

# [[4,2,2]] 오류 검출 코드 기반 양자 얽힘 증류

정혜단, 허준\*  
고려대학교

hyedan@korea.ac.kr, \*junheo@korea.ac.kr

## [[4,2,2]] Error Detection Code-based Entanglement Distillation

HUIDAN ZHENG, Jun Heo\*  
Korea Univ.

### 요 약

본 논문에서는 안정자 기반 오류 탐지 코드인 [[4,2,2]]를 이용한 얽힘 증류 프로토콜을 제안하였다. 제안 방식은 네 개의 벨 쌍에 대해 지역 안정자 측정과 양방향 고전 통신을 수행하여, 일치 결과에 한해 두 개의 고충실도 쌍을 보존하는 구조이다. 디폴라이징 채널 환경에서 수행한 성능 비교 결과, 본 프로토콜은 특정 입력 충실도 구간에서 BBPSSW 대비 더 높은 출력 충실도를 보이며, 고품질 얽힘 확보에 유리한 특성을 보인다.

### I. 서 론

양자 얽힘은 분산 양자정보처리와 양자키분배(Quantum Key Distribution) 등의 핵심 자원이지만 전송과 저장 과정에서 발생하는 노이즈로 충실도(Fidelity)가 감소한다[1]. 이를 보완하기 위해 다수의 저충실도 쌍에서 소수의 고충실도 쌍을 얻는 얽힘 증류(Entanglement Distillation Protocol, EDP)[2]와 양자 오류 정정(Quantum Error Correction, QEC)[3] 두 가지 접근이 연구되어 왔다. 본 논문은 안정자(stabilizer) 기반 오류 탐지(error-detecting) 코드인 [[4,2,2]] 코드를 EDP에 결합한 post-selection 방식을 다룬다. 4 개의 벨 쌍에 대해 안정자 측정(stabilizer measurement)과 양방향 고전 통신(2-way classical communication)을 수행하고 통과한 경우만 채택하여 더 높은 충실도의 2 쌍을 얻는다. 이 방식은 BBPSSW와 비교해 특정 입력 구간에서 1 라운드 충실도 이득을 기대할 수 있으나 수율(yield)은 감소한다. 본 논문은 회로 구성과 1 라운드 성능을 간략히 보고하고 양자 메모리와 근거리 중계기 응용 가능성을 언급한다.

### II. 본론

BBPSSW[2]가 제안된 이후 다양한 얽힘 증류 변형이 보고되었고 코드 구조를 증류 절차에 결합하여 성능을 개선하려는 연구가 이어졌다[4-6]. 코드 기반 접근은 안정자 측정과 LOCC 만으로 오류를 검출하고 불량 샘플을 폐기할 수 있어 회로가 단순하고 하드웨어 요구가 낮다는 장점이 있다. 본 연구에서는 이 흐름 속에서 오류 정정을 수행하지 않고 오류를 탐지하여 후선택하는 detection 모드를 채택한다.

그림 1은 QEC 기반 EDP의 개념도이다. 각 노드는 지역 안정자 측정을 수행한 뒤 고전 채널을 통해 결과를 교환하고 일치 여부에 따라 보존 또는 폐기를 결정한다. 우리는 안정적인 판정을 위해 양방향 고전 통신을 기본으로 사용하며 일방향 통신을 사용하는 변형도 가능성을 간단히 언급한다. 이 설정에서는 추가적인 양자 게이트나 비국소적 연산이 필요 없고 로컬 측정과 고전 통신만으로 증류를 구현할 수 있다.

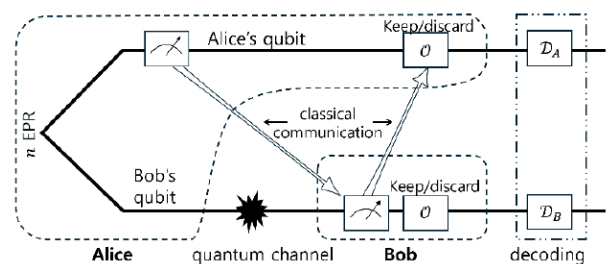


그림 1. QEC 기반 EDP 개념도 검출 모드

제안 기법을 EDC-EDP라 부른다. Alice는 네 개의 EPR 쌍을 준비하고 각 쌍의 한 큐비트를 디폴라이징 채널을 통해 Bob에게 전송한다. 그 결과 두 노드는 낮은 충실도의 네 쌍을 공유한다. 이후 Alice는 [[4,2,2]] 코드의 안정자를 자신의 네 개 물리 큐비트에 대해 측정하고 그 결과를 고전 채널로 Bob에게 보낸다. Bob은 동일한 안정자를 자신의 쪽에서 측정하고 Alice의 결과와 비교한다. 두 노드의 결과가 합치되는 경우에만 해당 자원을 보존하며 합치되지 않으면 폐기한다. 성공 시에는 두 개의 더 높은 충실도의 벨 쌍을 바로 사용하거나 복호를 생략하고 논리 얽힘 상태로 보관하는 운용도 가능하다.

그림 2 는 디폴라이징 채널을 가정한 성능 비교이다. 입력 충실도를  $F_{in}$  이라 할 때 출력 충실도 곡선  $F'_{EDC-EDP}$  와  $F'_{BBPSSW}$  그리고 yield 를 의미하는 곡선  $Y_{EDC-EDP}$  와  $Y_{BBPSSW}$  를 함께 나타냈다. EDC-EDP 는 입력 상태의 충실도가 일정 임계값을 넘는 구간에서 입력보다 더 높은 충실도의 얹힘 쌍을 산출한다. 같은 조건에서 BBPSSW 보다 출력 품질이 더 높게 나타난다. 다만 후선택으로 인해 성공 확률이 낮아져 전체 수율은 BBPSSW 보다 작다. 따라서 고품질의 얹힘을 우선하는 응용에서는 EDC-EDP 가 유리하고 많은 양의 자원을 빠르게 확보해야 하는 경우에는 BBPSSW 가 더 적합하다. 이러한 비교는 depolarizing channel 을 가정한 성능 곡선에서 확인할 수 있다.

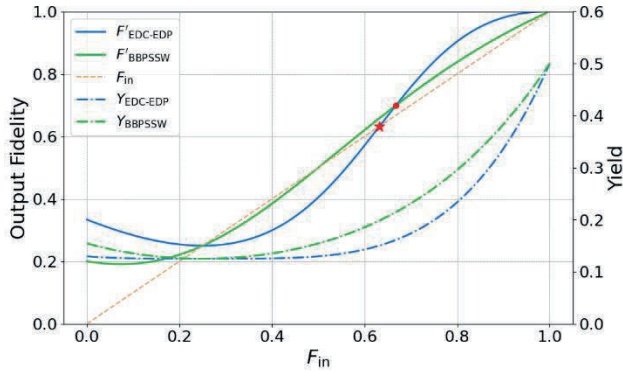


그림 2.  $[[4,2,2]]$  코드 기반 EDP 의 성능 비교

본 연구에서 고려하는 노이즈 모델은 디폴라이징 채널이다. 분배 과정에서 각 물리 쌍은 확률적으로 파울리 오류가 섞인 상태가 되며 결과적으로 낮은 충실도의 공유 상태로 모델링된다. 이러한 가정은 다양한 실험 환경에서 널리 사용되는 표준 모델이라는 점에서 비교의 공정성을 확보하며 코드 기반 증류의 장단점을 직관적으로 드러낸다.

### III. 결론

본 논문에서는 안정자 기반 오류 탐지 코드인  $[[4,2,2]]$  를 이용한 얹힘 증류 프로토콜(EDC-EDP)을 소개하고, 전통적인 BBPSSW 와의 성능을 비교하였다. 제안 방식은 네 개의 벨 쌍을 지역적 안정자 측정과 양방향 고전 통신을 통해 처리하고, 결과가 일치하는 경우에만 고충실도 상태를 얻는 후선택 구조를 따른다. 디폴라이징 채널 환경에서 시뮬레이션한 결과, EDC-EDP 는 특정 입력 충실도 구간에서 BBPSSW 보다 더 큰 출력 충실도를 보이며, 특히 고품질 얹힘이 요구되는 상황에 유리함을 확인하였다. 다만 수율 측면에서는 후선택으로 인한 폐기 비율이 존재하므로 응용 목적에 따라 품질과 자원 효율 사이의 균형이 필요하다. 향후 연구에서는 1-way LOCC 구조나 논리 상태 기반 재증류, 다중 라운드 구성으로의 확장 가능성에 대해 검토할 수 있다. EDC-EDP 는 간단한 회로와 낮은 구현 요구로 인해 양자 메모리, 근거리 양자 네트워크 등 자원이 제한된 실용 환경에서 유용한 증류 방식이 될 수 있다.

이 논문은 2025 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2022-0-00463, 양자인터넷 구현을 위한 유선 양자중계기 개발).

### 참 고 문 헌

- [1] M. Z. Ali et al., "Quantum for 6G communication: a perspective," IET Quant. Comm., vol. 4, no. 3, pp. 112-124, 2023.
- [2] C. H. Bennett, "Mixed State Entanglement and Quantum Error Correction," Phys. Rev. A, vol. 54, pp. 3824-3851, 1996.
- [3] A. M. Steane, "A tutorial on quantum error correction," Rep. Prog. Phys., vol. 76, no. 7, pp. 076001, 2013.
- [4] M. A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge: Cambridge University Press, 2000.
- [5] M. M. Wilde, H. Krovi, and T.A. Brun, "Convolutional Entanglement Distillation," Phys. Rev. A, vol. 75, pp. 060303, 2007.
- [6] H. Aschauer, "Quantum Communication in Noisy Environments," Phys. Rev. Lett., vol. 91, no. 5, pp. 057901, 2003.

### ACKNOWLEDGMENT