

양자 저밀도 패리티 검사 부호를 위한 계층적 신뢰 전파 복호 알고리즘

김재민, 정현우, 하정석

한국과학기술원

jmkin@kaist.ac.kr, destiny@kaist.ac.kr, jsha@kaist.edu

Layered Belief Propagation Decoding Algorithm for Quantum Low-Density Parity-Check Codes

Jaemin Kim, Hyunwoo Jung, Jeongseok Ha

Korea Advanced Institute of Science and Technology

요약

본 논문은 양자 저밀도 패리티 검사 부호를 위한 효율적인 복호 알고리즘을 제안한다. 기존 양자 저밀도 패리티 검사 부호의 신뢰 전파 알고리즘은 병렬 스케줄 방식으로 메시지 업데이트를 진행한다. 하지만 신뢰 전파 알고리즘을 활용한 양자 저밀도 패리티 검사 부호의 복호기는 사이클의 존재로 인해 오류율 성능 저하가 발생하며, 양자 저밀도 패리티 검사 부호를 설계하는 구조 특성상 사이클의 존재는 피할 수 없는 문제이다. 따라서 본 논문에서는 기존 신뢰 전파 알고리즘과 메시지 업데이트 방식이 다른 계층적 신뢰 전파 알고리즘을 활용하는 복호 알고리즘을 제안한다. 실험 결과를 통해 제안하는 알고리즘이 더 빠른 수렴 속도로 복잡도를 낮추는 동시에 오류율 성능 또한 향상시킬 수 있음을 확인하였다.

I. 서론

고전 영역에서 저밀도 패리티 검사 (low-density parity-check, LDPC) 부호 [1]는 정보 전달 기반의 저복잡도 복호 알고리즘을 활용하여 샤논 한계 (Shannon limit)에 가까운 강력한 오류 정정 능력을 갖는 부호로 통신 분야에서 널리 사용되고 있다. 따라서 양자 영역에서도 저밀도 패리티 검사 부호에 대한 연구가 활발히 이루어지고 있다. 양자 저밀도 패리티 검사 (quantum low-density parity-check, QLDPC) 부호는 최소 패리티 검사 행렬을 가지기 때문에 오류 정정을 위한 복호화 과정에서 외부 영향을 받는 큐비트 (qubit) 수가 상대적으로 적어 결함 허용 복호 (fault-tolerant decoding)에 유리하다. 고전 오류 정정 부호는 신뢰할 수 없는 채널을 통해 얻은 수신 벡터 형태의 메시지를 이용하여 복호화를 진행한다. 이와 달리 양자 저밀도 패리티 검사 부호의 복호화 과정은 신드롬 (syndrome) 정보를 이용한 정보 전달 기반의 복호 알고리즘을 사용한다. 저밀도 패리티 검사 부호의 복호 알고리즘은 테너 그래프 (Tanner graph) 상에서 변수 노드 (variable node, VN)와 검사 노드 (check node, CN) 사이의 반복적인 메시지 전달을 통해 수행된다. 이때, 복호 알고리즘으로는 일반적으로 신뢰 전파 (belief propagation, BP) 알고리즘을 활용한다. 신뢰 전파 알고리즘의 경우, 메시지 업데이트 방식을 선택할 수 있다. 신뢰 전파 알고리즘에서 메시지 업데이트는 검사 노드와 변수 노드에서 한 번씩 진행된다. 이때, 모든 노드들의 메시지 업데이트를 동시에 진행하는 방식을 병렬 스케줄 (parallel schedule), 노드들을 차례대로 하나씩 메시지 업데이트를 진행하는 방식을 직렬 스케줄 (serial schedule)이라고 한다. 직렬 스케줄 방식은 일반적으로 병렬 스케줄 방식과 비교하여 더 빠른 수렴 속도로 같은 성능을 낼 수 있는 업데이트 방식으로 알려져 있다. 하지만 충분한 하드웨어 자원이 있으면, 병렬 스케줄 방식이 직렬 스케줄 방식에 비해 시간적인 이득을 본다. 따라서 직렬 스케줄 방식을 이용한 신뢰 전파 알고리즘의 경우, 상대적으로 높은 시간 복잡도를 갖기 때문에 실제 상황에서는 병렬 스케줄 방식이 선호되지만, CSS (Calderbank-Shor-Steane) 부호와

같은 양자 저밀도 패리티 검사 부호 구조 특성상 사이클 (cycle) 수가 많아 낮은 오류 정정 성능을 갖는다.

본 논문에서는 양자 저밀도 패리티 검사 부호의 효율적인 복호 알고리즘을 제안한다. 양자 저밀도 패리티 검사 부호에서 신뢰 전파 복호의 시간 복잡도를 낮추기 위해 직렬 스케줄 방식의 일종인 계층적 신뢰 전파 (layered belief propagation, LBP) 알고리즘을 활용한다. 계층적 신뢰 전파 방식은 병렬 스케줄 방식과 비교하여 직렬 스케줄 방식을 활용하였을 때 생기는 시간적인 간극을 줄일 수 있다. 실험 결과를 통해 제안하는 알고리즘은 신뢰 전파의 필요 반복 횟수를 감소시키며, 동시에 오류 정정 성능의 이득을 얻을 수 있음을 확인하였다. 본 논문은 1장의 서론에 이어서 2장에서 계층적 신뢰 전파 알고리즘을 설명하고, 3장에서 결론과 함께 논문을 마친다.

II. 양자 저밀도 패리티 검사 부호를 위한 계층적 신뢰 전파 복호 알고리즘

본 논문에서는 양자 저밀도 패리티 검사 부호의 직렬 스케줄 방식의 일종인 계층적 신뢰 전파 복호 알고리즘을 다룬다. 양자 저밀도 패리티 검사 부호의 복호화 과정은 큐비트에 발생한 오류의 유무를 판단해주는 신드롬 정보를 이용하여 신뢰 전파 복호 알고리즘을 통해 오류를 추정하는 과정이다. 오류 채널은 디폴라이징 채널 (depolarizing channel)을 가정하여, 오류율 (error rate)은 p 로 나타낸다.

신뢰 전파 알고리즘은 주어진 채널 정보를 활용하여 개별 변수 노드의 오류 확률을 계산한다. 변수 노드와 검사 노드 사이에서 주고받는 메시지 정보는 채널 정보를 활용하여 로그-우도비 (log-likelihood ratio, LLR)의 형태 L_i 로 변환된다. 이때, L_i 는 i 번째 변수 노드의 로그-우도비를 나타낸다. 각 변수 노드의 오류 확률은 연결된 검사 노드로 전달되고, l 번째 반복 횟수에서 j 번째 검사 노드에서 i 번째 변수 노드로 전달되는 메시지, $L_{i \rightarrow j}$ 는 식 (1)과 같이 계산된다.

$$L_{i \rightarrow j}^{(l)} = 2 \tanh^{-1} \left(\prod_{j' \in N(i) \setminus j} \tanh \left(\frac{1}{2} L_{j' \rightarrow i}^{(l)} \right) \right). \quad (1)$$

이때, $N(i)$ 는 i 번째 변수 노드와 연결된 검사 노드의 집합이다. 이를 바탕으로 l 번째 반복 횟수에서 각 변수 노드의 메시지 정보는 식 (2)로 계산된다.

$$L_i^{(l)} = L_i + \sum_{j \in N(i)} L_{j \rightarrow i}^{(l)}. \quad (2)$$

각 변수 노드의 메시지 정보를 바탕으로 경판정 (hard decision)을 진행하여 오류를 추정한다.

계층적 신뢰 전파 알고리즘은 신뢰 전파의 매 반복 횟수마다 검사 노드에서 변수 노드들로 전달한 메시지 정보 업데이트를 노드 하나씩 진행하지 않고 노드들을 사전에 각 레이어 (layer)에 할당하여 순차적으로 진행한다. 이때, 레이어 수는 사전에 임의로 결정할 수 있는 초매개변수 (hyperparameter)이다. 사전에 레이어 수를 2개로 설정한 경우, 첫 번째 레이어에 할당된 검사 노드들의 메시지 업데이트를 먼저 진행하고 두 번째 레이어에 할당된 검사 노드들의 업데이트를 나중에 진행한다. 이때, 두 번째 레이어에 할당된 검사 노드들의 메시지 업데이트는 첫 번째 레이어에서 업데이트된 정보를 반영하여 수행된다. 따라서 병렬 스케줄 방식을 이용한 신뢰 전파 알고리즘과 계층적 신뢰 전파 알고리즘의 복호 복잡도는 같지만, 계층적 신뢰 전파 알고리즘의 경우 검사 노드 업데이트를 레이어별로 순차적으로 진행하기 때문에 오류율의 수렴 속도가 빨라진다. 즉, 계층적 신뢰 전파 복호 알고리즘은 병렬 스케줄 방식을 이용한 신뢰 전파 알고리즘보다 더 적은 반복 횟수로 비슷한 성능을 낼 수 있다.

계층적 신뢰 전파 알고리즘의 성능을 확인하기 위해, $[[400, 200]]$ bicycle 부호 [3]에 대해 성능 평가를 수행하였다. 그림 1은 디폴라이징 채널 ($p = 0.02$)에서 신뢰 전파 반복 횟수에 따른 성능을 비교한 그래프이다. 그림 1의 결과를 통해 레이어 수를 각각 2, 8로 설정한 계층적 신뢰 전파 알고리즘을 이용한 복호화 과정이 기존의 병렬 스케줄 방식을 이용한 것보다 오류율이 빠르게 수렴하는 것을 확인할 수 있으며, 오류 정정 성능 또한 향상되었음을 확인할 수 있다. 레이어 수를 8로 설정한 계층적 신뢰 전파의 경우, 오류율 성능을 병렬 방식보다 약 2.5배 향상시킬 수 있다. 여기서 얻는 성능 이득은 레이어 별로 업데이트를 진행하면서 사이클의 영향을 줄었다고 볼 수 있다. 또한, 그림 2는 디폴라이징 오류율에 따른 논리적 오류율 (logical error rate) 성능을 비교한 그래프이다. 그림 2의 결과를 통해 계층적 신뢰 전파 알고리즘이 설정한 모든 오류율 영역에서 기존의 병렬 방식을 이용한 신뢰 전파 알고리즘에 비해 좋은 성능을 내고 있음을 확인하였다.

III. 결론

본 논문에서는 양자 저밀도 패리티 검사 부호를 위한 계층적 신뢰 전파 복호 알고리즘을 제안한다. 양자 저밀도 패리티 검사 부호의 구조 특성상 사이클 수가 많아 기존 병렬 스케줄 방식을 이용한 신뢰 전파 복호 알고리즘은 낮은 오류 정정 성능을 갖는다. 하지만 노드들을 레이어에 할당하여 순차적으로 업데이트를 수행하는 계층적 신뢰 전파 복호 알고리즘을 활용하면 신뢰 전파의 필요 반복 횟수를 감소시킬 수 있으며, 복호 시 사이클의 영향을 줄여 오류 정정 능력도 향상시킬 수 있다. 실제 실험 결과를 통해 계층적 신뢰 전파 알고리즘이 오류율 수렴 속도가 더 빠르며, 오류 정정 성능 이득을 확인하였다.

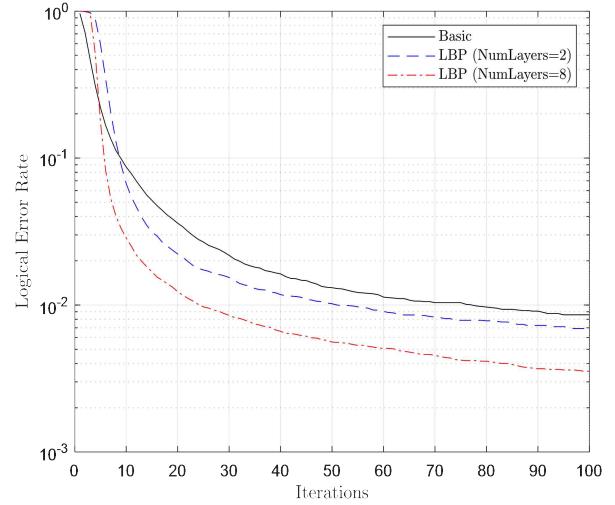


그림 1 디폴라이징 채널 ($p = 0.02$)에서 $[[400, 200]]$ bicycle 부호의 신뢰 전파 반복 횟수에 따른 성능 비교

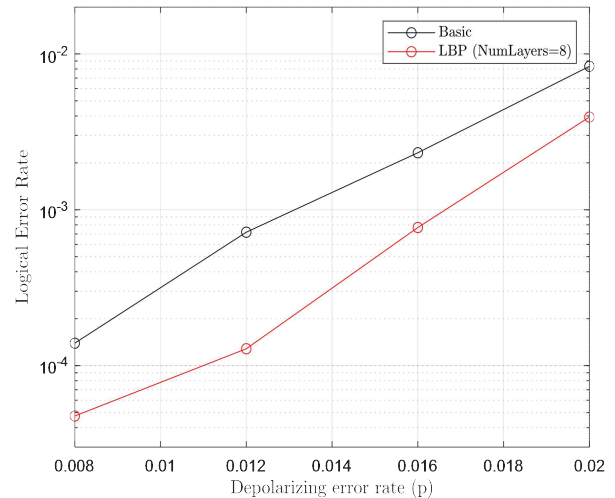


그림 2 $[[400, 200]]$ bicycle 부호에 대한 계층적 신뢰 전파 복호 알고리즘의 논리적 오류율 성능

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2023-2018-0-01402).

이 논문은 2022년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2021R1A2B5B01002204).

참고 문헌

- [1] R. Gallager, "Low-density parity-check codes," IRE Transactions on Information Theory, vol. 8, no. 1, pp. 21 - 28, Jan.1962.
- [2] Y.-M. Chang, et al., "Lower-complexity layered belief-propagation decoding of LDPC codes," IEEE International Conference on Communications, pp. 1155-1160, May.2008.
- [3] D. J. C. Mackay, et al, "Sparse-graph codes for quantum error corrections," IEEE Transactions on Information Theory, vol. 50, no. 10, pp. 2315-2330, Oct.2004.