

# 저밀도 양자 오류정정부호를 위한 반복 복호 알고리즘에 관한 연구

\*신정환, \*\*허 준

고려대학교

\*jhsh@korea.ac.kr

\*\*junheo@korea.ac.kr

## Study of the iterative decoding algorithm of sparse quantum code

Jeonghwan Shin, Jun Heo

Korea University

### 요약

본 논문에서는 기존 오류정정부호의 복호 과정에 사용되는 Belief propagation (BP) 알고리즘을 이용한 저밀도 양자 오류정정부호의 복호 기법에 대해 기술한다. Depolarizing 채널 가정하에 기존 오류정정부호와 다르게 양자 오류정정부호가 갖는 초기 채널 오류 확률에 의한 성능 열화를 개선하기 위해 초기 채널 오류 확률 정보를 개선하는 기법을 적용하였다. 테너 그래프를 바탕으로 각 체크 노드의 신드롬과 노드의 연결 상태를 고려하여 오류가 발생한 위치를 추적하고 BP 알고리즘에 입력되는 초기 채널 오류 확률 정보를 수정하여 반복 복호 시 발생할 수 있는 성능 열화를 개선하였다.

### 1. 서론

양자 전산의 연산 과정 중에 일어날 수 있는 다양한 오류로부터 정보를 보호하기 위해 양자 오류정정부호가 사용되고 있다. Stabilizer 코드[1]는 기존 선형 오류정정부호와 유사한 구조를 가지고 있는 양자 오류 정정부호로 파울리군에서 아벨군을 형성하는 부분 집합 Stabilizer군  $S$ 의  $+1$  고유치를 갖는 고유공간  $V$ 로 정의된다. Stabilizer 코드의 복호 기법은 오류가 발생한 큐비트  $|r\rangle$ 을 Stabilizer로 불리는 측정 연산자로 측정된 신드롬을 이용한 방법이 일반적으로 사용되고 있으며 최근에는 테너 그래프를 바탕으로 BP 알고리즘을 적용하는 연구가 진행되고 있다. [2][3]

$$m_{c \rightarrow q}(E_q) \equiv \sum_{E_c} \left( \delta_{s_c, S_c E_c} \prod_{q' \in n(c) \setminus q} m_{q' \rightarrow c}(E_{q'}) \right) \quad (1)$$

$$m_{q \rightarrow c}(E_q) \equiv p_q(E_q^i) \prod_{c' \in n(q) \setminus c} m_{c' \rightarrow q}(E_{q'}) \quad (2)$$

식 (1)과 (2)는 BP 알고리즘을 이용한 Stabilizer 코드의 복호 과정을 나타낸 것으로 각각 체크 노드와 큐비트 노드에서 전개되는 연산 과정을 보여준다. Stabilizer 코드의 테너 그래프를 보여주는 그림 1.을 참조하여 체크 노드에서 큐비트 노드로 전달되는 오류 정보  $m_{c \rightarrow q}$ 는 체크

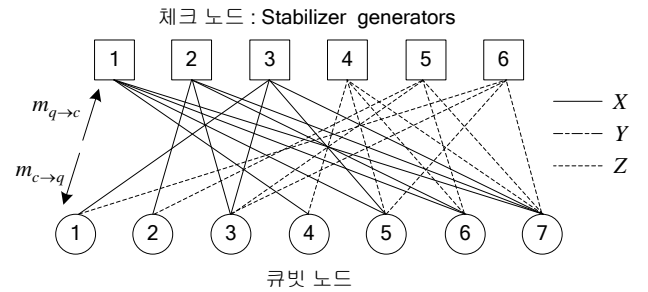


그림 1. 7-큐비트 Steane 7 코드의 테너 그래프

노드에 이웃한 큐비트 노드  $n(c)$ 에서 들어오는 오류 정보  $m_{q \rightarrow c}$ 와 체크 노드의 신드롬  $s_c$ 을 이용하여 계산 된다.

이 때, 신드롬  $s_c$ 는  $S_c$ 와 교환율이 성립하는 오류  $E \in \{x | [S_c, x] = 0\}$ 에 대해  $+1$ 의 값을 가지며 교환율이 성립하지 않는 오류  $E \in \{x | \{S_c, x\} = 0\}$ 에 대해서는  $-1$ 의 값을 갖는다. 신드롬을 이용한 체크 노드 연산은 체크 노드의 신드롬을 만족하는 모든 오류 패턴  $E_c$ 을 고려해야 한다. 큐비트 노드에서 체크 노드에 전달되는 오류 정보

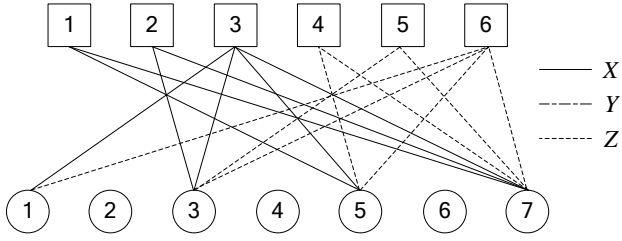


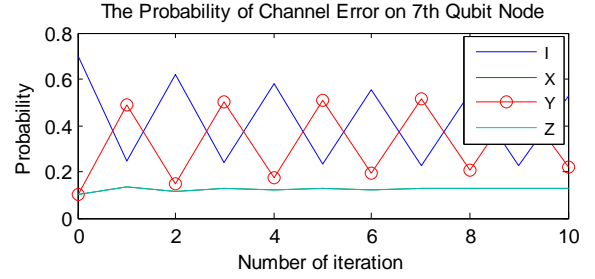
그림 2. 오류 위치 검출을 위한 테너 그래프

는 이웃한 체크 노드  $n(q)$ 에서 전달되는 오류 정보와 채널에 의해서 결정되는 초기 채널 오류 정보  $p_q(E_q^i)$ 를 이용하여 얻을 수 있다. 양자 오류 정정 부호는 연산 과정에서 큐비트의 정보를 측정할 수 없는 제약을 가지고 있다. Stabilizer 코드에 BP 알고리즘을 적용하는 경우 기존 오류정정부호와 다르게 Stabilizer 코드는 초기 채널 오류 정보  $p_q(E_q^i)$ 의 값이 수신된 큐비트  $|r\rangle$ 에 의해 결정되지 않고 채널 오류 확률에만 의존하게 되며 결과적으로 모든 큐비트 노드에 동일한 값이 입력된다. 동일한 초기 채널 정보의 입력은 실제 채널에서 발생한 오류에 대한 정확한 정보를 제공할 수 없으며 이는 오류 정정부호의 복호 실패로 이어지게 된다.[2]

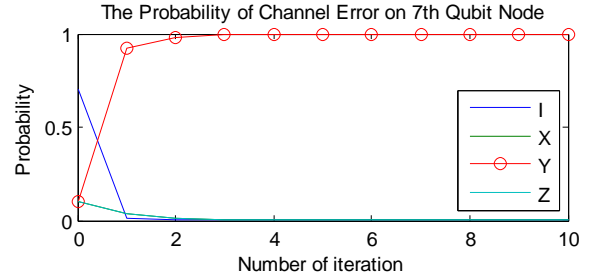
본 논문에서는 단일 오류가 발생하는 Depolarizing 채널 모델에서 Stabilizer 코드에 BP 알고리즘을 적용하는 기법에 대한 연구를 소개한다. BP 알고리즘을 적용함에 있어서 모든 입력 노드에 동일하게 적용되는 채널 오류 확률을 신드롬과 각 노드의 연결 상태를 바탕으로 분석하고 초기 채널 오류 확률을 임의로 조정하여 성능을 개선할 수 있음을 보여준다.

## 2. 본론

초기 채널 오류 정보의 수정을 위해 채널에서 오류가 발생한 위치를 추적해야 하며 이는 채널 오류에 의해 결정되는 신드롬을 이용하여 확인 할 수 있다.  $s_c = -1$ 을 갖는 체크 노드  $c_e$ 에 이웃한 큐비트 노드의 집합을  $n(c_e)$ 라고 하면 채널 오류는  $n(c_e)$ 에 속한 노드 중 한 노드에서 발생한 것을 알 수 있다. 테너 그래프에서 체크 노드와 큐비트 노드는 Stabilizer에 의해 X, Y, Z 중 하나의 연결  $d \in \{X, Y, Z\}$ 을 구성한다. 따라서 임의의 큐비트  $q_e \in n(c_e)$ 에서 오류가 발생했을 경우 오류의 종류는  $c_e$ 와  $q_e$ 의 연결  $d_e$ 와는 다른 종류의 파울리 매트릭스임을 알 수 있다. 오류의 위치는 신드롬과 각 체크 노드가 공유하는 큐비트 노드의 관계를 이용하여 파악 할 수



(a) 동일한 초기 입력을 갖는 BP 알고리즘



(b) 수정된 초기 입력을 갖는 BP 알고리즘

그림 3. 반복 복호에 의한 오류 확률 변화

있다. 오류의 위치를 알기 위해  $n(c_e)$ 에 속한 큐비트 노드 중  $c_e$ 과 동일한 연결을 갖는 +1 체크 노드에 의해 공유된 큐비트 노드를 제외하고  $c_e$ 와 서로 다른 연결을 갖는 +1 체크 노드에 의해 공유된 큐비트 노드에서 오류가 발생했다고 생각할 수 있다. 예를 들어 그림 2.에서  $|r\rangle$ 을 측정하여 얻은 각 체크 노드의 신드롬이  $s = [+1, +1, +1, +1, +1, -1]$ 이라면 6번 체크 노드에 이웃한 1, 3, 5, 7 큐비트 노드 중 한 곳에서 오류가 발생한 것을 알 수 있다. 3, 5, 7 큐비트 노드는 6번 체크 노드와 Z 연결을 이루고 있으며 다른 체크 노드와도 동일한 연결을 이루고 있음을 알 수 있다. 따라서 3, 5, 7에서 오류가 발생했을 경우 6번을 제외한 다른 체크 노드의 신드롬 값 또한 -1의 값을 가져야 할 것이다. 1번 큐비트의 경우 3, 6 체크 노드에 의해 공유되고 있으며 서로 다른 연결을 가지고 있다. 이는 3번 체크 노드에는 영향을 주지 않으며 6번 체크 노드에만 영향을 주는 X 오류가 발생 했음을 알 수 있다. 따라서 우리는 위의 과정을 통해서 오류가 발생한 위치를 파악하고 실제 발생 했을 오류를 고려하여 초기 채널 오류 확률 값을 임의의 값으로 수정하고 BP 알고리즘을 이용한 반복 복호를 수행할 수 있다.

제안한 알고리즘의 검증을 위해 Depolarizing 채널에서 Steane 7 코드의 이용하여 반복 복호를 수행하였다. Steane 7 코드는 Depolarizing 채널에서 단일 오류를 수정할 수 있도록 고안된 오류정정부호로서 6개의 Stabilizer generator를 이용하여 1-큐비트를 7-큐비트로

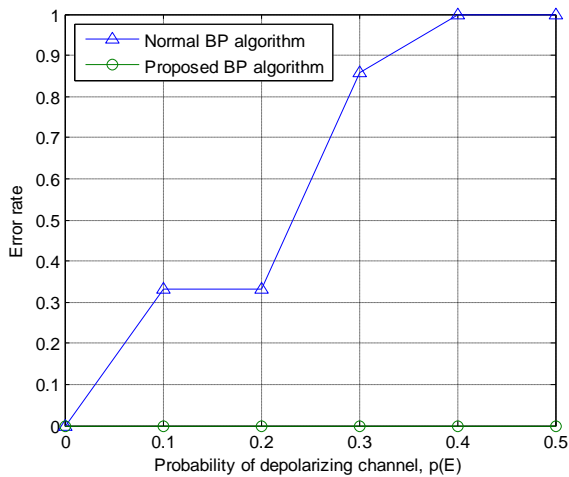


그림 4. Depolarizing 채널에서 기존 복호 기법과 제안된 복호 기법의 오류 확률에 따른 복호율 비교

부호화 한다. 그림 3.은  $p(E)=0.1$  인 Depolarizing 채널에서 7번째 큐비트 노드에 Y 오류를 발생했을 경우 BP 알고리즘에 의해 큐비트 노드의 오류 정보가 진화하는 과정을 보여주고 있다. 일반적인 BP 알고리즘을 수행하는 경우 그림 3의 a)에서 보는 것과 같이 채널에서 발생한 오류를 수정할 수 없음을 보여주지만 제안된 기법을 적용하는 경우 그림 3의 b)에서와 같이 실제 발생한 Y에 대한 확률이 가장 높은 값으로 선택되는 것을 확인할 수 있다.

그림 4.는 Depolarizing 채널에서 채널 오류 확률의 변화에 따른 기존 BP 알고리즘의 복호 기법과 본 논문에서 제안하는 복호 기법의 성능 차이를 보여주고 있다. 신드롬을 바탕으로 한 Steane 7 코드는 단일 오류에 대한 오류 정정 부호이지만 BP 알고리즘을 적용할 경우 모든 큐비트 노드에 동일한 초기 채널 오류 확률 정보가 전달되며 결과적으로 채널 오류 확률이 증가할수록 복호에 실패하는 것을 보여주고 있다. 하지만 동일한 Steane 7 코드에 대해 초기 오류 확률 정보를 신드롬과 테너 그래프를 바탕으로 수정할 경우  $p(E)=0.5$  인 경우에도 BP 알고리즘을 이용하여 단일 오류에 대해 완벽한 복호를 수행할 수 있음을 확인할 수 있다.

### 3. 결론

본 논문에서는 기존 오류정정부호의 복호 과정에 사용되는 BP 알고리즘을 이용한 저밀도 양자 오류정정 부호의 복호 기법에 대해 기술하였다. Depolarizing 채널 가정 아래서 BP 복호 알고리즘을 적용한 기존 오류정정 부호의 문제점을 확인하고 초기 채널 오류 확률의 개선을 위해 테너 그래프를 바탕으로 신드롬과 각 노드의 연결 상태를 고려하여 초기 채널 오류 확률을 수정하였다. 수정된 채널 오류 확률을 입력으로 하는 제안된 복호 알고리즘이 기존 복호 알고리즘에서 발생 하는 오류를 수정할 수 있음을 시뮬레이션을 이용하여 증명하였다.

### 4. ACKNOWLEDGMENTS

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터지원사업의 연구결과로 수행되었습니다. (NIPA-2010-C1090-1031-0009)

### 5. 참고문헌

[1] D. Gottesman, "Stabilizer Codes and Quantum Error Correction," Caltech Ph.D. dissertation, Pasadena, CA, ArXiv:quant-ph/9705052v1.

[2] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," Quantum Inform. Comput., vol. 8, pp. 987-1000, 2008.

[3] Y. J. Wang, B. C. Sanders, B.-M. Bai and X.-M. Wang, "Enhanced feedback iterative decoding of sparse quantum codes," arXiv.org:0912.4546.