00105

구두발표 I

NMR 양자 컴퓨터

이순칠
한국과학기술원 물리학과

양자전산(Quantum Computing)이란 양자역학계의 특징인 불확정성, 중첩, 간섭, 얽힘(entanglement) 등을 이용하여 지금까지와는 근본적으로 다른 방식으로 정보를 처리하고 전송하는 일련의 방법 및 기술로서, 전산 뿐 아니라 일반적으로 양자암호체계(Quantum Cryptography)와 양자원격이동(Quantum Teleportation) 등의 양자정보전달 기술을 포함하여 총칭한다. 양자전산은 근본적으로 도, 감청이 불가능한 정보전달이나 공상과학에나 나오던 원격이동을 실현하며, 기존의 컴퓨터로는 불가능한 문제를 해결하는 등 파격적인 내용을 담고 있어 정보 혁명을 몰고 올 것으로 예상된다. 작년 미국 물리학회장을 역임한 Broomley박사는 1999년 3월에 열린 미국물리학회 100주년 기념학회의 기조강연에서 새 천년에 주요한 물리학 연구주제로 양자전산을 꼽았다.

양자전산의 첫 번째 응용으로 꼽히는 분야는 국방이나 금융, 그리고 인터넷 등 암호를 사용하는 정보보안 분야이다. 양자암호체계는 이론상 도청이 불가능한 정보전송방식으로써 1994년 IBM에서 이미 특허를 획득했고, 현재 NASA에서 인공위성이나 우주선과 지상간의 정보전송에 이 기술을 적용하려고 계획하고 있으며 IBM에서의 지상실험결과로 그 가능성이 이미 입증되었다. 양자전산은 1982년 파인만에 의해 처음 개념이 도입된 후, 1994년 Bell lab의 Shor가 양자 알고리듬을 사용한 소인수분해법을 발표하고 이 알고리듬이 전 세계의 암호체계를 모두 격파할 수 있음이 알려진 후부터 각국 정부는 크게 긴장하여 양자정보기술을 국가적 차원에서 지원하기 시작하였다. 1997년에 발표된 NMR에 의한 양자컴퓨터의 실제 구현은 학자들의 연구를 폭발적으로 늘이는 계기가 되었다. 양자컴퓨터의 구현은 1995년 이온덫(ion trap)에 의한 것이 최초이며, 이밖에 양자점(quantum dot), 공진기 양자전기역학(cavity QED), 조셉슨소자 등을 이용한 방법들이 개발되었거나 제안되고 있다. 이 중 NMR은 결맞춤 시간이 길고 이미 실험기법들이 많이 개발되어 있기 때문에 현재 양자 알고리듬을 실제 구현할 수 있는 유일한 양자 컴퓨터이다.

양자전산 하드웨어 연구는 실용성 있는 양자컴퓨터를 제작해야 한다는 매우 뚜렷한 목표가 있다. 실용성 있는 양자컴퓨터의 개발을 위한 첫 번째 관건은 비트수를 수십 정도로 늘여야 한다는 것이다. 현재 NMR양자 컴퓨터는 3 비트를 다루는 수준이며, 4 비트 이상의 수준에서는 인공적인 분자를 합성하여 사용하여야 할

것으로 예상된다. 양자전산 알고리듬은 실제의 하드웨어 양자계에 적용하려면 대상 양자계의 하밀토니안에 근거하여 프로그램을 작성하여야 한다. 양자전산 프로그램이란 양자계에 작용할 상호작용의 순서도 작성에 해당하는데 이는 기계어로 프로그램을 작성하는 것과 같아서 대상 양자계에 따라 다르게 프로그램이 작성되어야 한다.

본 발표에서는 양자전산의 기본 개념과 현재의 연구현황을 알아보고 실제로 NMR 양자 컴퓨터에서 구현되는 기본 원리를 예를 들어 설명하고자 한다. 또한 양자 컴퓨터에서 프로그램의 구현을 위해 사용되는 펄스열이 2-D NMR 등에서 사용되는 펄스열과 어떻게 다른지, 어떤 정밀도를 요구하는지, 또 합성되어야할 분자가 어떤 조건을 가져야 하는지 등을 설명하고자 한다.