Quantum Random Access Memory

융합보안학과 윤세영 유투브 주소:

https://youtu.be/Ap9cg8H3udc



Quantum Random Access Memory (2008)

Quantum Random Access Memory

Vittorio Giovannetti, 1 Seth Lloyd, 2 and Lorenzo Maccone 3

¹NEST-CNR-INFM & Scuola Normale Superiore, Piazza dei Cavalieri 7, I-56126, Pisa, Italy

²MIT, RLE and Department of Mechanical Engineering MIT 3-160, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA

³QUIT, Dipartimento di Fisica "A. Volta," Università di Pavia, via Bassi 6, I-27100 Pavia, Italy

(Received 10 September 2007; revised manuscript received 12 November 2007; published 21 April 2008)

A random access memory (RAM) uses n bits to randomly address $N = 2^n$ distinct memory cells. A quantum random access memory (QRAM) uses n qubits to address any quantum superposition of N memory cells. We present an architecture that exponentially reduces the requirements for a memory call: $O(\log N)$ switches need be thrown instead of the N used in conventional (classical or quantum) RAM designs. This yields a more robust QRAM algorithm, as it in general requires entanglement among exponentially less gates, and leads to an exponential decrease in the power needed for addressing. A quantum optical implementation is presented.

DOI: 10.1103/PhysRevLett.100.160501 PACS numbers: 03.67.Lx, 03.65.Ud, 89.20.Ff



RAM 이란?

- Random Access Memory (RAM)
- 컴퓨터가 데이터를 임시로 저장하고 빠르게 접근하기 위해 사용하는 기억장치
- 사용자가 자유롭게 내용을 읽고 쓰고 지울 수 있음
- 메모리 배열, 입력 레지스터(주소 레지스터), 출력 레지스터로 구성됨



Quantum RAM 이란?

- 고전 컴퓨터에서 RAM이 가장 근본적인 기능을 수행하고 있으므로, 충분히 큰 양자컴퓨터가 개발될 경우 'Quantum RAM' 도 양자컴퓨터의 필수적인 구성 요소가 될 것임
- QRAM도 RAM처럼 메모리 배열, 입력 레지스터, 출력 레지스터 세 가지로 구성되어 있지만, 레지스터가 비트가 아닌 큐비트로 이뤄져 있다는 차이가 있음 (* 메모리 배열은 QRAM의 사용 방식에 따라 다름)
- *** QRAM은 "양자 중첩 상태로 메모리 접근을 수행할 수 있음"



RAM vs QRAM

| | RAM | QRAM |
|-------------|---|--|
| 기본 개념 | 임의의 주소를 지정해 해당 메모리 셀의 데이터를 읽고 쓰는 장치 | 임의의 주소(큐비트 중첩)를 지정해, 중첩 상태로 여러 메 모리 셀의 데이터를 동시에 접근하는 장치 |
| 주소 레지스터(입력) | 고전적 비트들로 구성 (예: 0 또는 1) | 양자 비트(큐비트)로 구성 (예: IO), I1), 또는 두 상태의 중첩) |
| 출력 레지스터 | 고전적 비트로 구성 메모리 셀에서 읽은 데이터를 저장 | 큐비트(또는 상황에 따라 고 전적 비트)에 기반 메모리 셀에서 읽은 데이터를 중첩 상태로 저장 |
| 주소 지정 방식 | 한 번에 하나의 주소만 정확 히 선택 | 중첩 상태인 여러 주소를 동 시에 가리킬 수 있음 |
| 디코딩(접근) 방식 | 입력 주소 → 해당 주소의 데이터를 출력 | 중첩 주소 → 각 주소의 데이터를 대응되는 중첩 상태로 동시에 출력 |



bucket-brigade

- QRAM을 기존 RAM 구조에서 그대로 확장할 경우, 메모리 접근 시 발생하는 에너지 소모가 매우 커짐
- 특히 양자컴퓨팅에서는 "Quantum decoherence" 문제가 심각하게 발생할 수 있음
- 따라서 본 논문에서는 "bucket-brigade"라는 새로운 구조를 제시함.

->

- 메모리 접근 시 필요한 스위치 작동 횟수를 O(N^(1/d))에서 O(log N)으로 줄임
- 디코딩(decoding) 과정의 계산 복잡도를 지수적으로 낮춤
- 양자 게이트가 얽혀야 하는 횟수도 크게 줄어들어 에너지 소모와 decoherence 문제를 완화시킴

디코딩(decoding):

주어진 주소(address)를 읽어서 그 주소에 해당하는 메모리 셀을 실제로 선택(활성화)하는 과정



기존 RAM

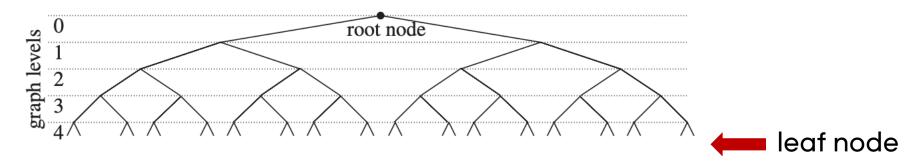


FIG. 1. Bifurcation graph of the RAM addressing.

- 맨 위의 "root node"에서 시작하여, 각 레벨마다 왼쪽/오른쪽으로 분기되어 최종적으로 메모리 셀(leaf node)에 도달하는 형태
- 레벨 0, 1, 2, … 와 같이 내려갈수록 주소 비트를 하나씩 결정(0이면 왼쪽, 1이면 오른쪽)하는 구조
- 주소 레지스터가 n비트라면, 트리의 높이도 n레벨이 됨
- 주소 레지스터가 n비트라면 표현할 수 있는 주소는 2^n개

양자 주소 레지스터가 여러 주소를 동시에 가리키면, 메모리 트리의 수많은 스위치들도 그 중첩에 맞춰 전부 얽혀야 하므로, 회로 규모와 오류 문제가 폭발 적으로 커진다.



bucket-brigade

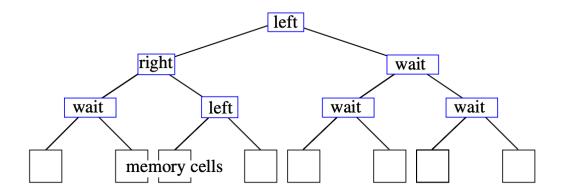
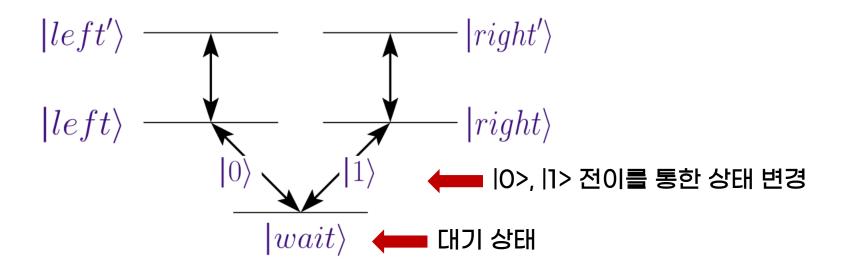


FIG. 2 (color online). Bifurcation graph of the bucket-brigade architecture. Here the third memory cell is addressed (address register 010).

- Wait / left / right 세개의 상태로 나눠져 있음
- 상태 결정 전: wait, 들어오는 비트가 0: left, 들어오는 비트가 1: right
- 첫 번째 비트가 노드의 상태를 left/right 중 하나로 결정 → 해당 노드를 지난 두 번째 비트가 다시 다음 노드에 적용 → logN 비트를 거치면 하나의 경로가 완성
- 한 번의 메모리 호출에 실제로 동작하는(상태가 wait에서 바뀌는) 노드는 logN개 뿐이므로, 에너지 소모와 회로 복잡도가 크게 줄어듦



bucket-brigade



- 주소 레지스터가 트리를 통과하며 노드들을 Iwait〉에서 Ileft〉 / Iright〉 상태로 전환시켜 경로를 만듦
- 버스 (광자)가 해당 경로를 따라가서 메모리 셀에 접근
- 돌아오는 길에는 반대로 노드들이 다시 Iwait) 상태로 되돌아가는 과정을 거쳐서 초기화됨
- 대규모의 양자 얽힘이 필요하지 않음, 한 번의 주소 지정에 필요한 에너지와 회로 복잡도를 크게 줄일 수 있어서 실제 구현 가능성을 높일 수 있음



결론

- 활성 게이트(active gates)가 세 가지 상태를 지닌 메모리 요소(three-level memory elements)로 대체한 RAM 구조 제시
- QRAM 구현이 크게 간소화되고, decoherence율이 지수적으로 줄어들며, 에너지도 절감될 수 있다고 언급
- (연구 당시) RAM의 경우, (정적 RAM에서는) 메모리 셀의 누설 전류, (동적 RAM에서는) 메모리 셀의 재충전 (refresh) 과정이 주된 소모원이었으며, 따라서 메모리 접근 절차에서의 에너지 비용이 크게 문제되는 부분이 아님
- 버킷 브리게이드가 요구하는 추가 지연이나 메모리 요소를 감수할 이유가 충분치 않았음
- 그러나 양자 메모리와 같은 새로운 RAM에서는 디코딩 에너지 비용이 더 중요해질 수 있으므로, 그 시점에는 버 킷 브리게이드 구조가 제공하는 지수적 에너지 절감 효과가 의미 있을 수 있다고 언급



RAM vs QRAM(bucket-brigade)

| | RAM | QRAM(bucket-brigade) |
|----------|--|---|
| 주소 지정 방식 | 이진 트리 분기(0=왼쪽, 1=오 른쪽)로 N=2^n 개 셀에 접근 | 각 노드가 3상태(trit, qutrit) 메모리 요소(Iwait), Ileft), Iright)) |
| 에너지 사용 | 디코딩 과정에서 다수 스위치 활성화 → 에너지 많이 소모 | 디코딩 과정에 필요한 게이트 수가 크게 줄어듦 → 이론적으 로 에너지 절약 |
| 미래 전망 | 양자컴퓨팅 활용 시 기존 방 식은 비효율·오류 문제 커질 우려 | 양자 메모리 시대에는 디코딩에너지가 큰 문제가 될 수 있음 -> bucket-brigade 방식이 효율적일 것 |
| 장점 | (현재 컴퓨터에서는) 빠른 접 근 가능 | 양자 환경에서 효율적으로 메 모리 접근 가능 |
| 단점 | (양자 확장 시) 회로 규모가 크고 오류에 민감 | 현재 CMOS 기반에서 디코 딩 에너지는 상대적으로 중요 한 이슈가 아님 |



Post-quantum Cryptography & Quantum Computing [CryptoCraft Lab]

감사합니다

