

IBM Q 양자 컴퓨터를 이용한 Recurrence Protocol의 구현 및 Twirling Operation 유무에 따른 성능 비교

하진영(고려대학교), 강유진(고려대학교), 허준(고려대학교)*
ksuwer@korea.ac.kr, yujin20@korea.ac.kr, *junheo@korea.ac.kr

Implementation of Recurrence Protocol Using IBM Q Quantum Computer and Performance Comparison Based on the Presence of Twirling Operation

Ha Jin Young(Korea Univ.), Kang Yu Jin(Korea Univ.), *Heo Jun(Korea Univ.)

요약

본 논문에서는 IBM Q 양자 컴퓨터를 이용하여 Recurrence protocol 을 구현하고, Recurrence protocol 과정에서 Twirling operation 의 유무에 따른 성능을 비교한다. 5 큐비트 프로세서 manila 에서 Recurrence protocol 을 수행하는 양자 회로를 수행하여 fidelity 를 확인하였다. 실제 구현 결과 Recurrence protocol 미 수행 시, Twirling 없는 Recurrence protocol 수행 시, Twirling 을 포함한 Recurrence protocol 수행 시 충실도가 각각 96.5%, 83.1%, 80.1%로 측정되었다.

I. 서론

Entanglement distillation 은 여러 개의 entanglement state 를 local operation 과 classical communication 만을 사용하여 유사 pure Bell pair 를 만들어내는 방식이다. 1996 년에 Bennet et al. 은 pure state 에 대한 최초의 Entanglement distillation protocol 을 개발하였으며 [1], 같은 해에 Bennet et al. 은 mixed state 에 대한 entanglement distillation protocol 인 Recurrence protocol 을 개발하였다 [2]. 구글과 IBM 과 같은 몇몇 회사들은 양자 컴퓨터의 실용적인 사용을 위한 노력을 이끌고 있다[3,4]. IBM 에서는 클라우드를 통해 전세계에서 사용할 수 있는 IBM Q 양자 컴퓨터 프로토타입을 공개하였다 [4]. 본 논문에서는 Recurrence protocol 을 수행하는 양자 회로를 설계하여 IBM Q 상에서 구현한다. Entanglement distillation 을 수행하지 않았을 때, Twirling operation 을 수행하지 않는 Recurrence protocol 을 수행하였을 때, Twirling operation 을 수행하는 Recurrence protocol 을 수행하였을 때 각각 결과를 비교한다.

II. 본론

Entanglement distillation 은 충실도가 낮은 Bell state 여러 개를 사용하여 높은 충실도의 Bell state 를 만들어내는 방식이다. Entanglement distillation 을 통해 얻고자 하는 Bell state 는 다음과 같다.

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (1)$$

한편, Bennet 은 mixed state 에 대한 entanglement distillation 을 위하여 Recurrence protocol 을 개발하였다. Recurrence protocol 은 전송 과정에서 오류가 생겨 충실도가 낮아진 Bell state 인 ρ_s 두 개를 사용하여 좀 더 높은 충실도를 가지는 Bell state 를 만들어낸다. 이후 목표로 하는 충실도를 얻을 때까지 Recurrence protocol 을 반복한다. Recurrence protocol 은 Twirling 을 통한 Werner state 생성, Bell state 중 하나인 $|\psi^-\rangle$ 상태를 $|\phi^+\rangle$ 상태로 만드는 과정, bilateral CNOT 과정, Target 큐비트 측정 과정으로 이루어진다.

A. Recurrence protocol 의 수행 과정

1) Twirling 을 통한 Werner state 생성

Recurrence protocol 이 성공적으로 수행되기 위해서는 (2)식과 같이 정의되는 Werner state 를 생성해야 한다.

$$W_F = F|\psi^-\rangle\langle\psi^-| + \frac{1-F}{3}(|\psi^+\rangle\langle\psi^+| + |\phi^-\rangle\langle\phi^-| + |\phi^+\rangle\langle\phi^+|) \quad (2)$$

(2) 식에서 $|\psi^\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$, $|\phi^\pm\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$, F 는 W_F 상태의 $|\psi^-\rangle$ 에 대한 충실도이다. 전송 과정에서 ρ_s 에 어떤 오류가 발생했는지 확인할 수 없기 때문에, ρ_s 를 W_F 로 만드는 Twirling 과정이 필요하다. Twirling operation 은 ρ_s 의 각각 큐비트에 $k(k \in \{x, y, z\})$ 축으로 $\pi/2$ 회전을 수행하는 B_k 를 랜덤하게 수행한다. 이 때 랜덤한 선택은 B_k 의 12 가지 조합으로 이루어지는 U_i 중 하나를 랜덤하게 선택하여 수행한다. U_i 는 다음과 같이 구성된다.

$$\{U_i\} = \{I, B_x B_x, B_y B_y, B_z B_z, B_x B_y, B_y B_z, B_z B_x, B_y B_x, B_x B_z, B_z B_y, B_x B_z B_x, B_y B_z B_y, B_z B_x B_z, B_x B_y B_x\} \quad (3)$$

따라서 Twirling operation 을 통해 생성되는 최종 상태는 다음과 같다.

$$W_F = \frac{1}{12} \sum_{i=1}^{12} U_i \rho_s U_i^\dagger \quad (4)$$

2) $|\psi^-\rangle$ 상태를 $|\phi^+\rangle$ 상태로 변형

Entanglement distillation 과정에서 최종적으로 얻고자 하는 상태는 $|\phi^+\rangle$ 이므로, W_F 에서 $|\psi^-\rangle$ 를 $|\phi^+\rangle$ 로 변형하는 과정이 필요하다. 해당 과정은 얽힘 상태의 한 큐비트에 Y operation 을 수행한다. 해당 과정 수행 이후의 상태를 ρ_F 라고 할 때, ρ_F 는 다음과 같이 정의된다.

$$\rho_F = Y W_F = F|\phi^+\rangle\langle\phi^+| + \frac{1-F}{3}(|\psi^+\rangle\langle\psi^+| + |\phi^-\rangle\langle\phi^-| + |\psi^-\rangle\langle\psi^-|) \quad (5)$$

3) Bilateral CNOT 및 Target qubit 측정

Y operation 을 수행한 이후, 얽힘 쌍을 나누어 가지고자 하는 Alice 와 Bob 은 각각 ρ_F 큐비트 쌍을

두 개씩 나누어 가지게 된다. Alice 와 Bob 이 보유하고 있는 큐비트 쌍 중 Controlled 연산을 수행할 한 쌍을 $\rho_{F,C}$, Target 연산을 수행할 다른 한 쌍을 $\rho_{F,T}$ 로 정의한다. Alice 와 Bob 은 각각 가지고 있는 큐비트 2 개 중 $\rho_{F,C}$ 에 속하는 큐비트를 controlled 큐비트로, $\rho_{F,T}$ 에 속하는 큐비트를 Target 큐비트로 CNOT 연산을 수행한다. 이 과정에서 Alice 와 Bob 이 각각 local 한 CNOT 을 수행하므로 해당 과정을 Bilateral CNOT 이라 명명한다. 이후 Alice 와 Bob 은 각각 본인이 가지고 있는 Target qubit 를 computational basis 로 측정한다. 측정 이후의 $\rho_{F,C}$ 의 충실도 F' 은 식 (6)과 같다.

$$F' = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2} \quad (6)$$

따라서, $F > \frac{1}{2}$ 일 때 Recurrence protocol 이 충실도를 증가시키는 것을 확인할 수 있다.

B. IBM Q 를 이용한 Recurrence protocol 구현

위 과정에서 확인할 수 있듯이, Recurrence protocol 의 구현을 위해서는 여러가지 양자 연산이 수행되어야 한다. 이러한 양자 연산은 실제 수행 시 오류율을 가지게 된다. 이러한 오류율로 인하여 Recurrence protocol 을 수행 시 양자 연산의 성능에 따라 충실도가 감소할 가능성이 존재한다. 본 논문에서는 현재 양자 컴퓨터의 성능이 Recurrence protocol 을 성공적으로 수행할 수 있을지 확인하기 위하여 IBM Q 양자 컴퓨터 상에서 Recurrence protocol 을 사용하지 않는 얽힘 분배, Twirling 없는 Recurrence protocol, Recurrence protocol 을 각각 구현하고 결과를 비교한다.

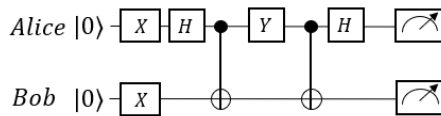


그림 1(a). Recurrence protocol 을 사용하지 않는 얽힘 분배 회로도

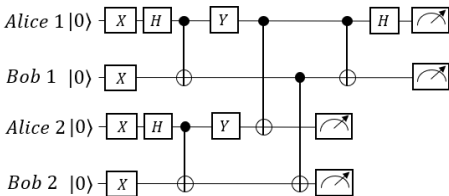


그림 1(b). Twirling 없는 Recurrence protocol 회로도

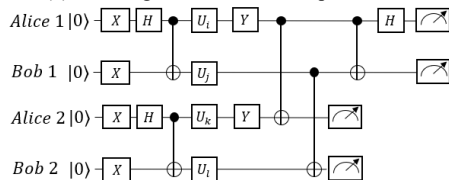


그림 1(c). Twirling 을 포함한 Recurrence protocol 회로도

그림 1 은 각각 세가지 조건에 대한 양자 회로를 나타낸다. 충실도의 쉬운 측정을 위하여 최종 얽힘 상태에 CNOT gate 와 H gate 를 수행하여 측정시 00 의 결과를 얻을 확률이 충실도가 되도록 회로를 설계하였다. 그림 1(c)에서 i, j, k, l 은 1 에서 12 사이의 정수이며, 회로 수행마다 무작위로 설정된다. 양자 프로그래밍 언어인 QISKit 을 사용하여 IBM 의 5 큐비트 양자 프로세서 manila 에서 양자 회로를 각 10,000 회 수행하였다.

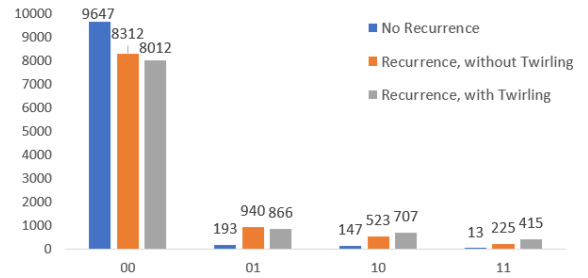


그림 2. Manila 상에서 양자 회로 10000 회 수행 결과

그림 2 에서 Recurrence protocol 을 수행하지 않는 얽힘 상태의 충실도가 96.5%, Twirling 을 수행하지 않는 Recurrence protocol 수행 시 충실도가 83.1%, Recurrence protocol 수행 시 충실도가 80.1%로 측정되었다. 따라서 얽힘 상태의 충실도를 높이기 위해 연산이 추가될수록 충실도가 오히려 낮아지는 결과를 얻었다. Recurrence protocol 을 수행하지 않은 경우보다 수행했을 때 충실도가 낮아지는 주요 원인은 CNOT 연산의 높은 오류율과 manila 에서 CNOT 연산의 Connectivity 때문이다. 예를 들어, Recurrence protocol 에서 Bilateral CNOT 을 수행하는 큐비트 사이에 CNOT 을 직접 수행할 수 없기 때문에 큐비트 간 SWAP 이 필요하고, 따라서 수많은 CNOT 을 추가적으로 사용을 하여야 한다. 따라서 Recurrence protocol 이 성공적으로 수행되기 위해서는 양자 프로세서 상에서 연산의 오류율이 더욱 낮아지고, 큐비트 간의 connectivity 가 개선되어야 함을 확인할 수 있다.

III. 결론

본 논문에서는 Twirling 연산을 포함하거나 포함하지 않는 Recurrence protocol 을 수행하는 양자회로를 설계하여 실제 양자 컴퓨터에서 실행을 하였으며, Recurrence protocol 을 사용하지 않고 얽힘을 분배하는 방식과 성능을 비교하였다. 양자 회로에서 연산이 추가될수록 결과 상태의 충실도가 떨어지는 것을 확인하였으며, Recurrence protocol 의 성공적인 수행을 위해서는 연산의 정확도, 큐비트 간의 connectivity 가 개선되어야 함을 확인하였다.

ACKNOWLEDGMENT

이 논문은 2022 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] Bennett, C. H., Bernstein, H. J., Popescu, S., & Schumacher, B. (1996). Concentrating partial entanglement by local operations. *Physical Review A*, 53(4), 2046.
- [2] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., & Wootters, W. K. (1996). Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5), 3824.
- [3] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505-510.
- [4] IBM Quantum. <https://quantum-computing.ibm.com/>, 2022.