

클라우드 양자 컴퓨팅에서 얽힘 생성 회로의 검증

성 지현, 배 준우*

한국과학기술원

jiheon94@kaist.ac.kr, *joonwoo.bae@kaist.ac.kr

Detecting Entanglement Generating Circuits in Cloud-Based Quantum Computing

Jiheon Seong, Joonwoo Bae*

Korea Advanced Institute of Science and Technology

요약

CNOT 게이트 혹은 Toffoli 게이트로 생성되는 얽힘은 양자 이점을 달성하기 위한 중요한 자원이다. 본 논문은 클라우드 양자 컴퓨팅에서 얽힘을 생성하는 양자 회로를 검증하는 방법을 제시한다. 회로 기반의 양자 컴퓨팅 모델에서 양자 얽힘의 생성을 검증하는 양자 회로를 구축하는 방법을 제시한다. 이 방법은 클라우드 컴퓨팅 서비스에서 자체적으로 수행하는 큐비트 배열 (Qubit Allocation), 즉 사용자가 송신한 회로와 양자 하드웨어의 큐비트를 연계하는 과정을 신뢰해야 한다는 추가 가정 없이 얽힘을 검증할 수 있다. 본 연구에서 제시한 얽힘 검증 방법을 IBMQ와 IonQ에서 실제 구현하여 얽힘 생성 회로를 규명하였다. 특히 큐비트 배열 과정을 신뢰할 수 없는 IonQ의 클라우드 서비스에서 얽힘을 성공적으로 검증하였다. 본 양자 얽힘 검증 체계는 양자 이점을 달성하기 위한 실용적인 양자정보처리에서 유용하게 적용될 수 있을 것이다.

1. 서론

양자역학의 원리를 정보처리에 적용하여 현재 IT 수준의 한계를 극복하는 것이 가능하다 [1]. Noisy intermediate scale quantum (NISQ) 기술로 요약되는 현재 양자 기술은 모든 과정에서 잡음의 발생을 포함한다 [2]. 중요한 사실은, 잡음을 포함한 NISQ 기술이라 할 지라도, 양자역학의 원리에 기반하여 정보처리를 수행함으로써 기존의 정보처리의 한계를 뛰어넘는 것이 가능하게 되었다는 것이다. 얽힘은 양자 우위 (양자계의 사용에 의한 기존 정보처리 대비 우위) 를 확보하는 데에 핵심적인 자원이다. 얽힘은 CNOT 게이트 혹은 Toffoli 게이트를 통해 생성되므로, 얽힘의 검증은 이러한 게이트의 작동을 검증하는 과정이기도 하다.

이미 글로벌 기업 및 스타트업 기업들은 클라우드 컴퓨팅 형태로 양자 컴퓨터를 쉽게 사용할 수 있는 플랫폼을 구현하였다. 현재의 양자 컴퓨터는 대개 클라우드 서비스 방식으로 접근 가능한데, 이 시나리오는 양자 실

험실의 시나리오와는 다소의 차이가 존재한다. 클라우드 양자 컴퓨터의 사용자는 회로를 디자인하여 입력하면, 클라우드 서비스는 입력된 회로를 실제 하드웨어에서 구현한 후 결과 통계를 종합하여 사용자에게 제공한다 (그림 1). 여기서 큐비트 배열은 양자 하드웨어가 사용자가 제공한 회로를 실제 하드웨어의 물리 큐비트와 대응시키는 과정을 의미한다.

본 연구는 양자 실험실에 대응되는 준비와 측정 (Prepare and measure, P&M) 시나리오에서의 얽힘 검증 연산자를 양자 회로 시나리오로 옮겼을 때의 얽힘 검증 회로(Entanglement-Witnessing Circuits, EWC)에 대해 소개한다. 이는 양자 얽힘 검증 2.0을 활용한 것이기 때문에 양자 얽힘 검증을 효율적으로 수행할 수 있고, 또한 클라우드 기반의 양자컴퓨터에서 사용자가 직접 큐비트 분배를 할 수 없는 경우에도 얽힘을 검증할 수 있다. 이 얽힘 검증 회로 체계를 IBMQ와 IonQ의 양자컴퓨터에 적용하여 얽힘을 검증할 수 있음을 보였다.

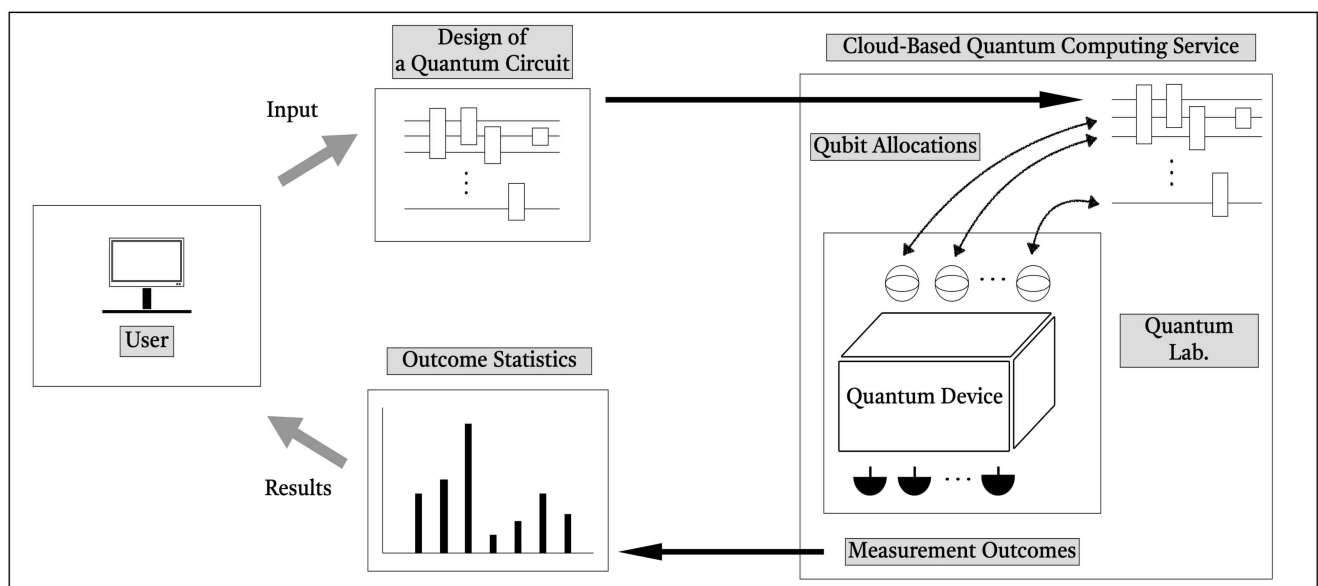


그림 1. 클라우드 양자 컴퓨팅 서비스의 개요. 사용자가 양자 회로의 설계를 전송하면 클라우드 컴퓨팅은 양자 회로를 구현하여 측정 결과를 다시 사용자에게 전송한다. 사용자는 측정 결과를 분석하여 결론에 도달한다. 일반적인 양자 실험과 달리 사용자가 전송한 양자 회로와 큐비트 배열을 클라우드 서비스가 수행한다. 큐비트 배열(Qubit Allocations)을 신뢰해야 한다는 가정이 추가로 요구된다.

II. 본론

일반적으로 N 개 큐비트에 대한 양자 회로는 단일 큐비트를 제외하고 2개 혹은 3개 큐비트 게이트로 분해될 수 있다. 얽힘이 없는 상태 $|\psi\rangle$ 에 대해서 회로 후 상태 $U|\psi\rangle$ 가 얽힘을 포함할 때, 양자 회로 U 는 얽힘 생성 회로라 한다.

양자 얽힘 검증 2.0 프로그램 (EW 2.0)은 기존의 얽힘 검증 방법의 효율을 약 2배 향상한다. 이 과정은 EW 2.0 연산자 \tilde{W} 에 대한 기댓값을 실험적으로 얻는 것이며 여기서 \tilde{W} 는 측정가능량 (observable)이다. EW 2.0 연산자는 얽힘을 포함하지 않는 모든 상태에 대해 다음을 만족한다:

$$B_L(\tilde{W}) \leq \text{tr}[\tilde{W}\sigma_{\text{sep}}] \leq B_U(\tilde{W}).$$

위의 식에서 상한 및 하한은 각각 다음과 같다,

$$B_L(\tilde{W}) = \min_{\sigma_{\text{sep}}} \text{tr}[\tilde{W}\sigma_{\text{sep}}], \quad B_U(\tilde{W}) = \max_{\sigma_{\text{sep}}} \text{tr}[\tilde{W}\sigma_{\text{sep}}].$$

상한 및 하한에 의한 검증은 두 개의 얽힘 검증 연산자 (Entanglement Witness, EW) $W^{(+)}$ 와 $W^{(-)}$ 에 대응한다. 상한과 하한이 이루는 구간 $[B_L(\tilde{W}), B_U(\tilde{W})]$ 은 얽힘이 없는 상태들이 만족하는 영역으로서 얽힘 없는 영역 (Separability Window, SW) 이라고 한다 [3].

EW 2.0 프로그램에 기반하여 양자 회로의 얽힘 생성을 검증하는 과정은 다음과 같다. EW 2.0 연산자에 대해 순수화 과정 (purification)을 적용하여 다음의 Rank-1 연산자를 구현한다:

$$\tilde{W} = \text{tr}_A |\tilde{W}\rangle_{SA} \langle \tilde{W}|.$$

검증하고자 하는 회로에서 사용하는 큐비트 개수 만큼을 더 추가하여 상태 $|\tilde{W}\rangle$ 를 구현할 수 있으며, 이 상태를 구현하는 양자 회로를 얽힘 검증 회로 (Entanglement Witness Circuits, EWC)라 한다 (그림 2).

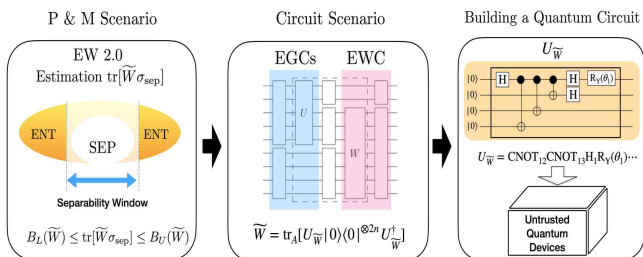
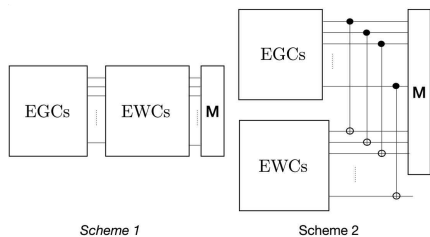


그림 2 P&M의 EW 2.0에 대해 EWC를 구현 및 검증 과정

EWC를 통한 얽힘 생성 검증은 아래와 같이 두 가지 방법으로 구현할 수 있다:



첫 번째 방법은 해당 회로 후에 곧바로 EWC를 적용하여 측정을 통해 얽힘을 검증한다. 두 번째 방법은 EWC를 추가로 구성하고 해당 회로와 CNOT을 적용하여 측정을 통해 얽힘을 검증한다. 첫 번째 방법은 추가 큐비트를 사용하지 않는 장점이 있고 두 번째 방법은 회로의 깊이가 증가하지 않는다는 장점이 있다.

위의 방법을 통해 **IBMQ와 IonQ에서의 얽힘 생성을 검증**할 수 있다. IBMQ는 큐비트 배열 기능을 제공하고 IonQ는 제공하지 않는다. 본 논문에서 제시하는 방법은 큐비트 배열의 신뢰에 의존하지 않으므로, 큐비트 배열에 대한 명령어와 무관하게 얽힘을 검증할 수 있다 (그림 3). 특별히 IonQ의 경우는 큐비트 배열 기능이 없는 시나리오에서 얽힘 생성을 검증한 첫 사례에 해당한다 (그림 4).

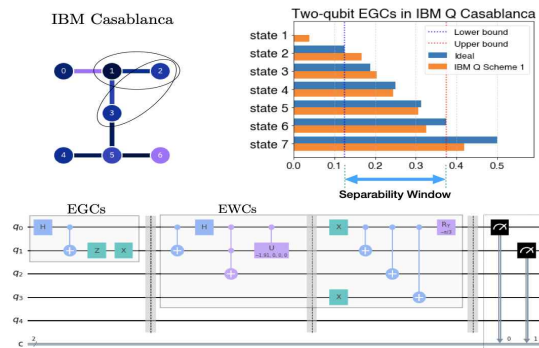


그림 3. IBMQ Casablanca의 (1,2)와 (2,3)의 두 큐비트 얽힘 생성 검증. SW 위반을 통해 얽힘 검증.

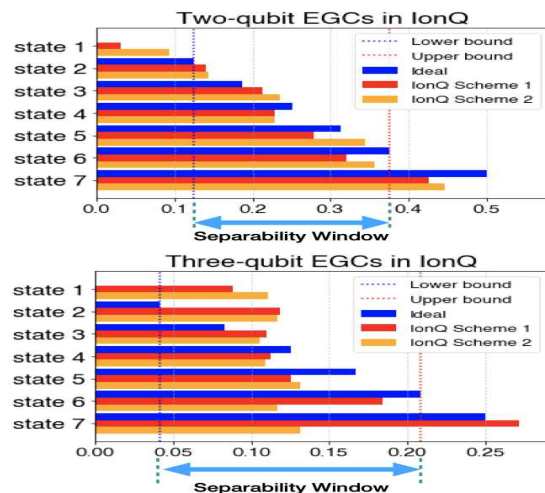


그림 4. IonQ에서의 얽힘 검증. 상단의 그래프는 2개 큐비트, 하단은 3개 큐비트에서 얽힘 생성 검증 결과.

III. 결론

클라우드 양자 컴퓨팅 서비스는 양자 실험과 비교할 때 큐비트 분배라는 추가적인 과정을 포함한다. 본 논문은 클라우드 양자컴퓨팅 서비스에서 수행되는 큐비트 배열에 대한 신뢰도와 무관하게 얽힘 생성을 검증할 수 있는 방법을 제시하였다. 이 방법을 통해 IBMQ와 IonQ의 회로에서 얽힘 생성을 검증하였다. 본 연구 결과는 클라우드 양자 컴퓨팅 서비스에서 얽힘을 검증하는데 일반적으로 활용될 수 있다.

양자 하드웨어가 양자 우위를 달성하기 위해서 얽힘 생성은 반드시 수반되어야 한다. 클라우드 양자컴퓨팅 서비스에서 실용적인 정보처리를 수행하고자 할 때, 제시된 해당 검증 기법은 양자 우위를 달성하기 위해 선행되어야 할 얽힘 생성 능력을 검증하는데 적용될 수 있을 것이다.

ACKNOWLEDGMENT

본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행되었습니다. (NRF-2021R1A2C2006309, NRF-2021M3E4A1080001)

참고 문헌

- [1] D. Deutsch and R. Penrose, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 400, 97 (1985).
- [2] J. Preskill, Quantum 2, 79 (2018).
- [3] J.Bae, D. Chruscinski, and B. C. Hiesmayr, npj Quantum Information 6, 15 (2020).