윌첵의 상상은 현실이 된다-항하사에서 영겁까지

MIT 교수 프랭크 윌첵(Frank Wilczek, 1951 년생)은 천재이면서 행운의 물리학자다. 대학원생 시절 22 세때 쓴 논문으로 52 세에 노벨물리학상을 받았다. 입자물리학자들 사이에 우주에 존재하는 입자는 보손과 페르미온이라는 두 종류로 나뉜다는 사실이 십계명 같은 진리로 여겨지던 1982 년에 그는 홀로 기발한 생각을 했다. 만약 우주 공간 같은 3 차원이 아니라 오직 2 차원인 평면에서 운동하는 입자가 있다면 그 입자는 꼭 보손이나 페르미온일 필요가 없다는 것이다. 윌첵은 이 가상의 새로운 입자를 애니온(anyon)이라고 불렀다. 삼성 휴대폰 애니콜이 장소를 가리지 않고 통화가 가능하다는 특성을 강조한 이름이었던 것처럼 무엇이든 될 수 있다는 의미의 'any'를 넣어 새로운 입자를 만들어낸 것이다 [1].

동화에 단골로 등장하는 상상의 동물 용처럼 윌첵의 상상의 산물로 여겨지던 애니온은 실험실에서 분수 양자홀 상태가 발견됨으로써 놀랍게도 현존하는 입자로 확인되었다. 샌드위치 속 잼처럼 두 고체 사이의 경계면에 갇혀 있는 아주 얇은 층의 2 차원 전자계에 수직 방향으로 대단히 강한 자기장을 걸어주면 전자의 운동이 직선 운동에서 원운동으로 극단적으로 바뀌면서 양자 홀 상태(quantum Hall state)라는 걸 만든다. 운동장이 댄스홀로 바뀐 것이다. 전자의 춤에는 아마추어 선수들이 추는 서툰 춤 같은 정수(integer) 양자 홀 상태와 전문가들의 춤을 방불케하는 분수(fractional) 양자 홀 상태가 있는데 그 중 우리의 관심을 끄는 건 분수 양자 홀 상태다. 잘 조화된 군무를 보면 마치 한 명의 전문가가 추는 세련된 안무를 보는 착각을 일으키듯 여러 입자가 모이면 말 잘 듣는 개미로봇군단처럼 입자들이 조직적으로 움직여 하나의 입자처럼 거동하는 준입자를 만들어내는 능력이 있다. 분수 양자 홀 상태의 경우에는 마치 전자 하나를 세 조각으로 쪼개서 전하량을 나눠 가진 것처럼 거동하는 준입자가 있다. 이 모습이 마치 정수 1 의 전하량을 갖고 있던 전자가 ⅓, ⅕ 같은 분수값을 가진 전하량으로 쪼개지는 것 같다고 해서 분수 양자 홀 상태라고 부른다. 이렇게 분수화된 전하를 갖는 준입자는 윌첵이 예측한 애니온의 성질을 그대로 갖고 있다. 윌첵이 애니온을 상상한 이론 물리학 논문은 1982 년 4 월에 나왔고, 분수 양자홀 상태의 존재를 발견한 실험 물리학 논문은 그 해 5 월에 출판됐다. 상상이 한 달 후에 현실로 증명되었으니 이 행운은 정말 역사에 기록될만하다. 윌첵의 애니온은 가환 애니온(abelian anyon)이다. 아벨이라는 수학자가 만든 이론에서 이름을 따왔는데, 영화 '매트릭스'의 '스미스 요원'처럼 서로 다른 점이 하나도 없는 복제 인간같은 존재라서 두 입자의 위치가 바뀌어도 그 사실을 누구도 알아차릴 수 없다.

새로운 입자에 대한 윌첵의 상상이 현실이 되자 애니온에 대한 연구는 봇물이 터진 듯 활발해졌고, 1991 년에는 윌첵의 가환 애니온보다 한층 더 기이한 입자도 2 차원에 존재할 수 있다는 이론적 제안이 나왔다. 미국 예일 대학교의 그렉 무어(Greg Moore)와 니콜라스 리드(Nicholas Read), 매사추세츠 공대의 샤오강 웬(Xiao-Gang Wen) 등이 주창한 비가환 애니온(non-abelian anyon) 입자이다. 이들은 두 개의 비가환 애니온 위치를 바꾸면, 비록 동일해 보이는 애니온을 교환했다 하더라도, 교환 후의 상태가 이전의 상태와 달라질 수 있다는 점을 증명했다. 입자의 위치만을 안다고 해서 그 입자의 성질을 모두 아는 것은 아니라는 간단하지만 중요한 통찰의 결과였다. 비가환 애니온 입자들이 사는 세상에서는 내가 없는 사이 누군가 두 비가환 애니온의 위치를 바꾸어 놓으면 금방 알아차릴 수 있다. 비가환 애니온의 위치를 교환하면 본래 상태가 아니라 새로운 상태가 만들어진다. 비가환

애니온에는 '위치'라는 정보 말고 또다른 정보가 있기 때문이다. 두 입자가 자리를 바꾸면 위치 정보는 같지만 그 밖의 정보는 달라지기에 자리를 바꾼 사실이 그만 탄로나는 것이다. N 개의 비가환 애니온에 1 부터 N 까지 숫자를 매긴 뒤, 처음엔 (1,2)번 애니온을 교환하고, 그 다음엔 (2,3)번, 그 다음엔 (4,6)번, 이런 식으로 입자를 서로서로 교환하다 보면 계속 새로운 상태가 나온다. 가능한 교환 과정을 모두 이용해서 만들 수 있는 서로 다른 상태의 개수는 애니온의 숫자 N 에 지수적으로 비례해 증가한다. 이렇게 지수적으로 많은 비가환 애니온이 존재하는 분수 양자홀 상태도 있다는 점을 무어-리드의 논문에서 예언했다 [2].

무어-리드가 예언한 비가환 애니온은 아직도 실험으로 결정적인 존재 증거를 찾지 못하고 있다. 그러나 신기하지만 여전히 리드-무어의 상상 속에만 존재하는 환상같은 비가환 애니온 예언이 요즘 양자 컴퓨터 분야에서 주목받고 있다. 비가환 입자를 이용한 위상 양자 연산(topological quantum computation) 덕분이다. 위상 양자 연산은 1990 년대 후반 알렉세이 키타예프(Alexei Kitaev)가 주창했고 [3,4], 마이클 프리드먼(Michael Freedman) 등이 수학적 토대를 다진 분야다 [5]. 비가환 입자가 양자 컴퓨터의 기본 소자가 될 수 있다는 인식이 퍼지면서 마이크로소프트는 대표적인 후보 물질이었던 분수 양자 홀 상태를 이용해 양자 컴퓨터를 만드는 데 투자하기 시작했고, 연구의 중심지 역할을 할 스테이션-Q 를 캘리포니아에 있는 산타 바바라 주립대학의 한 건물을 빌려서 만들었다.

양자 홀 물질을 통한 양자 컴퓨터 구현이란 접근법에는 '제어'의 문제가 있다. 양자 홀 물질에는 수많은 전자가 있다. 이 전자들 틈에서 몇 개의 말 잘 듣는 비가환 애니온을 준입자 상태로 만들어낸 뒤 그걸 개별적으로 제어하고 양자 연산을 할 수 있어야 비로소 마이크로소프트가 원하는 양자 컴퓨터가 만들어진다. 결국 전자 하나하나를 잘 제어할 수 있어야 양자 컴퓨터에 필요한 연산을 할 수 있게 된다. 그러나 전자는 너무 작고, 인간에게 죽음의 숙명이 있듯 전자에게도 반드시 따라야 할 쿨롱 법칙 같은 그 나름의 자연 법칙이 있다. 쿨롱이 발견해서 쿨롱 법칙이 라 불리는 전자의 숙명은 서로를 강한 힘으로 밀어낸다는 것이다. 그런 자연 법칙을 다스리면서 개별적으로 전자를 제어한다는 건 결코 쉽지 않다. 그 탓인지 마이크로소프트는 양자 컴퓨터 연구의 선발 주자임에도 아직 뚜렷한 성과를 보이지 않고 있다.

비가환 입자와 양자 컴퓨터의 관계를 이해하려면 먼저 일반 컴퓨터에 작동하는 기본 소자인 비트(bit)에 대해 알아야 한다. 컴퓨터는 문자 그대로 계산을 하는 기계다. 간단한 프로그램을 통해 복잡한 수학 계산을 인간의 두뇌보다 훨씬 빨리 할 수 있는 기계다. 인간은 두개골 속 뇌의 뉴런을 이용해 계산을 하지만 컴퓨터는 아주 작은 크기의 물질(이걸 흔히 소자라고 부른다)을 통해 계산을 한다. 일단 모든 수학적 연산을 0 과 1 이라는 두 가지 숫자(이진수)를 기반으로 한 연산으로 변환한다. 그리고 실리콘을 기반으로 한 아주 작은 소자의 물리적인 상태가 단 두 종류만 있도록 만든다. 이 작은 소자를 비트라고 부른다. 전기를 흘려 비트의 상태를 0 에서 1 로, 혹은 1 에서 0 으로 바꿔주는 과정을 대규모로, 빠른 속도로 수행하면서 수학적 연산이 이루어진다.

가령 다섯 개짜리 비트가 있고 그 상태는 |00110>이라고 하자. 첫 번째 비트는 0, 두 번째 비트도 0, 이런 식이다. 이 상태를 다른 상태, 가령 |01010>으로 바꾸는 게 이른바 연산이다. 여기 든 예에서는 두 번째와 세 번째 비트의 상태가 뒤바뀌었다. 이런 조작을 게이트(gate) 연산이라고 한다. 몇 가지 단순한 게이트 연산을 끊임없이 적용해 비트의 상태를 계속

바꿔나가는 게 컴퓨터가 하는 '계산'이다. 군중을 모아 카드섹션으로 온갖 무늬를 만들어내는 것과 비슷하다. 인간이 실수하듯 때론 0 이어야 할 비트가 실수로 1 이 될 수도 있다. 이럴 땐 오류를 찾아내 보정해주어야 한다. 오류 보정 과정은 컴퓨터 속에서 쉴새없이 이루어지고 있고, 그 덕분에 우리는 안심하고 컴퓨터를 사용할 수 있다.

양자 연산은 비트 대신 큐빗(qubit)을 이용한다. 큐빗이 표현하는 정보는 0,1 의 이진수가 아니라 허수와 실수를 합한 복소수에 가깝다. 이진수는 0 과 1 두가지 뿐이지만 허수와 실수는 0, 0.1, 0.01……나열할 수조차 없는 무한대다. 게다가 큐빗의 상태는 중첩될 수 있다. 살아있는 것도 아니고 죽은 것도 아닌 슈뢰딩거의 고양이가 큐빗에 존재하면서 큐빗이 2 개 있으면 제곱 개의 가능한 상태를, n 개 있으면 n 제곱 개의 상태를 만들어 낸다.

불교에서는 갠지스강의 모래알만큼 많은 수인 항하사(恒河沙)를 시작으로, 인간의 한계를 넘어 수로 나타낼 수 없음을 뜻하는 무량대수(無量大數)라는 것이 있다고 한다. 이러한 단계적인 수에서 벗어나 무량대수보다 더욱 큰 절대적인 시간개념의 수로 겁(劫)도 있다. 겁은 우주가 생겨나 멸망하기까지의 무한함이다. 비유적으로 1 겁은 가로, 세로와 높이가 10km 인 바위에 선녀가 백년에 한 번씩 지나가면서 옷깃을 스쳐 옷이 다 닳아 없어지는 시간, 또는 이 바위와 같은 크기의 성 안에 겨자씨를 가득 채우고 백년마다 겨자씨를 하나씩 꺼내어 그것이 없어질 때까지의 시간이라고 한다. 큐빗으로 행하는 양자 연산은 항하사에서 시작해서 무량대수를 지나 영겁을 떠올리게 한다.

다섯 개짜리 비트가 가질 수 있는 상태는 |00000>부터 |11111>까지 총 32 개가 있고, 보통의 컴퓨터라면 서른 두 개의 상태 중 어떤 특정한 상태만 가질 수 있다. 컴퓨터의 연산은 하나의 가능한 비트 상태에서 다른 가능한 비트 상태로 변환하는 과정에서 이루어진다. 반면 다섯 큐빗짜리 양자 컴퓨터는 이 서른 두 개의 비트 상태를 중첩한 상태로도 존재할 수 있다. 쉬레딩거의 고양이를 떠올리게 하는 중첩이란 건 양자 컴퓨터가 이런 상태에 있을 수도 있고 저런 상태에 있을 수도 있다는 걸 의미한다. 모든 가능한 5-비트 상태가 중첩된 형태로 공존하는 게 5-큐빗의 상태라고 이해하면 된다. 5-큐빗의 상태를 지정하려면 각각의 5-비트 상태에 있을 (총 32 개의) 확률을 지정해 주어야 한다. 문제는 이 확률이란 게 0 또는 1 처럼 이진수가 아니라 0 과 1 사이의 아무 값이나 다 가질 수 있는 실수라는 점이다. 이런 유연성은 양자 컴퓨터가 갖는 강력한 연산 능력의 원천이 되지만 반대로 양자 컴퓨터를 만들고 운영하기 어려운 이유이기도 하다. 0.1 로 주어야할 확률 값을 0.2 로 주었을 때, 이미 그 양자 회로는 오류를 담고 있다. 0 이어야 할 비트 값이 1 일 때 그걸 보정해주는 것보다 훨씬 어려운 문제다. 열 개의 큐빗으로 만들어진 양자 컴퓨터는 2^10=1024 개의 확률을 표시하는 숫자를 항상 제어할 수 있어야 한다. 큐빗의 개수가 늘어날수록 제어해야 할 숫자의 개수도 지수적으로 늘어난다. 문제는 이 숫자들이 저절로 바뀌는 경향이 있다는 점인데 이런 현상을 결깨짐(decoherence)이라고 부른다. 결깨짐을 방지할 대비책이 없으면 양자 컴퓨터는 아주 잠깐 작동하다 고장나버리는 무용지물에 불과하다.

이런 어려움을 단숨에 피해갈 수 있는 방법이 있다. 위상학적 양자연산이다. 개인의 실수를 집단의 실수로 대치해 오류 확률을 줄인다는 생각이다. 가령 열 명이 손을 잡고 강강술래를 한다고 상상하자. 왼쪽으로 돌 때를 0, 오른쪽으로 돌 때를 1 이라고 부르자. 한 개인 대신 열 명이 비트 상태를 구현하니까 그만큼 오류가 생길 가능성도 적어진다. 게다가 회전 방향이란 건 연속적으로 바뀌는 게 아니다. 시계 방향 아니면 반시계 방향, 이렇게 두 가지 뿐이다.

자연스럽게 비트를 구현할 수 있고 오류 발생 가능성도 적어진다. 위상학적 양자연산은 수많은 큐빗을 동원해 한 개의 집단적 큐빗 상태를 만들어내는 방법이다. 많은 큐빗을 동원해야하는 번거로움이 있긴 하지만 일단 만들고 나면 각종 오류에 대한 안정성을 얻을 수 있다.

비트를 기반으로 하는 연산은 수학적으로 말하면 이진수가 존재하는 공간에서 이루어진다. 수학적으로 이보다 더 단순한 구조를 상상할 수 있을까 싶을 정도로 아주 단순한 구조의 수학적 공간이다. 컴퓨터로 연산을 제대로 하려면 이진수 공간에 있는 모든 가능한 상태를 물리적으로 구현할 수 있어야 한다. 반면 양자 연산을 수행하는 수학적 공간을 힐버트 공간(Hilbert space)라고 부른다. 수학자 힐버트가 이런 공간을 처음으로 상상했기 때문에 붙은 이름이다. 양자 연산을 제대로 하려면 힐버트 공간에 있는 모든 양자 상태를 큐빗으로 구현할 수 있어야 한다. N 개의 비가환 애니온이 있으면 그들이 만들어내는 힐버트 공간의 크기는 N 에 지수적으로 증가한다고 했는데, 이런 공간에서 양자 연산이 잘 작동하려면 지수적으로 많은 모든 상태에 다 접근할 수 있어야 한다. 위상 양자 연산의 출발점은 비가환 애니온이 N 개 있을 때 이 애니온의 위치를 이리저리 교환하는 작업만으로도 힐버트 공간의 모든 상태를 다 구현할 수 있다는 수학적 증명이다. 마이크로소프트는 양자 홀 물질에서 비가환 입자를 만든 뒤 그 위치를 바꾸는 조작을 통해 양자 컴퓨터를 만들고 싶어한다.

비가환 입자는 자신의 과거를 기억하는 입자다. 과거를 기억하는 입자를 양자 연산에 이용하자는 생각이 위상 양자 연산이다. 일반 컴퓨터가 하는 연산은 비트의 상태를 0 에서 1 로, 1 에서 0 으로 바꾸는 물리적 과정을 통해 이루어진다. 위상 양자 연산에서는 비가환 애니온의 위치를 맞바꾼다. 궤도는 중요하지 않다. 한바퀴 감았다 또는 안 감았다, 혹은 몇 번 감았다라는 정보만이 중요하다. 설령 연산 과정에서 자질구레한 오류가 있다 하더라도 감았다는 사실 자체를 번복하기는 힘들다. 위상 양자 연산이 양자 연산의 희망으로 자리잡는 이유다.

키타예프를 비롯한 양자 연산 이론가들의 통찰이 위대한 이유는 양자 연산을 하기에 적합한 구조를 양자 홀 물질같은 자연의 선물에 의존하지 말고 아예 인위적으로 만들어 놓고 시작하자는 데 있다. 가령 초전도체를 기반으로 한 조셉슨 소자라는 걸 이용해서 큐빗을 만든다. 조셉슨 소자는 대량으로 만드는 방법이 이미 공정화되어 있다. 가로, 세로 0.1-0.2 마이크론 정도 크기의 조셉슨 소자를 기판 위에 가지런히 만든 뒤 전자기파를 이용해 소자 하나하나의 양자 상태를 조작하는 게 가능하다. 구글이나 IBM 에서 추진하는 양자 컴퓨터는 조셉슨 소자를 기반으로 만들어졌고 현재 가장 고성능 양자 컴퓨터로 인정받는다. 원자를 이용해 양자 컴퓨터를 만드는 방법도 있다. 원자에서 전자 하나를 없앤 것을 이온(ion)이라고 부르는 데, 이온은 전기적으로 중성인 원자와는 달리 전하를 띠기 때문에 전기장을 이용해 그 위치를 제어하기 쉬워진다. 이 원리를 이용하여 수십 개의 원자를 가지런히 진공 속에 배열한 뒤 레이저 등을 이용해 이온 상태를 제어하거나 게이트 연산, 측정을 한다. 한국에서 대학을 마치고 유학을 가 미국 듀크대학교에 재직 중인 김정상 교수가 공동 창업한 것으로 잘 알려진 Ion-Q, 거대기업 허니웰의 자회사로 성장한 퀀티니엄(quantinuum)은 이온 기반 양자 컴퓨터를 만드는 데 성공한 대표적인 기업이다. 조셉슨 소자를 이용하든 이온을 이용하든 모두 몇 십 큐빗 정도로 작동하는 양자 컴퓨터를 만들어 활용하는 중이고, 양자 연산을 수행할 능력을 갖춘 조셉슨 소자의 집합, 혹은 이온의 집합을 양자 플랫폼이라고 부른다. 현재 양자

연산의 구도는 조셉슨 소자 기반, 이온 원자 기반 등 서로 다른 양자 플랫폼이 경쟁하는 모양새다.

그 다음 단계는 양자 플랫폼에서 비가환 애니온을 만드는 작업이다. 키타예프는 토릭 코드라는 상태를 양자 플랫폼에서 만들면 가환 애니온이 준입자 상태로 만들어진다는 것과 양자쌍(quantum double)상태라는 것을 만들면 비가환 애니온이 준입자 상태로 만들어진다는 것을 1997 년에 이미 증명했다. 이것만해도 대단한 발견이다. 1982 년에 가환 애니온이 분수 양자홀 계에서 발견된 것은 자연이 우리에게 준 기적같은 선물이었고 과학자들의 예상 밖에 있던 사건이었다. 이제 키타예프의 증명을 통해 우리는 가환이든 비가환이든 모든 애니온을 우리가 원하는만큼 공학적으로, 인위적으로 만들어내는 방법을 알게 되었다. 2022 년에는 양자 플랫폼을 이용해 실험실에서 드디어 가환 애니온을 만들어내는 토릭 코드 상태를 만들어냈다.

아쉽게도 토릭 코드에서 만들어내는 가환 애니온은 위상학적 양자 연산을 수행하기엔 불충분하다. 가환 애니온 두 개의 위치를 맞바꾸어도 여전히 동등한 양자 상태가 얻어진다는 그 '가환성' 때문에 양자 연산이 요구하는 풍부한 힐버트 공간을 제공하지 못하기 때문이다. 위상 기반 양자 컴퓨터라는 목적을 위해서는 비가환 애니온을 만들 방법을 찾아야 한다. 그러나 비가환 양자쌍 상태를 양자 플랫폼에서 구현한다는 건 기환 애니온에 비해 한층 더 요원해서, 지름길을 찾아야만 했다.

상상할 수 있는 지름길 중 하나는 일단 가환 애니온을 만든 뒤 추가적인 조작을 가해 이것을 비가환 애니온으로 탈바꿈시키는 방법이다. 큐빗을 가로세로 반듯하게 배열하는 대신 일부러 찌그러진 형태로 만들면 가환 애니온이 마치 비가환 애니온처럼 거동한다는 수학적 증명이 있었다. 그 증명을 착실하게 실험적으로 구현한 성과가 2023 년에 구글에서 나왔다 [6].

또 다른 지름길은 비가환 애니온을 만드는 데 들어가는 시간을 줄여주는 방법이다. 가환 애니온을 만들려면 얽힘이 없는 초기 양자 상태를 위상학적인 상태로 바꾸어야 하는데, 이 변환 과정에 동원되는 양자 게이트의 개수는 큐빗의 개수에 비례해서 증가한다. 큐빗이 많을수록 게이트 연산의 숫자도 늘어나고, 연산 과정에서 오류가 생길 가능성도 커진다. 이 어려움을 정면 돌파하는 대신 우회하는 방법이 있다. 중간중간 전략적으로 기획된 측정을 하고, 그 측정 결과를 이용해 그 다음 양자 게이트 연산을 어떻게 할지를 결정하는 일종의 혼합적 방법이다. 이 방법을 이용하면 위상학적 질서를 갖는 상태를 만드는 데 들어가는 게이트 연산의 개수가 큐빗의 개수와 무관하게 일정해진다.

구글처럼 가환 애니온을 만든 뒤 비가환 애니온을 만들지 않고, 처음부터 비가환 애니온을 만들고자 할 때도 측정이란 기술이 들어간다. 흔히 양자역학적 상태는 측정을 당하는 순간 붕괴된다고 알려져 있고, 측정은 양자 연산에 해로운 것, 또는 금기로 생각하기 쉽다. 하지만 이런 오해를 정면으로 거스르는 측정 기반 양자 연산이란 방법론이 이미 20 년 전에 나왔다. 어떤 양자 상태에 잘 준비된 측정을 전략적으로 하면 새로운 양자 상태가 된다. 다음 측정은 또다른 양자 상태를 준다. 이렇게 계속 바뀌어 가는 양자 상태가 결국 우리가 원하는 양자 연산을 다 수행할 수 있다는 제안이었다. 예전에는 쓸모없다고 버려지거나 제값을 못받았지만 이제는 몸값이 높아진 소곱창이나 양같은 소 부산물처럼 이 제안의 가치높은

부산물 중 하나는 위상학적 상태를 비위상학적인 상태로부터 만들어내는 게 측정을 통해 가능하다는 점이다. 그냥 가능한 게 아니라 손쉽게 가능하다.
2022 년에 하버드 대학의 응집 이론 물리학자 비쉬와나트 교수와 그의 젊은 연구진은 측정을 전략적으로 이용해서 비가환 애니온계를 구현하는 정교한 이론을 발전시켰다. 마침 퀀티니엄에는 이 이론을 따라 비가환 애니온을 만들어낼 만큼 크기가 큰 이온 기반 양자 컴퓨터가 막 만들어졌다. 27 개의 이온을 자유자재로 조작할 능력을 갖추자마자 퀀티니엄은 하버드 연구진의 제안을 실험으로 옮겼고, 2023 년에 드디어 비가환 애니온 세 개를 만들고 서로 감는데 성공했다 [7].

양자역학의 토대인 슈뢰딩거 방정식이 만들어진 1925 년으로부터 거의 한 세기가 지났다. 양자 파동함수는 원자나 그보다 작은 세계를 설명하기 위한 도구였다. 그런데 양자 연산에서는 양자 파동 함수가 계산하는 도구 역할을 한다. 양자 컴퓨터 소자로 사용되는 초전도체 큐빗, 또는 원자 큐빗이 갖는 양자 파동 함수는 자연적으로 존재하는게 아니라 인간이 조작하는대로 만들어진다. 양자 컴퓨터에서 파동 함수는 자연을 설명하는 도구가 아니라 양자 계산을 하기 위해 인위적으로 만들어진 도구가 되었고, 한 세기 전에 시작된 물리법칙인 양자역학은 양자공학의 시대를 여는 도구로써 주목받고 있다. 한 시대에서 발견된 법칙이 다음 시대를 여는 도구가 될 수 있다는 인식 전환을 한번 겪어보면 양자 컴퓨터가 일반 컴퓨터, 심지어 양자역학과도 얼마나 다른지 이해할 수 있다. 컴퓨터의 연산이란 0000 이란 비트의 물리적 상태를 0010 이란 새로운 물리적 상태로 바꾸는 식의 조작을 계속하는 과정을 통해 어떤 수학적 연산을 수행한다. 양자 컴퓨터는 양자 파동함수로 기술되는 어떤 양자 상태를 계속 변환시키면서 그 변환 과정 속에 어떤 수학적 연산을 수행하도록 한다.

2023 년에 성공한 비가환 애니온의 생성과 교환 실험은 위상 양자 연산이란 거대한 목표에 비하면 아기가 드디어 제발로 서서 한 걸음을 뗀 정도이다. 하지만 천리길도 한걸음부터라고 했으니 지금 걸음마를 시작한 아기가 40 년 뒤엔 어떻게 자라나 있을까 상상해보면 저절로 가슴이 부풀어 오른다. 두 입자의 양자 얽힘을 최초로 증명한 실험은 1980 년부터 이루어졌고 40 여년이 지난 뒤에야 노벨상 수상으로 이어졌다. 지금부터 40 년 뒤 양자 컴퓨터가 보편화된 세상을 한 마디로 설명한다면 '상상초월(imaginatio transcendit)'일 것이다.

Topological quantum computation - from Wilczek's dream to reality

Frank Wilczek, a professor at MIT, is both a genius and a lucky physicist. He won the Nobel Prize in Physics at the age of 52 for a paper he wrote at the age of 22 while a graduate student at Princeton. In 1982, at a time when it was considered a God-given truth among physicists that there are only two kinds of particles in the universe: bosons and fermions, he had a brilliant idea that ran counter to this widely-held belief. He argued that, if there were particles that could move only in a two-dimensional plane rather than the three-dimensional world we are living in, the those particles wouldn't necessarily be bosons or fermions. Wilczek called this hypothetical new particle an anyon. Just as Samsung's AnyCall was named to emphasize its ability to make calls anywhere, the "any" in the name of the new particle suggests that it can be anything, not just bosons or fermions [1].

Such a particle could easily have been nothing more than a figment of Wilczek's imagination, however brilliant it may have been, in a way that the wonderful creature of a dragon can only be found in fairy tales. Much to everybody's surprise including (I am sure) Wilczek's own, the anyon was confirmed as a real particle as soon as Wilczek's idea was published, when fractional quantum Hall states were discovered by condensed matter physicists in the laboratory. When a very strong magnetic field is applied perpendicularly to a very thin layer of two-dimensional electrons trapped at the interface between two solids, like jam in a sandwich, the motion of the electrons changes dramatically from rectilinear to circular, creating what is called a quantum Hall state. Basically, the playground where children used to run around randomly turns into a dance floor where people execute polished circular motion around the other dancers. More precisely, there are integer quantum Hall states where the electrons dance like amateurs, and fractional quantum Hall states, where the electronic dance parallels that of seasoned dancers expertly swinging other equally competent dancers. Among the two, it is the fractional quantum Hall states that interest us.

A well-coordinated group dance can give the illusion of watching a polished choreography performed by a single professional. A collection of particles has the similar ability to create 'quasiparticles' that behave like a single particle, while in fact it is a consequence of a large collection of underlying particles moving together in a coordinated fashion, perhaps like an army of highly coordinated ants. In fractional quantum Hall states, there are quasiparticles that behave as if an electron had been split into three pieces, each with the charge only one-third of the electron's charge. This is why such a state is called a fractional quantum Hall state, because an electron appears to have been split into several fractional charges. Quasiparticles with such fractionalized charges turn out to have exactly the properties of anyons predicted by Wilczek. The theoretical paper in which Wilczek imagined the anyon was published in April 1982, and the experimental paper in which Dan Tsui and Horst Stormer discovered the existence of the fractional quantum Hall state was published in May of that year. A stroke of Wilczek's imagination proved to be real in just a month, in a highly two-dimensional system synthesized by material scientists. Wilczek's anyon is an abelian anyon, so named after a mathematical theory created by a famed Norwegian mathematician, Niels Henrik Abel. Like Agent Smith in the movie *The Matrix* that can be replicated without a fault, anyons are totally indistinguishable from each other that no one would notice if the positions of two anyons were swapped.

Once Wilczek's fantasy of a new particle became a reality, theoretical research into anyons entered an explosive stage, and by 1991, a novel proposal was made that particles even more bizarre than Wilczek's abelian anyon could exist in two dimensions. Greg Moore and Nicholas Read of Yale University and Xiao-Gang Wen of the Massachusetts Institute of Technology, among others, proposed a particle called the non-abelian anyon. They showed that if you swap the positions of two non-abelian anyons, the state after the swap can be different from the state before, even if all the anyons appear to be identical. This resulted in a simple but important insight: knowing the position of a particle does not tell you everything about the properties of the whole system. In a world of non-abelian anyons, if someone switches the positions of two non-abelian anyons while you're not looking, you'd still be able to detect the swap had occurred. This is because swapping the positions of non-abelian anyons creates a new state, not the original state. Deep down, this is due to the fact that non-abelian anyons have information other than their "positions". When two particles swap places, their positional information remains the same, but other information changes, so the

fact that they swapped places can no longer be hidden. If we number the N non-abelian anyons from 1 to N, and start exchanging anyons 1 and 2, followed by the swap of 2 and 3, then anyons 4 and 6, and so on, we will keep creating new states unlike any of the previous states. The number of different states that can be created using all possible exchange processes grows exponentially with the number N of anyons. It was predicted in Moore-Read's paper that certain fractional quantum Hall states will indeed possess non-abelian anyons as quasiparticles [2].

The non-abelian anyons predicted in Moore-Reed theory has yet to find conclusive experimental evidence of their existence. Nevertheless, the wildly fascinating prophecy of non-abelian anyons has been steadily gaining traction in a totally different field - that of quantum computing. This is thanks to the brilliant idea of topological quantum computation, based on using non-abelian anyons as tools of computation, quantum computation nonetheless. Topological quantum computation is a field championed by Alexei Kitaev in the late 1990s [3,4] and whose mathematical foundations were laid by Fields medalist Michael Freedman and others [5]. As recognition spread that non-abelian particles could be the fundamental building blocks of quantum computers, Microsoft began investing in the possibility of creating a quantum computer using fractional quantum Hall states, which were a prime candidate for realizing non-abelian particles at the time, and created Station Q to spearhead its effort inside a building located at the University in California at Santa Barbara.

The effort to implement quantum computers through quantum Hall materials has what one might call a `control issue'. Quantum Hall matter, after all, consists of a lot of electrons. A small number of well-behaved non-abelian anyons are then created as quasiparticles out of these electrons, and then one applies carefully chosen controls over these quasiparticles to perform desired quantum operatitons. When all is said and done to perfection, one can hand over the quantum computer to Microsoft for commercialization. Before anything remotely analogous to a practical quantum computer can be built, one must face the fact that the underlying electrons are constantly executing a dancing motion and are in what physicists call the strongly interacting regime, where electrons jostle with other electrons with all the might of the Coulomb force. Exercising total control over these `mighty' electrons is not easy. After all, electrons are the tiniest and the lightest of all the particles that we see in a laboratory. Maybe because of that, Microsoft has yet to make tangible breakthroughs in making a quantum computer.

To understand the relationship between non-abelian particles and quantum computers, we must first understand the basic elements that make a regular computer work: bits. A computer is literally a machine that calculates. They are machines that can perform complex mathematical calculations through simple programs much faster than the human brain can. Humans use neurons in their brains to make calculations, but computers use tiny pieces of materials (called devices) to make calculations. First, it converts all mathematical operations into operations based on two binary numbers, 0 and 1. Then we make sure that there are only two physical states in very small devices typically made with silicon. These tiny devices are called bits. The process of changing the state of a bit from 0 to 1, or 1 to 0, by passing electricity through it, is a mathematical operation that can be performed on a large scale and at high speed.

For example, let's say there are five bits and they are in a state |00110>. This mean that the first bit is in state 0, the second bit in state 0, and so on. Replacing this state with another state, say |01010>, is the kind of operation that computers do all the time. In the example here, the states of the second and third bits are reversed. This manipulation is called a gate operation. A computer "computes" by constantly applying a few simple kinds of gate operations to keep changing the state of bits. One might compare it to getting a crowd of people together and making all sorts of patterns out of card sections. Just as humans make mistakes, sometimes a bit that should be a zero will accidentally become a one. When this happens, the error must be detected and corrected. Error correction is a process that's happening constantly in our computers, and thanks to it, we can safely rely on computers to perform their tasks.

Quantum computation uses qubits instead of bits. The information represented by a qubit is not a binary number of 0 or 1, but rather a complex number that combines both real and imaginary numbers. There are only two binary numbers, 0 and 1, but there are an infinite variety of real and imaginary numbers, including 0, 0.1, 0.01....., which cannot even be counted. Furthermore, the states of a qubit can be superposed like a Schrödinger's cat, which is neither alive nor dead, A qubit, as a non-biological analogue of Schrödinger's cat, can be in a superposition of two possible states (dead-state and alive-state). With two qubits, the possibilities are dead-dead, dead-alive, alive-dead, alive-alive, a total of four states. With N qubits, the possibilities would have grown exponentially to 2x2x…x2=2^n different states. Being quantum means that the N-qubit state can be in a superposition among these exponentially many possibilities!

There are 32 possible states for five bits, ranging from |00000> to |11111>, and a typical computer can only be in one particular state out of the thirty-two. A computer's computation consists of converting from one possible bit state to another. On the other hand, a five-qubit quantum computer can easily exist in a superposition of these thirty-two bit states. The superposition, reminiscent of Schrödinger's cat, means that the quantum computer can be in this state or that state. A 5-qubit state is a superposition of all possible 5-bit states. To specify a 5-qubit state, we need to specify the probability of being in each 5-bit state (32 in total). The problem is that this probability is not a binary number like 0 or 1, but a real number that can take on any value between 0 and 1. This flexibility is the source of the computational power of quantum computers, but it's also what makes them so difficult to build and operate. If you give a probability value of 0.2 when it should be 0.1, the quantum computer already contains an error. This is a much harder problem than correcting for a bit value of 1 when it should be 0. A quantum computer made of ten qubits must always be able to control all 2^10=1024 numbers representing the probabilities of that particular state occurring in a superposition. As the number of qubits increases, the number of probabilities to be placed under control grows exponentially. The ultimate problem, unique to the quantum computer, is that these numbers tend to change spontaneously, in a phenomenon called decoherence. Without a well-crafted plan to prevent decoherence, a quantum computer is but a useless machine that works for a short time and then breaks down.

There is a way to avoid this difficulty once and for all. It's called topological quantum computation. The idea is that the probability of error is reduced by replacing an individual mistake with that of a group. For example, imagine ten people holding hands and playing a human merry-go-round. Let's call it 0 when they turn clockwise and 1 when they turn

counterclockwise. With ten people implementing the bit state instead of one person, there's less room for error. Furthermore, the direction of rotation is not continuous. There are only two directions: clockwise or counterclockwise. In this setting bits can be implemented robustly and are less prone to error. Topological quantum computation is a way to mobilize many qubits to create a single collective qubit state. While it is cumbersome to mobilize a large number of qubits, it provides stability against various errors once it is created.

Bit-based operations take place in the space of binary numbers. It's a mathematical space with such a simple structure that it's hard to imagine anything simpler. In order for a computer to perform computations properly, it must be able to physically realize every possible state in this space of binary numbers. On the other hand, the mathematical space in which quantum operations are performed is called Hilbert space. For quantum computation to work well, it must be possible to represent every quantum state in a Hilbert space by qubits. If there are N non-abelian anyons, the size of the Hilbert space they create grows exponentially with N. For quantum computation to work well in this Hilbert space, we need to have access to an exponential number of all the states. The starting point for topological quantum computation is the mathematical proof that when there are N non-abelian anyons, all states of the Hilbert space can be realized by simply swapping the positions of these anyons. Microsoft wants to create quantum computers by creating non-abelian particles in quantum Hall matter and then manipulating them to swap their positions.

A non-abelian particle is a particle that remembers its past. Computations in an ordinary computer is accomplished through the physical process of changing the state of bits from 0 to 1 and 1 to 0. In topological quantum computer, we swap the positions of non-abelian anyons. The exact orbit involved in the swapping doesn't matter. The only information that matters is whether the winding has taken place or not, and how many times. Even if there is some marginal error in the computation, it's hard to undo the fact that winding has taken place. This kind of robustness is the reason why topological quantum computation is viewed with great hope for quantum computing.

The brilliance of Kitaev's and other quantum theorists' insight is that we don't have to rely on nature's gifts such as quantum Hall materials to create structures suitable for quantum computation. Rather, we can create quantum platforms, also called quantum circuits, artificially. For example, qubits are made using something called a Josephson device, which is based on superconducting materials. There are well-developed processes for fabricating Josephson devices in large quantities. It is possible to make Josephson devices that are about 0.1-0.2 microns across on a substrate, and then use electromagnetic waves to manipulate the quantum state of each Josephson device individually. The quantum computers being promoted by Google and IBM are based on Josephson devices and are currently recognized as one of the most high-performance quantum computers. Another way to build a quantum computer is with atoms. When one electron is removed from an atom, it becomes an ion, and unlike atoms, which are electrically neutral, ions have a charge, making it easier to control their position using an electric field. Using this principle, dozens of atoms are arranged in a vacuum, and then lasers are used to control the state of the ions, perform gate operations, and do some measurements. Ion-Q, co-founded Kim Jung-Sang at Duke University, and quantinuum, a subsidiary of the industrial giant Honeywell, are among the companies that have succeeded in creating ion-based quantum computers. Both approaches have resulted in quantum computers operating on the order of a few tens of

qubits. These days the various systems used to build a quantum computer is called a quantum platforms. Josephson junctions, ions, and Rydberg atoms are among the most popular quantum platforms now in use and under rapid development these days.

The next step is to create non-abelian anyons on a quantum platform. As early as 1997, Kitaev proved that creating a state called a toric code on a quantum platform would create an abelian anyon as a quasiparticle, and creating a state called a quantum double would create non-abelian anyons as quasiparticles. This was a landmark discovery. Recall that the discovery of the abelian anyons in the fractional quantum Hall system in 1982 was, after all, a miraculous gift from nature totally unexpected to human ingenuity. Now, Kitaev's proof showed us how to engineer and artificially create anyons, whether abelian or non-abelian, through pure human ingenuity. In 2022, using Josephson junctions and Rydberg atoms as quantum platforms, scientists have created the toric code in the lab and confirmed the existence of abelian anyons.

Unfortunately, the abelian anyons produced by toric code are insufficient to perform topological quantum operations. Because of their "commutativity" - the fact that you can swap the positions of two abelian anyons and still get the same quantum state - they are not capable of producing all of the rich Hilbert space that quantum computation requires. For the purposes of a topological quantum computer, we need to find a way to create non-abelian anyons. However, implementing a non-abelian anyon state on a quantum platform is much more challenging than their abelian counterpart, so much so that one has to find a shortcut to reach that lofty goal.

One conceivable shortcut is to create an abelian anyon and then apply additional manipulations to turn it into a non-abelian anyon. There is a mathematical proof that an abelian anyon behaves like a non-abelian anyon if the qubits are intentionally arranged on a squashed lattice instead of a perfectly regular grid of qubits. An experimental implementation of this proof was published by Google in 2023 [6].

Another shortcut is to reduce the time required to create non-abelian anyons. To create an abelian anyon, the initial unentangled quantum state must be converted to a topological state, and the number of quantum gate operations involved in this conversion process grows with how many qubits there are in a given quantum platform. The more qubits you have, the more gate operations you need to perform, and the greater the chance of errors in the computation. Instead of tackling this challenge head-on, there is a clever way around it. It's a hybrid method that involves making strategically planned measurements on a quantum platform and then using the results of those measurements to determine how to perform the next phase of quantum gate operations. If this hybrid method can be implemented, the number of quantum gate operations required to create a topologically ordered state can be dramatically reduced.

If you want to build non-abelian anyons from scratch, instead of building first the abelian anyons and then converting them to non-abelian anyons as Google did, you need to use this technique of measurement. It was commonly believed that quantum states collapse once they have been measured, and that measurement is detrimental to quantum computation. However, a methodology for measurement-based quantum computation that directly contradicts this common conception has been around for 20 years. Strategically applying a

well-intended measurement to a quantum state creates a new quantum state. And then the next round of measurements gives us another quantum state. The proposal was that these ever-changing quantum landscape painted by measurements could eventually perform all the quantum operations we ever wanted. One of the valuable byproducts of this proposal is that it is now possible to create topological states from non-topological states through measurement. It's not just possible, it's easy - at least in theory.

In 2022, Ashvin Vishwanath, a brilliant theoretical condensed matter physicist at Harvard in collaboration with a formidable team of young collaborators, developed a sophisticated theory of how to build non-abelian anyons by strategically using measurements. Fortunately for the theorists, quantum engineers at Quantinuum had just finished building an ion-based quantum computer powerful enough to create those non-abelian anyons using Vishwanath's theory. As soon as the Quantinuum mustered the ability to manipulate 27 ions in their device, they put the Harvard researchers' proposal to the test, and in 2023 they finally succeeded in creating three non-abelian anyons and braiding them [7].

It's been almost a century since 1925, when the Schrödinger equation, the foundation of quantum mechanics, was created. For a very long time, quantum wave functions were deemed a tool for describing atoms and the world beneath the atomic scale, in short the natural world. In quantum computation, we have a new perspective on these wave functions. Here they serve as devices for computation. The quantum wave functions of superconducting qubits, or atomic qubits are not the naturally occurring wave functions like those of a hydrogen atom, but are created and manipulated by human intent and control. Their intent is not to understand nature, but to manipulate certain quantum operation in a quantum computer. This is a beautiful instance of great physical laws discovered in one era gradually become the powerful tool of engineering for the next.

The successful creation and exchange of a non-abelian anyons in 2023 is nothing more than a baby's first step toward the grand goal of topological quantum computation. However, as a thousand-mile journey must begin with a single step, it's exciting to think about how a baby who has started walking now will grow up in 40 years. One can draw inspiration from the first experiment demonstrating the quantum entanglement of two particles that took place in 1980, and how it took some 40 years for the work to be recognized with Nobel prize and the foundation of what we now call the quantum engineering. If all the promises that we see these days of the quantum computer are to be fulfilled some 40 years from now, such world would be *imaginatio transcendit* (beyond recognition).

1. Magnetic flux, angular momentum, and statistics, Frank Wilczek, Physical Review Letters **48**, 1144 (1982)
2. Nonabelions in the fractional quantum Hall effect, Gregory Moore and Nicholas Read, Nuclear Physics B **360**, 362 (1991)
3. Fault-tolerant quantum computation by anyons, Alexei Kitaev, Annals of Physics, 303, **2** (2003)
4. Anyons in an exactly solvable model and beyond, Alexei Kitaev, Annals of Physics, 321, **2** (2006)

5. Non-Abelian anyons and topological quantum computation, Chetan Nayak, Steven Simon, Ady Stern, Michael Freedman, Sankar das Sarma, Reviews of Modern Physics **80**, 1083 (2008)
6. Non-Abelian braiding of graph vertices in a superconducting processor Authors: Google Quantum AI and Collaborators, Nature **618**, 264 (2023).
7. Creation of Non-Abelian Topological Order and Anyons on a Trapped-Ion Processor, Mohsin Iqbal et al. arXiv:2305.03766