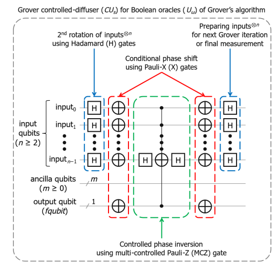
Nov 30, 2024 Version 2

Grover controlled-diffuser (CU_s) for quantum Boolean oracles of Grover's algorithm V.2



DOI
https://dx.doi.org/10.17504/protocols.io.e6nvw1wj9lmk/v2

Ali Al-Bayaty[1], Marek Perkowski[1]

[1]Portland State University

Ali Al-Bayaty: Department of Electrical and Computer Engineering
Marek Perkowski: Department of Electrical and Computer Engineering

Ali Al-Bayaty
Portland State University

DOI: https://dx.doi.org/10.17504/protocols.io.e6nvw1wj9lmk/v2

Protocol Citation: Ali Al-Bayaty, Marek Perkowski 2024. Grover controlled-diffuser (CUs) for quantum Boolean oracles of Grover's algorithm. **protocols.io https://dx.doi.org/10.17504/protocols.io.e6nvw1wj9lmk/v2**Version created by **Ali Al-Bayaty**

Manuscript citation:
A. Al-Bayaty and M. Perkowski, "A concept of controlling Grover diffusion operator: A new approach to solve arbitrary Boolean-based problems," *Scientific Reports*, vol. 14, pp. 1-16, 2024. https://doi.org/10.1038/s41598-024-74587-y

Protocol status: Working
We use this protocol and it's working

Created: November 30, 2024

Last Modified: November 30, 2024

Protocol Integer ID: 113362

Keywords: Grover's algorithm, Grover diffusion operator, controlled-diffusion operator, Boolean oracle, Phase oracle, logical structures, quantum boolean oracles of grover, quantum boolean oracle, new approach for grover, algorithm the grover, standard grover diffuser, quantum circuit of the cus operator, grover, quantum circuit, states of the output qubit, qubit, reflection of boolean decision, output qubit, cus operator, such oracle, boolean decision, solutions for arbitrary logical structure, boolean, correct solutions for all uω, arbitrary logical structure, different logical structure, correct solutions for some logical structure

Disclaimer

Abstract

The Grover controlled-diffuser (CU_S) for quantum Boolean oracles (U_ω) is introduced as a new approach for Grover's algorithm [1-3], to search for all solutions for arbitrary logical structures of such oracles, since the standard Grover diffuser (U_S) [1-3] is not able to find all correct solutions for some logical structures of U_ω.

This protocol constructs the quantum circuit of the CU_S operator [4] of Grover's algorithm, which relies on the states of the output qubit (as the reflection of Boolean decisions from a U_ω) without relying on the conventional phase kickback mechanism. The CU_S operator successfully searches for all correct solutions for all U_ω regardless of their different logical structures, such as POS, SOP, ESOP, CSP-SAT, XOR-SAT, just to name a few.

Troubleshooting

Preliminary Notes

1

Note

Grover’s algorithm [1-3] is the most well-known quantum search algorithm that:

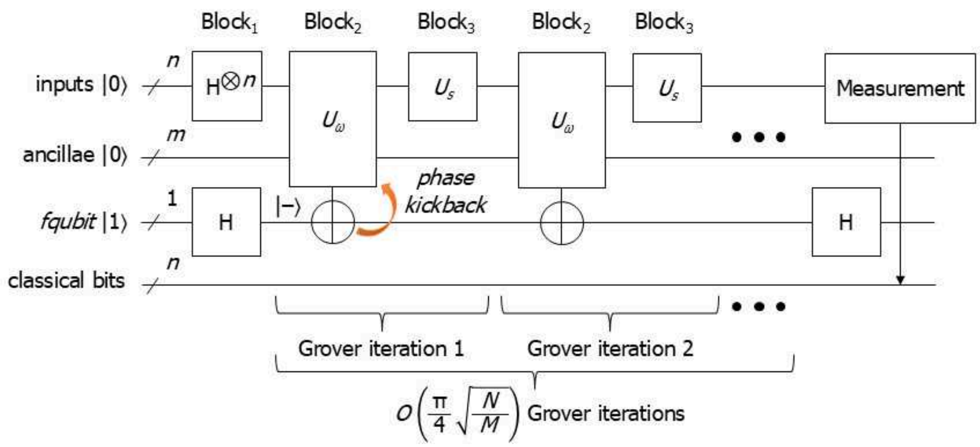
1. Finds solutions for both Boolean and Phase oracles in quadratic speedup.
2. Constructs other quantum algorithms, such as the quantum counting algorithm [5, 6].

2

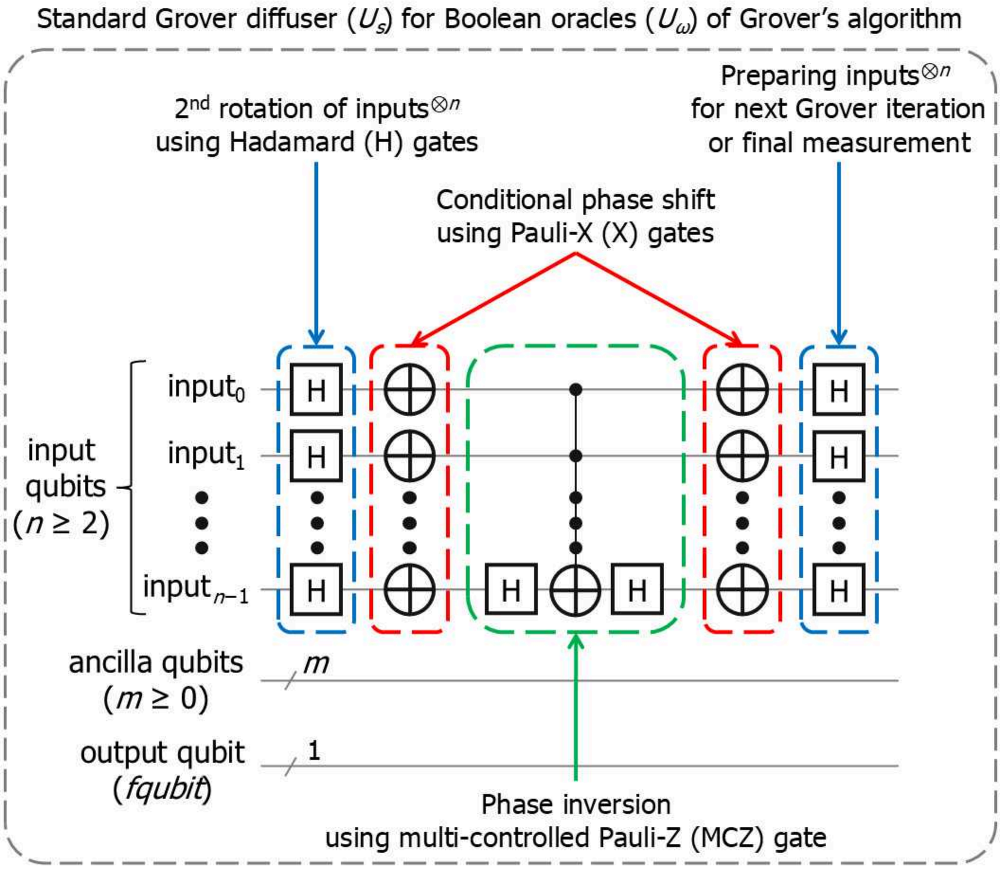
Note

In general, Grover's algorithm consists of three components (Blocks), as illustrated below:

1. $Block_1$ initializes n input qubits to a uniform distribution using Hadamard (H) gates, i.e., generates a complete quantum search space of $\{|0\rangle, |1\rangle\}^{\otimes n}$ for Grover's algorithm to search for solutions (marked elements).
2. $Block_2$ consists of a Boolean or Phase oracle (U_ω) [1-4] that inverts the phase of marked elements, as the "first rotation of solutions" over the complete quantum search space. Such phase inversion occurs due to the phase kickback for a Boolean oracle or the effect of quantum phase-based gates on n input qubits for a Phase oracle.
3. $Block_3$ consists of the Grover diffusion operator (U_s) that performs the "second rotation of solutions", conditional phase shift, and phase inversion, by rotating and amplifying the amplitudes of the marked elements from $Block_2$, as the final found solutions, as demonstrated below.



Schematic of Grover's algorithm to solve a Boolean oracle (U_ω) using the standard Grover diffusion operator (U_s), for a number of Grover iterations (loops). Please observe that both $Block_2$ and $Block_3$ are treated as one Grover iteration.



The quantum circuit of the standard Grover diffusion operator (U_s).

3

Note

1. In the quantum domain, an oracle (U_ω) is the conceptual expression of a problem in the classical domain.
2. A U_ω can be constructed as a Boolean oracle (using quantum Boolean-based gates) or a Phase oracle (using quantum phase-based gates).
3. Grover's algorithm solves a U_ω ($Block_2$) using the U_s operator ($Block_3$), which searches for one solution in the evaluation complexity of $O(\sqrt{N})$ or for a number of solutions in the evaluation complexity of $O\left(\frac{\pi}{4}\sqrt{\frac{N}{M}}\right)$ for $M < N/2$ as an algorithmic constraint, where:

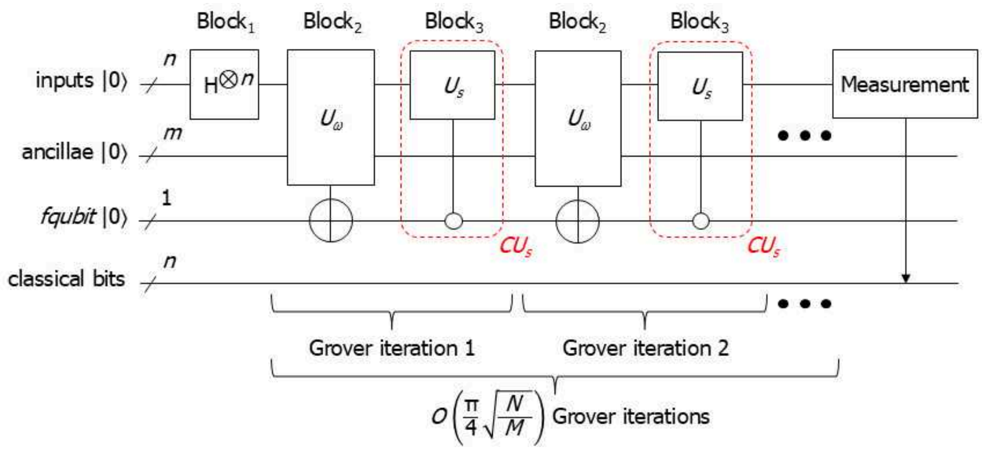
- $N = 2^n$.
- n is the total number of input qubits for a U_ω.
- M is the total number of solutions for a U_ω, i.e., the solutions of an expressed problem as a U_ω.

Please observe that the U_s operator is designed to rotate and amplify the amplitudes of N by their average (*inversion about average* [1-3]), and when more than half of quantum search space ($\{|0\rangle, |1\rangle\}^{\otimes n}$) is filled by M, Grover's algorithm makes random guesses of marked and unmarked elements as solutions!

4

Note

Our Grover controlled-diffuser (CU_s) is introduced as a new approach to overcome the algorithmic constraint of $M < N/2$, by controlling the operation of U_s using the output qubit (*fqubit*) of a Boolean oracle (U_ω), without relying on the conventional phase kickback mechanism, as shown below. Such that, the CU_s operator is designed for Boolean oracles only, since Phase oracles do not have any output qubit.

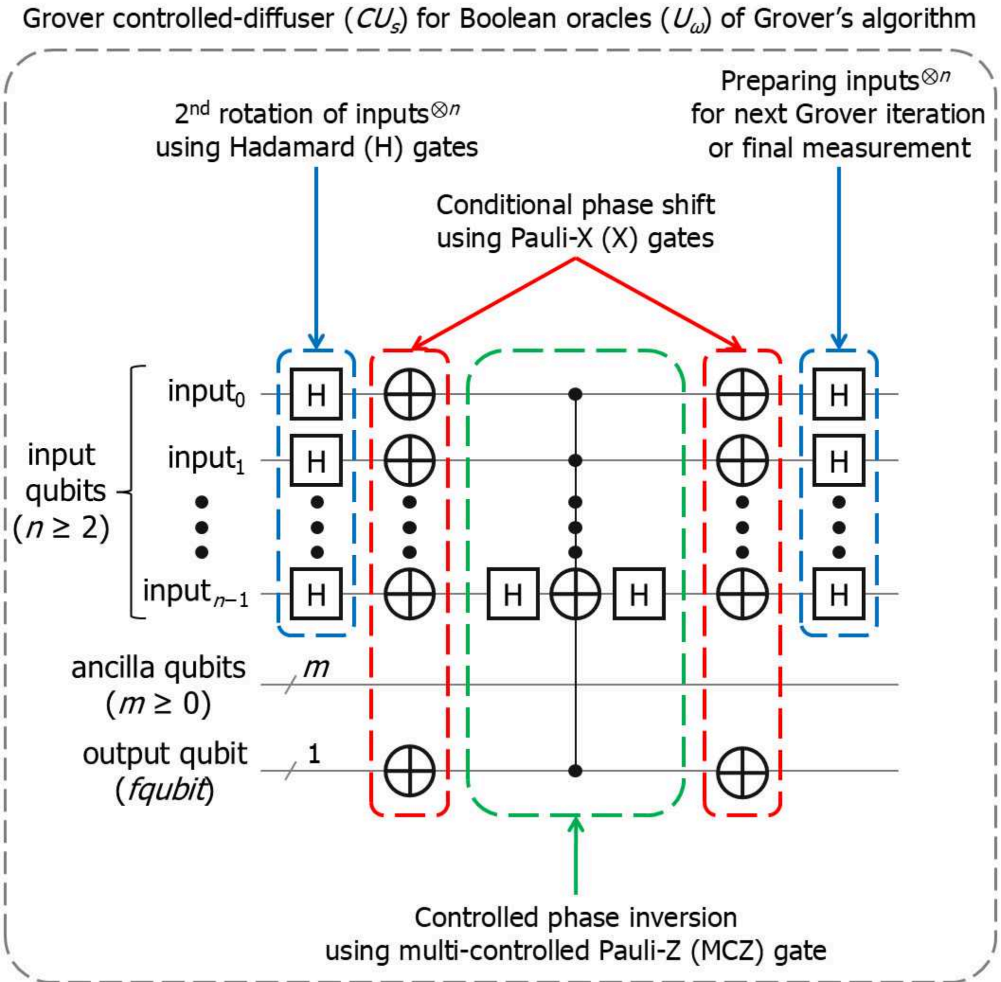


Schematic of Grover's algorithm to solve a Boolean oracle (U_ω) using our Grover controlled-diffusion operator (CU_s), for a number of Grover iterations (loops). Note that both $Block_2$ and $Block_3$ are treated as one Grover iteration.

Please observe that *fqubit* is the "functional qubit" as the one ancilla output qubit for a Boolean oracle (U_ω). When the state of *fqubit* = $|1\rangle$, a solution is found by a U_ω, and there is no need to activate the quantum operation of CU_s, i.e., a solution is passed through and $CU_s \equiv I$. Otherwise, when the state of *fqubit* = $|0\rangle$, a non-solution is found by a U_ω, and the quantum operation of CU_s is activated to search for any remaining solutions (residues) [4], i.e., $CU_s \equiv U_s$.

Hence, the states of *fqubit* instruct the quantum operations of CU_s to search for all correct solutions, as stated in the following algebraic formula and demonstrated in the figure below.

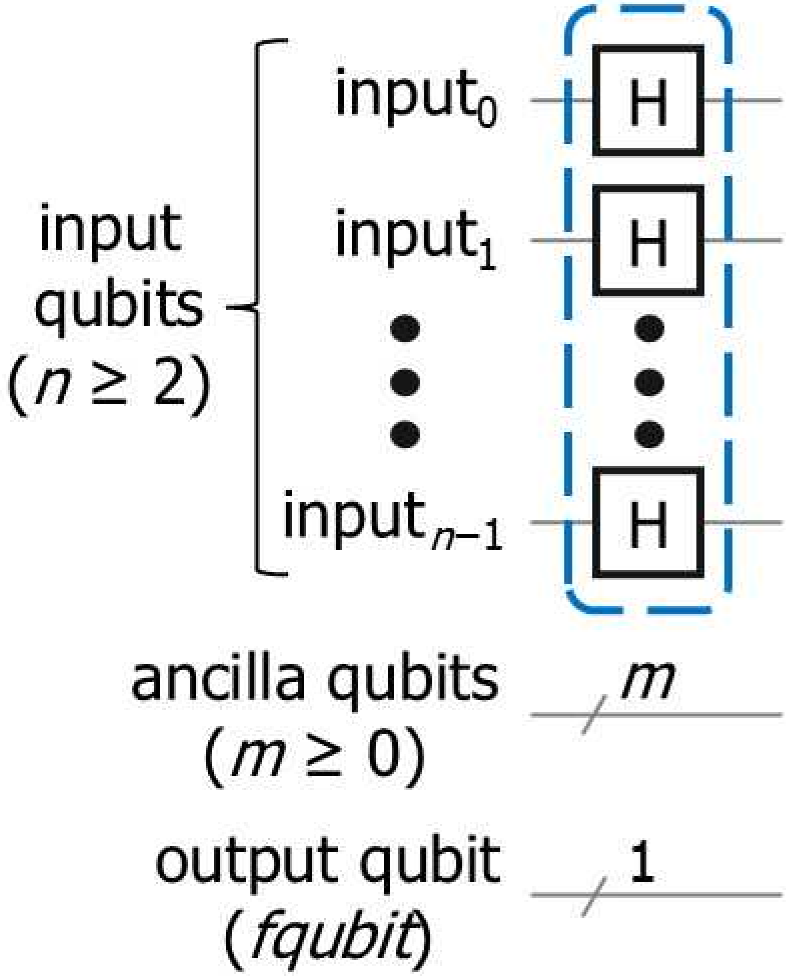
$$CU_s = U_{s\ (\ fqubit\ =\ |0\rangle\ )} + I_{(\ fqubit\ =\ |1\rangle\ )}$$



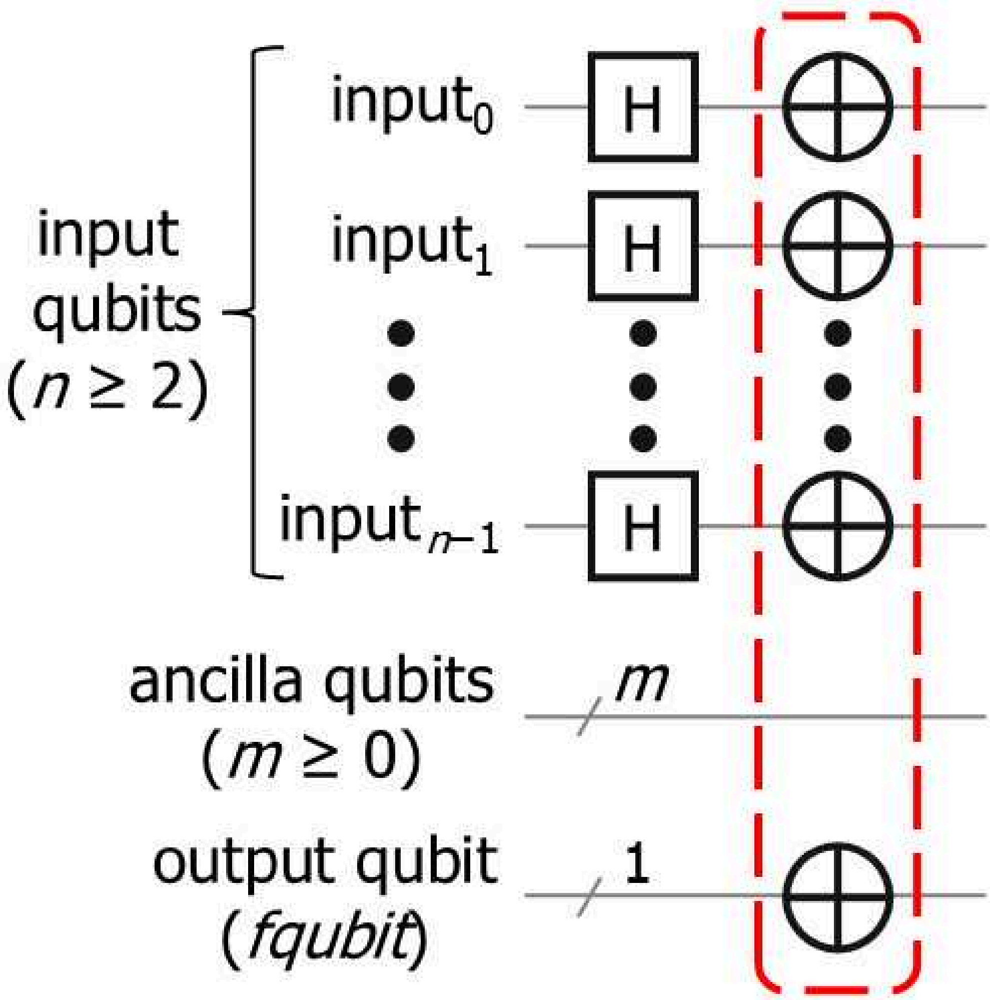
The quantum circuit of our Grover controlled-diffusion operator (CU_s).

The CU_s Protocol (for Boolean oracles of Grover's algorithm)

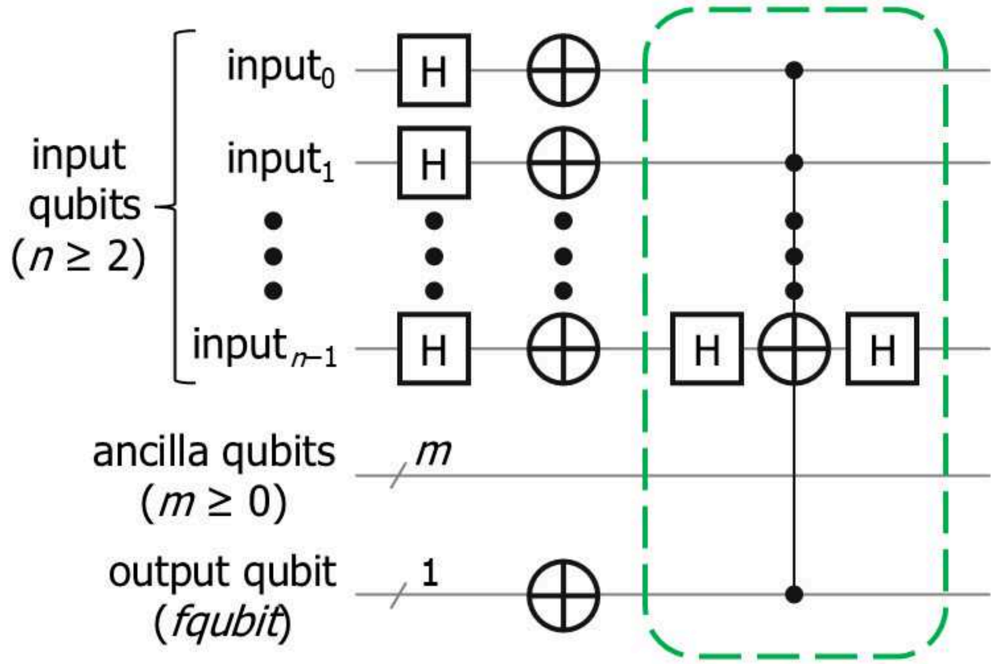
5 Rotate all n input qubits of a Boolean oracle (U_ω), as the "second rotation of solutions", using n Hadamard (H) gates, where $n \geq 2$. Note that all m ancilla qubits including the *fqubit* do not require such a rotation, where $m \geq 0$.



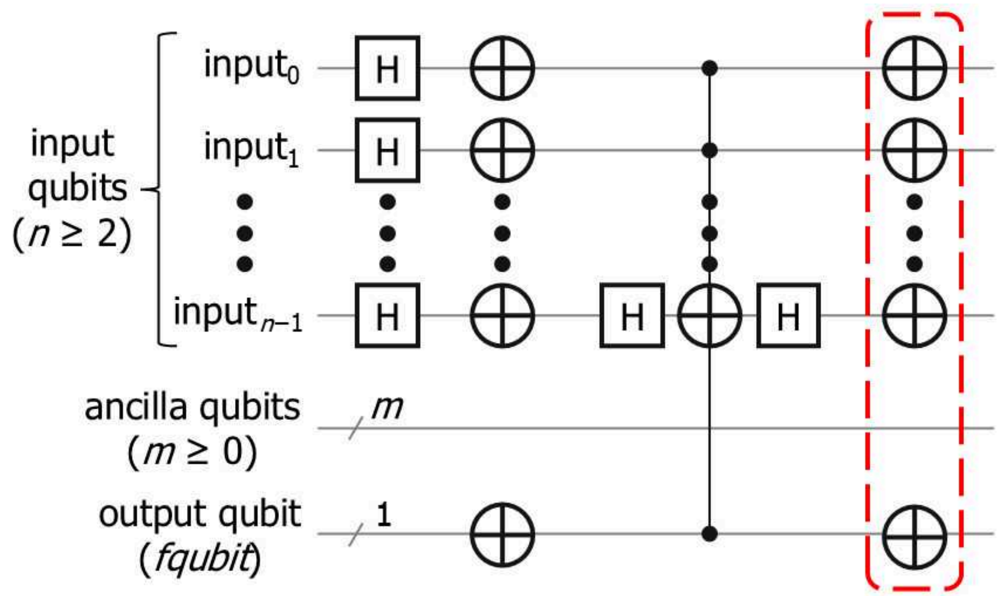
6 Conditionally shift the phases of all *n* input qubits and *fqubit*, using *n*+1 Pauli-X (X) gates. Note that all *m* ancilla qubits are not included for such a conditional phase shift.



7 Invert the phases of all *n* input qubits depending on the inverted states of *fqubit*, using one multi-controlled Pauli-Z (MCZ) gate of *n*+1 qubits. Note that all *m* ancilla qubits are not included for such a controlled phase inversion.

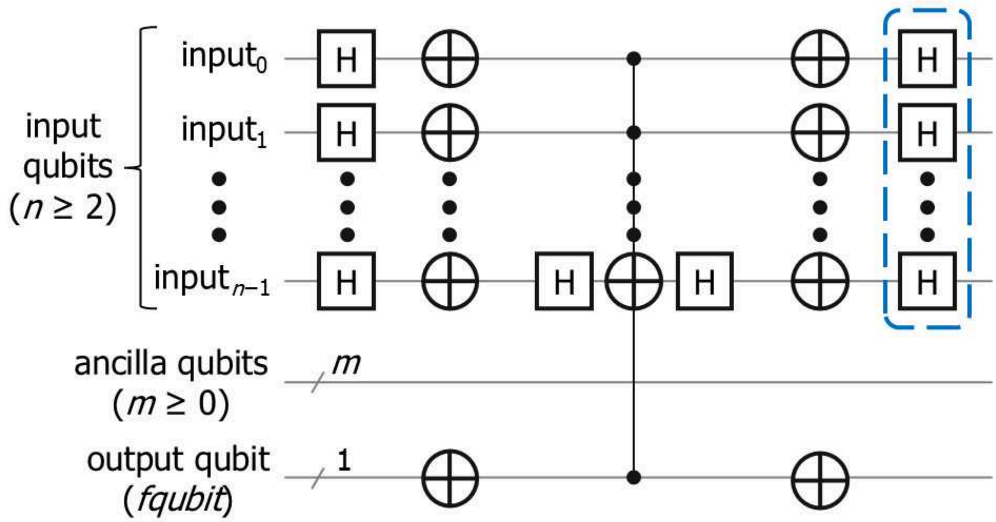


8 Uncompute (mirror) the aforementioned step of the conditional phase shift, using n+1 X gates.



9 Finally, uncompute (mirror) the aforementioned step of the "second rotation of solutions", using n H gates, to prepare all n inputs qubits for the next Grover iteration (if

required) or the final measurement.



The Quantum Cost of CU_s Operator

10 For a Boolean oracle (U_ω) of Grover's algorithm consisting of n input qubits, m ancilla qubits, and one *fqubit,* the quantum cost of CU_s operator that defines the total utilized number of standard quantum gates is stated as follows, where $n > 2$ and $m > 0$.

$$Quantum\ Cost_{\ CU_S} = (2n+2)\ H\ +\ (2n+2)\ X\ +\ MCX_{n+1}$$

Note that MCX_{n+1} is a multi-controlled Pauli-X gate of n+1 qubits, which is the (n+1)-bit Toffoli gate of n controls and one target.

Protocol references

[1] L.K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. of the 28th Ann. ACM Symp. on Theory of Computing*, 1996, pp. 212-219.

[2] L.K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Physical Review Letters*, vol. 79, no. 2, p. 325, 1997.

[3] L.K. Grover, "A framework for fast quantum mechanical algorithms," in *Proc. of the 30th Ann. ACM Symp. on Theory of Computing*, 1998, pp. 53-62.

[4] A. Al-Bayaty and M. Perkowski, "A concept of controlling Grover diffusion operator: A new approach to solve arbitrary Boolean-based problems," *Scientific Reports*, vol. 14, pp. 1-16, 2024.

[5] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik: Progress of Physics*, vol. 46, pp. 493-505, 1998.

[6] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *Contemp Math*, vol. 305, pp. 53-74, 2002.