Toffoli gate 분해에 대한 동향

김현준 [1], 임세진 [2], 서화정 [3]
[1] 한성대학교 정보컴퓨터공학과 박사과정
[2] 한성대학교 융합보안학과 석사과정
[3] 한성대학교 융합보안학과 부교수

khj930704@gmail.com, dlatpwls834@gmail.com, hwajeong84@gmail.com

Trends in Toffoli gate decomposition

Hyun-Jun Kim[1], Se-Jin Lim[2], Hwa-Jeong Seo[3]
[1]Dept. of Computer Science, Han-Sung University
[2]Dept. of Convergence Security, Han-Sung University
[3]Dept. of Convergence Security, Han-Sung University

요 약

양자 컴퓨터는 기존의 클래식 컴퓨터와 달리 양자역학 원리를 활용해 정보 처리를 수행하며, 특정 문제들을 훨씬 빠르게 해결할 수 있다. 양자 컴퓨터는 큐빗을 기본 단위로 사용하고, 아다마르 게이트, CNOT 게이트, 파울리 게이트, 토플리 게이트 등을 조합하여 양자 회로를 구성한다. Toffoli 게이트는 유니버설 게이트 중 하나로, 세 개의 큐빗을 입력받아 조건부 (Controlled-Controlled) NOT 연산을 수행한다. 이 게이트는 복잡한 작업을 기본 양자 게이트로 분해할 수 있어, 회로의 게이트 수, 깊이 및 오류율 측면에서 최적화할 수 있다. 기본 양자 게이트 중 T 게이트는 노이즈와 오류에 영향을 받을 수 있으므로, T 게이트의 수와 깊이를 최적화하는 것이 중요하다. 본 논문은 Toffoli 게이트 분해를 통해 양자 회로의 게이트 수와 깊이를 최적화하는 방법을 조사한다.

1. 서론

양자컴퓨터는 기존의 클래식한 컴퓨터와는 다르게 양자역학적 원리를 이용하여 정보를 처리하는 컴퓨터이다. 양자 컴퓨터는 기존의 고전적 컴퓨터와는 근본적으로 다른 방식으로 작동하며, 이로 인해 특정 문제들에 대해 기존 컴퓨터보다 훨씬 빠르고 효율적으로 해결할 수 있다. 1994 년, 피터 쇼어 (Peter Shor)는 소인수분해를 빠르게 해결할 수 있는 양자 알고리즘을 발견했다. 쇼어 알고리즘은 기존의 고전 컴퓨터보다 지수적으로 빠른 속도로 소인수분해 문제를 해결할 수 있어, 양자 컴퓨팅에 대한 관심이 크게 증가했다. 이후 그로버 알고리즘 (Lov Grover, 1996) 등 다양한 양자 알고리즘이 발견되면서 양자 컴퓨팅 분야가 더욱 활발하게 진행중이다. 양자 컴퓨터는 양자 비트(큐빗, qubit)라는 기본 단위를 사용한다. 큐빗은 고전적인 비트와 달리 중첩이라는 성질을 가지고 있어, 한 번에 여러 상태를 표현할 수 있다. 양자 컴퓨터에서는 아다마르 게이트, CNOT 게이트, 파울리 게이트, 토플리 게이트 등이 있으며, 이러한 게이트를 적절하게 조합하여 양자 회로를 구성하여 정보를 처리한다. 양자 회로를 설계하고 최적화하려면 종종 최소한의 게이트 수와 최소한의 깊이가 필요하다. Toffoli 분해를 사용하면 복잡한 작업을 더 작은 범용 게이트로 분해할 수 있으므로 게이트 수, 깊이 및 오류율 측면에서 회로를 더 쉽게 최적화할 수 있다. 또한 Toffoli 분해는 오류에 강한 양자 회로를 구성할 수 있어 계산의 신뢰성을 보장할 수 있다. 양자 상태의 취약한 특성으로 인해 큐비트는 불완전한 작업 및 환경과의 상호작용으로 인해 발생하는 노이즈, 결맞음 및 오류에 매우 취약하다. Toffoli 게이트는 노이즈와 오류에 강한 내결함성 게이트 세트(Fault-tolerant gate set)를 사용하여 분해 될수있다. 양자 회로의 기본 요소인 Toffoli 게이트 개선은 널리 적용될 수 있기 때문에 특히 중요하다. 본 논문에서는 Toffoli 분해를 이용하여 양자 회로의 게이트 수와 깊이를 최적화하는 방법을 조사한다.

2. Toffoli 게이트

Toffoli 게이트는 양자 컴퓨팅에서 사용되는 유니버설 게이트 중 하나이다. 이 게이트는 세 개의 큐빗을 입력받아 조건부 (Controlled-Controlled) NOT 연산을 수행한다. 두 개의 컨트롤 큐빗과 한 개의 타깃 큐빗이 사용되며, 두 컨트롤 큐빗이 모두 1 인 상태일 때만 타깃 큐빗에 NOT 연산이 수행된다. 'CCNOT'으로

도 표현된다. Toffoli 게이트는 다른 기본 양자 게이트들로 분해될 수 있습니다. 일반적으로 사용되는 기본 양자 게이트들은 (그림 1)의 CNOT, H (아다마르), T, S, 및 T†가 사용된다.

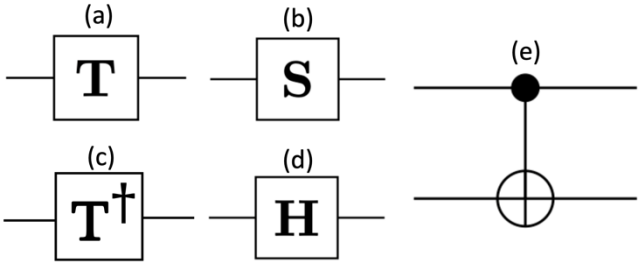
CNOT 게이트는 제어된 NOT 게이트로, 두 큐비트를 입력으로 받아서 제어 큐비트의 상태에 따라 대상 큐비트의 상태를 변환시키는 양자 게이트이다..

H (하다마드) 게이트: 주어진 큐비트의 상태를 동일한 확률로 중첩된 상태로 변환시키는 양자 게이트 이다.

T 게이트: 파이/4 게이트로도 알려져 있으며, 큐비트의 상태에 따라 특정 각도로 회전하는 양자 게이트이다. 이 게이트는 양자 오류 수정 및 양자 컴퓨팅의 고급 기능을 구현하는 데 사용된다.

S 게이트: $\pi/2$ 게이트로도 알려져 있으며, 큐비트의 상태에 따라 특정 각도로 회전하는 양자 게이트이다.

T† 게이트: T 게이트의 켤레 전치 게이트로, T 게이트의 역 연산을 수행하는 양자 게이트이다. 이를 사용하면 원래의 큐비트 상태로 돌아갈 수 있다.

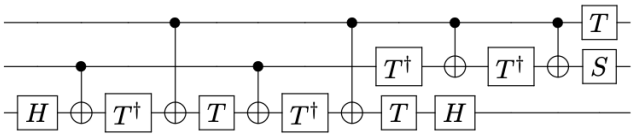


(그림 1) 양자 게이트 다이어그램. 각 선은 큐비트이며 왼쪽에서 입력하고 오른쪽에서 출력한다. 검은색 점이 있는 선는 제어 큐비트, 다른 선는 대상 큐비트 이다. (a) T 게이트 (b) S 게이트 (c) 역 T 게이트 (d) H 게이트 (e) CNOT 게이트

3. Toffoli 게이트 분해

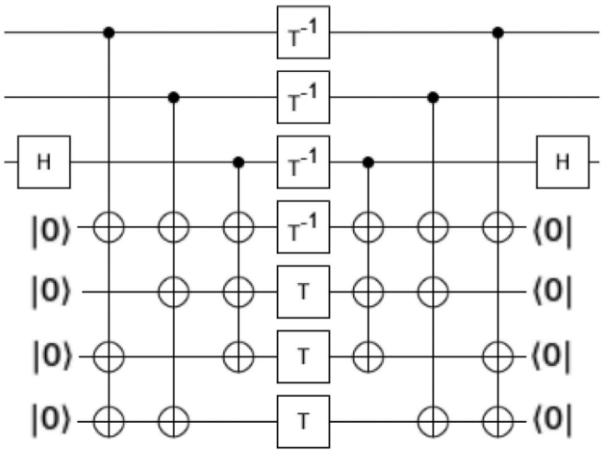
Toffoli 게이트 분해 방법은 회로의 길이, 큐 비트 수 T 게이트의 수, T 게이트의 깊이 등 다양한 요인을 고려하여 최적화 수 있다. 특히 T 게이트와 같은 기본 양자 게이트는 물리적으로 구현할 때 노이즈와 오류에 영향을 받을 수 있다. 예를 들어, T 게이트의 경우, 회전 각도가 조금씩 달라지거나, 간섭이나 분산 같은 양자 노이즈가 발생할 수 있다. 이런 물리적인 오류는 게이트 오류 확률과 관련이 있다. 따라서 T 게이트의 수, T 게이트의 깊이를 최적화하는 것이 중요하다. 본 장에서는 기존 연구에서 Toffoli 게이트 분해 방법에 대하여 설명한다.

Toffoli 게이트의 표준 분해[1]는 (그림 2)와 같다. 제어 비트 첫 번째 및 두 번째 큐비트이고 대상 비트는 세 번째 큐비이이다. 이 계산은 위상을 보존한다. T 게이트의 수(T-count) 7 이며 T 의 깊이(T-depth) 6 이다.



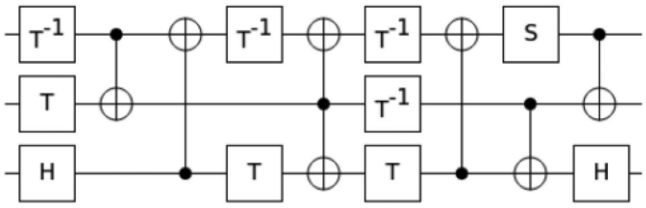
(그림 2) 표준 Toffoli 게이트 분해

[2]는 T 깊이의 최적화를 보인다. 표준 Toffoli 게이트와 동일한 7 의 T-count 를 사용하고 (그림 3)과 같이 4 개의 보조 큐비트를 추가하여 T -depth 1 로 병렬화 한다.



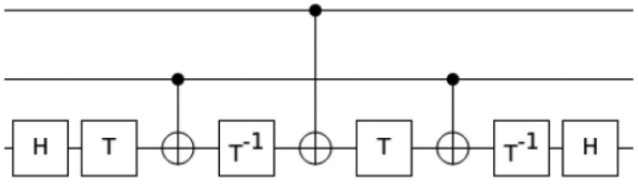
(그림 3) [2]의 T-depth 1 의 Toffoli 게이트 분해

[3]은 보조 큐빗트 없이 T-count 는 7 이고 T-depth 는 3 이다. 표준 Toffoli 게이트와 비교하여 회로의 깊이와 T-depth 를 절반으로 줄인다.



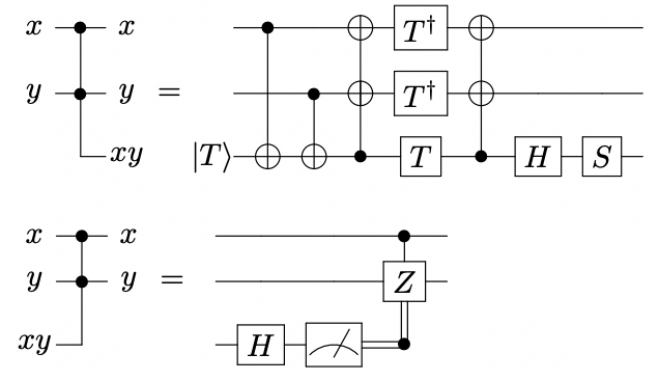
(그림 4) [3]의 보조 큐비트 0 의 T-depth 3 의 Toffoli 게이트 분해

[4]는 상대 위상 Toffoli 게이트로 Margolus 게이트 또는 단순화된 Toffoli 게이트로도 알려져 있다. 대칭 의 Toffoli 게이트를 RT3 또는 IRT3 로 대체하여 CNOT 게이트의 수를 줄일 수 있다.



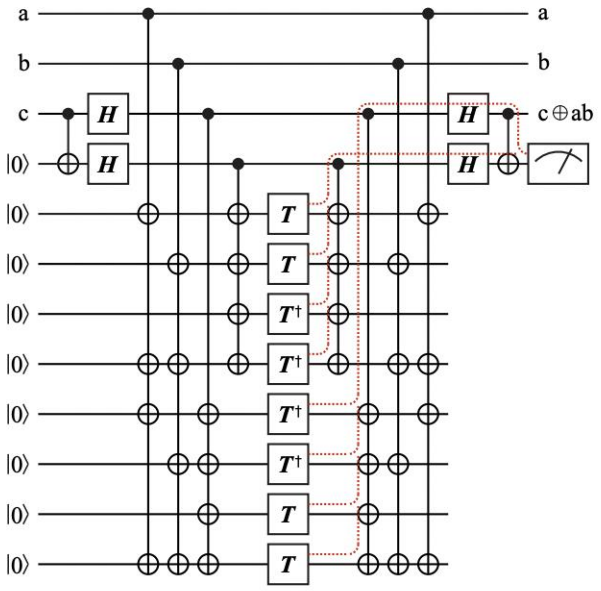
(그림 5) 3 CNOT(RT3)가 있는 상대 위상 Toffoli 게이트 RT3 의 역회로를 IRT3.

[5]는 2 개의 큐비트의 logical-AND 를 보조 큐비트에 저장하고, 나중에 보조 큐비트를 지우는 데 T 게이트 0 개를 사용(uncompute)하여 **T** 게이트 수 4 개로 개선한다. (그림 6)은 logical-AND 와 uncompute 이다.



(그림 6) [5]의 T-count 가 4 이고 측정 깊이가 1 의 logical-AND 회로(상단), uncomputation circuit(하단) T-count 가 0 이고 depth 가 1

[6] 은 (그림 7)의 오류감지 Toffoli 게이트를 제안한다. 8 개의 T 게이트 중 어느 하나에서 오류를 감지할 수 있다. 빨간색 점선은 단일 σz 오류가 판독 큐비트로 전파되는 방식을 나타낸다. 측정은 σz 기준이며 결과 |1⟩을 얻는 것은 오류가 감지되었음을 나타내므로 큐비트를 버려야 한다.



(그림 7) [6] 오류 감지 Toffoli 게이트

4. 결론

Toffoli 분해를 사용하여 양자 회로의 게이트 수와 깊이를 최적화할 수 있으며, 이는 게이트 수, 깊이 및 오류율을 줄여 계산의 신뢰성과 성능을 향상시키는 데 도움이 된다. 특히, T 게이트의 수와 깊이를 최적화하는 것이 물리적 구현 시 발생할 수 있는 노이즈와 오류에 대비하여 중요하다. 본 논문은 양자 컴퓨터와 양자 회로의 개념과 함께 Toffoli 게이트와 그 분해 방법에 대해 설명하였다. 추후 현재까지 제안된 Toffoli 분해 방법들을 개선하거나 새로운 방법을 개발하여 양자 회로의 게이트 수와 깊이를 더욱 최적화하거나 최적화된 양자 회로를 다양한 양자 알고리즘과 어플리케이션에 적용하여 그 성능과 실용성을 평가하고 개선하고자한다.

5. Acknowledgements

This work was partly supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (<Q|Crypton>, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity, 75%) and this work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 25%).

참고문헌

[1] Nielsen, Michael A., and Isaac Chuang. "Quantum computation and quantum information." (2002)

[2] Peter Selinger. “Quantum circuits of T-depth one”(2013)

[3] Amy, Matthew, et al. "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 32.6 (2013) [6] Nielsen, Michael A., and Isaac Chuang. "Quantum computation and quantum information." (2002)

[4] D. Maslov, “Advantages of using relative-phase Toffoli gates with an application to multiple control Toffoli optimization,” Physical Review A, vol. 93, no. 2, p. 022311, (2016)

[5] Gidney, Craig. "Halving the cost of quantum addition." Quantum 2 (2018)

[6] Jones, Cody. "Novel constructions for the fault-tolerant toffoli gate, (2013)