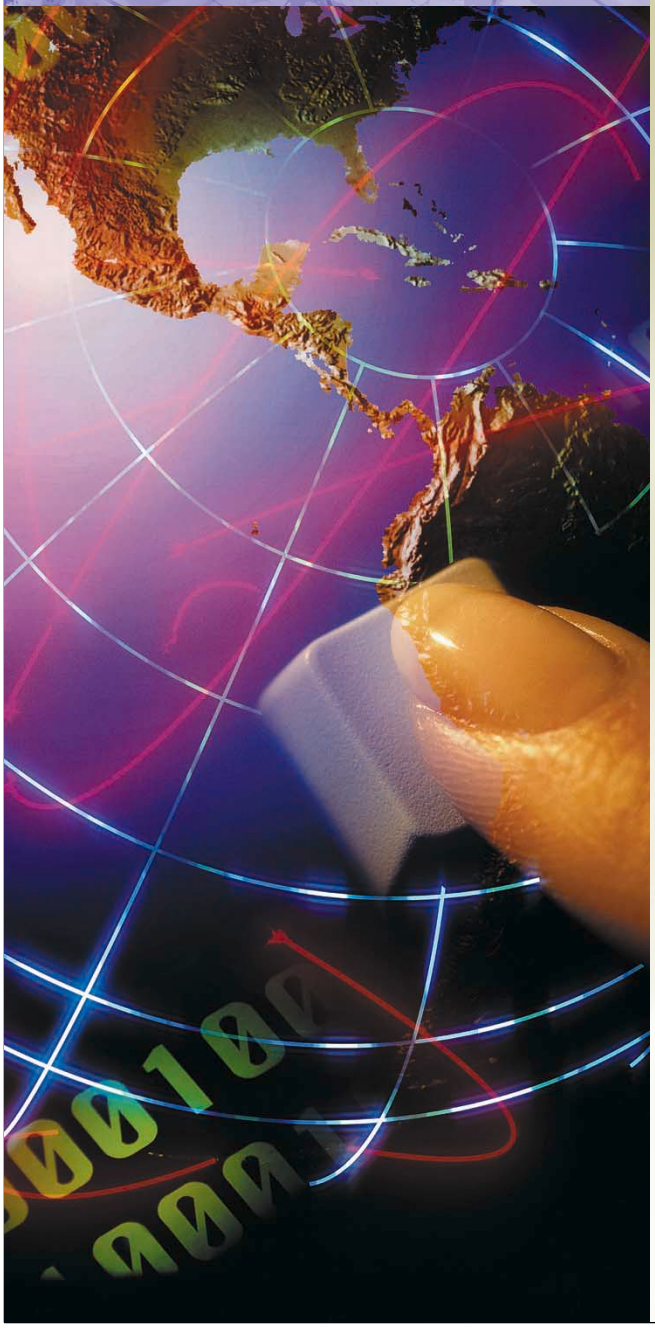
# 양자컴퓨터(Quantum Computer)
# 1조분의 1초 만에 정보 처리

글_ 김재완 고등과학원 계산과학부 교수 · 우종천 서울대 교수 jcwoo@plaza.snu.ac.kr

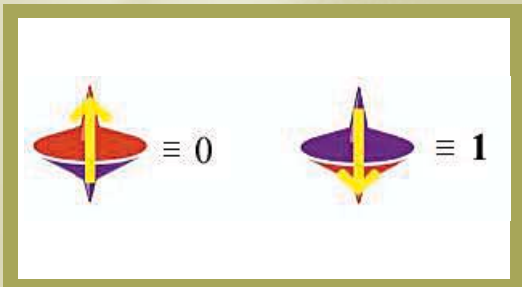


우리가 미래를 걸고 있고 선두 주자라고 자부하고 있는 정보 산업과 반도체 기술의 그 중심에는 컴퓨터가 있고, 이 컴퓨터는 디지털 기술이 이룩한 업적임은 삼척동자도 아는 사실이다. 그런데 이 디지털 컴퓨터는 지금 어디를 향해 발전해 나가고 있을까? 해가 갈수록 반도체 집적도는 기하급수적으로 증가하고 있다. 그래서 반도체 업계는 메모리의 기본인 비트의 크기를 나노미터 단위까지 줄인다면서 계속 피 말리는 경쟁을 하고 있지만, 비트의 크기가 원자의 크기에 이르면 비트의 생명인 0과 1의 구분을 불분명하게 만드는 양자효과 때문에 무한정 줄일 수는 없다. 그래서 일부 학자들은 10~20년 후에는 현재의 고전컴퓨터가 집적도의 한계에 도달할 것이라고 주장한다. 그러면서 다음 세대의 정보처리 기술로 대두된 아이디어가 원자의 양자학적 성질을 이용하여 정보를 처리하는 양자컴퓨터(quantum computer)이다.

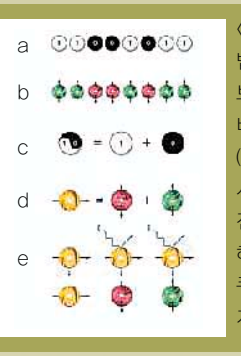
## 겹침 상태로 있는 디지털 정보 인지

양자정보처리의 가능성이 주목을 받기 시작한 것은 1990년대 초기로 극히 짧지만, 10여 년이 지난 지금 이미 일본은 페타플롭스(peta-flops) 슈퍼컴퓨터 개발이란 이름으로 문부과학성 10대 근간 기술로 선정했다. 미국은 2012년까지 시범용 완성이라는 목표 아래 ARDA주도로 로드맵을 수립해 놓고 양자컴퓨터 개발에 열을 올리고 있다. ARDA는 미국 정보기술분야의 고부가 고위험성 국가주도형 연구과제를 도출해 지원하는 조직으로 양자컴퓨터는 2004년 현재 제안되어 있는 5개의 과제 중 하나이다.

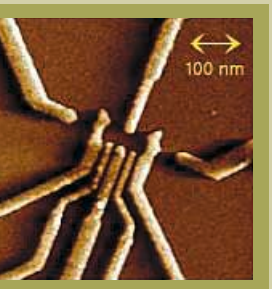
양자컴퓨터에서는 전자 혹은 원자핵 하나가 이진법을 수행하는 비트가 된다. 이를 양자비트 또는 큐빗(qubit)이라고 한다. ARDA 로드맵의 표지에는 '물리학의 법칙은 비트가 원자의 크기가 될 때까지 컴퓨터의 크기를 줄이는데 아무런 장애가 없을




〈그림 1〉 스핀 큐빗은 스핀 up과 down, 즉 오른쪽과 왼쪽으로 자전하는 것이 '0'과 '1'이 됨




〈그림 2〉 (a) 이진법의 "11001011"을 보여주는 고전 8-비트와 (b) 8-큐빗, (c) "0"과 "1"이 동시에 존재하는 고전 비트와 (d) 이에 해당하는 큐빗, (e) 큐빗을 작동시키는 계략도




〈그림 3〉 양자점 두개로 만든 큐빗 회로

것이다' 라는 페이만 교수의 1985년도 강연내용을 인용하면서 원자나 핵이 양자컴퓨터의 기본임을 제시한다.

전자의 스핀을 예로해서 큐빗을 설명하면, 〈그림 1〉에서 보는 바와 같이 전자의 자전, 즉 스핀은 외부 자기장과 같은 방향과 반대방향인 $|\uparrow\rangle$과 $|\downarrow\rangle$의 두 상태를 갖고 있는데, 이 두 스핀 상태로 전위차 '0'과 '+'를 비트로 하는 고전컴퓨터의 $|0\rangle$과 $|1\rangle$을 대치하는 것이 스핀 큐빗이다. 양자의 세계에서는 $|0\rangle$과 $|1\rangle$이 $1/\sqrt{2}(|0\rangle + |1\rangle)$인 겹침 상태로 존재하는데, 고전컴퓨터는 $|0\rangle$과 $|1\rangle$이 겹쳐 있는 상태를 인식하지 못하지만(그림 2c 참조) 양자컴퓨터는 겹침 상태로 있는 디지털 정보를 인지함은 물론(그림 2d 참조), 이 양자역학적 겹침 상태 자체를 정보처리 수단으로 활용하겠다는 것이 기본적인 발상이다.

고전컴퓨터의 경우 8비트 칩(chip)은 $2^8$=256가지의 상태 중에서 하나만 올릴 수 있는 반면, 8큐빗의 양자컴퓨터 경우에는 256가지 상태가 모두가 양자물리학적으로 중첩된 상태로 '한꺼번에' 올라가 있어서, 여기서 필요한 숫자만 선택하여 이용하면, 계산능력이 기하급수적으로 커지는 장점을 갖고 있다. 이를 양자병렬성(quantum parallelism)이라고 하는데, 인수분해를 예로 들어 보면 '? x ? = 77173' 같이, 곱이 77173이 되는 두 숫자를 찾는 경우, 모든 두 숫자의 곱이 동시에 올라와 있는 상태에서 답을 갖는 두 숫자를 골라내는 양자병렬성을 이용하면 쉽게 알 수 있지만, 고전 컴퓨터로는 '229 x 337 = ?'이 나올 때까지 모든 숫자를 한 쌍씩 곱해 나가야 되니까, 많은 시간과 노력이 소요된다. 고전컴퓨터로도 수천대를 연결하는 클러스터 방식으로 병렬 전산처리가 시도되고 있다. 그렇지만, 연결된 컴퓨터 대수에 따라 계산 능력이 산술적으로 증가하기 때문에 기하급수적으로 증가하는 양자병렬과는 근본적으로 다르다. 이 예를 통해 알 수 있듯이 양자컴퓨터는 고전컴퓨터와는 전혀 다른 개념과 방식으로 정보를 처리한다.

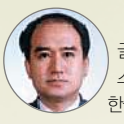
## 정보통신기술 분야 혁명 일으킬 것

양자컴퓨터는 무한에 가까운 정보처리 용량과 1조분의 1초($10^{-12}$초) 수준의 빠른 정보처리 속도 등 많은 장점을 갖고 있다. 따라서 양자컴퓨터가 현실화될 경우 정보통신 기술에 다시 한 번 혁신이 일어날 것이고, 국가안보체계도 새로 정비해야 하는 등 새로운 일거리도 많이 창출된다. 양자컴퓨터로는 비밀번호를 쉽게 해득할 수 있어 새 개념의 정보 보안책을 개발해야 하는 것도 중요한 일중 하나이다.

양자컴퓨터는 아직 잉태기라고 할 정도로 초창기이다. 양자컴퓨터의 기초인 큐빗도 결정되지 않은 상태로, ARDA 로드맵에서도 양자점의 전자 스핀, 원자핵의 스핀, 초전도체, 광자 등 모든 가능성을 열어놓고 있는 실정이다. 또 이제까지 이룩한 가시적인 성과라고 할 수 있는 것이 2001년 IBM에서 핵스핀 큐빗 일곱(7)개로 15를 소인수분해한 것, 두 개의 양자점 큐빗으로 된 소자를 제작한 것이 고작이다(그림 3 참조).

정보산업강국인 우리 나라가 미래의 정보처리기술인 양자정보기술에 관심을 가져야 하는 것은 당연하고, 초창기인 지금이 우리가 선두 연구 대열에 동참할 수 있는 최적의 기회이다. 양자컴퓨터 실현에 나노기술은 물론, 새로운 개념의 기초과학, 양자 정보처리 방법 개발이 필연적이기 때문에 관련 분야에 파급효과 또한 지대하다. 여러 과학기술분야에 새로운 서광을 비출 수 있는 이 분야의 육성에 과학기술계의 관심이 요망된다.

글쓴이 우종천은 플로리다주립대에서 물리학 박사학위를 받았다. 서울대학교 대학원 원장, 대통령 교육정책 자문기구 새교위 위원, 미국 USC 및 스탠퍼드 대학 방문교수를 역임했다.



글쓴이 김재완은 휴스턴대학교에서 물리학 박사학위를 받았다. 텍사스초전도체연구소 연구원, 삼성종합기술원 계산과학연구원 및 팀장, 한국과학기술원 연구 부교수를 역임했다.