle := \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$ • $\|1\rangle \mapsto \|-\rangle := \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$	

아다마르 게이트는 <표 Ⅱ-5>의 (2)와 같이 각각의 입력 큐비트를 확률 진폭의 절댓값이 모두 동일한 균등 중첩 상태로 변환해준다. 이와 같이 아다마르 게이트는 가장 중요한 양자적 특성인 중첩 상태를 출력한다는 점으로부터 양자 알고리즘에서 가장 핵심적인 작동을 수행하는 양자 게이트로 여겨지며, 가장 널리 사용된다(김영훈 & 허재성, 2020; Lala, 2019; McMahon, 2008; Nielsen & Chuang, 2010; Scherer, 2019).

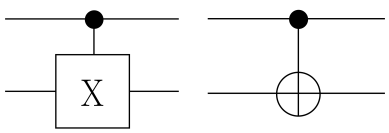
나. 2-큐비트 게이트(제어형 X 게이트, 제어형 Z 게이트)

제어형 양자 게이트(controlled quantum gate)는 양자 회로에서 조건문을 구현하기 위해 사용되는 양자 게이트로, 제어 큐비트와 대상 큐비트의 텐서 곱 상태를 입력 큐비트로 갖는다. 예를 들어, 2-큐비트에 작용하는 제어형 양자 게이트는 제어 큐비트 $|a\rangle$와 대상 큐비트 $|b\rangle$에 대하여 $|ab\rangle = |a\rangle \otimes |b\rangle$를 입력 큐비트로 받으며, 제어 큐비트 $|a\rangle$가 $|1\rangle$

인 경우에만 대상 큐비트 $|b\rangle$에 주어진 유니터리 연산을 적용한다.

제어형 X 게이트(controlled X gate)는 2-큐비트에 작용하는 다중 큐비트 게이트로 $\mathbb{C}^4$의 계산 기저 하에서 <표 Ⅱ-6>의 (3)과 같은 4×4 유니터리 행렬로 기술되며, 양자 회로도에서는 (4)와 같은 심볼로 표현된다.

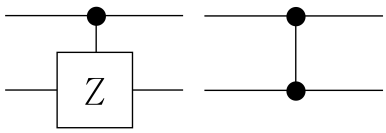
<표 Ⅱ-6> 제어형 X 게이트의 연산자, 연산 결과, 행렬, 심볼

(1) 연산자	(2) 연산 결과	(3) 행렬 표현	(4) 심볼
CX	• $\|00\rangle \mapsto \|00\rangle$ • $\|01\rangle \mapsto \|01\rangle$ • $\|10\rangle \mapsto \|11\rangle$ • $\|11\rangle \mapsto \|10\rangle$	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$	

제어형 X 게이트는 (2)와 같이 제어 큐비트가 $|1\rangle$인 경우에만 대상 큐비트에 X 게이트를 적용하여 출력한다.

제어형 Z 게이트(controlled Z gate)는 2-큐비트에 작용하는 다중 큐비트 게이트 $\mathbb{C}^4$의 계산 기저 하에서 <표 Ⅱ-7>의 (2)와 같은 4×4 유니터리 행렬로 기술되며, 양자 회로도에서는 (3)과 같은 심볼로 표현된다.

<표 Ⅱ-7> 제어형 Z 게이트의 연산자, 연산 결과, 행렬, 심볼

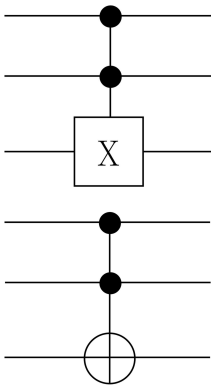
(1) 연산자	(2) 연산 결과	(3) 행렬 표현	(4) 심볼
CZ	• $\|00\rangle \mapsto \|00\rangle$ • $\|01\rangle \mapsto \|01\rangle$ • $\|10\rangle \mapsto \|10\rangle$ • $\|11\rangle \mapsto -\|11\rangle$	$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$	

제어형 Z 게이트는 제어 큐비트가 $|1\rangle$인 경우에만 대상 큐비트에 Z 게이트를 적용하여 출력한다. 즉, 입력 큐비트가 $|11\rangle$인 경우에만 위상을 전환하여 출력한다.

다. 3-큐비트 게이트(토폴리 게이트, 제어-제어형 Z 게이트)

토폴리 게이트(Toffoli gate)는 3-큐비트에 작용하는 다중 큐비트 게이트로 $\mathbb{C}^8$의 계산 기저 하에서 <표 Ⅱ-8>의 (3)과 같은 8×8 유니터리 행렬로 기술되며, 양자 회로도에서는 (4)와 같은 심볼로 표현된다.

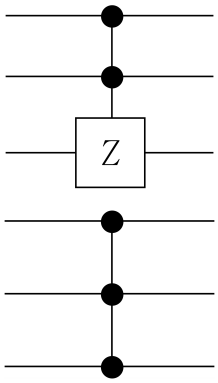
<표 Ⅱ-8> 토폴리 게이트의 연산자, 연산 결과, 행렬, 심볼

(1) 연산자	(2) 연산 결과	(3) 행렬 표현	(4) 심볼
CCX	• $\|000\rangle \mapsto \|000\rangle$ • $\|001\rangle \mapsto \|001\rangle$ • $\|010\rangle \mapsto \|010\rangle$ • $\|100\rangle \mapsto \|100\rangle$ • $\|011\rangle \mapsto \|011\rangle$ • $\|101\rangle \mapsto \|101\rangle$ • $\|110\rangle \mapsto \|111\rangle$ • $\|111\rangle \mapsto \|110\rangle$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$	

토폴리 게이트는 제어-제어형 X 게이트로(controlled-controlled X gate)라고도 불리며 고전 컴퓨터의 CCNOT 게이트[고전 토폴리 게이트]와 대응된다. 즉, 제어 큐비트 $|ab\rangle$와 대상 큐비트 $|c\rangle$에 대하여 $|abc\rangle$를 입력 큐비트로 받으며, <표 Ⅱ-8>의 (2)와 같이 제어 큐비트 $|ab\rangle$가 $|11\rangle$인 경우에만 대상 큐비트 $|c\rangle$에 X 게이트를 적용하여 출력한다.

제어-제어형 Z 게이트(controlled-controlled Z gate)는 3-큐비트에 작용하는 다중 큐비트 게이트로 $\mathbb{C}^8$의 계산 기저 하에서 <표 Ⅱ-9>의 (3)과 같은 8×8 유니터리 행렬로 기술되며, 양자 회로도에서는 (4)와 같은 심볼로 표현된다. 제어-제어형 Z 게이트는 제어 큐비트 $|ab\rangle$와 대상 큐비트 $|c\rangle$에 대하여 $|abc\rangle$를 입력 큐비트로 받으며, <표 Ⅱ-9>의 (2)와 같이 제어 큐비트 $|ab\rangle$가 $|11\rangle$인 경우에만 대상 큐비트 $|c\rangle$에 Z 게이트를 적용하여 출력한다. 즉, 입력 큐비트가 $|111\rangle$인 경우에만 위상을 전환하여 출력한다.

<표 Ⅱ-9> 제어-제어형 Z 게이트의 연산자, 연산 결과, 행렬, 심볼

(1) 연산자	(2) 연산 결과	(3) 행렬 표현	(4) 심볼
CCZ	• $\|000\rangle \mapsto \|000\rangle$ • $\|001\rangle \mapsto \|001\rangle$ • $\|010\rangle \mapsto \|010\rangle$ • $\|100\rangle \mapsto \|100\rangle$ • $\|011\rangle \mapsto \|011\rangle$ • $\|101\rangle \mapsto \|101\rangle$ • $\|110\rangle \mapsto \|110\rangle$ • $\|111\rangle \mapsto -\|111\rangle$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$	

제 3 절 Grover 알고리즘

1. 시간 복잡도

계산 복잡도(computational complexity)는 알고리즘 계산에 필요한 시간과 공간의 효율성으로, 소요되는 연산의 비용을 측정하는 시간 복잡도(time complexity)와 소요되는 메모리의 비용을 측정하는 공간 복잡도(space complexity)로 구분된다(김영훈 & 허재성, 2020, p. 130). 계산 복잡도의 모든 측면을 다루는 것은 본 연구의 범위를 벗어나므로, 여기서는 본 연구에서 개발한 교육 프로그램을 이해하는 데 필요한 시간 복잡도를 중심으로 그 범위를 제한하였다.

문제에 대한 해답이 '예' 또는 '아니오'로 반환되는 문제를 결정 문제(decision problem)라고 한다. 시간 복잡도는 n-비트 크기의 입력값을 갖는 어떤 결정 문제가 주어졌을 때, 알고리즘을 통해 그 문제를 해결하는 데 필요한 연산의 수이다. 이는 유동적이고 포괄적인 개념으로서 상황에 따라 데이터의 입/출력, 산술 연산, 제어 연산 등 다양한 기준을 적용할 수 있다. 양자 계산에서는 일반적으로 주어진 함수에 대한 함숫값의 연산 수를 복잡도의 기준으로 설정한다(p. 131).

주어진 문제마다 시간 복잡도의 계산 모델이 다르면 계산에 필요한 자원도 달라지기 때문에 정량화된 방법이 필요하다. 이를 위해 개발된 도구로 점근적 표기법(asymptotic notation)이 있다. 점근적 표기법은 함수의 본질적 거동(essential behavior)인 시간 단계(time step)를 요약하기 위해 사용되며, 상계를 설정하는 O 표기법(big-O notation)과 하계를 설정하는 Ω 표기법(big-omega notation), 그리고 O 표기법과 Ω 표기법을 절충한 Θ 표기법(big-theta notation)으로 구분된다. 이를 수학적으로 기술하면 다음과 같다. 첫 번째로 n_0보다 큰 모든 자연수 n에 대하여

$$f(n) \leq cg(n) \tag{2.20}$$

을 만족하는 상수 c와 n_0가 존재할 때 '$f(n)$은 함수 $O(g(n))$의 클래스에 속한다'고 하고, 두 번째로

$$f(n) \geq cg(n) \tag{2.21}$$

을 만족하는 상수 c와 n_0가 존재할 때 '$f(n)$은 함수 $\Omega(g(n))$의 클래스에 속한다'고 한다. 마지막으로 $f(n)$이 두 함수 $O(g(n))$, $\Omega(g(n))$의 클래스에 동시에 속할 때, '$f(n)$은 함수 $\Theta(g(n))$의 클래스에 속한다'고 한다 (Nielsen & Chuang, 2010, pp. 136-137).

한편 고전 컴퓨터로 풀기 어려운 문제를 컴퓨터 공학 용어로 '다루기 힘든 문제(intractable problem)'라고 하는데, 이 용어는 '다항시간 알고리즘(polynomial-time algorithm)'에 대한 수학적 개념을 이용하면 보다 상세히 기술할 수 있다. 다항시간 알고리즘은 자연수 n에 대하여 다항식 $p(n)$이 존재하여 함수 $O(p(n))$의 클래스에 속하는 알고리즘을 말하고, 다루기 힘든 문제는 다항시간 알고리즘으로 풀 수 없는 문제를 말한다 (Neapolitan, 2014, pp. 396-397). 즉 입력값의 크기가 커짐에 따라 다항식에 비례하여 증가하는 복잡도를 효율적인 비용으로 볼 수 있는데, 실세계에서 현실적인 비용은 $O(n)$, $O(n^2)$, $O(n^3)$까지 정도이다. 그러나 고

전 컴퓨터의 성능은 약 2년마다 2배만큼 향상되어 왔고, 이에 따라 주어진 문제의 다항시간 알고리즘을 찾기만 하면 그 문제는 대게 몇 년이 지나 $O(n^3)$ 또는 $O(n^4)$ 클래스에 속하는 알고리즘을 갖게 되며, 연구가 진행되면서 꾸준히 줄어든다. 즉, 최종적으로는 다항시간 정도의 비용을 현실적인 비용으로 볼 수 있다. 반면에 입력값의 크기가 커짐에 따라 기하급수적으로 증가하는 복잡도는 비현실적인 비용이다. 예를 들어 함수 $O(2^n)$의 클래스에 속하는 알고리즘의 경우, 고전 컴퓨터의 성능이 2배만큼 향상되어도 같은 시간에 풀 수 있는 입력값의 크기는 1밖에 증가하지 않는다. 다시 말해, 지수시간 알고리즘으로 풀 수 있는 문제는 효율적인지 아닌지를 떠나서 근본적으로 고전 컴퓨터를 통해 현실적인 시간 내에 해결할 수 없는 문제인 것이다(이광근, 2015, pp. 103-106).

컴퓨터 공학에서는 고전 컴퓨터로 다루기 힘든 문제들의 경계를 명확히 하기 위해 다항시간 알고리즘으로 풀 수 있는 결정 문제들의 집합을 '$\mathcal{P}$ 클래스'로 정의하고, $\mathcal{P}$ 클래스와 그 경계 근처에 있는 문제들을 모두 포함하는 '$\mathcal{NP}$ 클래스'를 정의한다(pp. 106-107). $\mathcal{NP}$ 클래스는 다항시간 알고리즘으로 풀 수 있는지는 모르나, 적어도 해답이 주어진 경우에는 다항시간 비용으로 검산할 수 있는 결정 문제들의 집합이다. 해당 정의는 '비결정적 알고리즘(non-deterministic algorithm)'의 개념을 이용하여 보다 상세하게 기술할 수 있다. 비결정적 알고리즘은 다음과 같은 두 단계로 구성된다.

1. (비결정적) 추측 단계: 주어진 문제의 사례를 가지고 임의의 문자열 S를 만든다. 이때 만든 문자열은 추측한 해답으로 볼 수 있다.
2. (결정적) 검증 단계: 입력은 문제 사례와 추측한 문자열 S이다. 이 단계는 일반적인 결정론적 실행 방식으로 다음과 같은 세 가지 경우 중 한 가지로 진행된다. (1) '예'의 출력을 내주면서 멈춘다. (2) '아니오'의 출력을 내주면서 멈춘다. (3) 멈추지 않는다(infinity loop).

검증 단계에서 (1)은 문제의 사례에 대한 답이 '예'라고 검증된 경우이며, (2)와 (3)은 문제의 사례에 대한 답이 '예'라고 검증되지 않은 경우이다.

실제로 비결정적 알고리즘을 통해 어떤 문제의 해답을 구할 수 있는 것은 아니지만, 다음 조건을 만족하는 경우 비결정적 알고리즘을 통해 결정 문제를 '푼다(solve)'고 정의한다.

1. 주어진 문제의 해답이 '예'가 되는 사례에 대하여 검증 단계의 결과가 '참'이 되는 문자열 S가 존재한다.
2. 주어진 문제의 해답이 '아니오'가 되는 사례에 대하여 검증 단계의 결과가 '참'이 되는 문자열 S가 존재하지 않는다.

검증 단계에서 다항시간 비용이 소요되는 비결정적 알고리즘을 다항시간 비결정적 알고리즘이라고 하며, $\mathcal{NP}$ 클래스는 다항시간 비결정적 알고리즘으로 풀 수 있는 모든 결정 문제들의 집합으로 정의된다(Neapolitan, 2014, pp. 408-409).

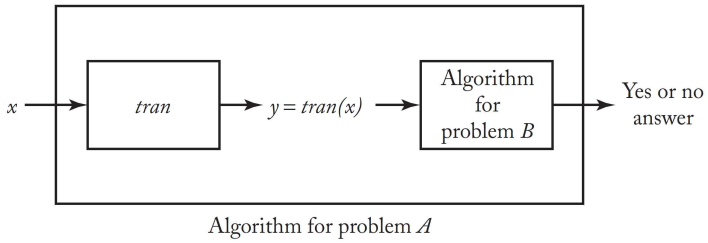
각 클래스의 정의로부터 $\mathcal{NP}$ 클래스는 $\mathcal{P}$ 클래스를 자명하게 포함한다. 그러나 $\mathcal{NP}$ 클래스에 속하면서 $\mathcal{P}$ 클래스에 속하지 않는 문제가 존재하는지는 아직 증명되지 않았다.[18] 더욱이 $\mathcal{NP}$ 클래스에 속하는 문제들의 경우 어려운 정도가 모두 동일한 것은 아닌데, 이는

$$\mathcal{NP} \text{ 클래스} \neq \mathcal{P} \text{ 클래스} \tag{2.22}$$

의 전제 하에서 '다항시간 축소변환가능도(polynomial-time reducibility)'의 개념을 이용하여 확인할 수 있다. 이를 논하기 위해서는 먼저 변환 알고리즘(transformation algorithm)에 대한 이해가 필요하다. 변환 알고리즘은 주어진 결정 문제 A를 어떤 결정 문제 B로 변환하여 풀기 위한 사상(mapping) 함수로, 보다 어려운 문제 B를 푸는 알고리즘을 이용하여 문제 A를 풀기 위해 문제 A의 각 사례 x를 문제 B의 사례 y로 대응시키는 다대일(many-one) 함수를 말한다. 해당 함수는 기호 $tran$로

18) $\mathcal{P} = \mathcal{NP}$의 여부를 묻는 $\mathcal{P}$-$\mathcal{NP}$ 문제는 아직 증명되지 않은 문제로, 2000년 5월 클레이 수학 연구소(Clay mathematics institute, CMI)에서 제시한 7가지 문제 중 하나이다(이광근, 2015, p. 114).

표현하며, 이에 대한 전반적인 과정은 [그림 Ⅱ-6](p. 413)과 같다.



[그림 Ⅱ-6] 문제 A를 풀기 위한 변환 알고리즘

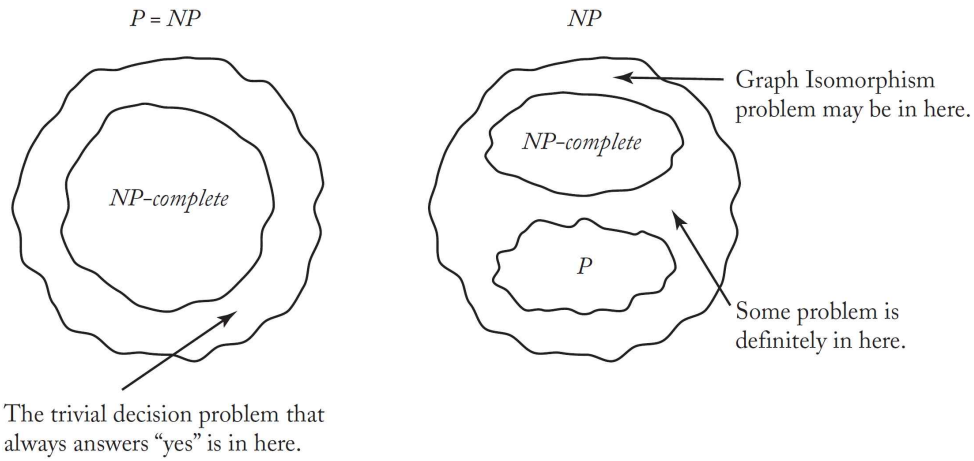
지금까지의 맥락으로부터 알 수 있듯이 변환 알고리즘 역시 다항시간의 비용으로 해결되어야 하는데, 이에 관한 정의가 바로 '다항시간 축소변환 가능'이다. 결정 문제 A를 결정 문제 B로 변환하는 다항시간 변환 알고리즘이 존재하면, 문제 A는 문제 B로 '다항시간 축소변환 가능하다'라고 정의하고, 기호 $A \propto B$로 표현한다(pp. 411-414).

$\mathcal{NP}$ 클래스에는 종결자 역할을 하는 대표적인 문제가 있다. 즉, $\mathcal{NP}$ 클래스 내의 모든 문제를 다항시간 내에서 축소변환 가능케 하는 가장 어려운 문제가 존재한다. 만약 이 문제를 푸는 다항시간 알고리즘을 찾을 수 있다면 $\mathcal{NP}$ 클래스 내의 모든 문제를 현실적인 비용 내에서 다항시간 알고리즘으로 풀 수 있게 된다(이광근, 2015, pp. 118-119). 즉,

$$\mathcal{NP} \text{ 클래스} = \mathcal{P} \text{ 클래스} \tag{2.23}$$

가 증명되는 것이다. 이러한 종결자 문제를 $\mathcal{NP}$-완전($\mathcal{NP}$-complete) 문제라고 하고, 수학적으로는 임의의 $\mathcal{NP}$ 클래스 문제 A에 대하여 $A \propto B$를 만족하는 $\mathcal{NP}$ 클래스 문제 B로 정의한다(Neapolitan, 2014, p. 415).[19] 이상의 내용을 종합하면 각 클래스의 포함 관계는 [그림 Ⅱ-7](p. 420)과 같이 두 가지로 나타낼 수 있다.

19) 임의의 $\mathcal{NP}$ 클래스 문제 A에 대하여 $A \propto B$를 만족하는 결정 문제 B는 보다 일반적인 $\mathcal{NP}$-난해($\mathcal{NP}$-hard) 클래스에 속하는 문제이다. 즉, $\mathcal{NP}$-완전 문제는 $\mathcal{NP}$ 클래스에 속하는 $\mathcal{NP}$-난해 문제로 볼 수 있다.



[그림 Ⅱ-7] $\mathcal{P}$, $\mathcal{NP}$, $\mathcal{NP}$-완전 클래스의 포함 관계

2. Grover 알고리즘

Grover 알고리즘은 여러 개의 객체로 구성된 비정형 데이터베이스가 주어졌을 때, 양자적 특성을 이용하여 특정 객체에 접근할 수 있는 양자 검색 알고리즘이다(Grover, 1996). Grover 알고리즘을 이용하면 고전 컴퓨터에서 $O(N/2)$의 복잡도를 갖는 비구조적 탐색 문제를 $O(\sqrt{N})$의 복잡도로 해결할 수 있다. Grover 알고리즘은 본 연구에서 개발한 교육 프로그램의 중심 소재로서, 여기서는 Grover 알고리즘의 의사 코드(pseudo code)와 수학적 구조를 자세히 개관한다.

2.1. Grover 알고리즘의 의사 코드

비구조적 탐색 문제는 '$N=2^n$ (n은 자연수)의 크기를 갖는 비정형 데이터베이스가 주어졌을 때, 함수 $f:\{0,\ 1,\ \cdots,\ N-1\} \rightarrow \{0,\ 1\}$에 대하여 조건 $f(x)=1$을 만족하는 x를 구하는 것'으로 모델링할 수 있다.[20]

20) 만약 객체의 총 개수가 N 보다 작은 L로 주어진 경우에는 $N-L$개의 객체를 추가하여 일반성을 잃지 않고 데이터베이스 $\{0,\ 1,\ \cdots,\ N-1\}$에서 특정 객체를 탐색한다고 가정할 수 있다(Scherer, 2019, p. 324).

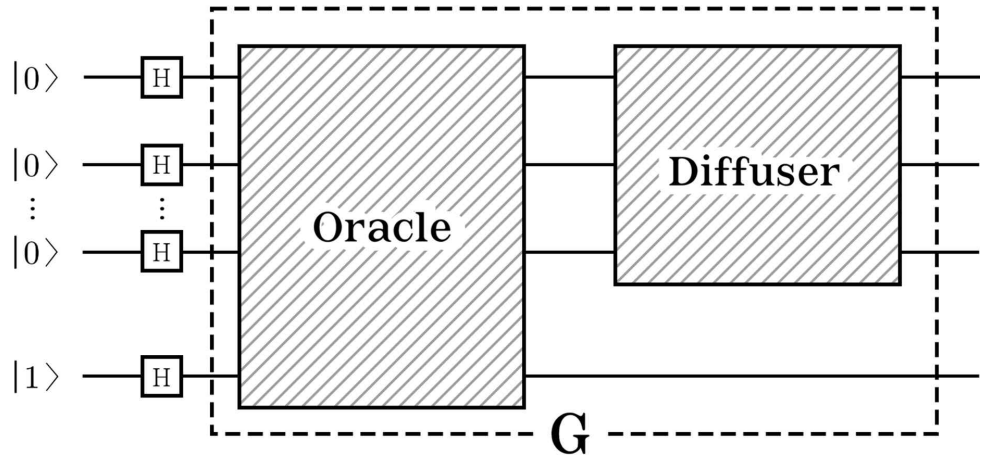
여기서 문제의 목표 객체를 특정하기 위한 함수 f를 오라클 함수(oracle function)라고 하고, 임의의 오라클 함수 f에 대한 Grover 알고리즘의 각 단계는 <표 Ⅱ-10>과 같은 의사코드로 기술한다.

<표 Ⅱ-10> Grover 알고리즘의 의사코드

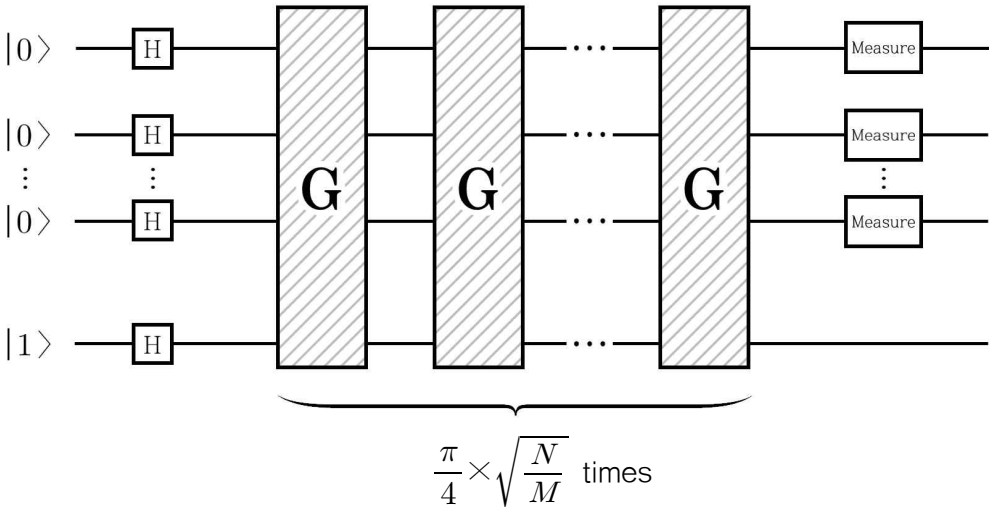
단계	단계별 의사 코드
①	n-큐비트 크기의 입/출력 레지스터와 1-큐비트 크기의 보조 레지스터를 준비하고[21], 입/출력 레지스터를 $\|0\rangle^{\otimes n}$, 보조 레지스터를 $\|-\rangle$로 초기화한다.
②	$\|0\rangle^{\otimes n}$을 확률 진폭이 모두 균등한 n-큐비트 크기의 중첩 상태로 변환한다.
③	균등 중첩 상태에서 조건 $f(x)=1$을 만족하는 $x\in\{0, 1, \cdots, N-1\}$의 상태 $\|x\rangle$의 위상을 반전시킨다.
④	주어진 각각의 상태들에 대하여 확률 진폭의 평균에 대한 반전을 수행한다.
⑤	③과 ④를 $\frac{\pi}{4}\times\sqrt{\frac{N}{M}}$ 번 반복한다.

<표 Ⅱ-10>에서 ①을 초기 단계, ②를 중첩 단계, ③을 오라클 단계, ④를 확산(diffusion) 단계, ⑤를 반복 단계라 한다. 이때 오라클 단계에 대응되는 연산자와 확산 단계에 대응되는 연사자의 합성을 Grover 연산자라 하고, [그림 Ⅱ-8]과 같이 기호 G로 표현한다. 또한 오라클 단계부터 반복 단계까지의 과정을 모두 포함한 일련의 변환을 Grover 반복(Grover iteration)이라 한다. Grover 알고리즘의 전반적인 양자 회로도는 [그림 Ⅱ-9]와 같다. 본 연구에서 개발한 교육 프로그램의 프로젝트 과제를 해결하기 위해 필요한 Grover 알고리즘의 양자 회로는 제2절 3.2에서 살펴본 양자 게이트들을 조합하여 구현할 수 있다. 이에 대한 자세한 과정은 제Ⅳ장 제2절에서 설명한다.

21) 컴퓨터의 프로세서(processor)가 계산을 수행하는 연산 처리의 기본 단위를 레지스터(register)라 한다. 본 논문에서는 고전 프로세서와 양자 프로세서를 구분하고, 각각의 레지스터를 고전 레지스터와 양자 레지스터로 부른다.



[그림 Ⅱ-8] Grover 알고리즘의 중첩・오라클・확산 단계



[그림 Ⅱ-9] Grover 알고리즘의 양자 회로도

2.2. Grover 알고리즘의 수학적 구조

Grover 알고리즘의 수학적 구조는 적합한 힐베르트 공간에서 비정형 데이터베이스의 객체를 정규화된 벡터인 양자 상태로 기술하는 것으로부터 시작한다. 목표 객체의 벡터들은 힐베르트 공간의 부분공간을 생성하고, 이때 Grover 반복은 주어진 초기 상태를 해당 부분공간에서 최대의 성분을 가지는 상태로 변환하는 회전 연산자(rotate operator)를 구성한

다. 이로부터 회전된 상태를 측정했을 때, 목표 객체의 벡터들이 생성한 부분공간의 상태를 발견하게 될 확률이 높아진다(Scherer, 2019, p. 324).

다음으로 이상의 내용을 엄밀하게 기술하기 위한 용어의 정의와 기호를 살펴보고, 구체적인 수학적 구조를 단계별로 정립한다. 먼저 데이터베이스의 크기를 $N=2^n$ (n은 자연수)이라고 하고, M개의 목표 객체로 이루어진 집합 S와 목표가 아닌 객체들의 집합 $S^{\perp} := \{0, 1, \cdots, N-1\} \setminus S$을 정의한다. 그다음 입/출력 레지스터를 $\mathcal{H}^{I,O} := (\mathbb{C}^2)^{\otimes n}$으로 정의하고, 보조 레지스터를 $\mathcal{H}^{W} := \mathbb{C}^2$으로 정의한 후 다음과 같은 입/출력 레지스터의 부분공간을 정의한다.

- $\mathcal{H}_S := \mathrm{span}\{|x\rangle \mid x \in S\} \subseteq \mathcal{H}^{I,O}$
- $\mathcal{H}_{S^{\perp}} := \mathrm{span}\{|x\rangle \mid x \in S^{\perp}\} \subseteq \mathcal{H}^{I,O}$

그리고 아래와 같이 $\mathcal{H}^{I,O}$에 작용하는 연산자와 상태 벡터를 정의한다. 여기서 P_S, $\mathrm{P}_{S^{\perp}}$는 각각 $\mathcal{H}_S$와 $\mathcal{H}_{S^{\perp}}$로의 사영 연산자, R_S, $\mathrm{R}_{S^{\perp}}$는 각각 $\mathcal{H}_S$와 $\mathcal{H}_{S^{\perp}}$에 대한 반사 연산자, $|\psi_S\rangle$, $|\psi_{S^{\perp}}\rangle$는 각각 $x \in S$와 $x \in S^{\perp}$에 대응하는 계산 기저 $|x\rangle$들의 균등 선형 조합이다.

- $\mathrm{P}_S := \sum_{x \in S} |x\rangle\langle x|$
- $\mathrm{P}_{S^{\perp}} := \sum_{x \in S^{\perp}} |x\rangle\langle x|$
- $\mathrm{R}_S := 2\mathrm{P}_S - \mathrm{Id}^{\otimes n}$
- $\mathrm{R}_{S^{\perp}} := \mathrm{Id}^{\otimes n} - 2\mathrm{P}_S$
- $|\psi_S\rangle := \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle$
- $|\psi_{S^{\perp}}\rangle := \frac{1}{\sqrt{N-M}} \sum_{x \in S^{\perp}} |x\rangle$

그러면 사영 연산자의 정의로부터 식 2.24가 성립하므로 $\mathcal{H}^{I,O}$에 속하는 임의의 상태 $|\psi\rangle$를 식 2.25와 같이 계산 기저로 표현할 수 있다. 이때 상태 $|\psi\rangle$에 있는 $\mathcal{H}^{I,O}$를 관측하면, $|\psi\rangle$를 $|x\rangle$로 사영하고 측정값 x를

생성한다.[22]

$$\mathrm{P}_{S^{\perp}} = \mathrm{Id}^{\otimes n} - \mathrm{P}_{S},\ \mathrm{P}_{S} + \mathrm{P}_{S^{\perp}} = \mathrm{Id}^{\otimes n} \tag{2.24}$$

$$|\psi\rangle = \left(\mathrm{P}_{S^{\perp}} + \mathrm{P}_{S}\right)|\psi\rangle = \sum_{x \in S^{\perp}} c_x |x\rangle + \sum_{x \in S} c_x |x\rangle \ (c_x \in \mathbb{C}) \tag{2.25}$$

$\mathcal{H}^{I,O}$의 초기 상태를 $|\psi_0\rangle$라고 할 때, 앞서 언급한 Grover 알고리즘의 수학적 구조는 목표 객체 $x \in S$의 측정 확률을 최대화하는 상태 $|\psi\rangle$를 생성하는 것이며, 이를 위해 $|\psi_0\rangle$에 $\mathcal{H}_S$의 성분을 증가시키는 회전 연산자를 반복 적용하는 것으로 기술할 수 있다. 즉, Grover 알고리즘은의 목표는 식 2.26과 같이 주어지는 측정값 $x \in S$를 얻어낼 확률을 최대화하기 위한 $|\psi\rangle$를 생성하는 회전 연산자를 구성하는 것이다.

$$\| \mathrm{P}_{S}|\psi\rangle \|^2 = \left\| \sum_{x \in S} c_x |x\rangle \right\|^2 = \sum_{x \in S} |c_x|^2 \tag{2.26}$$

가. 초기 단계와 중첩 단계

Grover 알고리즘의 초기·중첩 단계는 입/출력 레지스터 $\mathcal{H}^{I,O}$의 초기 상태 $|\psi_0\rangle$를 가능한 모든 상태들의 균등 선형 조합으로 정의하는 것으로부터 시작한다. 그러면 입/출력 레지스터와 보조 레지스터의 합성계 $\mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$의 초기 상태 $|\hat{\psi}_0\rangle$를 다음과 같이 정의할 수 있다.

---

22) 양자 레지스터 $\mathcal{H}^{\otimes n}$에서 상태의 측정은 $j \in \{0, 1, \cdots, n-1\}$에 대하여 인자 j에 대응되는 $\mathcal{H}_j$에서 호환 가능한(compatible) 관측 가능량[자기수반연산자] $\Sigma_z^j = \mathrm{Id}^{\otimes n-1-j} \otimes \sigma_z \otimes \mathrm{Id}^{\otimes j}$의 측정으로 정의한다. 이러한 측정을 레지스터를 '읽는다(read-out)'고 한다. $\Sigma_z^{n-1}, \cdots, \Sigma_z^0$를 측정해 $\mathcal{H}^{\otimes n}$을 읽으면 n개의 측정값 $(s_{n-1}, \cdots, s_0) \in \{\pm 1\}^n$을 얻고, 관측 가능량 Σ_z^j를 측정하면 $\mathcal{H}_j$의 상태를 측정값 s_j에 대응하는 고유 상태 $|0\rangle$, $|1\rangle$로 사영한다(Scherer, 2019, pp. 212-213).

• $|\psi_0\rangle := \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \in \mathcal{H}^{I,O}$ • $|\hat{\psi}_0\rangle := |\psi_0\rangle \otimes |-\rangle \in \mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$

나. 오라클 단계와 확산 단계

Grover 알고리즘의 오라클 단계는 0, 1, ⋯, $N-1$ 중에서 S에 속하는 객체들의 위상을 반전시킴으로써 M개의 목표 객체를 판별하는 단계이다. 이를 위해 적절한 힐베르트 공간에 아래와 같이 정의되는 오라클 함수 f가 존재하고, 이 함수 f를 이용하면 $S \cup S^{\perp}$ 내의 임의의 객체 x에 대한 목표 객체 여부를 N과 무관하면서 유한한 양의 연산으로 판별할 수 있다고 가정한다.

• $f : \{0,\ 1,\ \cdots,\ N-1\} \rightarrow \{0,\ 1\},\ x \mapsto f(x) := \begin{cases} 1\,, & x \in S \\ 0\,, & x \in S^{\perp} \end{cases}$

오라클 함수 f에 대응되는 연산자는 n-비트 크기의 입력값에 1-비트 크기의 출력값을 산출하는데, 이는 가역 변환도 아니고 유니터리 변환이 아니다. 즉 해당 연산자는 양자계에서 유효한 연산자가 아닌데, 이는 여분의 보조 레지스터 $\mathcal{H}^{W}$를 함수의 연산 결과에 이용함으로써 해결할 수 있다(Lala, 2019, p. 208). 보다 자세히는 오라클 연산자 U_f를 합성계 $\mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$의 계산 기저에 식 2.27[23]과 같이 작용하도록 정의하고, 선형 확장(linear continuation)을 이용하여 $\mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$ 내의 임의의 상태벡터에 대해 정의한다.

$$\mathrm{U}_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \boxplus f(x)\rangle \tag{2.27}$$

23) 우변에서 기호 ⊞는 인수별 이진법 덧셈(factor-wise binary addition)으로, $\boxplus : \mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n} \rightarrow \mathcal{H}^{\otimes n},\ |a\rangle \otimes |b\rangle \mapsto |a \boxplus b\rangle := \otimes_{i=n-1}^{0} |a_i \oplus b_i\rangle$으로 정의된다(Scherer, 2019, pp. 206-207).

해당 정의로부터 $\mathcal{H}^{I,O}\otimes\mathcal{H}^{W}$의 계산 기저 $|x\rangle\otimes|0\rangle$, $|x\rangle\otimes|1\rangle$에 대한 U_f의 연산 결과는 각각 식 2.28과 식 2.29와 같다. 이 두 식을 조합하면 U_f가 $\mathcal{H}^{I,O}$ 내의 임의의 계산 기저 $|x\rangle$와 $\mathcal{H}^{W}$의 초기 상태 $|-\rangle$에 대하여 식 2.30과 같이 작용함을 알 수 있다.

$$U_f(|x\rangle\otimes|0\rangle)=|x\rangle\otimes|0\oplus f(x)\rangle=\begin{cases}|x\rangle\otimes|1\rangle, & x\in S\\ |x\rangle\otimes|0\rangle, & x\in S^{\perp}\end{cases} \tag{2.28}$$

$$U_f(|x\rangle\otimes|1\rangle)=|x\rangle\otimes|1\oplus f(x)\rangle=\begin{cases}|x\rangle\otimes|0\rangle, & x\in S\\ |x\rangle\otimes|1\rangle, & x\in S^{\perp}\end{cases} \tag{2.29}$$

$$U_f(|x\rangle\otimes|-\rangle)=|x\rangle\otimes(|-\rangle\boxplus|f(x)\rangle)=(-1)^{f(x)}|x\rangle\otimes|-\rangle \tag{2.30}$$

최종적으로 식 2.25, 식 2.30, 식 2.24을 순차적으로 적용하면 사영 연산자와 반사 연산자의 정의로부터 $\mathcal{H}^{I,O}$에 내의 임의의 상태 벡터 $|\psi\rangle$에 대하여 U_f가 상태 $|\psi\rangle\otimes|-\rangle$에 식 2.31과 같이 작용함을 알 수 있다. 즉, 오라클 연산자 U_f는 $|\psi\rangle$를 $|\psi_{S^{\perp}}\rangle$을 기준으로 반사시킨다.

$$\begin{aligned}U_f(|\psi\rangle\otimes|-\rangle)&=\Big(\sum_{x\in S^{\perp}}c_x|x\rangle-\sum_{x\in S}c_x|x\rangle\Big)\otimes|-\rangle\\&=\big(P_S-P_{S^{\perp}}\big)|\psi\rangle\otimes|-\rangle\\&=\big(\mathrm{Id}^{\otimes n}-2P_S\big)|\psi\rangle\otimes|-\rangle\\&=R_{S^{\perp}}|\psi\rangle\otimes|-\rangle\end{aligned} \tag{2.31}$$

한편 Grover 알고리즘의 확산 단계는 오라클 단계로부터 주어진 상태 $U_f|\psi_0\rangle$를 확률 진폭의 평균을 기준으로 반전시키는 단계이다. 이때 확산 연산자는 $\mathcal{H}^{I,O}$의 초기 상태 $|\psi_0\rangle$에 의해 생성되는 일차원 부분공간에 대한 반사 연산자 $R_{\psi_0}=2|\psi_0\rangle\langle\psi_0|-\mathrm{Id}^{\otimes n}$으로 정의된다. 최종적으로 확산 연산자 R_{ψ_0}는 오라클 연산자 U_f와 함께 $|\psi_0\rangle$의 $\mathcal{H}_S$의 성분을 증가

시켜 $\mathcal{H}^{I,O}$에 대한 관측에서 목표 객체들의 측정 확률을 높인다.

다. 반복 단계

Grover 알고리즘의 반복 단계는 오라클 단계와 확산 단계의 순차적인 작용에 대응되는 Grover 연산자를 아래와 같이 정의하는 것으로부터 시작한다.

$$\cdot\ \mathrm{G} := (\mathrm{R}_{\psi_0} \otimes \mathrm{Id})\mathrm{U}_f$$

그다음 $\mathcal{H}^{I,O}$의 초기 상태 $|\psi_0\rangle$를 식 2.32와 같이 $|\psi_{S^\perp}\rangle$, $|\psi_S\rangle$를 이용하여 나타내고, $\mathcal{H}^{I,O} \otimes \mathcal{H}^W$의 초기 상태 $|\hat{\psi}_0\rangle = |\psi_0\rangle \otimes |-\rangle$에 Grover 연산자를 한 번 적용한 $\mathrm{G}|\hat{\psi}_0\rangle$를 $|\hat{\psi}_1\rangle = |\psi_1\rangle \otimes |-\rangle$로 나타낸다고 하자.

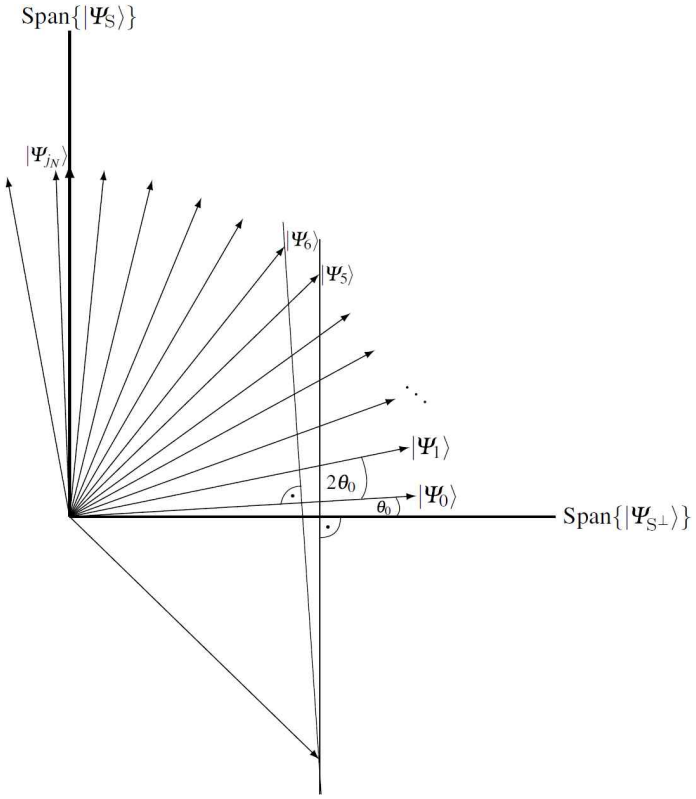
$$|\psi_0\rangle = \sqrt{\frac{N-M}{N}}\,|\psi_{S^\perp}\rangle + \sqrt{\frac{M}{N}}\,|\psi_S\rangle \tag{2.32}$$

그러면 식 2.31과 확산 연산자의 정의로부터 $|\psi_1\rangle$은 $|\psi_0\rangle$를 $\mathcal{H}_{S^\perp}$을 기준으로 반전시킨 후 $|\psi_0\rangle$를 기준으로 반전시킨 것과 같다. 이는 식 2.33을 만족하는 각 θ_0에 대하여 $|\psi_0\rangle$를 $|\psi_S\rangle$의 방향으로 $2\theta_0$만큼 회전시킨 것과 같은데, 여기서 각 θ_0는 기하학적으로 $\mathrm{span}\{|\psi_{S^\perp}\rangle\}$과 $|\psi_0\rangle$ 사이의 각을 의미한다.

$$\theta_0 = \arccos\left(\sqrt{\frac{N-M}{N}}\right) = \arcsin\left(\sqrt{\frac{M}{N}}\right) \in \left[0,\ \frac{\pi}{2}\right] \tag{2.33}$$

이상을 반복적으로 적용한 k번의 Grover 반복은 $\mathcal{H}^{I,O} \otimes \mathcal{H}^W$의 초기 상태 $|\hat{\psi}_0\rangle = |\psi_0\rangle \otimes |-\rangle$를 $|\hat{\psi}_k\rangle := |\psi_k\rangle \otimes |-\rangle$로 변환한다. 이때 $\mathcal{H}^{I,O}$의 $|\psi_k\rangle$는

k가 증가함에 따라 2차원 부분공간 span$\{|\psi_{S^\perp}\rangle, |\psi_S\rangle\}$에서 $|\psi_S\rangle$를 향해 회전한다. 이는 [그림 Ⅱ-10](Scherer, 2019, p. 332)에서 확인할 수 있다.



[그림 Ⅱ-10] Grover 반복의 기하학적 의미

즉, $|\psi_k\rangle$는 각 $\theta_k := (2k+1)\theta_0$에 대하여 식 2.34와 같이 주어진다.

$$|\psi_k\rangle = \cos\theta_k |\psi_{S^\perp}\rangle + \sin\theta_k |\psi_S\rangle \tag{2.34}$$

한편 k번의 Grover 반복 후 $\mathcal{H}^{I,O} \otimes \mathcal{H}^W$의 부분계 $\mathcal{H}^{I,O}$를 축약 밀도 연산자(reduced density operator)로 나타내면 식 2.35와 같이 순수 상태로 기술된다. 즉 k번의 Grover 반복 후 목표 객체의 측정 확률을 관측할 때, 상태 $|\hat{\psi}_k\rangle$에 있는 합성계 $\mathcal{H}^{I,O} \otimes \mathcal{H}^W$의 관측을 상태 $|\psi_k\rangle$에 있는 부분계 $\mathcal{H}^{I,O}$의 관측으로 제한할 수 있다(pp. 331-333).

$$\begin{aligned}\rho^{I/O} &= tr_W\left[\left|\hat{\psi}_k\right\rangle\left\langle\hat{\psi}_k\right|\right] = tr_W\left[\left(\left|\psi_k\right\rangle\otimes\left|-\right\rangle\right)\left(\left\langle\psi_k\right|\otimes\left\langle-\right|\right)\right] \\ &= tr_W\left[\left|\psi_k\right\rangle\left\langle\psi_k\right|\otimes\left|-\right\rangle\left\langle-\right|\right] = tr_W\left[\left|-\right\rangle\left\langle-\right|\right]\left|\psi_k\right\rangle\left\langle\psi_k\right| \\ &= 1\cdot\left|\psi_i\right\rangle\left\langle\psi_i\right| = \left|\psi_i\right\rangle\left\langle\psi_i\right|\end{aligned} \tag{2.35}$$

따라서 목표 객체 $x\in S$의 측정 확률은 식 2.36과 같이 계산할 수 있다.

$$\| \mathrm{P}_S\left|\psi_k\right\rangle \|^2 = \sin^2\theta_k \tag{2.36}$$

Grover 연산자에 의한 회전은 그 정도가 매우 작기 때문에 탐색의 성공 확률을 높이기 위해서는 여러 번 적용해야 하고(McMahon, 2008, p. 220), 이에 따라 목표 객체의 측정 확률을 최대화하는 최적의 반복 횟수 k^{opt}를 결정해야 한다. 식 2.34에서 $\theta_k = \pi/2$일 때 $\left|\psi_k\right\rangle$는 식 2.37과 같이 $\left|\psi_S\right\rangle$와 같아지므로 k^{opt}는 θ_k를 $\pi/2$에 최대한 가깝도록 결정할 때의 횟수임을 알 수 있다. 이는 기하학적인 관점에서 [그림 Ⅱ-10]을 통해서도 확인할 수 있다.

$$\left|\psi_k\right\rangle = \cos\frac{\pi}{2}\left|\psi_{S^\perp}\right\rangle + \sin\frac{\pi}{2}\left|\psi_S\right\rangle = \left|\psi_S\right\rangle \tag{2.37}$$

이 점을 이용하면 k^{opt}를 다음과 같이 구할 수 있다. 먼저 θ_0의 정의로부터 $\sin\theta_0 = \sqrt{M/N}$이므로 M이 N보다 매우 작은 경우[$M \ll N$] 작은 각도 근사(small angle approximation)에 의해 $\theta_0 \approx \sqrt{M/N}$이 성립한다. 그 다음 $\theta_{k^{\mathrm{opt}}} = \pi/2$이어야 하므로 k^{opt}는 $(2k^{\mathrm{opt}}+1)\theta_0 = \pi/2$로부터 식 2.38과 같이 계산된다.

$$k^{\mathrm{opt}} = \left\lfloor \frac{\pi}{4\theta_0} \right\rfloor \approx \frac{\pi}{4}\sqrt{\frac{N}{M}} \tag{2.38}$$

이때 식 2.38의 $k^{\mathrm{opt}} = \lfloor \pi/4\theta_0 \rfloor$ 에서 $k^{\mathrm{opt}} \le \pi/4\theta_0 < k^{\mathrm{opt}}+1$이고, $\theta_{k^{\mathrm{opt}}}$에 대하여 정리하면 $\pi/2-\theta_0 < \theta_{k^{\mathrm{opt}}} \le \pi/2+\theta_0$이므로 최대화된 확률의 하한은 식 2.39과 같이 계산된다.

$$\begin{aligned} \| \mathrm{P}_S |\psi_{k^{\mathrm{opt}}}\rangle \|^2 &= \sin^2\theta_{k^{\mathrm{opt}}} \\ &\ge \sin^2\left(\frac{\pi}{2}+\theta_0\right) = 1-\cos^2\left(\frac{\pi}{2}+\theta_0\right) \\ &= 1-\sin^2\theta_0 = 1-\frac{M}{N} \end{aligned} \tag{2.39}$$

이상의 내용을 종합하면 M개의 목표 객체 $x \in S$는 $\mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$의 초기 상태 $|\hat{\psi}_0\rangle = |\psi_0\rangle \otimes |-\rangle$에 Grover 연산자를 $\pi/4 \times \sqrt{N/M}$번 적용하여 $1-M/N$보다 같거나 큰 확률로 찾을 수 있음을 알 수 있다.

제 3 장 연구 방법

이상의 서론과 이론적 배경의 논의를 바탕으로 진술한 연구 목적을 달성하기 위해 본 연구에서 살펴보고자 하는 연구 문제는 다음과 같다. 첫째, Grover 알고리즘을 중등교육 기관 학생들에게 도입하기 위해 학문수학 수준에서 엄밀하게 기술되는 현 내용 체계는 어떻게 재구조화되어야 하는가? 둘째, Grover 알고리즘의 작동 원리에 대한 이해를 성취 기준으로 하는 공학적 도구 기반의 수업과 과제는 어떻게 설계되어야 하는가?

본 연구에서는 제시한 연구 문제에 답하기 위해, 연구 방법으로 개발 연구(developmental research)를 선택하였다. 개발 연구는 일관적이고 효율적인 교과과정 개발을 위해 적절한 이론을 바탕으로 수업을 설계하고 평가하며, 그 과정을 상세하고 솔직하게 기록하고 보고하는 연구이다(정영옥, 2005). 이러한 개발 연구는 교과과정의 개발을 통한 국소 교수 이론의 형성과 정당화를 목표로 한다(Gravemeijer & Cobb, 2006, p. 17). 여기서 국소 교수 이론은 특정한 주제를 지도하기 위해, 여러 차시의 수업에 걸쳐 다루게 되는 활동들과 그 활동들 사이의 관련성을 포함한 교수학적 논의를 가리킨다(이경화, 2016).

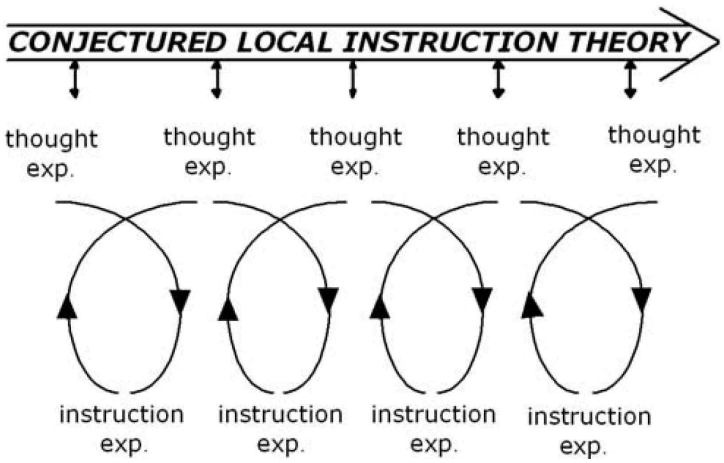
Freudenthal(2002)은 수학교과과정 개발에서 연구, 개발, 보급의 세 단계로 이루어진 전통적인 모델은 점진적 수학화를 통해 학습되는 실행 수학을 지도함에 있어 비효율적임을 지적하며, 유연한 교대 과정으로서의 개발과 연구 관계를 다음과 같이 강조하였다(p. 161).

> 개발 연구의 의미는 개발과 연구의 순한 과정을 의식적으로 경험하고, 그것에 대해 솔직하게 보고함으로써 정당화되고, 이러한 경험이 다른 사람에게 전이되어 그들 자신의 경험이 되도록 하는 것이다.

또한 정영옥(2005)은 개발 연구의 절차를 예비 설계, 교수 실험, 회고 분석의 세 단계로 구분하고, 각 단계의 순환 과정을 강조한 바 있다.

예비 설계 단계는 교수 실험을 준비하는 단계로 현 교과과정의 문제점에 기초하여 현재의 상황을 분석하고, 새로운 교과과정이 충족시켜야 할 사항들을 탐색하는 단계이다. 이를 바탕으로 연구자는 가르칠 주제에 대한 전반적인 개념을 형성하고 구체적인 수업 계열을 구성한다(정영옥, 2005). 즉, 예비 설계 단계는 정교한 국소 교수 이론의 형성을 위해 설계의 이론적 의도를 명료화하는 단계이다(Gravemeijer & Cobb, 2006, p. 24). 이때 가장 중요한 것은 명시한 학습 목표를 위한 교수·학습 과정이 실제 수업에서 어떻게 구체화될 것인지에 대해 미리 예상해보는 사고 실험이다(정영옥, 2005).

교수 실험 단계는 사고 실험을 통해 개발된 예비 교과과정과 가설적 국소 수업 이론을 정련하고 검증하는 단계이다. 즉, 교수 실험은 사고 실험을 확인하거나 반박하는 단계이며, 사고 실험에서 미처 예상하지 못했던 새로운 가능성을 열어놓기 위한 단계이다(정영옥, 2005). 또한 해당 단계에서 연구자는 학생들의 정신적 활동에 대한 통찰을 얻어 수정된 학습 경로의 구성을 위한 기초를 마련한다(전혜진 외, 2020). 이때 가장 중요한 것은 사고 실험과 교수 실험이 반복적으로 순환해야 한다는 것이다.



[그림 Ⅲ-1] 가설적 국소 교수 이론의 형성 과정

Gravemeijer & Cobb(2006)에 따르면, 사고 실험과 교수 실험은 반성적 관계에 있으며, 미시적 순환 과정을 형성한다. 이때, 가설적 국소 이론은

사고 실험과 교수 실험을 안내하고, 사고 실험과 교수 실험의 미시적 순환 과정은 가설적 국소 교수 이론을 수정 및 형성한다. 이에 대한 전반적인 과정은 [그림 Ⅲ-1](p. 28)과 같다.

회고 분석 단계는 교수 실험 단계에서 수집된 자료 전체를 분석하는 단계로, 가설적 국소 교수 이론을 최종적으로 수정하는 단계이다(정영옥, 2005). 해당 단계에서는 보다 광범위한 맥락에서 포괄적인 현상에 대한 패러다임적 예가 구조화된다. 또한 교수 실험 단계에서 미시적인 수준으로 나타났던 연구와 개발의 순환적 특징이 거시적인 수준에서 나타나며, 최종적으로는 국소 교수 이론을 바탕으로 앞으로의 개발 연구를 위한 기초적인 아이디어를 제공한다(Gravemeijer & Cobb, 2006, pp. 28-29).

본 연구의 목적은 교수학적 변환을 통해 Grover 알고리즘의 수학적 엄격함을 낮추고, 이를 바탕으로 <양자 알고리즘> 교육 프로그램을 개발하는 것이다. 따라서 본 연구에서는 개발 연구의 예비 설계 단계에 집중하되, 거시적 순환 과정의 초석이 되는 미시적 순환 과정에도 주목하고자 한다. 즉, 사고 실험을 통해 설계한 예비 <양자 알고리즘> 교육 프로그램을 학생들에게 적용하고, 최종적으로는 해당 교수 실험을 평가 및 분석함으로써 수정・보완된 교수・학습 과정을 제안하고자 한다.

제 1 절 연구 설계 및 절차

생태학적 타당도(ecological validity)를 목표로 하는 개발 연구는 경험에 근거한 이론을 전제로 다양한 상황에 적용 가능한 기초를 제공할 수 있어야 한다. 즉 연구자의 경험에 의해 형성된 국소 교수 이론이 제시하는 교수・학습 절차는 자신의 교실 또는 개인적인 목적에 맞게 활용하고자 하는 교사가 참조할 수 있는 틀로서 기능해야 한다. 이를 위한 방법 중의 하나는 참여자들의 세부 사항, 교수・학습 과정 등 개발 연구의 전반적인 과정을 상세히 밝히는 것이다(Gravemeijer & Cobb, 2006, p. 45). 본 절에서는 앞서 진술한 연구 문제에 답하기 위한 연구 절차에 대해서 자세히 설명한다.

1. 예비 설계

본 연구의 예비 설계 단계는 첫 번째 연구 문제에 답하기 위한 Grover 알고리즘의 내용 체계 재구조화와 두 번째 연구 문제에 답하기 위한 교육 프로그램 수업 및 프로젝트 과제 설계로 구성되어 있다.

먼저 Grover 알고리즘의 내용 체계 재구조화를 위해 다음과 같은 순서로 연구를 진행하였다. 첫째, 이론적 배경의 제2절과 제3절을 바탕으로 학문수학 수준에서 엄밀하게 기술되는 Grover 알고리즘의 핵심 내용 요소를 추출하여 현 내용 체계를 정립하였다. 둘째, 현 내용 체계를 기하학적 관점에서 고찰함으로써 공학적 도구를 통해 정당화할 수 있거나 맥락적인 추론을 통해 생략할 수 있는 요소들을 선별하였다. 셋째, 축소 과정에 포함되지 않은 요소들 중, 제4수준에서 내포적으로 정의된 요소들을 제3수준에서 외연적으로 재정의하였고 이러한 요소들을 유기적으로 연결시키기 위한 정리와 참고를 도출하였다. 넷째, Grover 알고리즘의 각 단계에 해당하는 일반화된 지식[24]을 도출하였고, 이상의 논의를 종합하여 재구조화된 Grover 알고리즘의 내용 체계를 제안하였다.

다음으로 Grover 알고리즘의 작동 원리에 대한 이해를 성취 기준으로 하는 공학적 도구 기반의 수업 및 과제의 설계를 위해 다음과 같은 순서로 연구를 진행하였다. 첫째, 재구조화된 내용 체계에서 Grover 알고리즘을 지도함에 있어 공학적 도구의 활용이 필요한 내용 요소를 선별하였고, 그에 따른 교육 자료를 개발하였다. 둘째, 본 연구에서 제시하고자 하는 <양자 알고리즘> 교육에 활용 가능한 공학적 도구 IBM Quantum Experience(이하 IBM QX)의 사용법을 익히고, Grover 알고리즘을 이용하여 문제를 해결함에 있어 유용한 연산 게이트를 얻을 수 있는 실습 과제를 설계하였다. 셋째, Grover 알고리즘을 통해 접근할 수 있는 문제들을 탐구한 선행 연구들을 조사하였고, 이를 바탕으로 IBM QX의 시각화 기능을 온전히 활용할 수 있는 프로젝트 활동 과제를 개발하였다.

---

24) 일반화된 지식이란, 학생들이 해당 영역의 핵심 개념에 대하여 알아야 할 보편적인 지식을 말한다(교육부, 2015).

2. 교수 실험

본 연구에서는 <표 Ⅲ-1>과 같이 설계된 교육 프로그램[25]을 선정된 학생들에게 적용해보며, 예비 설계 단계의 결과를 수정·보완하기 위한 교수 실험을 진행하였다. 이를 통해 중등교육 기관 학생들을 대상으로 Grover 알고리즘의 도입 가능성을 살펴보고, 본 연구에서 제시하는 수업과 과제의 교수·학습 과정을 위한 시사점을 도출하였다.

<표 Ⅲ-1> Grover 알고리즘 교육 프로그램 구성

주제(제목)	양자 계산과 수학, Grover 알고리즘을 중심으로	
차시별 학습 주제	1차시	선형대수학의 기초 - 벡터와 행렬
	2차시	양자 비트(큐비트)와 텐서 곱
	3차시	양자 게이트와 양자 회로
	4차시	Grover 알고리즘의 수학적 구조
	5차시	Grover 알고리즘의 응용과 심화
대상	서울대학교 사범대학 부설 시흥 영재교육원 R&E 과정 선발 학생	
인원	2명 (일반계 고등학교 2학년)	
기간	2022년 7월 1일 ~ 2022년 12월 20일	
소요 시간	총 30시간 (6시간×5차시)	
교수·학습 방법	이론 학습 및 문제 해결	
	IBM QX 프로그램 실습	
	(소집단) 프로젝트 활동	
	토의 및 발표	

25) 해당 교육 프로그램에 대한 교수 실험은 서울대학교 생명윤리위원회의 승인을 받아 진행하였다(IRB No. 2205/004-014).

본 연구의 참여자들은 2022학년도 서울대학교 사범대학 부설 시흥영재교육원 R&E 과정 수학분과 'Hat-game과 수학 그리고 오류정정코드'를 탐구 주제로 선택한 학생들 중 <양자 알고리즘> 교육 프로그램에 참여하고자 하는 의지가 있던 학생들로, 고등학교 2학년 학생 2명으로 구성되어 있다. 해당 학생들은 2021년에 소정의 문제 해결 및 심층 면접 과정을 통해 선발된 학생들이며, 사전에 비트와 큐비트의 차이를 알고 있을 정도로 양자 컴퓨터에 대한 관심과 흥미를 갖고 있던 학생들이다.

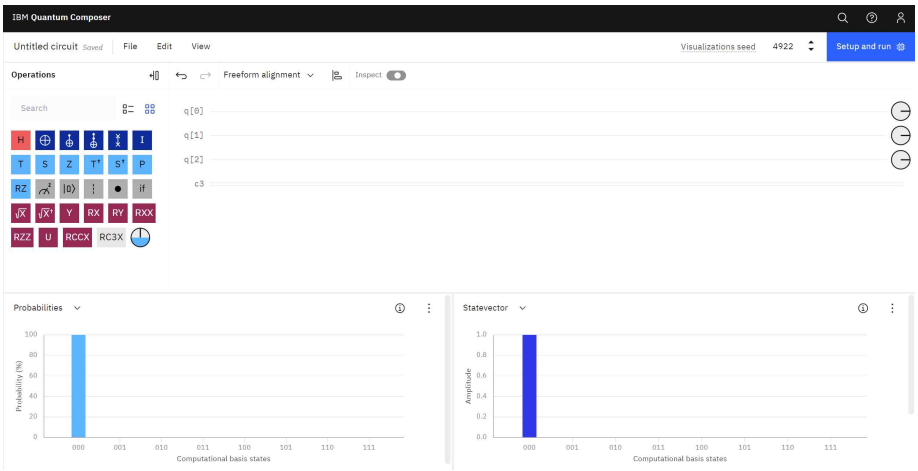
제 2 절 공학적 도구: IBM QX

IBM QX는 2016년에 IBM 사에서 공개한 양자 컴퓨터로, 클라우드 서비스(cloud service)의 형태로 사용자에게 양자 컴퓨팅 환경을 제공한다. IBM QX는 171개국에서 10만 명 이상의 사용자를 확보하고 있으며, 2019년 기준 530만 건 이상의 양자 디바이스 실험과 1,200만 건 이상의 가상 시험을 수용하고 있다. 특히 IBM QX는 타 기관 플랫폼과의 활발한 연동을 통해 양자 컴퓨팅 소프트웨어 플랫폼 중 성능 시험 정보가 많은 사례 중 하나이다(조은영 외, 2021).

IBM QX는 공식 웹 페이지(quantum-computing.ibm.com)에서 이용할 수 있으며, GUI 기반의 양자 회로 구성 편집기[작곡기](quantum circuit composer)와 오픈 소스(open source) 소프트웨어 개발 키트[26]인 QISKit (quantum information simulation kit)의 형태로 이용할 수 있다. 본 연구에서는 교사들의 접근성을 높이기 위해 코딩을 수반하지 않는 양자 회로 구성 편집기만을 이용하여 교육 프로그램의 수업과 과제를 설계하였다. 여기서는 IBM 사에서 제공하는 사용 안내서를 기준으로 양자 회로 구성 편집기의 인터페이스(interface)와 본 연구에서 활용하고자 하는 주요 시각화 기능에 대해서 정리한다.

---

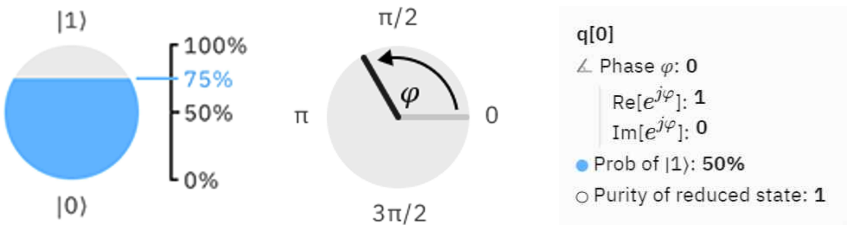
26) 소프트웨어 개발 키트(software development kit)란, 특정 운영 체제용 응용 프로그램을 만들기 위한 소스와 도구 패키지를 의미한다.



[그림 Ⅲ-2] 양자 회로 구성 편집기의 인터페이스

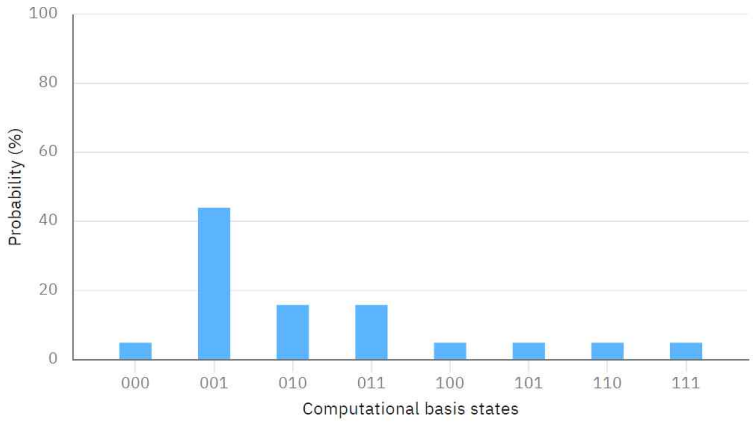
IBM QX의 양자 회로 구성 편집기에서 각종 다이어그램을 양자선에 끌어서 놓는(drag-and-drop) 방식으로 양자 회로도를 작성할 수 있다. [그림 Ⅲ-2]는 양자 회로 구성 편집기의 인터페이스로, 왼쪽의 다이어그램은 양자 게이트, 양자 측정 도구 등을 나타낸다. 오른쪽의 q_0, q_1, q_2, q_3는 상태 $|0\rangle$으로 초기화되어 있는 양자 레지스터이며, c_4는 q_0, q_1, q_2, q_3의 측정 결과를 저장하기 위한 고전 레지스터이다.

양자 회로 구성 편집기는 양자 회로가 큐비트에 미치는 영향을 실시간으로 시각화하여 제공한다. 이때 동기화된 가시화 형태로는 위상 디스크, 확률 보기, 상태 벡터 보기가 있다. 위상 디스크(phase disk)는 중첩 상태를 시각화하며, 각 큐비트의 로컬 상태를 제공한다. [그림 Ⅲ-3]에서 파란색 부분은 큐비트가 상태 $|1\rangle$으로 출력될 확률을 나타내고, 디스크의 중심으로부터 가장자리까지 연장선은 큐비트의 양자 위상을 나타낸다.



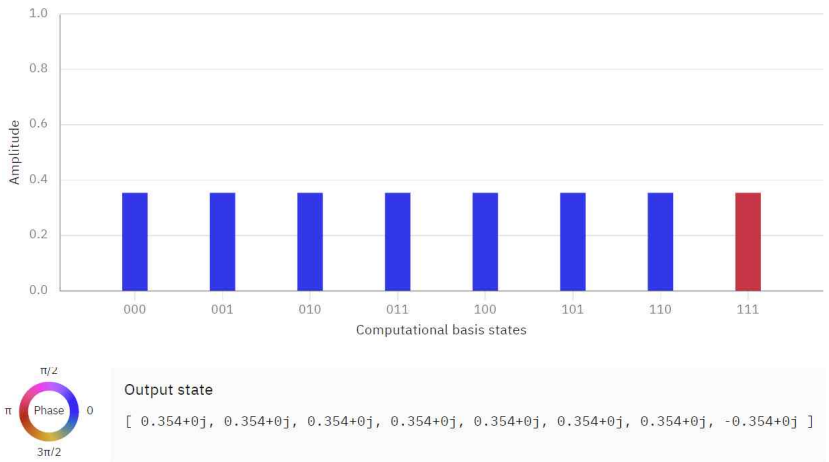
[그림 Ⅲ-3] 양자 회로 구성 편집기의 위상 디스크

확률 보기(probability view)는 8-큐비트 크기 이하의 입/출력 레지스터가 주어졌을 때, 각각의 계산 기저 상태에 대한 입력 큐비트의 측정 확률을 [그림 Ⅲ-4]와 같이 막대 그래프로 시각화하여 제공한다.



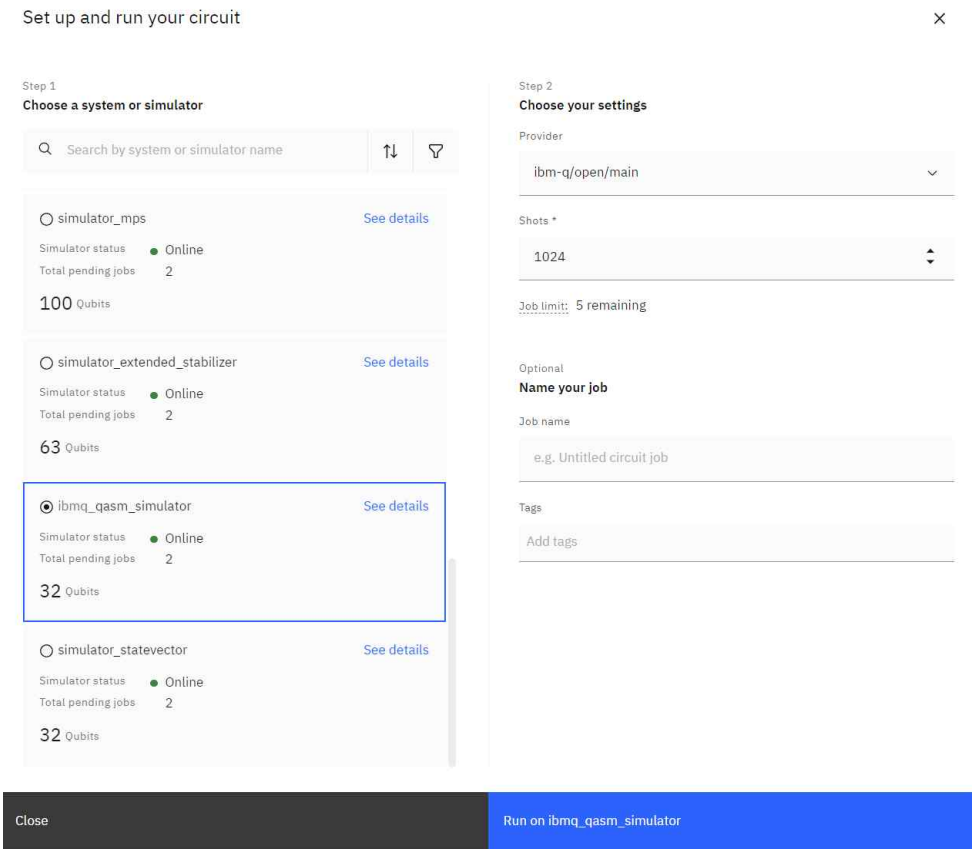
[그림 Ⅲ-4] 양자 회로 구성 편집기의 확률 보기

상태 벡터 보기(state vector view)는 6-큐비트 크기 이하의 입/출력 레지스터가 주어졌을 때, 각각의 계산 기저 상태에 대한 입력 큐비트의 확률 진폭을 막대 그래프로 시각화하여 제공하고, 동시에 입력 큐비트의 위상을 색을 통해 구별하여 제공한다. [그림 Ⅲ-5]는 |111〉의 위상을 반전시킨 3-큐비트 크기의 균등 중첩 상태에 대한 상태 벡터 보기이다.



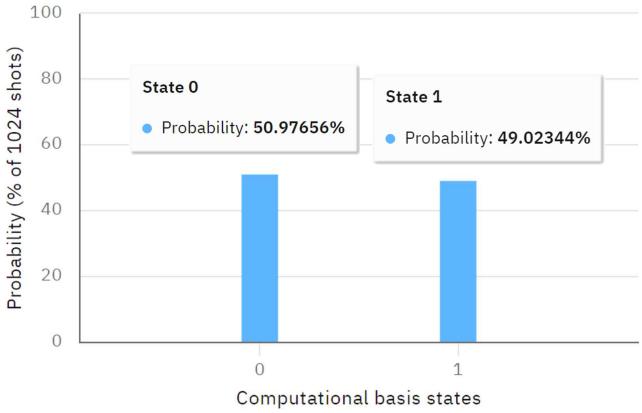
[그림 Ⅲ-5] 양자 회로 구성 편집기의 상태 벡터 보기

한편 양자 회로 구성 편집기에서 작성한 양자 회로도는 실물 양자 컴퓨터에서 직접 시뮬레이션을 수행할 수 있는데, 이는 [그림 Ⅲ-2]의 오른쪽 상단에 있는 'Setup and run'에서 몇 가지 환경을 설정한 후 진행할 수 있다. [그림 Ⅲ-6]은 Setup and run의 인터페이스로, 해당 창에서 양자 회로 실행에 사용할 시뮬레이터(simulator)와 백엔드(back - end)에서 수행할 회로의 실행 수(shot)를 설정할 수 있다.

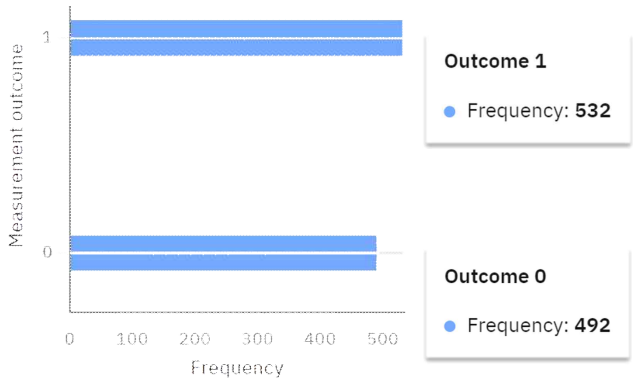


[그림 Ⅲ-6] Setup and run의 인터페이스

단 [그림 Ⅲ-7], [그림 Ⅲ-8]과 같이 임의의 양자 회로에 대한 시뮬레이션 결과와 측정 도구를 포함한 양자 회로의 확률 보기 기능에는 이론적인 측정 확률과 다른 결괏값이 나타날 수 있다. 이는 큐비트의 결어긋남(decoherence)[27]과 연산 및 측정 과정에서 발생하는 오류에 기인한다.



[그림 Ⅲ-7] 1-큐비트 균등 중첩 상태의 확률 보기



[그림 Ⅲ-8] 1-큐비트 균등 중첩 상태의 시뮬레이션 결과

양자 오류 정정(quantum error correction)은 양자 컴퓨터 개발의 마일스톤(milestone)으로 활발한 연구가 진행 중인 분야이다(김태현, 2018; 이혁성, 2019). 큐비트가 갖는 짧은 결맞음 시간과 오류율은 단시일 내에 해결될 수 없는 한계로 인식되고 있어(조은영 외, 2021), 근래에는 큐비트 제어 기술을 바탕으로 양자 연산 오류에 상대적으로 덜 민감한 양자 시뮬레이션 연구에 많은 노력이 집중되고 있다(Mohseni et al., 2017).

27) 양자 컴퓨터에서 발생하는 오류의 가장 일반적인 원인은 외부의 환경에 의해 양자계가 설계된 연산 프로세스와 일치하지 않는 것이다(Scherer, 2019, p. 343). 양자 시스템이 주위 환경과 상호 작용할 때 순수 상태가 진성 혼합 상태로 변할 수 있는데, 이를 '결어긋남'이라고 한다(p. 56). 결어긋남이 발생한 양자계는 양자정보처리에 이용할 수 없다(이종찬 외, 2013).

제 4 장 연구 결과

제 1 절 Grover 알고리즘 내용 체계 재구조화

본 절에서는 중등교육 기관 학생들을 대상으로 한 Grover 알고리즘의 내용 체계를 제안한다. 이를 위해 다음과 같은 순서로 연구 결과를 제시하였다. 첫째, 학문수학 수준에서 엄밀하게 기술되는 Grover 알고리즘의 현 내용 체계를 정립한다. 둘째, 현 내용 체계의 수학적 엄격함을 낮추기 위해 교수학적 변환을 시도한다. 셋째, 이상의 논의를 종합하여 재구조화된 Grover 알고리즘의 내용 체계를 제안한다.

1. Grover 알고리즘의 현 내용 체계

물리학의 근본적인 질문과 밀접한 관련이 있으며, 실질적인 활용성과 유용성이 잠재되어 있는 양자 컴퓨팅은 다양한 수학 분야로부터 유래되었다(Scherer, 2019, p. vii). 실제로 양자역학은 확률에 관한 서술만을 허용하는 수학적 형식화(formalism)를 통해 미시세계(microscopic system)를 설명하며, 계의 물리량을 수학적으로 엄밀히 기술함으로써 이론상으로 동시에 측정할 수 있는 최대 정밀도의 한계를 설명한다(p. 1). 이론적 배경 제3절에서 살펴보았듯이 Grover 알고리즘은 엄밀한 수학적 구조 하에서 기술된다. 즉, Grover 알고리즘의 작동 원리를 이해하기 위해서는 수학적인 원리를 이해하는 것이 필수적이다.

여기서는 Grover 알고리즘의 각 단계를 기술하는데 필요한 정의와 명제를 살펴보고, 그 내부에서 추출한 핵심 내용 요소들을 제시한다. 단, 벡터와 행렬에 관한 내용은 양자 알고리즘을 이해하기 위한 기초 선지식으로써 간주하고, 이론적 배경에서 살펴본 것 외의 내용 요소는 분석 결과에 포함시키지 않았다. 또한 각 요소의 정의 유형을 분석함에 있어 내

포적으로 정의된 용어를 기호화하기 위해 다시 동의적으로 정의하는 것은 분석 결과에 포함시키지 않았다.

Grover 알고리즘의 초기·중첩 단계를 기술하는데 필요한 정의는 입/출력 레지스터 $\mathcal{H}^{I,O}$, 보조 레지스터 $\mathcal{H}^{W}$, 초기 상태 $|\psi_0\rangle$, $|\hat{\psi}_0\rangle$로 모두 내포적 정의에 해당하며, 각 정의로부터 추출된 내용 요소와 하위 내용 요소는 <표 Ⅳ-1>과 같다.

<표 Ⅳ-1> 초기·중첩 단계의 정의와 내용 요소

단계	정의	내용 요소	하위 내용 요소
초기·중첩	힐베르트 공간 $\mathbb{C}^2$을 보조 레지스터 $\mathcal{H}^{W}$로 정의한다.	힐베르트 공간	–
	힐베르트 공간 $(\mathbb{C}^2)^{\otimes n}$을 입/출력 레지스터 $\mathcal{H}^{I,O}$로 정의한다.	n겹-힐베르트 공간	• 힐베르트 공간 • 텐서 곱
	균등 선형 조합 상태 $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\|x\rangle$를 입/출력 레지스터 $\mathcal{H}^{I,O}$의 초기 상태 $\|\psi_0\rangle$로 정의한다.	균등 선형 조합 상태 (중첩 상태)	• bra-ket 표기법 • 중첩의 원리 • 양자 측정(사영 측정) • Born의 규칙
	$\|\psi_0\rangle\otimes\|-\rangle$을 $\mathcal{H}^{I,O}\otimes\mathcal{H}^{W}$의 초기 상태 $\|\hat{\psi}_0\rangle$로 정의한다.	2겹-힐베르트 공간	• 힐베르트 공간 • 텐서 곱

n겹-힐베르트 공간의 정의를 이해하기 위해서는 명제 “두 힐베르트 공간의 텐서 곱은 힐베르트 공간이다.”를 이해해야 하며, 중첩 상태인 균등 선형 조합 상태를 이해하기 위해서는 중첩의 원리와 양자 측정 모델의 사영 측정 모델 및 Born의 규칙을 이해해야 한다.

<표 Ⅳ-2> 사영·직교 사영 연산자의 정의와 내용 요소

정의	내용 요소	하위 내용 요소
힐베르트 공간 $\mathcal{H}$에 대하여 $P^2=P$를 만족하는 연산자 $P\in L(\mathcal{H})$를 사영 연산자라 한다.	$\mathcal{H}$에 작용하는 선형 연산자들의 집합 $L(\mathcal{H})$	• 선형 연산자 • 힐베르트 공간
$P^*=P$를 만족하는 사영 연산자 P를 직교 사영 연산자라 한다.	사영 연산자	• $\mathcal{H}$에 작용하는 선형 연산자들의 집합 $L(\mathcal{H})$

이때 사영 측정 모델의 하위 요소인 사영 연산자와 직교 사영 연산자는 <표 Ⅳ-2>와 같이 내포적으로 정의된다. 한편 동의적 정의에 해당하는 bra-ket 표기법은 추가적인 요소의 이해를 필요로 하지 않는다.

Grover 알고리즘의 오라클 단계를 기술하는 데 필요한 정의는 목표 객체들의 집합 S, 목표가 아닌 객체들의 집합 $S^{\perp}$, 오라클 함수 f, 오라클 연산자 U_f, 확산 연산자 R_{ψ_0}이다. 이때 두 집합 S, $S^{\perp}$의 정의는 동의적 정의, 함수 f, 연산자 R_{ψ_0}의 정의는 내포적 정의, 연산자 U_f의 정의는 외연적 정의에 해당한다. 각 정의로부터 추출된 내용 요소와 하위 내용 요소는 <표 Ⅳ-3>과 같다.

<표 Ⅳ-3> 오라클・확산 단계의 정의와 내용 요소

단계	정의	내용 요소	하위 내용 요소
오라클・확산	목표 객체들의 집합을 S로 표기한다.	목표 객체	–
	목표가 아닌 객체들의 집합을 $S^{\perp}$로 표기한다.	목표가 아닌 객체	–
	집합 $\{0, 1, \cdots, N-1\}$를 A라 할 때, 임의의 $x \in A$에 대하여 $x \mapsto f(x) := \begin{cases} 1, & x \in S \\ 0, & x \in S^{\perp} \end{cases}$ 로 주어지는 함수 $f: A \to \{0, 1\}$를 오라클 함수라 한다.	집합 S	• 목표 객체
		집합 $S^{\perp}$	• 목표가 아닌 객체
	오라클 함수 f에 대응되는 오라클 연산자 U_f는 양자계에서 유효한 연산이 될 수 있도록 합성계 $\mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$의 계산 기저에 $\mathrm{U}_f(\|x\rangle \otimes \|y\rangle) = \|x\rangle \otimes \|y \boxplus f(x)\rangle$ 와 같이 작용하도록 정의하고, 선형 확장을 통해 $\mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$내의 임의의 상태 벡터에 대해 정의한다.	오라클 함수 f	• 집합 S • 집합 $S^{\perp}$
		양자계 내에서 유효한 연산자	• 가역 변환 • 유니터리 변환
		합성계 $\mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$	• 부분계 $\mathcal{H}^{I,O}$ • 부분계 $\mathcal{H}^{W}$
		계산 기저	• 정규직교기저
		인수별 이진법 덧셈	• 베타적 논리합 • 텐서 곱
		선형 확장	–
	일차원 부분공간에 대한 반사 연산자 $\mathrm{R}_{\psi_0} = 2\|\psi_0\rangle\langle\psi_0\| - \mathrm{Id}^{\otimes n}$ 를 확산 연산자로 정의한다.	일차원 부분공간에 대한 반사 연산자	• 반사 연산자 • 초기 상태 $\|\psi_0\rangle$ • n겹-항등 연산자 • 유니터리 변환

두 집합 S, $S^{\perp}$의 정의는 동의적 정의로서 정의항 내의 목표 객체, 목표가 아닌 객체 외에 추가적인 요소의 이해를 필요로 하지 않으며, 정의항에 두 집합 S, $S^{\perp}$의 요소만을 포함하는 함수 f의 정의 역시 추가적인 요소의 이해를 필요로 하지 않는다. 또한 내포적 정의에 해당하는 R_{ψ_0}의 정의 역시 해당 하위 요소를 제외하고는 추가적인 요소의 이해를 필요로 하지 않는다. 그러나 외연적 정의에 해당하는 U_f의 정의는 $\mathcal{H}^{I,O}$ 내의 임의의 상태 벡터 $|\psi\rangle$에 대하여 $|\psi\rangle\otimes|-\rangle$에 작용하는 방식(식 2.31)을 도출하기 위한 것으로 계산 요소에 해당하는 식 2.24, 식 2.25, 식 2.28 ~ 식 2.30에 대한 이해가 필요하며, 내포적 정의에 해당하는 입/출력 레지스터의 부분공간 $\mathcal{H}_S$, $\mathcal{H}_{S^{\perp}}$, 사영 연산자 P_S, 반사 연사자 $R_{S^{\perp}}$의 정의에 대한 이해가 필요하다. 이때 부분공간으로의 사영 연산자와 반사 연사자는 <표 Ⅳ-4>와 같이 내포적으로 정의된다.

<표 Ⅳ-4> 부분공간으로의 사영·반사 연산자의 정의와 내용 요소

정의	내용 요소	하위 내용 요소
힐베르트 공간 $\mathcal{H}$의 부분공간 $\mathcal{H}_{sub}$에 대하여 조건 $\forall|\psi\rangle\in\mathcal{H}_{sub}$, $P_{sub}|\psi\rangle=|\psi\rangle$ 을 만족하는 직교 사영 연산자 P_{sub}를 $\mathcal{H}_{sub}$로의 사영 연산자라 한다.	직교 사영 연산자	• 사영 연산자
힐베르트 공간 $\mathcal{H}$의 부분공간 $\mathcal{H}_{sub}$에 대하여 조건 $R_{sub}=2P_{sub}-Id$ 를 만족하는 연산자 R_{sub}를 $\mathcal{H}_{sub}$에 대한 반사 연산자라 한다.	부분공간으로의 사영 연산자	• 직교 사영 연산자
	항등 연산자	–

Grover 알고리즘의 반복 단계를 기술하는데 필요한 정의는 Grover 연산자 G, k번 Grover 반복 후의 상태 $|\hat{\psi}_k\rangle$, span$\{|\psi_{S^{\perp}}\rangle\}$와 $|\psi_k\rangle$ 사이의 각 θ_k, 축약 밀도 연산자이다. 이때 상태 $|\hat{\psi}_k\rangle$의 정의만 동의적 정의에 해당하고 나머지 정의들은 내포적 정의에 해당한다. 각 정의로부터 추출된 내용 요소와 하위 내용 요소는 <표 Ⅳ-5>와 같다.

<표 Ⅳ-5> 반복 단계의 정의와 내용 요소

단계	정의	내용 요소	하위 내용 요소
반복	오라클 단계와 확산 단계의 순차적인 작용에 대응되는 Grover 연산자 G는 $(R_{\psi_0}\otimes Id)U_f$로 정의한다.	오라클 연산자	• 오라클 함수 f • 양자계에서 유효한 연산자 • 합성계 $\mathcal{H}^{I,O}\otimes\mathcal{H}^{W}$ • 계산 기저 • 인수별 이전법 덧셈 • 선형 확장
		확산 연산자	• 일차원 부분공간에 대한 반사 연산자
		항등 연산자	–
	Grover 연산자를 합성계 $\mathcal{H}^{I,O}\otimes\mathcal{H}^{W}$의 초기 상태에 k번 반복 적용한 상태를 $\lvert\hat{\psi}_k\rangle=\lvert\psi_k\rangle\otimes\lvert-\rangle$로 표현한다.	Grover 연산자	• 오라클 연산자 • 확산 연산자 • 항등 연산자
		합성계 $\mathcal{H}^{I,O}\otimes\mathcal{H}^{W}$	• 부분계 $\mathcal{H}^{I,O}$ • 부분계 $\mathcal{H}^{W}$
		초기 상태 $\lvert\hat{\psi}_0\rangle=\lvert\psi_0\rangle\otimes\lvert-\rangle$	• 초기 상태 $\lvert\psi_0\rangle$ • 상태 $\lvert-\rangle$
	$[0,\pi/2]$에 속하는 $\mathrm{span}\{\lvert\psi_{S^\perp}\rangle\}$와 $\lvert\psi_0\rangle$ 사이의 각을 θ_0로 표현한다.	상태 $\lvert\psi_{S^\perp}\rangle$	• 균등 선형 조합 상태
		초기 상태 $\lvert\psi_0\rangle$	• 균등 선형 조합 상태
	자연수 k에 대하여 $(2k+1)\theta_0$을 만족하는 각을 θ_k로 표현한다.	각 θ_0	• 상태 $\lvert\psi_{S^\perp}\rangle$ • 초기 상태 $\lvert\psi_0\rangle$
	$\mathcal{H}^{A}\otimes\mathcal{H}^{B}$의 밀도 연산자를 ρ라 할 때, $\mathcal{H}^{A}$의 축약 밀도 연산자 ρ^{A}를 $tr_B(\rho)$, $\mathcal{H}^{B}$의 축약 밀도 연산자 ρ^{B}를 $tr_A(\rho)$, 로 정의한다.	부분 대각합	–
		밀도 연산자	• 순수 상태 • 혼합 상태

위의 정의 다섯 가지는 모두 해당 하위 요소를 제외하고는 추가적인 요소의 이해를 필요로 하지 않는다. 그러나 반복 단계에서는 해당 정의들을 이용하여 Grover 연산자가 근본적으로 회전 연산자와 동일함을 이해해야 하며, 이로부터 회전 연산자들의 합성으로 볼 수 있는 Grover 반복에 대한 최적 횟수의 존재함을 이해해야 한다. Grover 연산자가 회전 연산자인 것은 [그림 Ⅱ-10]에서 오라클 연산자와 확산 연산자의 기하학적인 의미를 순차적으로 살펴봄으로써 이해할 수 있다. 또한 최적 횟수 k^{opt}가 $\theta_{k^{\mathrm{opt}}}=\pi/2$에서 달성되는 것 역시 [그림 Ⅱ-10]을 통해 확인할 수

있으며, 식 2.37과 같이 간단한 대입을 통해 확인할 수도 있다. 물론 이를 논하기 위해서는 식 2.35를 통해 $\mathcal{H}^{I,O} \otimes \mathcal{H}^{W}$의 관측을 $\mathcal{H}^{I,O}$의 관측으로 제한할 수 있는 것에 대한 이해가 선행되어야 한다. 마지막으로 최적 횟수가 $k^{\mathrm{opt}} \approx \pi/4\sqrt{M/N}$로 계산되는 것은 작은 각도 근사를 이용하여 도출할 수 있으며, 최적 횟수에 대한 탐색 성공 확률의 하한이 $1-M/N$로 계산 되는 것은 식 2.39을 통해 이해할 수 있다.

2. Grover 알고리즘의 교수학적 변환

지금까지 살펴보았듯이 몇 가지 가정에 기반한 연역적인 논의를 통해 Grover 알고리즘의 수학적 구조를 이루는 정의 요소들은 외연적 정의에 해당하는 오라클 연산자와 동의적 정의에 해당하는 몇 가지 기호화를 제외하고는 대부분 내포적 정의에 해당한다. 여기서는 [그림 Ⅱ-10]과 같은 Grover 알고리즘의 기하학적인 의미에 집중하여 중등교육의 평면기하학을 기준으로 <표 Ⅱ-1>, <표 Ⅱ-2> 및 공학적 도구의 활용을 통해 교수학적 변환을 시도한다. 또한 최종적으로는 이상의 내용을 종합하여 Grover 알고리즘의 각 단계에 해당하는 일반화된 지식을 제안한다.

2.1. Grover 알고리즘의 축소 모델 선정

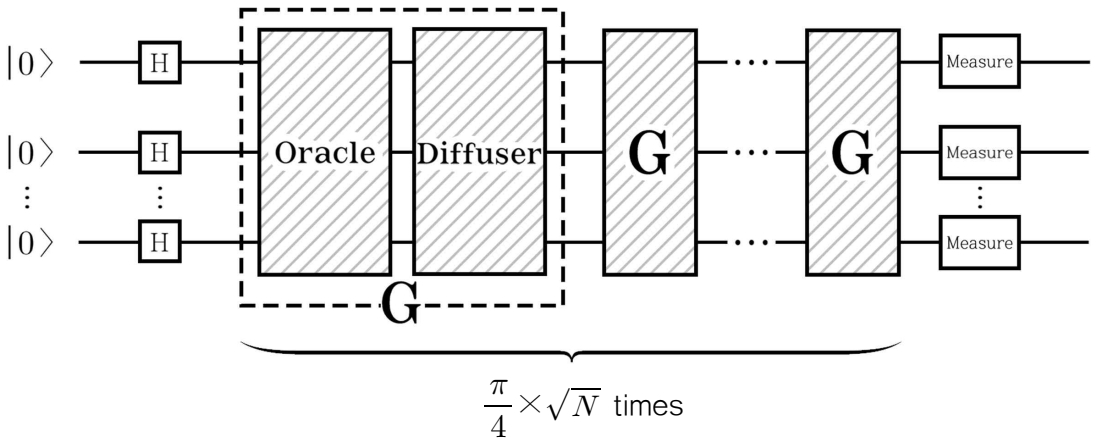
교수학적 변환에 앞서 본 연구에서는 Grover 알고리즘의 수학적 엄격함을 낮출수 있도록 유한개의 목표 객체를 탐색하기 위한 일반적인 모델을 1개의 목표 객체를 탐색하는 경우로 제한하였으며, 보조 레지스터를 제외한 축소 모델을 선정하였다. 양자계에서 유효한 오라클 연산자를 정의하기 위해 도입했던 보조 레지스터는 식 2.35에서도 알 수 있듯이 최종적으로는 오라클 연산자의 작용에 영향을 받지 않는다. 실제로 보조 레지스터는 오라클 함수 f를 식 4.1과 같이 주어지는 함수 $\hat{f}$으로 대응시킴으로써 제외할 수 있다(Lala, 2019, p. 208).

$$\hat{f}:\{0,\ 1,\ \cdots,\ N-1\}\ \rightarrow\ \{0,\ 1\},\ x\ \mapsto\ \hat{f}(x):=\begin{cases}-\ |x\rangle, & x\in S\\ \ \ |x\rangle, & x\in S^{\perp}\end{cases} \qquad (4.1)$$

즉, 보조 레지스터가 제외된 축소 모델에서는 오라클 연산자를 식 2.27 ~ 식 2.31에 관한 논의 없이 내포적인 방법을 통해 함수 $\hat{f}$에 대응하는 연산자 $\mathrm{U}_{\hat{f}}:=\mathrm{Id}^{\otimes n}-2\mathrm{P}_S$로 곧바로 정의할 수 있다. 이상으로부터 축소된 Grover 알고리즘(reduced grover algorithm, 이하 RGA) 모델의 의사코드는 <표 Ⅳ-6>과 같으며, 양자 회로도는 [그림 Ⅳ-1]과 같다.

<표 Ⅳ-6> 축소된 Grover 알고리즘 모델의 의사코드

단계	단계별 의사 코드
초기	n-큐비트 크기의 입/출력 레지스터를 준비하고, $\|0\rangle^{\otimes n}$으로 초기화한다.
중첩	$\|0\rangle^{\otimes n}$을 확률 진폭이 모두 균등한 n-큐비트 크기의 중첩 상태로 변환한다.
오라클	균등 중첩 상태에서 조건 $f(x)=1$을 만족하는 $x\in\{0,\ 1,\ \cdots,\ N-1\}$의 상태 $\|x\rangle$의 위상을 반전시킨다.
확산	주어진 각각의 상태들에 대하여 확률 진폭의 평균에 대한 반전을 수행한다.
반복	오라클 단계와 확산 단계를 순차적으로 $\frac{\pi}{4}\times\sqrt{N}$번 반복한다.



[그림 Ⅳ-1] 축소된 Grover 알고리즘 모델의 양자 회로도

2.2. 초기·중첩 단계의 내용 요소 재구성

RGA 모델의 초기·중첩 단계에서는 <표 Ⅳ-1>에서 제시한 보조 레지스터 $\mathcal{H}^W$의 정의와 합성계 $\mathcal{H}^{I,O}\otimes\mathcal{H}^W$의 초기 상태 $|\hat{\psi}_0\rangle$의 정의를 내용 요소로 포함하지 않는다. 즉, RGA 모델의 초기·중첩 단계를 이해하기 위해 필요한 정의는 입/출력 레지스터 $\mathcal{H}^{I,O}$의 정의와 $\mathcal{H}^{I,O}$의 초기 상태 $|\psi_0\rangle$의 정의 뿐이다.

입/출력 레지스터 $\mathcal{H}^{I,O}$의 정의는 n-겹 힐베르트 공간의 하위 요소로 힐베르트 공간과 텐서 곱을 포함한다. 이때 텐서 곱은 식 2.9, 식 2.11과 같이 벡터와 행렬 각각에 작용하는 연산 방식을 열거함으로써 외연적으로 정의할 수 있다. 반면에 힐베르트 공간은 평면기하 상에서 Grover 알고리즘의 작동 원리를 이해함에 있어 필요하지 않고, 앞으로 제시할 오라클 단계와 확산 단계의 수학적 정당화 과정에서 나타나는 내적을 통해 그 의미를 맥락적으로 추론할 수 있으므로 본 연구에서 제시하고자 하는 내용 체계에서는 제외하였다. 이에 따라 입/출력 레지스터를 새롭게 정의할 필요가 있었고, 본 연구에서는 양자 레지스터를 정의 1.1과 같이 동의적으로 정의함으로써 입/출력 레지스터로 이용할 n-큐비트 양자 레지스터를 정의 1.2로 도입하였다.

- **정의 1.1.** 양자 컴퓨터 프로세서가 큐비트에 대한 계산을 수행하는 연산 처리의 기본 단위를 양자 레지스터라 한다.
- **정의 1.2.** n개의 큐비트에 대한 연산을 수행하는 양자 레지스터를 n-큐비트 양자 레지스터라 한다. (단, n은 자연수)

한편 입/출력 레지스터 $\mathcal{H}^{I,O}$의 초기 상태 $|\psi_0\rangle$의 정의는 중첩 상태의 하위 요소로 bra-ket 표기법, 중첩의 원리, 사영 측정 모델, Born의 규칙을 포함한다. 앞서 언급했듯이 bra-ket 표기법은 동의적 정의에 해당하므로 교수학적 변환을 시도하지 않았다. 반면에 식 2.3에 의해 내포적으로 정의되는 중첩 상태의 정의는 학문수학 수준의 내용 요소를 포함

하므로 정의 1.3과 같이 외연적으로 재정의하였고, 해당 정의로부터 도출되는 확률 진폭을 정의 1.4와 같이 외연적으로 정의함으로써 양자 측정(참고 1.6)과 Born의 규칙(정리 1.7)을 도입하였다. 이때 해당 요소들을 이해하기 위해서는 먼저 <선형대수학>의 '벡터'와 '행렬'에 대한 이해가 선행되어야 한다. 그러나 이와 같은 도입 방식은 사영 연산자와 직교 사영 연산자를 하위 요소로 포함하는 사영 측정 모델의 이해를 필요로 하지 않는다.

- **표기 1.3 (bra-ket 표기법).** 열벡터를 $|\cdot\rangle$로 표기하고 '켓 벡터'라고 읽는다. 반면에 행벡터는 $\langle\cdot|$로 표기하고 '브라 벡터'라고 읽는다.
- **정의 1.4.** 두 상태 $|0\rangle$, $|1\rangle$와 $|\alpha|^2+|\beta|^2=1$을 만족하는 두 복소수 α, β에 대하여 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$와 같은 상태를 중첩 상태라 한다. 즉, 중첩 상태는 큐비트들의 확률적 결합을 말한다.
- **정의 1.5.** 중첩 상태 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$에서 α, β를 각각 $|0\rangle$과 $|1\rangle$의 확률 진폭이라 한다.
- **참고 1.6 (양자 측정).** 양자 측정 후의 큐비트에서는 중첩 상태를 확인할 수 없다. 즉, 중첩 상태 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$를 측정하면 측정값으로 0, 1 중 하나만 얻을 수 있다.
- **정리 1.7 (Born의 규칙).** 중첩 상태 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$가 0으로 측정 될 확률은 $|\alpha|^2=\alpha\cdot\alpha^*$와 같고 1으로 측정 될 확률은 $|\beta|^2=\beta\cdot\beta^*$와 같다. 즉, 중첩 상태 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$에서 0과 1로 측정될 확률은 각각 해당 상태에 대한 확률 진폭의 절댓값을 제곱한 것과 같다. 이를 Born의 규칙이라 한다.
- **정의 1.8.** 입/출력 레지스터가 n-큐비트 양자 레지스터로 주어졌을 때, 집합 $\{0, 1, \cdots, N-1\}$에 대하여 균등 중첩 상태 $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$를 입/출력 레지스터의 초기 상태 $|\psi_0\rangle$로 정의한다. (단, $N=2^n$)

양자 측정의 결과와 Born의 규칙의 엄밀한 정당화 과정은 공학적 도구를 이용한 시각화 자료를 통해 대체하고자 위 내용에서는 포함시키지 않았다. 이에 대한 자세한 과정은 제2절 '수업 자료 및 프로젝트 활동 과제

개발'에 제시하였다.

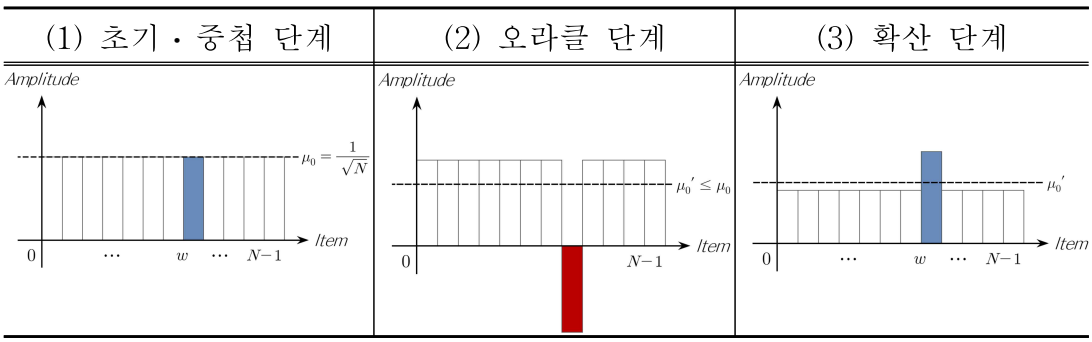
이상의 교수학적 변환을 종합하여 초기·중첩 단계에 대한 일반화된 지식을 다음과 같이 제안한다.

> Grover 알고리즘의 초기·중첩 단계는 n-큐비트 양자 레지스터로 준비된 입/출력 레지스터를 확률 진폭이 모두 균등한 중첩 상태로 초기화키는 단계이다. 즉, 해당 단계는 N개의 객체를 갖는 비정형 데이터베이스를 구성하는 단계로 볼 수 있다.

2.3. 오라클·확산 단계의 내용 요소 재구성

RGA 모델의 오라클 단계에서는 <표 Ⅳ-3>에서 제시한 두 집합 S, $S^{\perp}$의 정의를 내용 요소로 포함하지 않는다. 또한 오라클 함수 f의 정의 대신 식 4.1과 같이 주어지는 오라클 함수 $\hat{f}$의 정의를 내용 요소로 포함하며, 이로부터 함수 f에 대응하는 오라클 연산자 U_f 대신 함수 $\hat{f}$에 대응하는 오라클 연산자 $U_{\hat{f}}$의 정의를 내용 요소로 포함한다. 반면에 확산 단계에서 제외되는 내용 요소는 없다.

RGA 모델을 통해 탐색하고자 하는 목표 객체를 w라고 할 때, 초기·중첩 단계의 확률 진폭 그래프를 [그림 Ⅳ-2]-(1)와 같이 나타내면 오라클 단계의 확률 진폭 그래프는 [그림 Ⅳ-2]-(2)와 같이 목표 객체 w의 위상을 반전시켜 나타낼 수 있다.



[그림 Ⅳ-2] RGA 모델의 단계별 확률 진폭 그래프

또한 초기·중첩 단계에서의 확률 진폭의 평균을 μ_0, 오라클 단계에서의 확률 진폭의 평균을 μ_0'라고 하면 확산 단계의 확률 진폭 그래프는 [그림 Ⅳ-2]-(3)과 같이 나타낼 수 있다.

본 연구에서는 [그림 Ⅳ-2]와 같은 확률 진폭 그래프를 이용하여 내포적 정의에 해당하는 오라클 연산자 $U_{\hat{f}}$와 확산 연산자 R_{ψ_0}를 각각 정의 2.1, 정의 2.2와 같이 제3a수준에서 외연적으로 재정의하여 제시하였다.

- **정의 2.1.** [그림 Ⅳ-2]-(2)와 같이 초기·중첩 단계로부터 주어진 상태에서 목표 객체에 대한 상태의 위상을 반전시키는 연산자를 오라클 연산자라 하고, 기호 U로 표현한다.
- **정의 2.2.** [그림 Ⅳ-2]-(3)과 같이 오라클 단계로부터 주어진 상태를 확률 진폭의 평균을 기준으로 반전시키는 연산자를 확산 연산자라 하고, 기호 R로 표현한다.

물론 오라클 연산자 U의 경우 제3b수준에서 “초기·중첩 단계로부터 주어진 상태에서 목표 객체 w에 대하여 관계식 $U|w\rangle=-|w\rangle$을 만족하는 연산자 U를 오라클 연산자라 한다.”와 같이 내포적으로 정의할 수 있다. 그러나 주어진 문제에 따라 목표 객체 w를 특정할 수 없는 경우가 존재하며, 본 연구의 교육 프로그램에서는 이와 같은 프로젝트 활동 과제를 다룰 것이므로 해당 정의 방법을 내용 요소로 선정하지 않았다. 또한 확산 연산자의 경우, 기하학적인 관점에서 특정 상태에 대한 관계식을 도출할 수 없기 때문에 내포적으로 정의하지 않았다. 이에 따라 두 연산자의 정의 방식에 대한 통일성을 위해, 그리고 수학적 엄격함을 보다 낮추기 위해 제3b수준보다는 제3a수준에서 외연적으로 정의한 정의 2.1을 오라클 연산자의 정의로 선정하였다.

한편 RGA 모델의 반복 단계에서 최적의 반복 횟수를 구하는 대수적인 과정을 위해서는 기하학적 관점에서 정의된 오라클 연산자와 확산 연산자를 행렬 표현으로 나타낼 필요가 있다. 이는 증명과 함께 정리 2.4, 정리 2.5로 제시하였으며, 이에 앞서 앞으로 전개하고자 하는 논의의 기호를 간단히 하기 위한 표기 2.3을 도입하였다.

• **표기 2.3.** 집합 $\{0, 1, \cdots, N-1\}$을 A로 표기하고, 목표 객체가 $w \in A$로 주어진 경우 집합 $\{0, 1, \cdots, N-1\} \backslash \{w\}$를 B로 표기한다.

• **정리 2.4.** 목표 객체가 $w \in A$로 주어졌을 때, 오라클 연산자 U에 대하여 $\mathrm{U} = \mathrm{Id}^{\otimes n} - 2|w\rangle\langle w|$가 성립한다.

(증명)

초기 · 중첩 단계로부터 주어진 상태 $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in A} |x\rangle$에 대하여

$$\mathrm{U}|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B} |x\rangle - \frac{1}{\sqrt{N}} |w\rangle \cdots ㉠$$

이 성립함을 보이면 된다.

먼저 정규직교집합 $\{|0\rangle, |1\rangle, \cdots, |N-1\rangle\}$에 대하여

1) 임의의 $a \in A$에 대하여 $\langle a|a\rangle = 1$

2) 서로 다른 $a_1, a_2 \in A$에 대하여 $\langle a_1|a_2\rangle = \langle a_2|a_1\rangle = 0$

이므로 목표 객체 w와 임의의 $x \in B$에 대하여 다음을 계산할 수 있다.

① $\mathrm{U}|x\rangle = (\mathrm{Id}^{\otimes n} - 2|w\rangle\langle w|)|x\rangle$
$= |x\rangle - 2|w\rangle\langle w|x\rangle$
$= |x\rangle - 2|w\rangle \cdot 0 = |x\rangle$

② $\mathrm{U}|w\rangle = (\mathrm{Id}^{\otimes n} - 2|w\rangle\langle w|)|w\rangle$
$= |w\rangle - 2|w\rangle\langle w|w\rangle$
$= |w\rangle - 2|w\rangle \cdot 1 = -|w\rangle$

따라서 ①, ②를 이용하여 정리하면

$$\mathrm{U}|\psi_0\rangle = \mathrm{U}\left(\frac{1}{\sqrt{N}} \sum_{x \in A} |x\rangle\right) = \mathrm{U}\left(\frac{1}{\sqrt{N}} \sum_{x \in B} |x\rangle + \frac{1}{\sqrt{N}} |w\rangle\right)$$
$$= \frac{1}{\sqrt{N}} \left(\sum_{x \in B} \mathrm{U}|x\rangle + \mathrm{U}|w\rangle\right) = \frac{1}{\sqrt{N}} \left(\sum_{x \in B} |x\rangle - |w\rangle\right)$$
$$= \frac{1}{\sqrt{N}} \sum_{x \in B} |x\rangle - \frac{1}{\sqrt{N}} |w\rangle$$

이므로 ㉠이 성립한다. □

• **정리 2.5.** 확산 연산자 R에 대하여 $\mathrm{R} = 2|\psi_0\rangle\langle\psi_0| - \mathrm{Id}^{\otimes n}$가 성립한다.

(증명)

오라클 단계로부터 주어진 상태를 $\mathrm{U}|\psi_0\rangle = \sum_{x \in A} c_x |x\rangle$라 할 때,

$$\mathrm{RU}|\psi_0\rangle = \sum_{x \in A} (2\mu_0 - c_x)|x\rangle$$

이 성립함을 보이면 된다.

먼저 각각의 $x \in A$에 대하여 우변의 확률 진폭 값을 계산한다. 정리 2.4의 증명 ㉠으로부터 임의의 $x \in B$에 대하여 $c_x = \frac{1}{\sqrt{N}}$이고, $x = w$에 대하여 $c_w = -\frac{1}{\sqrt{N}}$이므로 확률 진폭의 평균 μ_0는

$$\mu_0 = \frac{1}{N} \cdot \sum_{x \in A} c_x = \frac{1}{N} \cdot \left(\frac{N-1}{\sqrt{N}} - \frac{1}{\sqrt{N}} \right) = \frac{N-2}{N\sqrt{N}}$$

와 같다. 따라서 다음을 계산할 수 있다.

(1) 임의의 $x \in B$에 대하여

$$2\mu_0 - c_x = \frac{N-4}{N\sqrt{N}}$$

(2) $x = w$에 대하여

$$2\mu_0 - c_w = \frac{3N-4}{N\sqrt{N}}$$

다음으로 좌변을 계산한다. 정리 2.4의 증명에서 ㉠은

$$\mathrm{U}|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B} |x\rangle - \frac{1}{\sqrt{N}} |w\rangle = |\psi_0\rangle - \frac{2}{\sqrt{N}} |w\rangle$$

와 같이 나타낼 수 있다. 그러면 정리 2.4의 ①, ②로부터

$$\begin{aligned} \mathrm{RU}|\psi_0\rangle &= \left(2|\psi_0\rangle\langle\psi_0| - \mathrm{Id}^{\otimes n}\right)\left(|\psi_0\rangle - \frac{2}{\sqrt{N}}|w\rangle\right) \\ &= 2|\psi_0\rangle\langle\psi_0|\psi_0\rangle - |\psi_0\rangle - 2 \cdot \frac{2}{\sqrt{N}} |\psi_0\rangle\langle\psi_0|w\rangle + \frac{2}{\sqrt{N}}|w\rangle \\ &= \frac{N-4}{N}|\psi_0\rangle + \frac{2}{\sqrt{N}}|w\rangle \quad \cdots ㉡ \end{aligned}$$

와 같고, ㉡을 다시 두 상태 $|x\rangle$, $|w\rangle$에 대해서 정리하면

$$\mathrm{RU}|\psi_0\rangle = \sum_{x \in B} \frac{N-4}{N\sqrt{N}}|x\rangle + \frac{3N-4}{N\sqrt{N}}|w\rangle$$

와 같다. 따라서 (좌변)=(우변)이 성립한다. □

이와 같이 정의 2.1 ~ 정리 2.5를 이용한 오라클 · 확산 단계의 도입 방식은 RGA 모델의 오라클 함수 $\hat{f}$, 오라클 연산자 $\mathrm{U}_{\hat{f}}$을 내용 요소로 포함하지 않으며, 이들의 하위 요소인 사영 연산자, 직교 사영 연산자, 반사 연산자 등 역시 포함하지 않는다.

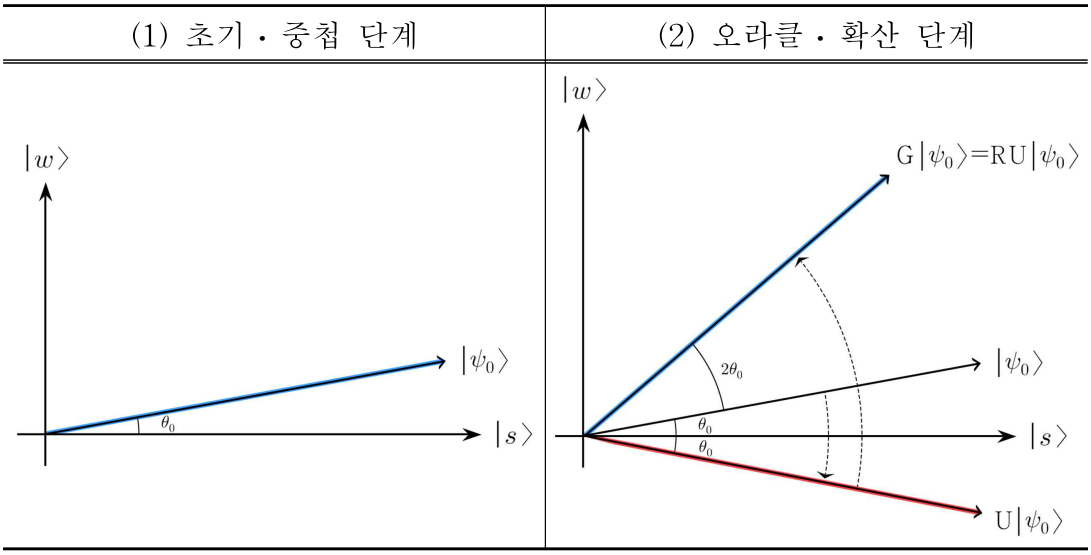
이상의 교수학적 변환을 종합하여 오라클 단계와 확산 단계에 대한 일반화된 지식을 다음과 같이 제안한다.

Grover 알고리즘의 오라클 단계는 초기・중첩 단계로부터 주어진 상태에서 목표 객체에 대한 상태의 위상을 반전시키는 단계이다. 즉, 해당 단계는 데이터베이스로에서 목표 객체를 특정화하는 단계로 볼 수 있다. 이때 확률 진폭의 평균은 초기・중첩 단계보다 작아진다.

Grover 알고리즘의 확산 단계는 오라클 단계로부터 주어진 상태를 확률 진폭의 평균을 기준으로 반전시키는 단계이다. 즉, 해당 단계는 모든 객체가 동일한 확률 진폭을 갖는 비정형 데이터베이스에서 목표 객체의 확률 진폭을 높이고 나머지 객체들의 확률 진폭을 낮추는 단계로 볼 수 있다.

2.4. 반복 단계의 내용 요소 재구성

RGA 모델의 반복 단계에서는 <표 Ⅳ-5>에서 제시한 두 축약 밀도 연산자 ρ^A, ρ^B의 정의를 내용 요소로 포함하지 않으며, 이들의 하위 요소인 밀도 연산자, 부분 대각합, 순수 상태, 혼합 상태 등 역시 포함하지 않는다. 반면에 일반적인 Grover 알고리즘의 모델에 맞게 정의된 Grover 연산자 G, k번 Grover 반복 후의 상태 $|\hat{\psi}_k\rangle$, 각 θ_k의 정의 등은 RGA의 모델에 맞춰 재정의할 필요가 있다.



[그림 Ⅳ-3] RGA 모델의 단계별 평면 벡터 그래프

내포적 정의에 해당하는 Grover 연산자 G는 기하학적인 관점을 통해 외연적으로 재정의할 수 있다. 이를 위해서는 먼저 [그림 Ⅳ-3]-(1)에서 각 θ_0를 정의하고, 오라클 단계와 확산 단계를 [그림 Ⅳ-3]-(2)와 같은 평면 벡터 그래프로 나타내야 한다.

먼저 각 θ_0는 동의적 정의 유형의 기호화에 해당하는 표기 3.1과 계산 및 시각화 요소에 해당하는 참고 3.2를 이용하여 표기 3.3과 같이 제2b수준에서 외연적으로 재정의하여 제시하였다.

- **표기 3.1.** 목표 객체가 $w \in A$로 주어졌을 때, 상태 $|w\rangle$를 제외한 나머지 상태들에 대하여 균등 중첩 상태 $\sum_{x \in B} \frac{1}{\sqrt{N-1}} |x\rangle$를 기호 $|s\rangle$로 표기한다.
- **참고 3.2.** 상태 $|s\rangle$를 이용하면 초기 · 중첩 단계로부터 주어진 상태 $|\psi_0\rangle$를 다음과 같이 나타낼 수 있다.

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{N}} \sum_{x \in B} |x\rangle + \frac{1}{\sqrt{N}} |w\rangle \\ &= \frac{\sqrt{N-1}}{\sqrt{N}} \sum_{x \in B} \frac{1}{\sqrt{N-1}} |x\rangle + \frac{1}{\sqrt{N}} |w\rangle \\ &= \frac{\sqrt{N-1}}{\sqrt{N}} |s\rangle + \frac{1}{\sqrt{N}} |w\rangle \end{aligned}$$

  이때 상태 $|\psi_0\rangle$는 목표 객체 w에 대한 상태 $|w\rangle$와 상태 $|s\rangle$가 생성하는 2차원 평면에 [그림 Ⅳ-3]-(1)과 같이 나타낼 수 있다.
- 표기 **3.3.** [그림 Ⅳ-3]-(1)에서 $[0, \pi/2]$에 속하면서 두 상태 $|s\rangle$와 $|\psi_0\rangle$가 이루는 각을 기호 θ_0로 표기한다.

그다음 [그림 Ⅳ-3]-(2)는 각 θ_0에 대한 두 삼각함수 값을 제시하는 정리 3.4와 삼각함수의 덧셈정리에 해당하는 보조 정리 3.5를 이용하여 정리 3.5와 같이 도입하였다. 이때 해당 내용 요소들의 정당화 과정을 이해하기 위해서는 고등학교 수학과 일반선택 과목 <기하>의 '평면벡터의 내적' 그리고 <선형대수학>의 '벡터와 행렬의 전치(transpose)'와 '유니터리 행렬'에 대한 이해가 선행되어야 한다.

• **정리 3.4.** 각 θ_0에 대하여 $\cos\theta_0 = \frac{\sqrt{N-1}}{\sqrt{N}}$와 $\sin\theta_0 = \frac{1}{\sqrt{N}}$가 성립한다.

(증명)

초기 · 중첩 단계로부터 주어진 상태 $|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{x\in A}|x\rangle$와 상태 $|s\rangle$에 대하여 내적의 정의에 의해

$$\langle\psi_0|s\rangle = |\psi_0||s|\cos\theta_0$$

이 성립하므로 $|\psi_0|$, $|s|$, $\langle\psi_0|s\rangle$를 구하면 된다.

먼저 정규직교관계를 이용하면 다음을 계산할 수 있다.

① $|\psi_0|^2 = \langle\psi_0|\psi_0\rangle = \frac{1}{N}\left(\sum_{x\in A}\langle x|x\rangle + 0\right) = \frac{N}{N} = 1$이므로 $|\psi_0| = 1$

② $|s|^2 = \langle s|s\rangle = \frac{1}{N-1}\left(\sum_{x\in B}\langle x|x\rangle + 0\right) = \frac{N-1}{N-1} = 1$이므로 $|s| = 1$

③ $\langle w|s\rangle = \frac{1}{\sqrt{N-1}}\sum_{x\in B}\langle w|x\rangle = \frac{1}{\sqrt{N-1}}\cdot 0 = 0$

그러면 참고 3.2에서 $\langle\psi_0| = \frac{\sqrt{N-1}}{\sqrt{N}}\langle s| + \frac{1}{\sqrt{N}}\langle w|$이므로 ②, ③에 의해

$$\langle\psi_0|s\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}\langle s|s\rangle + \frac{1}{\sqrt{N}}\langle w|s\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} \quad \cdots ④$$

이 성립한다.

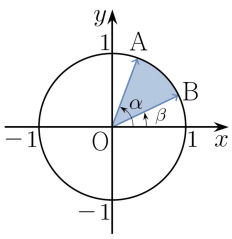
따라서 ㉠에 ①, ②, ④를 대입하면 $\cos\theta_0 = \frac{\sqrt{N-1}}{\sqrt{N}}$임을 알 수 있다.

또한, 관계식 $\sin^2\theta_0 + \cos^2\theta_0 = 1$로부터 $\sin\theta_0 = \frac{1}{\sqrt{N}}$가 성립한다. □

• **보조 정리 3.5 (코사인함수의 덧셈정리).** 임의의 두 각 α, β에 대하여 등식 $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$가 성립한다.

(증명)

오른쪽 그림과 같이 원점을 중심으로 하는 단위원 위의 두 점 A, B에 대하여 두 벡터 $\overrightarrow{OA}$, $\overrightarrow{OB}$가 x축의 양의 방향과 이루는 각의 크기를 각각 α, β라 하자. 그러면 내적의 정의에 의해



$$\overrightarrow{OA}\cdot\overrightarrow{OB} = |\overrightarrow{OA}||\overrightarrow{OB}|\cos(\alpha-\beta) = \cos(\alpha-\beta)$$

이 성립한다.

또한, 두 점 A, B의 좌표를 $A(\cos\alpha,\ \sin\alpha)$, $B(\cos\beta,\ \sin\beta)$로 나타낼 수 있으므로 내적의 성질에 의해

$$\overrightarrow{OA}\cdot\overrightarrow{OB}=\cos\alpha\cos\beta-\sin\alpha\sin\beta$$

가 성립한다.

따라서 ㉠, ㉡에 의해 $\cos(\alpha+\beta)=\cos\alpha\cos\beta-\sin\alpha\sin\beta$가 성립한다. □

• **정리 3.6.** $RU|\psi_0\rangle$는 [그림 Ⅳ-3]-(2)와 같이 초기 상태 $|\psi_0\rangle$를 $|w\rangle$-축 방향으로 $2\theta_0$만큼 회전시킨 것과 같다.

(증명)

두 평면벡터 $|\psi_0\rangle$와 $RU|\psi_0\rangle$가 이루는 각을 θ^*라 할 때,

$$\cos\theta^*=\cos 2\theta_0$$

이 성립함을 보이면 된다.

먼저 보조 정리 3.5에 의해 우변의 값은

$$\cos 2\theta_0=1-2\sin^2\theta_0=1-2\cdot\frac{1}{N}=\frac{N-2}{N}$$

와 같이 계산할 수 있다.

다음으로 좌변의 값을 계산한다. 먼저 내적의 정의에 의해

$$\langle\psi_0|RU|\psi_0\rangle=|\psi_0||RU\psi_0|\cos\theta^*\ \cdots ㉠$$

이 성립한다. 정리 3.5의 증명 ①에서 $|\psi_0|=1$임을 구하였으므로 $|RU\psi_0|$, $\langle\psi_0|RU|\psi_0\rangle$의 값만 구하면 된다. 이는 다음과 같이 계산할 수 있다.

① $|RU\psi_0|^2=(RU|\psi_0\rangle)^T\cdot RU|\psi_0\rangle=\langle\psi_0|U^TR^TRU|\psi_0\rangle$

$=\langle\psi_0|U^T\cdot Id^{\otimes n}\cdot U|\psi_0\rangle=\langle\psi_0|U^TU|\psi_0\rangle$

$=\langle\psi_0|Id^{\otimes n}|\psi_0\rangle=\langle\psi_0|\psi_0\rangle=1$

(∵ R, U: 유니터리 행렬)이므로 $|RU\psi_0|=1$

② 정리 2.5의 증명 ㉡에 의해 $RU|\psi_0\rangle=\frac{N-4}{N}|\psi_0\rangle+\frac{2}{\sqrt{N}}|w\rangle$이므로

$$\langle\psi_0|RU|\psi_0\rangle=\frac{N-4}{N}\langle\psi_0|\psi_0\rangle+\frac{2}{\sqrt{N}}\langle\psi_0|w\rangle$$

$$=\frac{N-4}{N}\cdot 1+\frac{2}{\sqrt{N}}\cdot\frac{1}{\sqrt{N}}\sum_{x\in A}\langle x\,|\,w\rangle$$

$$=\frac{N-4}{N}+\frac{2}{N}\cdot 1=\frac{N-2}{N}$$

따라서 ㉠에 ①, ②를 대입하면 $\cos\theta^{*} = \frac{N-2}{N}$임을 알 수 있다.

그러므로 (좌변)=(우변)이 성립한다. □

이상의 내용으로부터 본 연구에서는 정리 3.6과 같은 기하학적인 관점을 이용하여 내포적 정의에 해당하는 Grover 연산자를 정의 3.7과 같이 제3b수준에서 외연적으로 재정의하여 제시하였다.

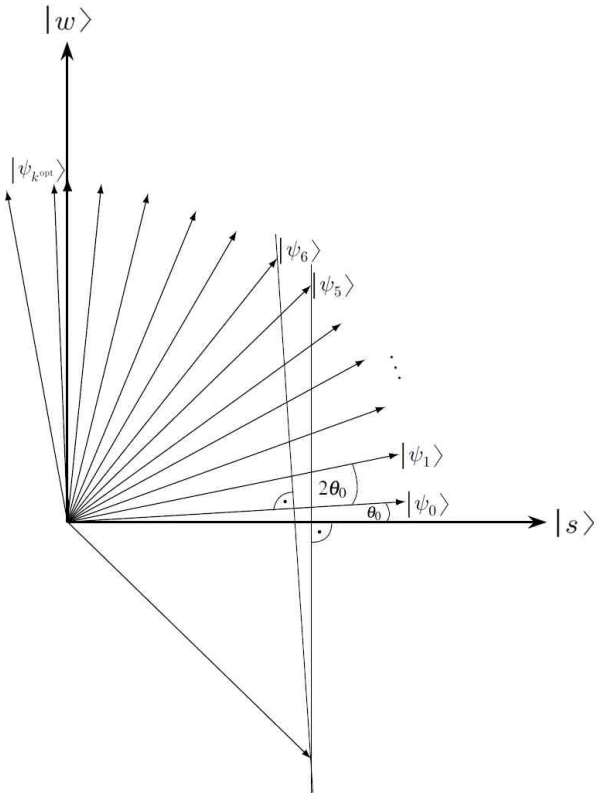
- **정의 3.7.** [그림 Ⅳ-3]-(2)와 같이 초기·중첩 단계로부터 주어진 상태에 오라클 연산자와 확산 연산자를 순차적으로 작용시켜 $\langle w|$-축 방향으로 $2\theta_0$만큼 회전시키는 연산자를 Grover 연산자라 하고, 기호 G로 표현한다. 즉, G = RU이다.

마지막으로 RGA 모델을 기준으로 k번 Grover 반복 후의 상태 $|\psi_k\rangle$와 각 θ_k를 재정의한 후, 이에 맞춰 최적의 반복 횟수 k^{opt}를 구하기 위한 대수적인 과정을 재기술해야 한다. 먼저 동의적으로 정의된 k번 Grover 반복 후의 상태 $|\psi_k\rangle$에 대하여 각 θ_k를 정의 4.1과 같이 제2b수준에서 내포적으로 재정의하여 제시하였고, Grover 연산자의 정의로부터 도출 가능한 정리 4.2를 증명 없이 제시하였다. 이때 각 θ_k를 외연적으로 정의하지 않고 내포적으로 정의한 이유는 표기 3.3에서 [그림 Ⅳ-3]-(1)을 통해 정의된 각 θ_0와 이후에 등장할 [그림 Ⅳ-4]로부터 이의 시각적인 이미지를 충분히 유추할 수 있기 때문이다.

- **표기 4.1.** k번 Grover 반복 후의 상태를 기호 $|\psi_k\rangle$로 나타낼 때, $[0, \pi/2]$에 속하면서 두 상태 $|s\rangle$와 $|\psi_k\rangle$가 이루는 각을 기호 θ_k로 표기한다.
- **정리 4.2.** 음이 아닌 정수 k에 대하여 $\theta_k = (2k+1)\theta_0$이 성립한다.

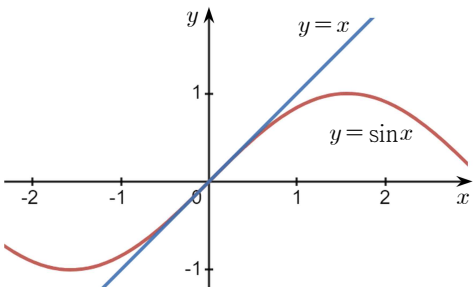
다음으로 Grover 반복의 최적 반복 횟수를 정리 4.5로 제시하면서 이에 대한 정당화 과정을 보조 정리 4.3과 참고 4.4를 이용하여 제시하였다. 이때 [그림 Ⅳ-4]는 [그림 Ⅱ-10](Scherer, 2019, p. 332)을 RGA 모델에

맞춰 개작한 것이다.



[그림 Ⅳ-4] RGA 모델에서 Grover 반복의 기하학적 의미

- **보조 정리 4.3 (작은 각도 근사).** 오른쪽 그림에서 확인할 수 있듯이 θ가 충분히 작을 때, 사인함수에 대하여 $\sin\theta \approx \theta$가 성립한다.



- **참고 4.4.** k번 Grover 반복 후의 상태 $|\psi_k\rangle$는 k가 증가함에 따라 목표 객체 w에 대한 상태 $|w\rangle$를 향해 회전한다. 그러나 그 회전 정도는 매우 작기 때문에 탐색의 성공 확률을 높이기 위해서는 Grover 연산자를 여러 번 적용해야 한다. 이때 [그림 Ⅳ-4]를 보면 상태 $|\psi_k\rangle$를 상태 $|w\rangle$에 최대한 가까워지는 최적의 반복 횟수가 $\theta_{k^{opt}} = \pi/2$를 만족하는 횟수 k^{opt}로 존재함을 알 수 있다.

• **정리 4.5.** Grover 반복의 최적 횟수는 $k^{\mathrm{opt}} \approx \frac{\pi}{4}\sqrt{N}$이다.

(증명)

정리 3.4에 의해 $\sin\theta_0 = \frac{1}{\sqrt{N}}$이므로 N이 충분히 커지는 경우 작은 각도 근사에 의해 $\theta_0 \approx \frac{1}{\sqrt{N}}$이 성립한다.

한편 참고 4.4에서 살펴보았듯이 최적 반복 횟수 k^{opt}는 $\theta_{k^{\mathrm{opt}}} = \frac{\pi}{2}$일 때 달성되므로 정리 4.2에 의해 $(2k^{\mathrm{opt}}+1)\theta_0 = \frac{\pi}{2}$이 성립한다.

따라서 이상의 내용을 종합하면

$$k^{\mathrm{opt}} = \left\lfloor \frac{\pi}{4\theta_0} - \frac{1}{2} \right\rfloor = \left\lfloor \frac{\pi}{4\theta_0} \right\rfloor \approx \frac{\pi}{4}\sqrt{N}$$

임을 알 수 있다. □

이상의 교수학적 변환을 종합하여 반복 단계에 대한 일반화된 지식을 다음과 같이 제안한다.

Grover 알고리즘의 반복 단계는 초기·중첩 단계로부터 주어진 상태에 오라클 연산자와 확산 연산자의 순차적 작용인 Grover 연산자를 여러 번 적용시켜 해당 상태를 목표 객체에 대한 상태에 최대한 가까워질 수 있도록 회전시키는 단계이다.

3. Grover 알고리즘 내용 체계 재구조화 제안

여기서는 교수학적 변환을 통해 제시한 내용 요소들과 일반화된 지식을 종합하여 RGA 모델을 기준으로 재구조화된 Grover 알고리즘 내용 체계를 제안한다. 이때 교수학적 변환 과정에서 선지식으로서 제시된 <기하>와 <선형대수학>의 내용들은 첫 번째 핵심 개념[28]인 '벡터와 행렬'의 내용 요소로 제시하였다. 전반적인 내용 체계는 <표 Ⅳ-7>과 같다.

28) 핵심 개념이란, 교과의 기초 개념이나 원리를 말한다(교육부, 2015).

<표 Ⅳ-7> 재구조화된 Grover 알고리즘 내용 체계

영역	핵심 개념	내용 요소	하위 요소
RGA 모델의 수학적 구조	벡터와 행렬	• 평면벡터의 내적 • 벡터와 행렬의 전치 • 유니터리 행렬 • 정규직교집합	• 두 평면벡터 사이의 각 • 벡터와 행렬의 연산 • 정사각 행렬 • 단위 벡터와 직교 벡터
		(일반화된 지식) 벡터는 크기와 방향을 갖는 양을 표현하여 탐구하는 도구이고, 행렬은 수와 문자를 배열하여 탐구하는 도구이다.	
	초기・중첩 단계	• 양자 레지스터 • n-큐비트 양자 레지스터 • 초기 상태(균등 중첩 상태) • 비정형 데이터베이스	• bra-ket 표기법 • 중첩 상태(확률적 결합) • 확률 진폭 • 양자 측정과 Born의 규칙
		(일반화된 지식) 초기・중첩 단계는 n-큐비트 양자 레지스터로 준비된 입/출력 레지스터를 확률 진폭이 모두 균등한 중첩 상태로 초기화키는 단계이다. 즉, 해당 단계는 N개의 객체를 갖는 비정형 데이터베이스를 구성하는 단계로 볼 수 있다.	
	오라클 단계	• 오라클 연산자 • 오라클 연산자의 행렬 표현 • 목표 객체의 특정화	• 확률 진폭 그래프 • 위상 반전 • 정규직교집합
		(일반화된 지식) 오라클 단계는 초기・중첩 단계로부터 주어진 상태에서 목표 객체에 대한 상태의 위상을 반전시키는 단계이다. 즉, 해당 단계는 데이터베이스로부터 목표 객체를 특정화하는 단계로 볼 수 있다. 이때 확률 진폭의 평균은 초기・중첩 단계보다 작아진다.	
	확산 단계	• 확산 연산자 • 확산 연산자의 행렬 표현 • 목표 객체의 확률 증가	• 확률 진폭 그래프 • 평균에 대한 반전 • 정규직교집합
		(일반화된 지식) 확산 단계는 오라클 단계로부터 주어진 상태를 확률 진폭의 평균을 기준으로 반전시키는 단계이다. 즉, 해당 단계는 최종적으로 모든 객체가 동일한 확률 진폭을 갖는 비정형 데이터베이스로부터 목표 객체의 확률 진폭을 높이고 나머지 객체들의 확률 진폭을 낮추는 단계로 볼 수 있다.	
	반복 단계	• Grover 연산자 • Grover 반복 • Grover 반복의 최적 횟수 • 벡터의 회전	• 2차원 평면 벡터 그래프 • 코사인함수의 덧셈정리 • 작은 각도 근사 • 두 평면벡터 사이의 각
		(일반화된 지식) 반복 단계는 초기・중첩 단계로부터 주어진 상태에 오라클 연산자와 확산 연산자의 순차적 작용인 Grover 연산자를 여러 번 적용시켜 해당 상태를 목표 객체에 대한 상태에 최대한 가까워질 수 있도록 회전시키는 단계이다.	

한편 Grover 알고리즘의 수학적 구조를 이해하고, 이를 바탕으로 IBM QX의 양자 회로 구성 편집기에서 주어진 문제를 해결하기 위해서는 '양자 게이트'와 '양자 회로'에 대한 이해가 필요하다. 이에 따라 이론적 배경의 제2절을 바탕으로 해당 내용 체계를 <표 Ⅳ-8>와 같이 제안하였다. 이때 양자 게이트는 재구조화된 Grover 알고리즘 내용 체계의 정의 수준에 맞춰 n겹 힐베르트 공간 상에서 유니터리 변환으로 기술되는 정의를 $n \times n$ 유니터리 행렬로 기술하여 그 엄격함의 수준을 제한하였다.

<표 Ⅳ-8> 재구조화된 양자 게이트와 양자 회로의 내용 체계

영역	핵심 개념	내용 요소	하위 요소
양자 게이트와 양자 회로	양자 게이트와 양자 회로	• 양자 게이트 • 양자 회로도 • 직렬 연산과 행렬 표현 • 병렬 연산과 행렬 표현	• 단일, 다중 큐비트 게이트 • 양자선과 입/출력 큐비트 • 유니터리 행렬 • 되돌릴 수 있는[가역] 계산
		(일반화된 지식) 양자 컴퓨터에서 보다 복잡한 계산을 수행하기 위해 양자 게이트들을 연결한 것을 양자 회로라 하고, 다이어그램을 이용하여 양자 회로를 가시화한 것을 양자 회로도라 한다.	
	단일 큐비트 게이트	• 2×2 유니터리 행렬	• X, Z, 아다마르 게이트
		(일반화된 지식) 단일 큐비트 게이트는 1 - 큐비트에 작용하면서 2×2 유니터리 행렬로 기술된다.	
	다중 큐비트 게이트	• 제어형 양자 게이트 • 4×4 유니터리 행렬 • 8×8 유니터리 행렬	• 제어형 X, Z 게이트 • 토폴리 게이트 • 제어-제어형 Z 게이트
		(일반화된 지식) 다중 큐비트 게이트는 n - 큐비트에 작용하면서 $n \times n$ 유니터리 행렬로 기술된다.	

제 2 절 Grover 알고리즘 교육 프로그램 개발

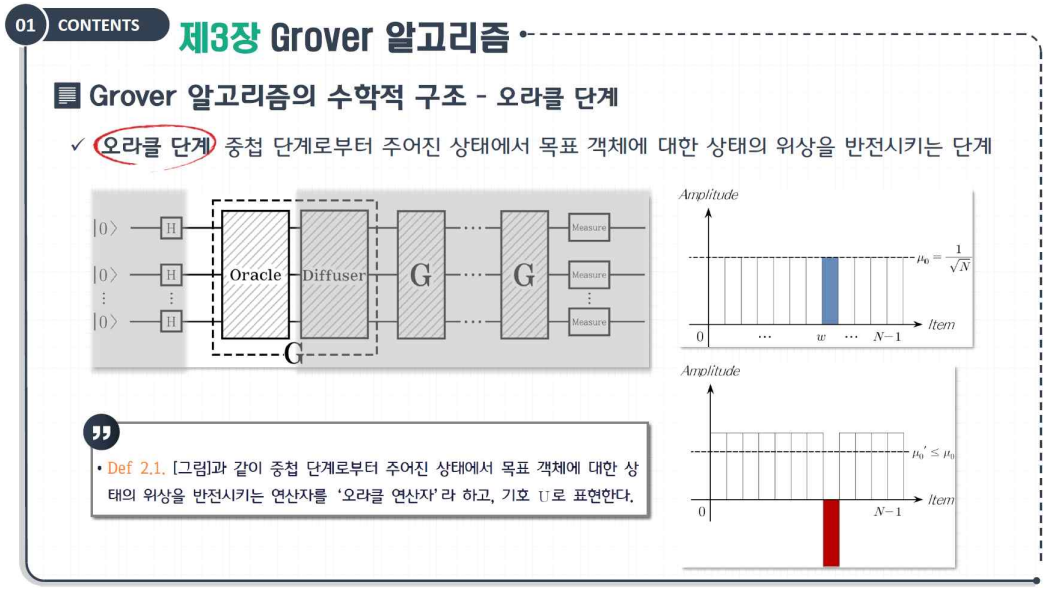
본 절에서는 제3장 연구 방법의 <표 Ⅲ-1>과 같은 Grover 알고리즘 교육 프로그램에 활용할 수 있는 수업 자료와 과제를 제시한다. 또한 중등교육 기관 학생들을 대상으로 적용한 교수 실험을 통해 수정·보완 과정을 거친 교수·학습 과정을 제시한다.

1. 수업 자료 및 과제 개발

본 연구에서 개발한 교육 프로그램은 이론 학습 및 실습 과정과 프로젝트 활동으로 구성되어 있다. 학습자들은 교수자가 제시한 수업 자료를 통해 차시별 학습 주제를 온전히 이해하였으며, 실습 과정을 통해 IBM QX의 양자 회로 구성 편집기에 대한 사용법을 충분히 익혔다. 또한 이를 바탕으로 Grover 알고리즘을 이용하여 주어진 문제를 해결하는 프로젝트 활동을 수행하였다. 해당 프로젝트 활동은 Grover 알고리즘의 적용 단계, 응용 단계, 심화 단계로 구성되어 있다. 여기서는 이론 학습 과정과 실습 및 프로젝트 활동 과정에서 활용한 수업 자료와 과제를 설명한다.

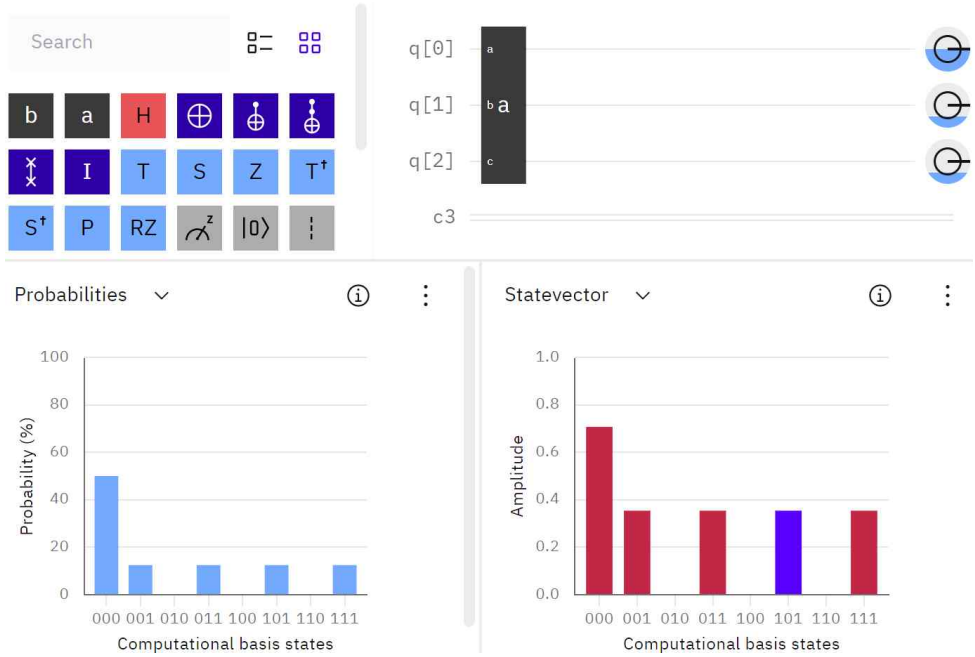
1.1. 수업 자료 개발

이론 학습 과정에서는 <표 Ⅳ-7>, <표 Ⅳ-8>에서 제시한 내용 요소들의 학습이 이루어졌다. [그림 Ⅳ-5]는 본 교육 프로그램의 4차시 수업에서 활용한 수업 자료의 예시이다.

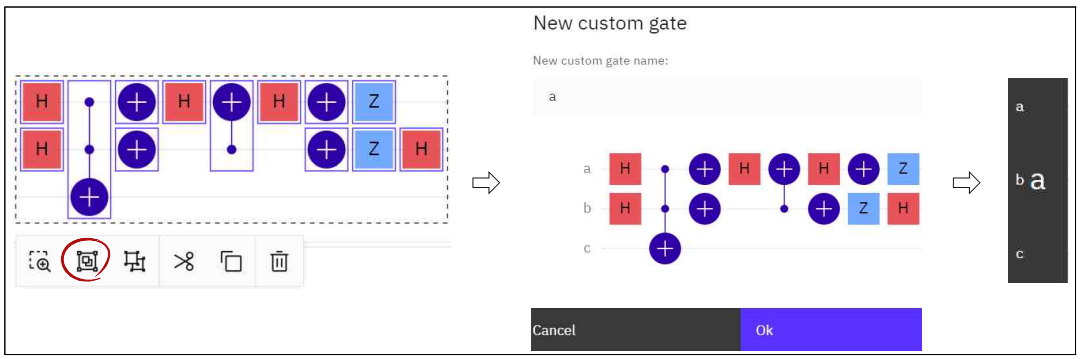


[그림 Ⅳ-5] Grover 알고리즘 교육 프로그램 4차시 수업 자료의 예시

해당 과정에서 Born의 규칙(정리 1.7)을 시각화하여 전달하고, 동시에 실물 양자 컴퓨터의 결과에 노이즈(noise)가 있음을 안내하기 위해 제3장의 [그림 Ⅲ-7]과 아래의 [그림 Ⅳ-6]을 제공하였다. 이때 학생들이 확률 진폭과 측정 확률값에 주목할 수 있도록 주어진 양자 회로를 그룹화하여 회로의 구조가 나타나지 않도록 제시하였다. 이는 IBM QX의 커스터마이즈(customize) 기능을 통해 수행할 수 있으며, 그룹화하고자 하는 회로를 드래그한 후 [그림 Ⅳ-7]과 같은 순서로 이용할 수 있다.

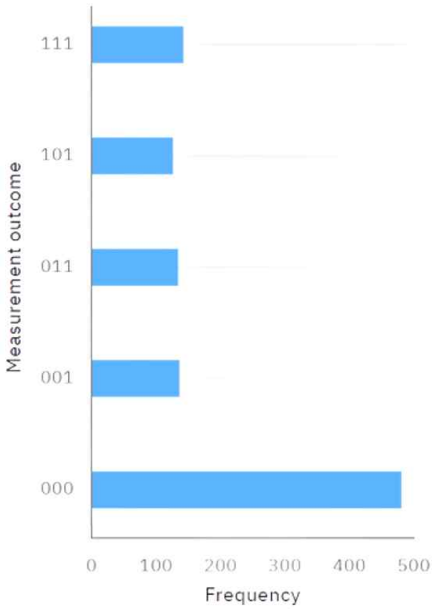


[그림 Ⅳ-6] Born의 규칙의 정당화를 위한 시각화 자료



[그림 Ⅳ-7] 커스터마이즈 기능을 활용한 양자 회로 a의 정의

또한 학생들에게 양자 측정(참고 1.6)의 결과를 시각화하여 전달하기 위해 [그림 Ⅳ-6]에서 주어진 양자 회로 a의 시뮬레이션의 결과를 아래의 [그림 Ⅳ-8]과 같이 제공하였으며, 동시에 제3장에서 제시한 [그림 Ⅲ-8]을 활용하였다.



[그림 Ⅳ-8] 양자 회로 a의 시뮬레이션 결과

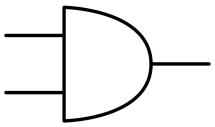
1.2. 실습 및 프로젝트 활동 과제 개발

실습 과정에서 학습자들에게 주어진 과제는 문제 5.1과 같다. 문제 5.1은 양자 컴퓨터 내에서 고전 논리 게이트를 구현함으로써 IBM QX의 사용법을 익히고, 프로젝트 활동에서 필요한 논리 연산 게이트를 얻는 것을 목적으로 설계되었다.

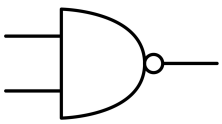
프로젝트 활동 과정의 적용 단계에서 학습자들에게 주어진 과제는 문제 5.2와 같다. 문제 5.2는 비구조적 탐색 문제에서 목표 객체가 주어진 경우로, 정답에 해당하는 양자 회로에서 오라클 연산자와 확산 연산자의 행렬 표현을 각각 정리 2.4, 정리 2.5를 이용하여 수학적으로 구할 수 있도록 설계되었다.

• **문제 5.1.** 다음은 고전 컴퓨터의 AND, NAND, OR, XOR 게이트들의 심볼과 진리표이다. 각각의 논리 게이트를 양자 게이트를 이용하여 구현하여라.

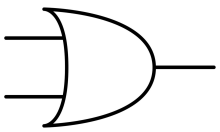
AND 게이트

진리표			심볼
x_1	x_2	$x_1 \wedge x_2$	
0	0	0	
0	1	0	
1	0	0	
1	1	1	

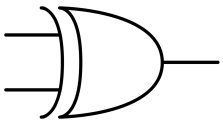
NAND 게이트

진리표			심볼
x_1	x_2	$\overline{x_1 \wedge x_2}$	
0	0	1	
0	1	1	
1	0	1	
1	1	0	

OR 게이트

진리표			심볼
x_1	x_2	$x_1 \vee x_2$	
0	0	0	
0	1	1	
1	0	1	
1	1	1	

XOR 게이트

진리표			심볼
x_1	x_2	$x_1 \oplus x_2$	
0	0	0	
0	1	1	
1	0	1	
1	1	0	

• **문제 5.2.** 비정형 데이터 베이스 {00, 01, 10, 11}가 주어진 비구조적 탐색 문제에 대하여 다음 물음에 답하여라.

(1) 객체 11을 목표 객체로 하는 양자 회로도를 작성하여라.

(2) 객체 01을 목표 객체로 하는 양자 회로도를 작성하여라.

(3) 객체 10을 목표 객체로 하는 양자 회로도를 작성하여라.

(4) 객체 00을 목표 객체로 하는 양자 회로도를 작성하여라.

프로젝트 활동 과정의 응용 단계에서는 목표 객체를 특정할 수 없는 문제를 제공하고자 하였다. 이에 본 연구에서는 응용 단계에서 학습자들에게 제공할 과제로 충족 가능성(satisfiability, 이하 SAT) 문제를 선정하였다. SAT 문제는 칩 테스트와 컴퓨터 디자인부터 이미지 분석과 소프트웨어 공학에 이르기까지 넓은 분야에서 응용되어 실용적으로 매우 중요한 문제이다(Dasgupta et al., 2008, p. 395).

SAT 문제는 참/거짓을 할당 받을 수 있는 부울(boolean) 변수에 대하여 논리곱 정규형(conjunctive normal form, 이하 CNF)으로 주어지는 논리식을 참으로 만드는 할당을 찾는 문제이다. CNF는 AND 연산자(∧)

로 연결된 절(clause)들의 모임이며, 각 절은 OR 연산자($\vee$)로 연결된 리터럴(literal)들로 구성된다. 여기서 리터럴은 부울 변수 x 또는 x의 부정 $\overline{x}$를 뜻한다.[29] 이때 모든 절 안에 리터럴의 개수가 정확히 k개로 주어진 경우를 k-SAT 문제라고 한다. 예컨대 다음 논리식의 충족 가능성을 살펴보는 것은 3-SAT 문제에 해당한다.

$$\left(x_1 \vee x_2 \vee x_3\right) \wedge \left(x_1 \vee \overline{x_2} \vee \overline{x_3}\right) \wedge \left(\overline{x_1} \vee \overline{x_2} \vee x_3\right) \tag{4.1}$$

3-SAT는 대표적인 $\mathcal{NP}$-완전 문제이며[30], 이외의 무수히 많은 문제들이 $\mathcal{NP}$-완전 문제라는 것에 대한 증명의 토대가 된다(Nielsen & Chuang, 2010, p. 149). 반면에 2-SAT 문제는 다항시간 내에 해결 가능한 $\mathcal{P}$ 문제에 해당한다.

프로젝트 활동 과정의 응용 단계에서 학습자들에게 주어진 과제는 문제 5.3과 같다. 문제 5.3은 2-SAT 문제로 IBM QX의 시각화 기능을 온전히 활용할 수 있도록 제한 큐비트 크기(8-큐비트) 이하의 비정형 데이터베이스 위에서 정의되었다. 한편 3-SAT 문제는 오라클 연산자를 구성함에 있어 제한 큐비트 크기 이상의 입/출력 레지스터가 필요하므로 포함시키지 않았다. 시각화 기능을 활용하지 않고 해결해야 하는 문제는 심화 단계에서 탐구해볼 수 있도록 구성하였다.

- **문제 5.3.** 다음의 논리식을 참으로 만드는 입력값을 구하여라.
  (1) $\left(x_1 \vee x_2\right) \wedge \left(\overline{x_1} \vee x_2\right) \wedge \left(\overline{x_1} \vee \overline{x_2}\right)$
  (2) $\left(x_1 \vee x_2\right) \wedge \left(x_1 \vee \overline{x_2}\right) \wedge \left(\overline{x_1} \vee x_2\right)$

문제 5.3은 비구조적 탐색 문제에서 목표 객체를 특정할 수 없는 경우에

---

29) x의 부정을 $\neg x$로 표현하기도 한다.
30) 단, 제약이 걸린 3-SAT 문제는 $\mathcal{P}$ 클래스에 해당할 수 있다. 예컨대 모든 절에 최대 하나의 긍정(positive) 리터럴만을 포함하는 호른식(Horn formula)은 $\mathcal{P}$ 문제에 해당한다(p. 397).

해당한다. 즉, 적용 단계의 과제(문제 5.2)처럼 정리 2.4를 이용하여 오라클 회로를 구성할 수 없다. 따라서 해당 과제는 IBM QX 내에서 상태 벡터 보기 기능과 확률 보기 기능을 활용하여 양자 게이트들을 조합해보고, 이를 바탕으로 각 절의 논리식을 만족하는 양자 게이트들을 구현함으로써 오라클 회로를 구성해야 한다.

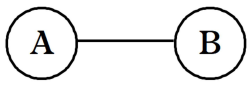
프로젝트 활동 과정의 심화 단계에서는 실세계의 문제를 수학적으로 탐구해보고, 이를 SAT 문제로 모델링한 후 Grover 알고리즘을 이용하여 해결할 수 있는 과제를 제공하고자 하였다. 이에 본 연구에서는 심화 단계에서 학습자들에게 제공할 문제로 그래프 색칠(Graph colo[u]ring) 문제를 선정하였다. 실세계에서 국가 또는 지역 구분을 위한 지도 색칠 문제, 무선 기지국 사이의 주파수 간섭을 없애기 위한 주파수 할당 문제, 스도쿠(number place) 문제 등은 일종의 그래프 색칠 문제로 볼 수 있다.

그래프 색칠 문제는 무향 그래프(undirected graph)가 주어졌을 때, 서로 인접한 꼭짓점(vertex)에는 같은 색을 칠하지 않으면서 모든 꼭짓점에 한 가지 색을 칠할 수 있는 방법을 찾는 문제이다. 이때 무향 그래프는 꼭짓점 v_1, v_2, …, v_n들의 집합 V와 변(edge) (v_i, v_j)들의 집합 E에 대하여 $G=(V, E)$로 정의된다. 한편 이러한 그래프 G에 대하여 채색수(chromatic number)가 k개로 주어진 경우를 k-coloring 문제라고 한다.

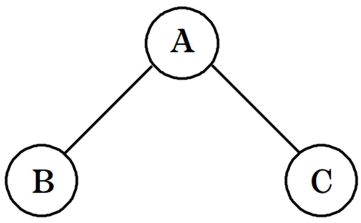
프로젝트 활동 과정의 심화 단계에서 학습자들에게 주어진 과제는 문제 5.4와 같다.

- **문제 5.4.** 다음과 같이 주어진 각각의 그래프에 두 가지 색(빨강, 파랑)을 이용하여 인접한 꼭짓점에는 같은 색을 칠하지 않으면서 각 꼭짓점에 한 가지 색을 칠할 수 있는 방법을 구하여라.

(1)



(2)



문제 5.4는 2-coloring 문제로 빨강색을 0, 파랑색을 1으로 표현하는 등 직관적인 방법을 통해 모델링할 수 있도록 설계되었다. 이때 논리식은 모델링의 방법에 따라 다양하게 도출될 수 있다. 단, 문제 5.4는 목표 객체가 2개인 경우로 RGA 모델을 이용하여 해결할 수 있는 문제에 해당하지 않는다. 즉, 해당 과제는 RGA 모델에서 일반적인 Grover 알고리즘의 모델로 사고의 확장을 위해 설계되었다. 한편 3-coloring 이상의 문제는 다소 복잡한 모델링 과정을 필요로 하므로 포함시키지 않았다.

2. 교수・학습 과정 설계 및 적용

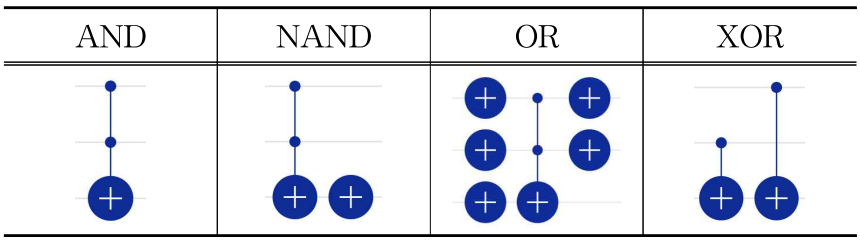
여기서는 본 연구에서 개발한 실습 과제와 프로젝트 활동 과제에 대한 연구 참여자들의 탐구 과정 및 결과에 대해서 소개한다. 또한 해당 과정을 분석함으로써 도출한 교수・학습 과정에 대해서도 상세히 설명한다. 실습 과정의 과제와 적용 단계의 과제는 4차시에 배부되었으며, 응용 단계와 심화 단계의 과제는 5차시에 배부되었다. 모든 과제는 참여자들 간의 토의를 통해 탐구할 수 있도록 지도하였으며, 탐구 결과를 정리 및 발표하도록 안내하였다. 또한 참여자들이 프로그램에 더욱 흥미를 갖고 적극적으로 참여할 수 있도록 참여자들의 다양한 응답에 대해 즉각적으로 정답 여부를 판단해주기보다는 해당 근거를 설명할 수 있는 기회를 제공하였다. 이와 같이 학습 내용에 대한 음미의 시간을 충분히 제공하는 것은 학습자들의 창의성 신장에 기여할 수 있다(한정민 & 박만구, 2010).

2.1. 실습 과정

실습 과정의 과제는 앞으로의 프로젝트 과제를 해결함에 있어 활용할 수 있는 논리 연산 게이트를 얻는 것과 동시에 IBM QX의 사용법을 체득하는 것에 목적을 두고 있으므로 교수자는 학습자들이 과제를 탐구하는 동안 지속적으로 순회하며 안내할 필요가 있다. 또한 해당 과제에 대해서는 양자 게이트의 행렬 표현을 탐구하는 것보다는 주어진 진리표를

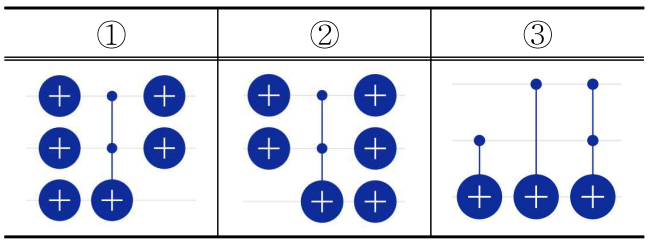
기준으로 다양한 양자 게이트들을 조합해보면서 결과를 도출할 수 있도록 지도해야 한다.

학습자들은 [그림 Ⅳ-9]와 같이 문제 5.1에서 주어진 모든 논리 게이트를 양자 게이트로 구현하였다.



[그림 Ⅳ-9] 문제 5.1에 대한 학습자들의 1차 도출 결과

이 시점에서 본 연구자는 양자 회로의 경우 다양한 방법으로 구현할 수 있음을 안내하였고, 학습자들은 추가 토의를 통해 또 다른 OR 게이트의 구현 방식을 [그림 Ⅳ-10]의 ②, ③과 같이 도출하였다.



[그림 Ⅳ-10] 문제 5.1의 OR 게이트에 대한 학습자들의 2차 도출 결과

2.2. 프로젝트 활동

가. 적용 단계

프로젝트 활동 과정의 적용 단계 과제에서는 정리 2.4와 정리 2.5에 의한 수학적 접근 과정이 필요하므로 교수자는 과제를 배부하기 전 선수학습 내용에 대한 학습자들의 내면화 상태를 점검할 필요가 있다.

주어진 과제의 중첩 단계는 초기 단계로부터 주어진 $|0\rangle^{\otimes 2} = |00\rangle$를 균등 중첩 상태로 변환시키는 단계이다. 해당 단계는 두 아다마르 게이트를 병렬로 연결함으로써 구현할 수 있으며, 이는 아다마르 게이트의 연산 결과와 텐서 곱의 성질을 이용하여 식 4.2와 같이 정당화할 수 있다.

$$\begin{aligned} |\psi_0\rangle &= (\mathrm{H}\otimes\mathrm{H})(|0\rangle\otimes|0\rangle) = \mathrm{H}|0\rangle\otimes\mathrm{H}|0\rangle \\ &= \left\{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right\}\otimes\left\{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right\} \\ &= \frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle) \end{aligned} \tag{4.2}$$

오라클 단계는 중첩 단계로부터 주어진 균등 중첩 상태 $|\psi_0\rangle$에서 목표 객체에 대한 상태의 위상을 전환시키는 단계이다. 문제 5.2의 (1)은 상태 $|11\rangle$의 위상을 전환시켜야 하는 경우로, 오라클 연산자 U의 행렬 표현은 정리 2.4에 의해 식 4.3과 같이 계산된다.

$$\begin{aligned} \mathrm{U} &= \mathrm{Id}^{\otimes 2} - 2|11\rangle\langle 11| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - 2 \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} [0 \;\; 0 \;\; 0 \;\; 1] \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - 2 \cdot \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \end{aligned} \tag{4.3}$$

이 시점에서 학습자들은 오라클 연산자 U의 행렬 표현이 CZ 게이트의 행렬 표현과 동일함을 파악한다. 그리고 입력 큐비트가 $|11\rangle$인 경우에만 위상을 전환하여 출력하는 CZ 게이트의 연산 결과를 복기함으로써 최종적으로 CZ 게이트를 통해 오라클 단계를 구현하였다. 문제 5.2의 나머지 과제들 역시 이와 같이 오라클 연산자의 행렬 표현을 먼저 구하고, 이에 대응하는 양자 게이트를 찾아가는 방식으로 구현을 시도하였다. 문제 5.2

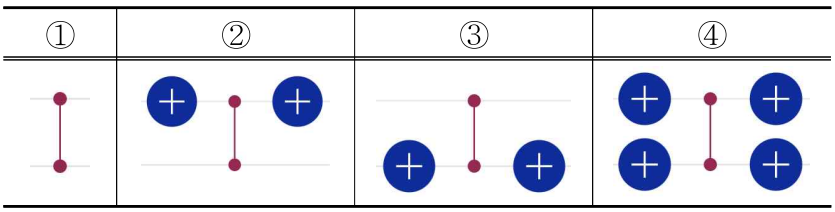
의 (2), (3), (4) 각각에 대한 오라클 연산자의 행렬 표현은 다음과 같다.

$$(2)\ U = Id^{\otimes 2} - 2|01\rangle\langle 01| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.4}$$

$$(3)\ U = Id^{\otimes 2} - 2|10\rangle\langle 10| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.5}$$

$$(4)\ U = Id^{\otimes 2} - 2|00\rangle\langle 00| = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{4.6}$$

식 4.3과 달리 식 4.4 ~ 식 4.6의 행렬 표현들은 이론 학습 과정에서 학습한 단일 큐비트 게이트 또는 다중 큐비트 게이트 하나에 곧바로 대응되지 않는다. 이에 따라 해당 오라클 단계들은 계산한 행렬을 분해한 후 각각에 대응되는 양자 게이트들을 조합하여 구현해야 한다. 하지만 행렬 분해는 본 교육 프로그램에서 다루는 내용 요소가 아니므로, 이때 교수자는 학습자들이 다른 방향에서 접근할 수 있도록 안내할 필요가 있다. 이에 본 연구자는 학습자들이 역의 관점에서 문제 5.1를 해결한 방식으로 접근할 수 있도록 지도하였다. 즉 양자 게이트들을 조합해보면서 주어진 목표 객체의 위상을 전환시킬 수 있는 회로를 구성하게 한 후, 이에 대응되는 행렬 표현을 계산하게 함으로써 실제로 식 4.4 ~ 식 4.6이 도출되는 것을 확인할 수 있게 지도하였다.



[그림 Ⅳ-11] 오라클 단계 대한 학습자들의 도출 결과

학습자들은 이와 같은 방식으로 식 4.4 ~ 식 4.6 각각에 대응되는 오라클 단계를 [그림 Ⅳ-11]과 같이 구현하였으며, 식 4.7 ~ 식 4.9와 같은 계산을 통해 수학적으로 정당화하였다.

$$(2)\ (\mathrm{X}\otimes\mathrm{Id})\mathrm{CZ}(\mathrm{X}\otimes\mathrm{Id})=\begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \tag{4.7}$$

$$(3)\ (\mathrm{Id}\otimes\mathrm{X})\mathrm{CZ}(\mathrm{Id}\otimes\mathrm{X})=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&-1&0\\0&0&0&1\end{bmatrix} \tag{4.8}$$

$$(4)\ (\mathrm{X}\otimes\mathrm{X})\mathrm{CZ}(\mathrm{X}\otimes\mathrm{X})=\begin{bmatrix}-1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \tag{4.9}$$

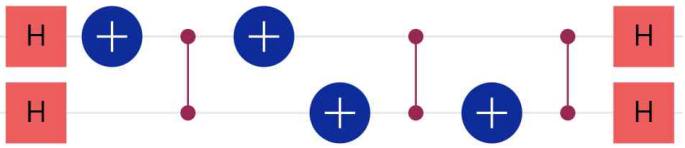
확산 단계는 오라클 단계로부터 주어진 상태 $\mathrm{U}|\psi_0\rangle$를 확률 진폭의 평균을 기준으로 반전시키는 단계이다. 2-큐비트 크기의 입/출력 양자 레지스터에 적용 가능한 확산 연산자 R은 정리 2.5를 이용하여 식 4.10과 같이 계산할 수 있다. 이때 ㉠은 아다마르 게이트의 가역 성질에 의해 성립한다.

$$\begin{aligned}\mathrm{R}&=2|\psi_0\rangle\langle\psi_0|-\mathrm{Id}^{\otimes 2}\\&=2\cdot\mathrm{H}\otimes\mathrm{H}|00\rangle\langle 00|\mathrm{H}\otimes\mathrm{H}-\mathrm{Id}^{\otimes 2}\\&=2\cdot\mathrm{H}\otimes\mathrm{H}|00\rangle\langle 00|\mathrm{H}\otimes\mathrm{H}-\mathrm{H}^{\otimes 2}\cdot\mathrm{H}^{\otimes 2}\ \cdots ㉠\\&=\mathrm{H}\otimes\mathrm{H}\underbrace{(2|00\rangle\langle 00|-\mathrm{Id}^{\otimes 2})}_{㉡}\mathrm{H}\otimes\mathrm{H}\end{aligned} \tag{4.10}$$

식 4.10에서 ㉡의 양쪽에 있는 H⊗H는 아다마르 게이트의 병렬 연결을 통해 곧바로 구현할 수 있으므로 ㉡의 행렬 표현만 구하면 확산 단계를 온전히 구현할 수 있다. ㉡의 행렬 표현은 식 4.11과 같다.

$$2|00\rangle\langle 00| - \mathrm{Id}^{\otimes 2} = 2 \cdot \begin{bmatrix}1\\0\\0\\0\end{bmatrix}[1\ 0\ 0\ 0] - \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} = \begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&-1\end{bmatrix} \quad (4.11)$$

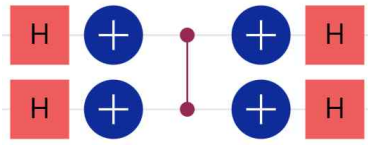
학습자들은 오라클 단계를 구현했던 방식과 동일한 방식으로 확산 단계를 [그림 Ⅳ-12]와 같이 구현하였다.



[그림 Ⅳ-12] 확산 단계 대한 학습자들의 1차 도출 결과

이 시점에서 본 연구자는 학습자들에게 다양한 방식으로 양자 회로를 구현할 수 있다는 점과 Born의 규칙을 복기할 수 있도록 안내하였다. 이에 학습자들은 행렬의 스칼라배를 이용하여 식 4.11을 식 4.12로 변형한 후, Born의 규칙에 따라 음의 부호를 제외할 수 있음을 파악하고, 식 4.9의 구현 결과를 이용하여 [그림 Ⅳ-13]과 같이 확산 단계를 구현하였다.

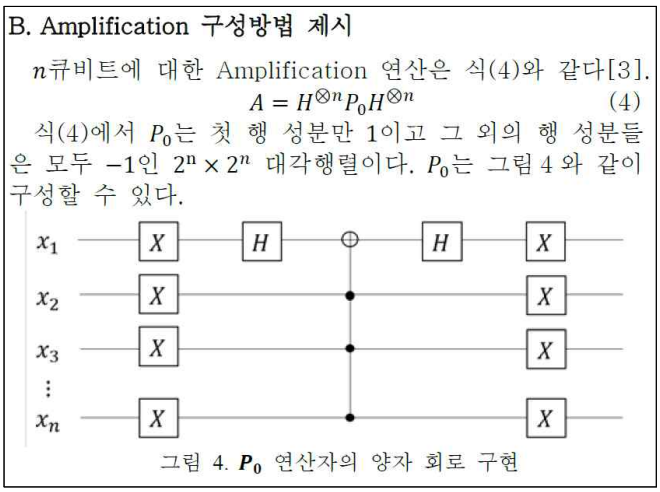
$$2|00\rangle\langle 00| - \mathrm{Id}^{\otimes 2} = \begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&-1\end{bmatrix} = -\begin{bmatrix}-1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \quad (4.12)$$



[그림 Ⅳ-13] 확산 단계 대한 학습자들의 2차 도출 결과

마지막으로 본 연구자는 다양한 방식으로 양자 회로를 구현할 수 있다는 점을 다시 한 번 강조하기 위하여 여러 연구(김정민 & 허준, 2020; 하진

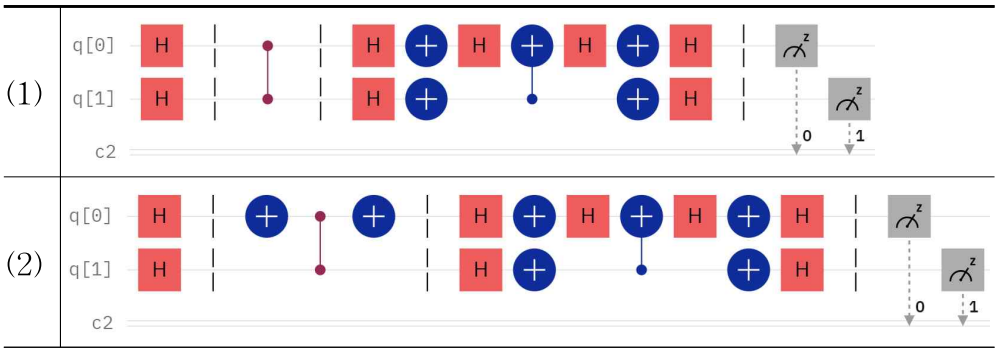
영 외, 2019; Botsinis et al., 2013; Mukherjee, 2022; Vinod & Shaji, 2021)에서 택하고 있는 n-큐비트 크기의 양자 레지스터에 대한 확산 연산자의 구현 방식을 소개하였다. 이때 활용된 수업 자료는 [그림 Ⅳ-14](하진영 외, 2019)와 같다.

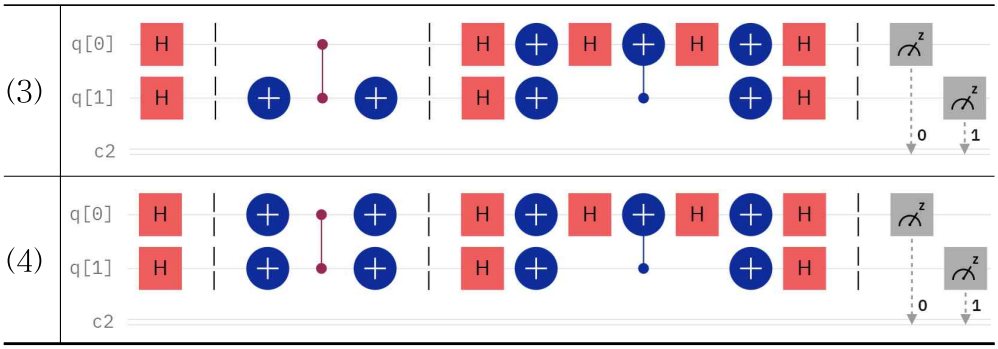


[그림 Ⅳ-14] <양자 알고리즘> 교육 프로그램 4차시 수업 자료의 일부

최종적으로 학습자들은 최적의 반복 횟수를 식 4.13과 같이 계산하고, 이상의 구현 결과를 종합하여 문제 5.2의 답으로 [그림 Ⅳ-15]와 같은 양자 회로들을 제시하였다.

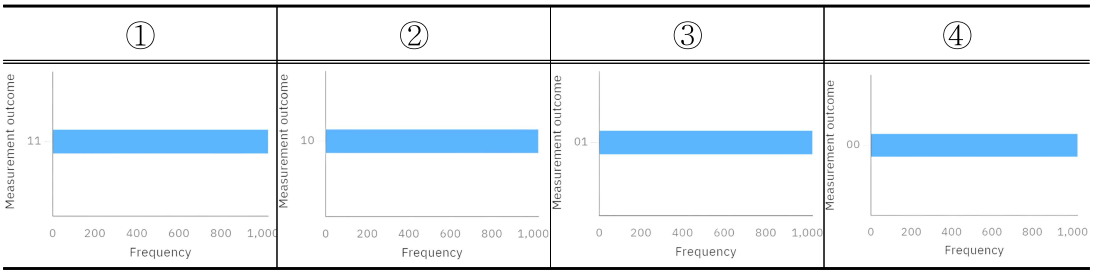
$$\left\lfloor \frac{\pi}{4} \times \sqrt{N} \right\rfloor = \left\lfloor \frac{\pi}{4} \times \sqrt{4} \right\rfloor = \left\lfloor \frac{\pi}{4} \times 2 \right\rfloor = 1 \qquad (4.13)$$





[그림 Ⅳ-15] 문제 5.2에 대하여 학습자들이 도출한 양자 회로

또한 학습자들은 실물 양자 컴퓨터를 이용한 시뮬레이션을 수행하여 각각의 목표 객체가 [그림 Ⅳ-16]과 같이 올바르게 측정됨을 확인하였다.



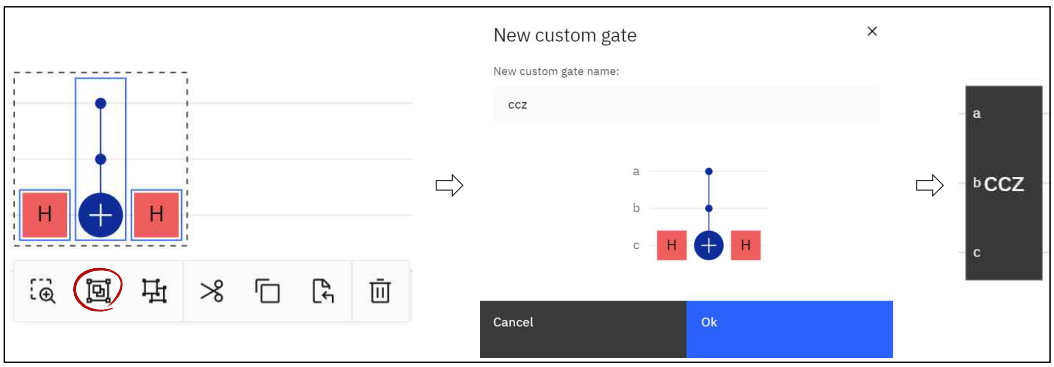
[그림 Ⅳ-16] 문제 5.2에 대한 양자 회로의 시뮬레이션 결과

나. 응용 단계

프로젝트 활동 과정의 응용 단계 과제에 대한 중첩 및 확산 단계의 구현 방식은 적용 단계의 문제 5.2와 동일하다. 이에 따라 교수자는 학습자들에게 해당 과제를 탐구하는 과정의 핵심이 오라클 단계에 있음을 강조할 필요가 있다. 단, 문제 5.3은 문제 5.2와 달리 목표 객체를 특정할 수 없는 경우에 해당하므로 학습자들에게 IBM QX 양자 회로 구성 편집기의 시각화 기능을 적극적으로 활용할 것을 권장해야 한다.

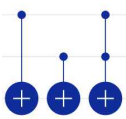
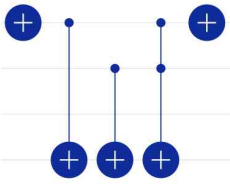
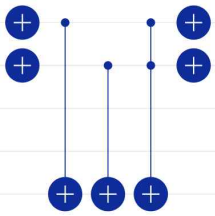
주어진 과제의 오라클 단계는 각 절의 값을 보조 레지스터에 임시로 저장한 후, CNF를 참으로 만드는 할당 값 $|111\rangle$의 위상을 전환시키는 방식으로 구현할 수 있다. 즉 CCZ 게이트를 이용해야 하는데, 해당 게이

트는 IBM QX 양자 회로 구성 편집기에 다이어그램으로 제공되어 있지 않기 때문에 행렬 분해를 통해 직접 구현해서 이용해야 한다. 하지만 앞서 언급했듯이 행렬 분해는 본 교육 프로그램에서 다루는 내용 요소가 아니므로 교수자는 IBM QX 내의 커스터마이즈 기능을 통해 사전에 학습자들에게 CCZ 게이트를 제공할 필요가 있다.

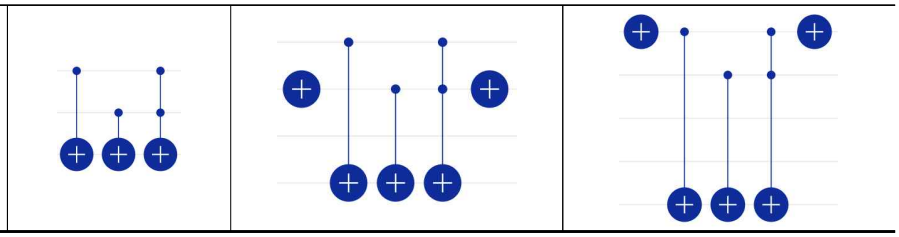


[그림 Ⅳ-17] 커스터마이즈 기능을 이용한 CCZ 게이트 정의

문제 5.3은 2-SAT 문제이므로 두 부울 변수를 표현하기 위한 2-큐비트 크기의 양자 레지스터와 3개의 절 값을 임시로 저장하기 위한 3-큐비트 크기의 보조 레지스터가 필요하다. 즉, 주어진 부울 변수 값에 해당하는 두 양자 레지스터 q_0, q_1에 대하여 첫 번째 절 값은 q_2, 두 번째 절 값은 q_3, 세 번째 절 값은 q_4에 저장한다. 각 절의 연산은 이론 학습 과정에서 학습한 X 게이트와 실습 과정에서 구현한 OR 게이트 및 AND 게이트를 이용하여 구현할 수 있다. [그림 Ⅳ-18]는 각 절의 연산에 대해서 학습자들이 도출한 구현 결과이다.

	첫 번째 절	두 번째 절	세 번째 절
(1)			

(2)

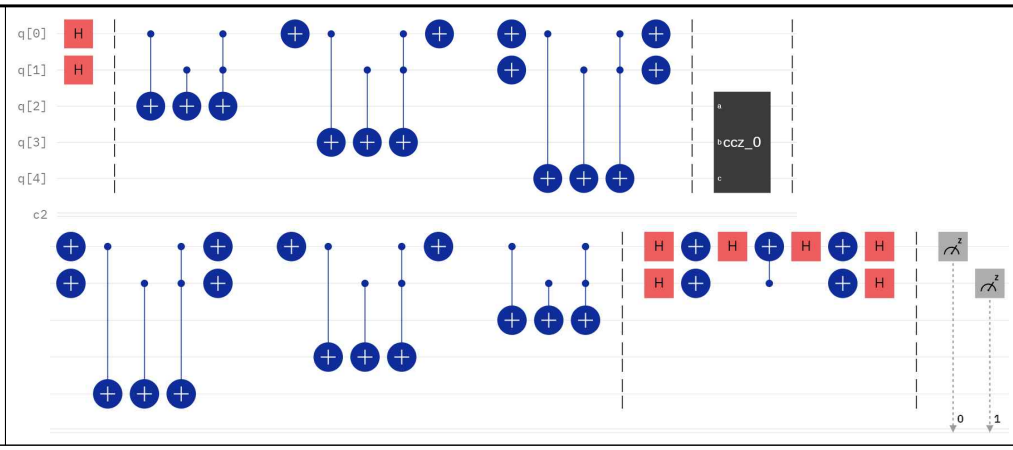


[그림 Ⅳ-18] 각 절의 연산에 대한 학습자들의 도출 결과

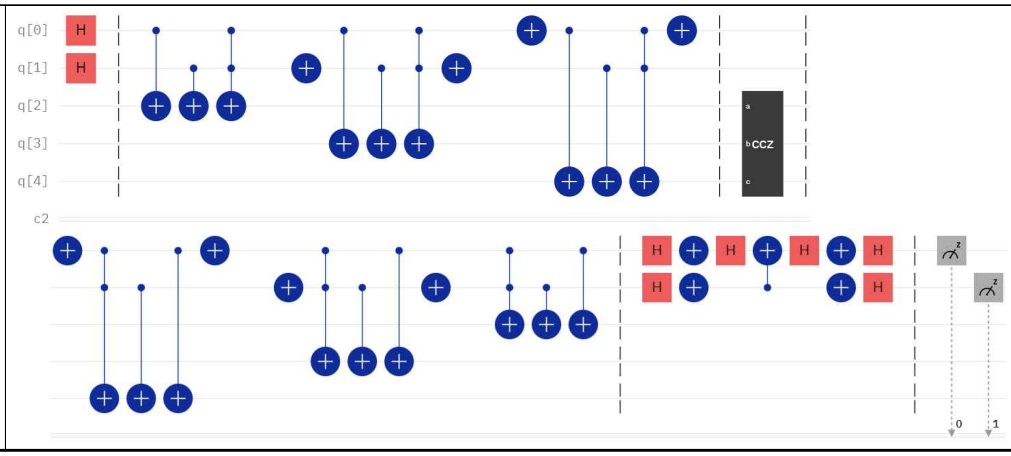
임시로 값을 저장하기 위해 활용한 보조 레지스터는 반드시 초기 상태 $|0\rangle$으로 되돌려주어야 한다. 실제로 해당 입/출력 레지스터의 부분 시스템을 축약 밀도 연산자로 나타내면 순수 상태가 아닌 혼합 상태로 기술된다. 그러나 밀도 연산자는 본 교육 프로그램에서 다루는 내용 요소가 아니므로 교수자는 학습자들에게 보조 레지스터를 초기화하지 않은 경우와 초기화한 경우의 비교 분석 결과를 제공해야 한다. 이는 해당 과제의 목표 객체를 공개한 후, IBM QX 양자 회로 구성 편집기의 시각화 기능을 통해 보조 레지스터가 초기화되지 않으면 목표 객체가 출력되지 않음을 직접 확인하게 하여 지도할 수 있다.

최종적으로 학습자들은 최적의 반복 횟수가 식 4.13과 동일함을 파악하고, 이상의 구현 결과를 종합하여 문제 5.3의 답으로 [그림 Ⅳ-19]와 같은 양자 회로들을 제시하였다. 또한 실물 양자 컴퓨터를 이용한 시뮬레이션을 수행하여 각각의 목표 객체가 [그림 Ⅳ-20]과 같이 올바르게 측정됨을 확인하였다.

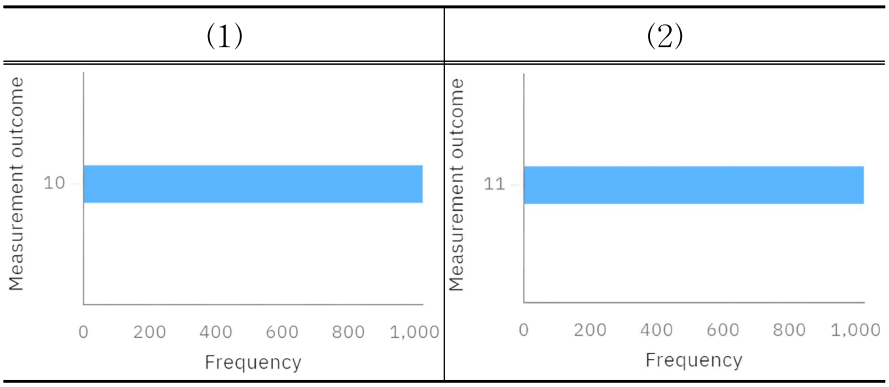
(1)



(2)



[그림 Ⅳ-19] 문제 5.3에 대하여 학습자들이 도출한 양자 회로



[그림 Ⅳ-20] 문제 5.3에 대한 양자 회로의 시뮬레이션 결과

다. 심화 단계

프로젝트 활동 과정의 심화 단계 과제는 SAT 문제로 모델링한 후 Grover 알고리즘을 이용하여 해결할 수 있도록 설계되었으므로 교수·학습 과정은 SAT 문제를 탐구한 응용 단계로부터 도출된 것과 유사하다. 단, 문제 5.4는 문제 5.3과 달리 목표 객체가 2개인 경우로 RGA 모델을 이용하여 해결할 수 없는 문제에 해당하므로 교수자는 일반적인 Grover 알고리즘 모델의 최적 횟수가 $k^{\mathrm{opt}} \approx \pi/4 \times \sqrt{N/M}$ 임을 알려진 사실로서 전달할 필요가 있다.

한편 해당 과제는 모델링의 방법에 따라 다양한 논리식이 도출될 수 있는데, 그 중에서 3-큐비트 크기 이상의 입/출력 레지스터 위에서 정의되는 논리식은 적용 단계에서 도출한 중첩 단계 및 확산 단계의 구현 방식을 적용할 수 없다. 그럼에도 학습자들은 양자 게이트 간의 조합을 필요로 하지 않는 중첩 단계의 특징과 [그림 Ⅳ-14]에서 제시된 n-큐비트 크기에 대한 확산 연산자를 이용하여 어렵지 않게 구현하였다.

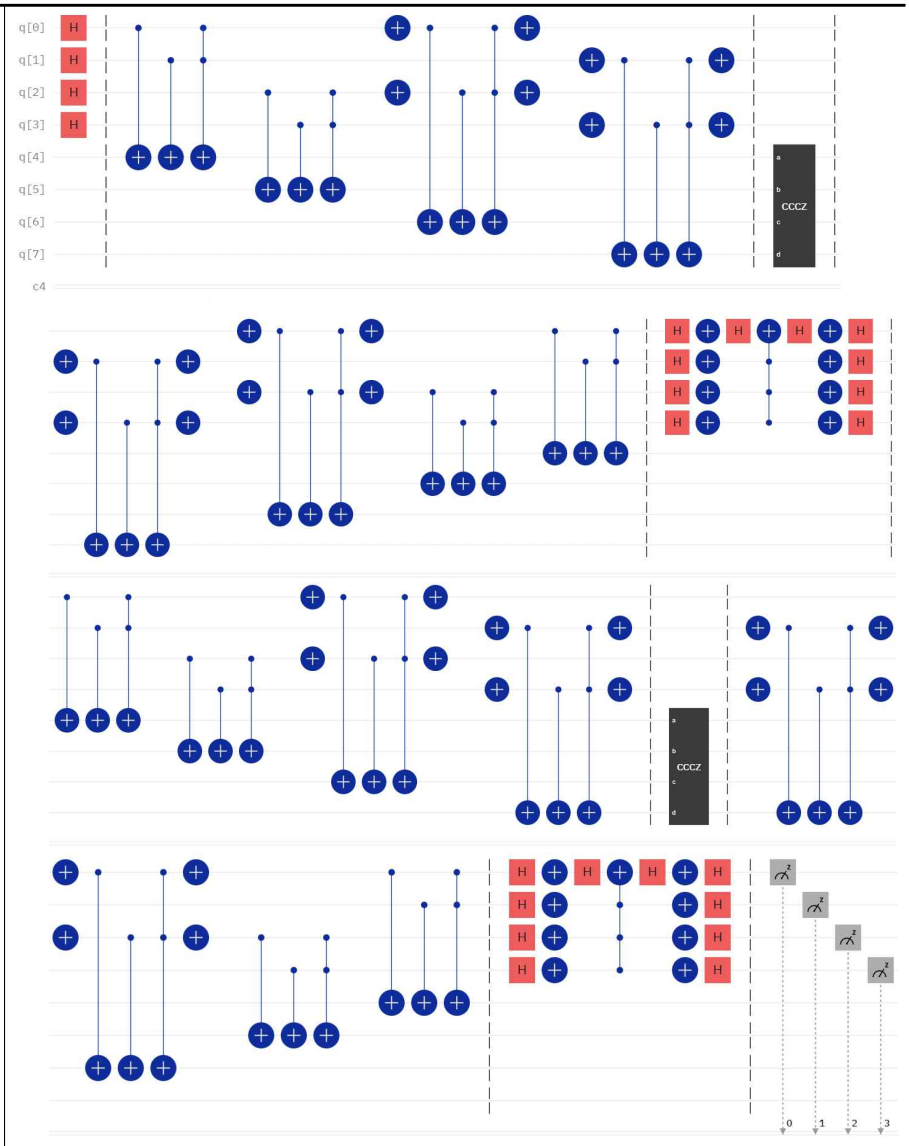
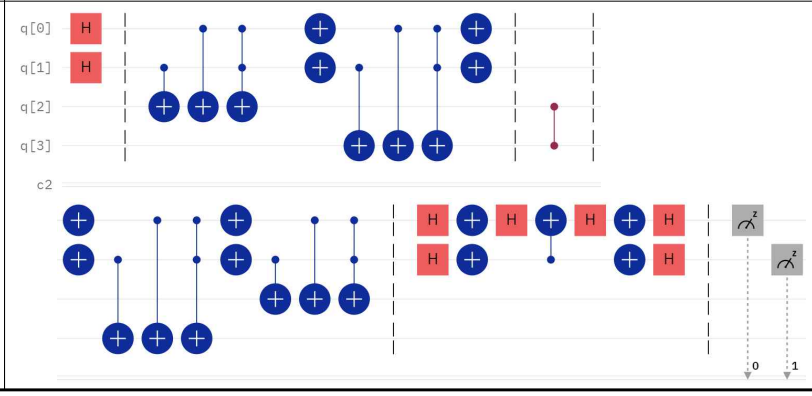
학습자들은 문제 5.4의 (1)에 대해서 다음과 같은 두 가지 논리식을 도출하였다.

$$\left(x_1 \vee x_2\right) \wedge \left(x_3 \vee x_4\right) \wedge \left(\overline{x_1} \vee \overline{x_3}\right) \wedge \left(\overline{x_2} \vee \overline{x_4}\right) \tag{4.14}$$

$$\left(x_1 \vee x_2\right) \wedge \left(\overline{x_1} \vee \overline{x_2}\right) \tag{4.15}$$

식 4.14는 꼭짓점 A에 빨간색과 파란색을 칠하는 경우 각각을 x_1, x_2, 꼭짓점 B에 빨간색과 파란색을 칠하는 경우 각각을 x_3, x_4로 모델링한 후, '칠한다'에 1, '칠하지 않는다'에 0을 할당하여 도출한 논리식이다. 이때 식 $\left(x_1 \vee x_2\right) \wedge \left(x_3 \vee x_4\right)$는 각 꼭짓점에 한 가지의 색을 칠하는 조건에 대한 논리식이고, 식 $\left(\overline{x_1} \vee \overline{x_3}\right) \wedge \left(\overline{x_2} \vee \overline{x_4}\right)$는 인접한 꼭짓점에 같은 색을 칠하지 않는 조건에 대한 논리식 $\overline{x_1 \wedge x_3} \wedge \overline{x_2 \wedge x_4}$에 드모르간의 법칙(De Morgan's law)을 적용한 논리식이다. 반면에 식 4.15은 꼭짓점 A를 x_1, 꼭짓점 B를 x_2로 모델링한 후, '빨간색을 칠한다'에 1, '파란색을 칠한다'에 0을 할당하여 도출한 논리식이다. 식 4.14와 마찬가지로 식 $x_1 \vee x_2$는 각 꼭짓점에 한 가지 색을 칠하는 조건에 대한 논리식, $\overline{x_1} \vee \overline{x_2}$는 인접한 꼭짓점에 같은 색을 칠하지 않는 조건에 대한 논리식 $\overline{x_1 \vee x_2}$에 드모르간의 법칙을 적용한 논리식이다.

[그림 Ⅳ-21]은 학습자들이 식 4.15와 식 4.16에 대해 문제 5.3의 구현 방식을 적용하여 도출한 구현 결과이다.

식 4.14	
식 4.15	

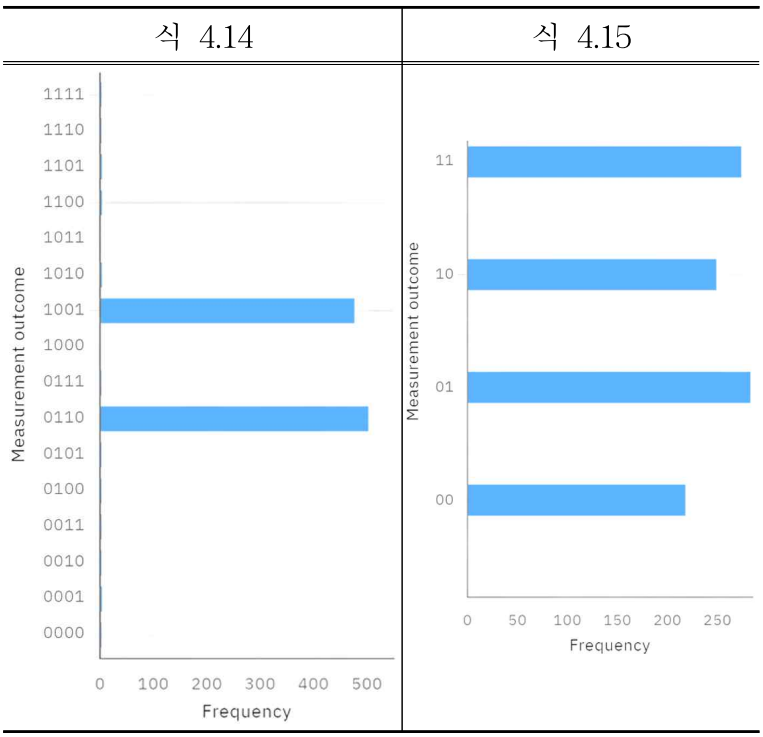
[그림 Ⅳ-21] 문제 5.4의 (1)에 대하여 학습자들이 도출한 양자 회로

식 4.14에 대한 구현에는 식 4.16와 같이 구한 최적의 반복 횟수 2번을 적용한 것이다. 그러나 식 4.15에 대한 구현에 대한 최적의 반복 횟수는 아래의 식 4.17과 같이 0번으로 계산된다.

$$\left\lfloor \frac{\pi}{4}\times\sqrt{\frac{N}{M}} \right\rfloor = \left\lfloor \frac{\pi}{4}\times\sqrt{\frac{16}{2}} \right\rfloor = \left\lfloor \frac{\pi}{4}\times 2\sqrt{2} \right\rfloor = 2 \qquad (4.16)$$

$$\left\lfloor \frac{\pi}{4}\times\sqrt{\frac{N}{M}} \right\rfloor = \left\lfloor \frac{\pi}{4}\times\sqrt{\frac{4}{4}} \right\rfloor = \left\lfloor \frac{\pi}{4} \right\rfloor = 0 \qquad (4.17)$$

학습자들은 이 시점에서부터 식 4.15을 도출한 모델링 방법에 오류가 있음을 감지하였다. 그럼에도 우선 반복 횟수를 1번으로 가정한 후 실물 양자 컴퓨터로 시뮬레이션을 수행하였다. 각각의 논리식을 참으로 만드는 할당은 [그림 Ⅳ-22]과 같이 도출되었는데, 실제로 식 4.14의 경우는 올바르게 도출되었지만 식 4.15의 경우에는 올바르게 도출되지 않았다.



[그림 Ⅳ-22] 문제 5.4의 (1)에 대한 양자 회로의 시뮬레이션 결과

해당 오류의 원인은 식 4.15의 모델링 방법이 확산 단계에서 확률 진폭의 평균을 0으로 만들기 때문이다. 즉, $\mu_0 = 0$을 기준으로 반전을 수행하였기 때문에 상태들에 대한 확률 진폭의 증가·감소 변화가 이루어지지 않는다. 학습자들은 이를 확산 단계의 회로를 반영하였을 때와 반영하지 않았을 때의 두 상태 벡터 그래프를 비교하고, 이때 그래프의 변화가 없음을 확인함으로써 파악하였다. 이렇게 논의의 오류를 정확하게 파악할 수 있었던 것은 IBM QX에서 제공하는 동적인 시각화 기능에 기인한다. 즉, 프로그램의 수행 단계를 가시화함으로써 학습자들로 하여금 효율적인 디버깅(debugging)을 가능케 한 것이다(정인기, 2004).

학습자들은 문제 5.4의 (2)에 대해서 아래의 식과 같은 논리식을 도출하였다.

$$\left(x_1 \vee x_2\right) \wedge \left(x_1 \vee x_3\right) \wedge \left(\overline{x_1} \vee \overline{x_2}\right) \wedge \left(\overline{x_1} \vee \overline{x_3}\right) \tag{4.18}$$

식 4.18은 식 4.15와 동일한 방식으로 모델링하여 도출한 논리식이다. 즉, 꼭짓점 A를 x_1, 꼭짓점 B를 x_2, 꼭짓점 C를 x_3으로 모델링한 후, '빨간색을 칠한다'에 1, '파란색을 칠한다'에 0을 할당하여 도출한 논리식이다.

학습자들은 해당 모델링 방법에 오류가 있었음에도 식 4.15가 식 4.14보다 효율적으로 알고리즘을 작성할 수 있었음을 상기하고, 주어진 과제의 경우 8개의 객체를 갖는 비정형 데이터 베이스에서 2개의 목표 객체가 존재함을 추론함으로써 확률 진폭의 평균이 0이 되지 않음을 미리 파악하였다. 더욱이 학습자들은 필요한 큐비트의 개수를 줄이기 위해 식 4.18을 다음과 같이 변형하였다.

$$\left(x_1 \oplus x_2\right) \wedge \left(x_1 \oplus x_3\right) \tag{4.19}$$

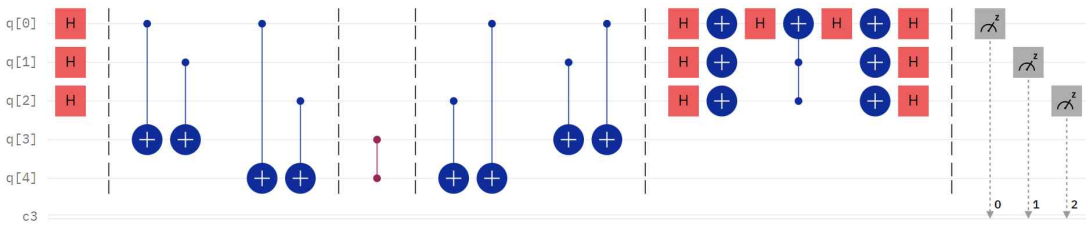
식 4.19는 베타적 논리합의 성질 $(a \vee b) \wedge \left(\overline{a} \vee \overline{b}\right) = a \oplus b$에 의해 성립한다. 식 4.19는 2-SAT 논리식에 해당하지는 않지만, 학습자들이 창의적 사고

를 통해 보다 효율적인 모델링한 방법을 도출한 것으로 볼 수 있다. 즉, 학습자들 간의 메타인지적 상호 작용이 활발하게 이루어져 집단적 사고의 폭이 확장된 것을 살펴볼 수 있다.

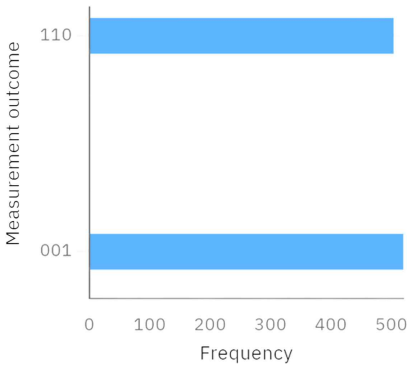
최종적으로 학습자들은 식 4.20과 같이 최적의 반복 횟수를 계산하고,

$$\left\lfloor \frac{\pi}{4}\times\sqrt{\frac{N}{M}}\right\rfloor=\left\lfloor \frac{\pi}{4}\times\sqrt{\frac{8}{2}}\right\rfloor=\left\lfloor \frac{\pi}{4}\times 2\right\rfloor=1 \qquad (4.20)$$

이상의 논의를 종합하여 문제 5.4-(2)의 답으로 [그림 Ⅳ-23]과 같은 양자 회로를 제시하였다. 또한 실물 양자 컴퓨터를 이용한 시뮬레이션을 수행하여 각각의 목표 객체가 [그림 Ⅳ-24]와 같이 올바르게 측정됨을 확인하였다.



[그림 Ⅳ-23] 문제 5.4의 (2)에 대하여 학습자들이 도출한 양자 회로



[그림 Ⅳ-24] 문제 5.4의 (2)에 대한 양자 회로의 시뮬레이션 결과

제 5 장 결론 및 제언

제 1 절 요약 및 결론

양자 우월성(quantum supremacy)을 달성했다는 것에 큰 이견이 없는 현재(김한영, 2020), 앞으로 학생들이 살아갈 시대는 양자 컴퓨터에 의해 기존의 과학 기술의 난제가 해결되고, 새로운 응용 산업 및 연구 분야가 출범하는 시대이다. 따라서 미래 교육은 양자 컴퓨터에 대해 전문성을 갖춘 창의·융합 인재 양성에 주목해야할 것으로 보인다. 이러한 시대적 요구에 발맞춰 주요 선도 기업들은 클라우드 서비스의 형태로 사용자에게 양자 컴퓨팅 환경을 제공하고 있다. 이에 본 연구자는 <양자 알고리즘> 교육에서 클라우드 기반 양자 컴퓨터의 교육적 활용 가능성은 어떠한지에 대한 물음에서 출발하여 중등교육 기관 학생들에게 도입할 수 있는 양자 알고리즘은 무엇이 있는지, 그 여부에 대해서 탐구하였다.

탐구에 대한 결과로 본 연구의 중심 소재를 Grover 알고리즘으로 선정하였으며, 해당 소재에 대해 중등교육 기관 학생들을 대상으로 한 공학적 도구 기반의 <양자 알고리즘> 교육 프로그램 개발을 목적으로 다음과 같은 연구 문제를 설정하였다. 첫째, Grover 알고리즘을 중등교육 기관 학생들에게 도입하기 위해 학문수학 수준에서 엄밀하게 기술되는 현 내용 체계는 어떻게 재구조화되어야 하는가? 둘째, Grover 알고리즘의 작동 원리에 대한 이해를 성취 기준으로 하는 공학적 도구 기반의 수업과 과제는 어떻게 설계되어야 하는가?

첫 번째 연구 문제에 답하기 위하여, 본 연구에서는 Grover 알고리즘의 핵심 내용 요소들을 추출하여 현 내용 체계를 정립하였다. 그다음 일반적인 Grover 알고리즘의 구성 요소를 제한하여 RGA 모델을 선정하였다. 이후 RGA 모델의 기하학적 작동 원리에 집중하여 조영미(2001)의 분석 틀을 기준으로 제4수준에서 내포적으로 정의된 요소들을 제3b수준

아래에서 외연적으로 재정의하였으며, IBM QX의 시각화 기능을 통해 가시화를 제시할 수 있는 요소에 대해서는 엄밀한 수학적 정당화 과정을 최소화하였다. 최종적으로는 교수학적으로 변환된 요소들을 유기적으로 연결시켜 줄 수 있는 정리와 참고, 그리고 일반화된 지식을 도출함으로써 재구조화된 Grover 알고리즘의 내용 체계를 제안하였다.

두 번째 연구 문제에 답하기 위하여, 본 연구에서는 재구조화된 내용 체계에서 Grover 알고리즘을 지도함에 있어 공학적 도구의 활용이 필요한 내용 요소를 선별하였고, 그에 따른 교육 자료를 개발하였다. 그다음 IBM QX의 사용법을 익히고 Grover 알고리즘을 이용하여 문제를 해결함에 있어 유용한 연산 게이트를 얻기 위한 실습 과제를 설계하였다. 또한 Grover 알고리즘을 통해 접근할 수 있는 문제들을 탐구한 선행 연구들을 조사하여 교육 프로그램에서 활용할 프로젝트 활동 과제를 개발하였다. 최종적으로는 개발 연구의 예비 설계와 교수 실험의 순환 과정에 주목하여 사고 실험을 통해 설계된 교육 프로그램을 선정된 연구 참여자들에게 적용하였다. 그리고 해당 교수 실험을 평가 및 분석함으로써 단계별 과제 탐구 과정에 대한 지도상의 유의점을 포함한 교수·학습 과정을 제시하였다.

본 교육 프로그램의 프로젝트 활동 과제는 Grover 알고리즘의 적용 단계, 응용 단계, 심화 단계로 구성되어 있다. 적용 단계와 응용 단계의 과제들은 Grover 알고리즘을 이용하여 해결할 수 있는 다양한 문제들을 경험할 수 있도록 설계되었으며, 심화 단계의 과제들은 프로젝트 활동 전반에 걸쳐 실세계 현상의 수학적 원리와 구조를 이해하여 수학의 유용성과 가치를 경험할 수 있도록 설계되었다(서지영 & 윤상균, 2022).

본 연구에서 제시한 교수·학습 과정에서는 토의를 통한 탐구를 바탕으로 학습자들로 하여금 그 결과를 정리 및 발표할 수 있도록 지도해야 함을 강조하였다. 또한 학습자들이 프로그램에 더욱 흥미를 갖고 적극적으로 참여할 수 있도록 학습자들의 다양한 응답에 대해 즉각적으로 정답 여부를 판단해주기보다는 해당 근거를 설명할 기회를 제공해주어야 함을 강조하였다.

제 2 절 의의 및 제언

적성과 진로에 따라 학생들 스스로가 원하는 과목을 선택하고 학업 계획을 수립하는 고교학점제 제도를 전면에 세운 2022 개정 교육과정의 전면 시행이 예고된 현재, 미래지향적인 수학교육에 관한 연구들은 차기 교육과정 개정에서 미래 사회에 대비하기 위한 수학 교과 신설의 필요성을 강조하고 있다(김화경 외, 2021). 이에 본 연구는 학교수학의 도입을 목적으로 한 새로운 수학 교과의 가능성을 제시했다는 점에서 그 의의를 갖는다. 한편 본 연구에서 개발한 <양자 알고리즘> 교육 프로그램이 갖는 교육적 의의는 다음과 같다.

첫째, 의사소통 및 추론 역량을 함양할 수 있다. 추론은 수학적 사실을 추측하고 논리적으로 분석하고 정당화하며 그 과정을 반성하는 능력을 말한다. 의사소통은 수학 지식이나 아이디어, 수학적 활동의 결과, 문제 해결 과정, 신념과 태도 등을 말이나 글, 그림, 기호로 표현하고 다른 사람의 아이디어를 이해하는 능력을 말한다(교육부, 2015, p. 4). 본 교육 프로그램의 학습자들은 심화 단계의 첫 번째 과제에서 자신들의 모델링 방법에 기인한 오류를 분석 및 반성함으로써 두 번째 심화 단계 과제에 대한 올바른 모델링 방안을 추론하였고, 이를 수학적으로 정당화하여 반영하였다. 또한 학습자들은 교수자의 사고 실험을 통해 설계된 심화 단계 과제의 해결 방안보다 더 효율적인 모델링 방법을 제안하였는데, 이는 의사소통을 통해 학습자들 간의 메타인지적 상호 작용이 활발하게 이루어져 집단 창의성이 발휘된 것으로 볼 수 있다.

둘째, 본 연구의 교육 프로그램은 코팅을 수반하지 않도록 IBM QX의 선별된 기능만을 이용하여 설계되었으며, 추후 프로그램 자료를 쉽게 활용할 수 있도록 단계별 교수·학습 과정을 상세히 제시하였다는 점에서 교사들에 대한 접근성이 높다는 의의를 갖는다.

다만 본 연구의 교육 프로그램은 영재교육원 학생들을 대상으로 개발되었기 때문에 일반 학생들로 그 대상을 확장하기에는 어려움이 있다. 따라서 다른 학군을 대상으로도 다양한 <양자 알고리즘> 교육 프로그램을

개발하고, 이의 적용 가능성을 탐색해보는 후속 연구가 필요하다. 또한 본 연구의 교육 프로그램은 단 두 차시 동안만 진행된 프로젝트 활동에 초점을 두고 있으므로 후속 연구를 통해 보다 긴 시간 동안 이루어질 수 있는 프로젝트 활동을 개발할 필요가 있다. 마지막으로 본 연구는 회고 분석 단계에서 특정 검사 도구를 바탕으로 프로젝트의 효과성을 검증하지는 않았는데, 향후 질적·양적 연구를 수행하기에 충분한 참여자 수가 확보되었을 때 다년간에 걸친 후속 연구가 이루어질 필요가 있다.

참 고 문 헌

강완(1991). 수학적 지식의 교수학적 변환. **수학교육, 30**(1), 71 - 89.

고상숙, 홍석만(2002a). Tess를 이용한 교수학습에서 변환지도에 대한 사례연구-부진아를 대상으로. **E-수학교육 논문집, 14**(14), 85-102.

고상숙, 홍석만(2002b). Amazing Triangle을 이용한 기하 학습자료 개발. **E-수학교육 논문집, 13**(1), 361-379.

공민숙, 강윤수(2014). GeoGebra를 활용한 극한 지도가 고등학생들의 수학 학습에 미치는 영향. **한국학교수학회논문집, 17**(4), 697-716.

교육부(2015). **수학과 교육과정**. 교육부 고시 제2020-236호 [별책8]. 세종: 교육부.

교육부(2017a). **2015 개정 교육과정 총론 해설: 고등학교**. 교육부 고시 제2015-74호. 세종: 교육부.

교육부(2017b). **수학 2-1**. 서울: ㈜비상교육.

교육부(2017c). **수학 2-1 교사용 지도서**. 서울: ㈜비상교육.

교육부(2017d). **수학 3-2 교사용 지도서**. 서울: ㈜비상교육.

교육부(2021). **2022 개정 교육과정 총론 주요 사항(시안)**. 보도자료(2021. 11.24.)

국방과 기술(2021). 현대중공업-KT, 글로벌 조선업계 최초 양자암호통신 구축: 방산기술과 산업기술 보호를 위한 더 완벽한 보안체계 구축. **국방과 기술, 506**, 25-27.

김범일, 김건후, 허준(2021). W state를 이용한 Hamiltonian path 문제 접근법. **한국통신학회 학술대회논문집, 2021**(2), 290-291.

김범일, 민건식, 허준(2020). Grover search algorithm을 이용한 Hamiltonian path 문제 접근법. **한국통신학회 학술대회논문집, 2020**(8), 52-53.

김선희, 서동엽, 강성권, 김수민(2016). 교육과정과 교과서에 제시된 용어 기호에 대한 비판적 고찰. **학교수학, 18**(3), 611-623.

김영훈, 허재성(2020). **선형 대수학과 함께 배우는 양자 정보 이론**. 서울: 경문사.

김원경 외 14인(2019). **고등학교 미적분**. 서울: ㈜비상교육.

김정민, 허준(2020). Grover algorithm을 이용한 최솟값 찾기 분석 및 회로 구현. **한국통신학회 학술대회논문집, 2020**(8), 1352-1353.

김진하(2016). 제4차 산업혁명 시대, 미래사회 변화에 대한 전략적 대응방안 모색, **KISTEP InI, 15**, 45-58.

김창준, 박경덕, 이준구(2020a). 기계학습을 통한 양자 회로 에러 보정 방법. **한국통신학회 학술대회논문집, 2020**(8), 32-33.

김창준, 박경덕, 이준구(2020b). 합성곱 신경망을 통한 양자 회로 에러 보정 방법. **한국통신학회 학술대회논문집, 2020**(11), 102-103.

김태현(2018). 양자컴퓨터의 소개 및 전망. **전자공학회지, 45**(4), 32-39.

김한영(2020년, 12월 15일). 양자 우월성. **Horizen, 양자 컴퓨터**. 검색일 2023.02.06. 자료 출처: https://horizon.kias.re.kr/16137.

김향숙(2001). 평면변환기하에 있어서 Mathematica를 이용한 교수-학습 방법. **A-수학교육, 40**(1), 93-102.

김화경 외 6인(2021). 고교학점제 도입에 따른 고등학교 수학과 교육과정 1차 재구조화. **학교수학, 23**(2), 291-315.

류건, 노정원, 윤상균(2022). 사범대학 해석학 전공 교재에서 나타나는 지수함수 미분법의 정당화 방식에 관한 연구. **학교수학, 24**(3), 387-411.

류희찬, 이지요(1993). 수학교육에서의 시각화의 중요성과 LOGO. **수학교육학연구, 3**(1), 75-85.

문광호, 우정호(1999). 중고등학교 수학의 시각화. **학교수학, 1**(1), 135-156.

문현승, 이성훈, 민건식, 박동규, 허준(2019). IBM Q를 이용한 [[7,1,3]] Steane Code 분석. **한국통신학회 학술대회논문집, 2019**(1), 267-268.

민건식, 허준(2020a). 자원 할당을 위한 낮은 복잡도의 양자 Grover 알고리즘 설계. **한국통신학회논문지, 45**(12), 2046-2054.

민건식, 허준(2020b). Grover Search 알고리즘을 이용한 4 coloring problem 해결 및 분석. **한국통신학회 학술대회논문집, 2020**(2), 70-71.

박래성, 권종겸, 이동엽(2019). 중학교 수학 기하 단원에서 공학적 도구 활용이 학생들의 수학 학업 성취도와 수학 학습 태도에 미치는 효과. **디지털융복합연구, 17**(12), 67-75.

서영진, 안병규, 박주윤, 신정환, 허준(2018). IBM Q를 이용한 3 qubit bit-flip 부호 분석. **한국통신학회 학술대회논문집, 2018**(1), 27-28.

서영진, 허준(2020). Graph Coloring Problem에 적용한 Grover Search 알고리즘 설계 기법. **한국통신학회 학술대회논문집, 2020**(2), 76-77.

서지영, 윤상균. (2022). 수학 정보과학 융합을 위한 창의적 문제해결 활동 개발: 영재 학생을 대상으로 한 모자 게임을 중심으로. **E-수학교육 논문집, 36**(3), 439-467.

손일권, 이원혁, 석우진(2019). 결함 허용 양자 계산과 소요자원 개요. **전자공학회지, 46**(9), 38-45.

손홍찬(2011). 우리나라 수학교육에서 공학 활용의 역사와 현황. **학교수학, 13**(3), 525-542.

송경주, 장경배, 서화정(2021). 해시함수 LSH 양자 회로 최적화를 통한 그루버 알고리즘 적용 자원 추정. **정보보호학회논문지, 31**(3), 323-330.

신동선, 류희찬(1998). **수학교육과 컴퓨터**. 서울: 경문사.

신용재, 허준(2021). Grover's algorithm을 이용한 Graph coloring problem 풀이. **한국통신학회 학술대회논문집, 2021**(6), 1471-1477.

양성현, 강옥기(2011). GeoGebra를 활용한 역동적인 시각적 표상에 기반한 이차곡선 지도 방안. **학교수학, 13**(3), 447-468.

양성현(2021). GeoGebra를 활용한 연립이차방정식 교수・학습 방안 연구. **East Asian Mathematical Journal, 37**(2), 37(2), 265-288.

여미주, 권혁진(2012). 고등학생들의 수학적 언어 유형 및 수학적 언어와 Polya의 문제 해결 4단계의 관련성 분석. **교과교육학연구, 16**(4), 1071-1099.

오경숙 외 5인(2011). 기초 알고리즘 학습을 위한 알고리즘 시각화 시스템의 효용성 분석. **한국전자통신학회 논문지, 6**(2), 212-218.

오경숙, 류남훈, 이상진, 이혜미, 김응곤(2009). 순서도를 활용한 알고리즘 교육 시스템 설계. **한국콘텐츠학회 종합학술대회 논문집, 7**(1), 1087-1091.

오연재, 박경욱, 김응곤(2012). 구조적 프로그램밍 언어 교육을 위한 알고리즘 시각화 시스템의 효용성 분석. **한국전자통신학회 논문지, 7**(1), 45-51.

우정호, 조영미(2001). 학교수학 교과서에서 사용하는 정의에 관한 연구. **수학교육학연구, 11**(2), 363-384.

우정호(2011). **수학 학습-지도 원리와 방법**. 서울: 서울대학교출판부.

윤진호, 문봉교(2019). IBM Q를 이용한 양자 컴퓨팅 개념의 구현 및 분석. **한국정보처리학회 학술대회논문집, 26**(1), 9-12.

이경화(1996). 교수학적 변환론의 이해. **수학교육학연구, 6**(1), 203 - 213.

이경화(2016). 현실적 수학교육 이론의 재음미: 수학적 창의성 교육의 관점에서. **수학교육학연구, 26**(1), 47-62.

이광근(2015). **컴퓨터 과학이 여는 세계: 세상을 바꾼 컴퓨터, 소프트웨어의 원천 아이디어 그리고 미래.** 서울: 인사이트.

이동근, 양성현, 신재홍(2017). 자연상수 e에 대한 이해를 기반으로 지수함수 $y=2^x$의 $x=0$에서의 순간변화율 구성에 관한 연구. **학교수학, 19**(1), 95-116.

이상구, 이재화, 김영록, 함윤미(2018). 4차 산업혁명과 대학수학교육 - 산업수학 프로그램 소개 및 관련 수학강좌 사례. **E-수학교육 논문집, 32**(3), 245-255.

이상구, 장지은, 김경원, 박경은(2014). GeoGebra와 미분적분학 개념의 시각화. **E-수학교육 논문집, 28**(4), 457-474.

이상희, 이종학, 김원경(2012). 부등식 영역의 최대·최소 문제에서 학생들의 수학적 사고에 GeoGebra가 미치는 영향. **교원교육, 28**(4), 1-44.

이종찬, 임향택, 홍강희, 김윤호(2013). 약한 측정과 양자정보. **물리학과 첨단기술, 22**(5). 13-18.

이준, 이상민(2019). 과학기술 한계 극복의 길을 여는 양자컴퓨터; 양자컴퓨터 R&D 현황과 정책. **KISTI ISSUE BRIEF 제11호**, 1-16.

이중권(2015). 수학교육에서 테크놀로지의 역사. 고상숙 외 22인 (편). **수학교육에서 공학적 도구** (pp. 3-23). 서울: 경문사.

이혁성(2019). 양자컴퓨터 기술 동향 및 산업 응용. **한국콘텐츠학회지, 17**(2), 25-28.

임현정, 고상숙(2016). GeoGebra를 활용한 반힐레 기하교수법에서 도구화에 관한 연구. **E-수학교육 논문집, 30**(4), 435-452.

장경배, 김현준, 박재훈, 송경주, 서화정(2021). 그루버 알고리즘 적용을 위한 LEA 양자 회로 최적화. **정보처리학회논문지, 10**(4), 101-106.

장경배, 김현지 외 4인(2021). Grover 알고리즘 공격 비용 추정을 통한 DES에 대한 양자 암호 분석. **정보보호학회논문지, 31**(6), 1149-1156.

장종욱, 김화선(2004). CAI를 활용한 수업의 효과성에 관한 연구-초등학교 도형학습. **정보통신연구지, 5**, 85-93.

전혜진, 정혜윤, 이경화(2020). 초등학생의 비형식적 통계적 추리 개발을 위한 자료 모델링 과제 및 수업의 설계. **학교수학, 22**(3), 689-716.

정영옥(2005). 교과과정 개발을 위한 기초로서의 개발연구에 대한 고찰. **수학교육학연구, 15**(3), 353-374.

정인기(2004). 정렬 프로그래밍 교육을 위한 시각화 도구의 개발. **컴퓨터교육학회 논문지, 7**(6), 27-35.

조영미(2001). **학교수학에 제시된 정의에 관한 연구**. 박사학위논문, 서울대학교 대학원.

조영미(2002). 수학 교과서에서 사용하는 정의의 특성 분석과 수준 탐색. **학교수학, 4**(1), 15-27.

조윤호, 허준(2020). IBM Q를 이용한 논리 게이트 기반 양자 곱셈기 구현. **한국통신학회 학술대회논문집, 2020**(8), 1356-1358.

조은영, 김영철, 정희범, 차규일(2021). 양자컴퓨팅 소프트웨어 최신 기술 동향. **전자통신동향분석, 36**(6), 67-77.

조지민 외 6인(2011). 국제 학업성취도 평가 연구(PISA/TIMSS): PISA 2012 예비검사 시행보고서. **한국교육과정평가원 연구보고 RRE**, 4-2.

주순종, 김응환(2009). 중학교 1학년 함수지도에서의 공학적 도구 활용에 관한 연구. **한국학교수학회논문집, 12**(3), 189-209.

하진영, 김태현, 이홍석, 허준(2019). 양자 검색 알고리즘을 이용한 Exactly-1 3-SAT 문제 접근법. **한국통신학회 학술대회논문집, 2019**(1), 265-266.

하진영, 안병규, 이종현, 신정환, 허준(2018). IBM Q 양자 컴퓨터를 이용한 양자 정보 전송 알고리즘 구현. **한국통신학회 학술대회논문집, 2018**(1), 25-26.

한정민, 박만구(2010). 수학적 창의성 관점에서 본 교사의 발문 분석. **한국초등수학교육학회지, 14**(3), 865-884.

홍영석, 손홍찬(2021). 중학교 수학 영재아의 수학적 정당화에 대한 인식과 특성에 관한 연구. **한국학교수학회논문집, 24**(3), 261-282.

황혜정, 김수진(2019). 반성과 메타인지의 의미에 대한 고찰. **E-수학교육 논문집**, 33(1), 35-45.

황혜정, 최승현, 조성민, 박지현(2019a). **수학교육학신론 1**. 용인: 문음사.

황혜정, 최승현, 조성민, 박지현(2019b). **수학교육학신론 2**. 용인: 문음사.

황혜정(2019). 교수학적 변환에서의 배경화와 반성에 관한 이해. **East Asian Mathematical Journal, 35**(2), 35(2), 259-275.

Balacheff, N. (1987). Procesus de preve et situations de validation. *Educational Studies in Mathematics, 18*, 147-176.

Botsinis, P., Ng, S. X., & Hanzo, L. (2013). Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design. *IEEE access, 1*, 94-122.

Brousseau, G., & Otte, M. (1991). *The fragility of knowledge. In mathematical knowledge: Its growth through teaching* (pp. 11-36). Dordrecht: Springer.

Bruner, J. S. (1960). *The process of education*. Cambridge: Harvard University Press.

CadwalladerOlsker, T. (2011). What Do We Mean by Mathematical Proof? *Journal of Humanistic Mathematics, 1*(1), 33-60.

Chevallard, Y. (1985). *La transposition didactique. du savoir savant au savoir enseigné*. Grenoble: La Pensée Sauvage.

Dasgupta, S., Vazirani, U., & Papadimitriou, C. (2008). *Algorithms*. Dubuque: McGraw-Hill.

강신원 역(2016). **알고리즘**. 부천: 프리렉.

Dreher, A., Lindmeier, A., Heinze, A., & Niemand, C. (2018). What kind of content knowledge do secondary mathematics teachers need? *Journal für Mathematik - Didaktik, 39*(2), 319 - 341.

Fischbein, E. (1982). Intuition and Proof. *For the Learning of Mathematics, 3*(2), 9-24.

Fischbein, E. (1987). *Intuition in science and mathematics*. Dordrecht: Reidel.

Freudenthal, H. (1978). *Weeding and sowing: preface to a science of mathematical education*. Dordrecht: D. Reidel.

Freudenthal, H. (2002). *Revisiting Mathematics Education: China lectures*. New york: Kluwer academic publishers.

Ginther, J. L. (1964). *A Study of definition in high school mathematics textbooks*. Doctral Dissertation, University of Illinos.

Gravemeijer, K., & Cobb, P. (2006). Design research from a learning design perspective. In J. Van den Akker, K. Gravemeijer, S. McKenny, & N. Nieveen (Eds.), *Educational design research* (pp. 17-51). London: Routledge

Grover, L. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*. 212-219.

Harel, G., & Sowder, L. (1998). Type of students' justification. *Mathematics Teacher, 91*(8), 670-675.

Knuth, E., & Elliott, R. (1998). Characterizing Students' Understandings of Mathematical Proof. *Mathematics Teacher, 91*(8), 714-717.

Laborde, C. (1993). The Computer as Part of the Learning Environment: The Case of Geometry. In Keitel, C., & Ruthven, K. (Eds). *Learning from Computers: Mathematics Education and Technology*. NATO ASI Series, vol 121. Berlin: Springer.

Lala, P. K. (2019). *Quantum computing: A beginner's introduction*. New York: McGraw Hill Education.
이태휘 역(2020). **양자 컴퓨팅 입문: 간결하게 배우는 양자 컴퓨팅**. 서울: 에이콘.

McMahon, D. (2008). *Quantum computing explained*. New Jersey: John Wiley & Sons, Inc.

Mohseni, M. et al. (2017). Commercialize quantum technologies in five years. *Nature, 543*(7644), 171-174.

Mukherjee, S. (2022). A grover search-based algorithm for the list coloring problem. *IEEE Transactions on Quantum Engineering, 3*, 1-8.

National Council of Teachers of Mathematics(NCTM) (2000). *Principles and standards for school mathematics*. Reston: The Council.
류희찬 외 5인 역(2014). **학교수학을 위한 원리와 규준**. 서울: 경문사.

Neapolitan, R. (2014). *Foundations of algorithms*. Sudbury: Jones and Bartlett Learning

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. New York: Cambridge University Press.

Samandeni, Z. (1984). Action proof in primary mathematics teaching and in teacher training. *For the Learning of Mathematics, 4*(1), 32-34.

Scherer, W. (2019). *Mathematics of quantum computing*. Cham: Springer.

Schwartz, J. L. (1989). Intellectual mirrors: A step in the direction of making schools into knowledge making places. *Harvard Educational Review, 59*(1), 51-62.

Vinod, G. M., & Shaji, A. (2021). Finding solutions to the integer case constraint satisfiability problem using Grover's algorithm. *IEEE Transactions on Quantum Engineering, 2*, 1-13.

Yershalmy, M., & Chazan, D. (1990). Overcoming visual obstacles with the aid of the Supposer. *Educational Studies in Mathematics, 21*(3), 199-219.

Abstract

Development of Quantum Algorithm Education Program using IBM QX

- Focusing on the Grover algorithm -

Ryu, Geon

Department of Mathematics Education

The Graduate School

Seoul National University

The era in which students will live in the future is an era in which existing scientific and technological challenges are solved by quantum computers, and new application industries and research fields are launched. Therefore, it seems that future education should pay attention to fostering creative convergence talent with expertise in quantum computers.

The purpose of this study is to lower the mathematical rigor of Grover's algorithm through didactic transposition and to develop an engineering tool-based <Quantum Algorithm> education program for students in secondary education institutions. To this end, the Grover

algorithm's content system was established, and the restructured Grover algorithm's content system was proposed by declaring teaching knowledge at the school mathematics level within the engineering integrated education environment through analysis of definition types and definition levels. In addition, a task based on the understanding of the Grover algorithm operating principle was developed, and a teaching and learning process plan was designed accordingly. Finally, in 2022, the <Quantum Algorithm> education program developed in this study was applied to the second grade of high school students belonging to the Siheung Gifted Education Center affiliated with Seoul National University College of Education, and the process was revised and supplemented by evaluating and analyzing it.

This study is significant in that it presents the possibility of a new mathematics subject for the introduction of school mathematics, as the necessity of establishing a new mathematics subject to prepare for the future society is emphasized. Meanwhile, the educational program developed in this study has educational significance in that learners can cultivate communication and reasoning skills. In addition, it is meaningful that access to teachers is high in that it does not involve coding and explanations of the teaching and learning process are presented in detail.

keywords : Grover algorithm, IBM QX,
education program, pedagogical transformation
Student Number : 2021-21157