Examples on quantum search algorithm with optimized depth

Kun Zhang and Vladimir E. Korepin

December 11, 2019

1 Notations

The size of input is $N = 2^n$. Here n is number of qubits to represent N states. Grover's algorithm finds one marked state in N states (assuming only one marked state) [1]. The marked state (target state) is denoted as $|t\rangle$. The initial state in Grover's algorithm is the superposition of all N basis. The initialization of input can be realized by single-qubit Hadamard gate H:

$$|s_n\rangle = H^{\otimes n}|0\rangle^{\otimes n} \tag{1}$$

Grover's algorithm is realized by repetition of Grover operator on initial state $|s_n\rangle$. Grover operator is composed by two parts: oracle U_t and diffusion operator I_n:

$$U_t = \mathbb{1}_{2^n} - 2|t\rangle\langle t|; \tag{2}$$

$$I_n = 2|s_n\rangle\langle s_n| - \mathbb{1}_{2^n}. \tag{3}$$

Here $\mathbb{1}$ is identity operator. Oracle U_t flips the sign of target state. Diffusion operator I_n reflects the amplitude around average. Combined with U_t and I_n, we have Grover operator:

$$G_n = I_n U_t \tag{4}$$

Repeatedly acting the Grover operator G_n on initial state $|s_n\rangle$, the success probability finding the target state will grow. In our optimized depth search algorithm [2], we define another diffusion operator called local diffusion operator $I_{n,m}$ $(m < n)$:

$$I_{n,m} = \mathbb{1}_{2^{n-m}} \otimes (2|s_m\rangle\langle s_m| - \mathbb{1}_{2^m}) \tag{5}$$

Local diffusion operator reflects the amplitude around subspace average. See next section for quantum circuits diagrams of $I_{n,m}$. Combined with U_t and $I_{n,m}$, we have Grover operator (called local Grover operator):

$$G_{n,m} = I_{n,m} U_t \tag{6}$$

Without confusion, we simplify the notation as: $I_m = I_{n,m}$ and $G_m = G_{n,m}$.

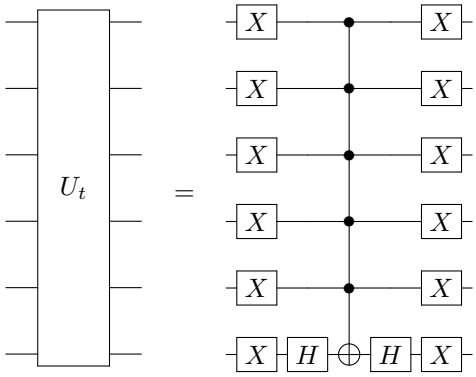
2 Quantum circuit diagrams

In the following, we consider examples on $n = 6$ search algorithms ($N = 2^6 = 64$).

2.1 Oracle

Different problems have different oracles. For demonstration, we can consider the simplest oracle. As mentioned in [3], oracle is single-qubit gate equivalent with n-qubit Toffoli gate. Suppose $|t\rangle = |000000\rangle$ $(n = 6)$. We have

the oracle:



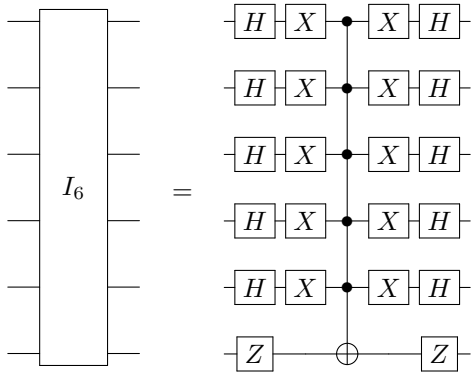
(7)

Here X is Pauli gate. And we use conventional quantum circuit diagram for 6-qubit Toffoli gate, denoted as $\Lambda_5(X)$. The 5 subscript suggests that it has five target qubits. The 6-qubit Toffoli gate $\Lambda_5(X)$ is highly non-trivial. In real quantum computers, we need to further decompose it into single- and two-qubit gates. According to [4], $\Lambda_5(X)$ gate can be realized by depth 61 circuits: $\mathrm{d}(\Lambda_5(X))$ (if the quantum computer can perform any single-qubit gates and any two-qubit controlled gates.). We use notation $\mathrm{d}(U)$ to represent the depth of unitary transformation U. In real quantum computers, the depth $\mathrm{d}(\Lambda_5(X))$ may be much larger since not all qubits are connected. Nevertheless, we use

$$\mathrm{d}(U_t) = \mathrm{d}(\Lambda_5(X)) + 2 = 63. \tag{8}$$

2.2 Diffusion operators

We have two kinds of diffusion operator. One is global diffusion operator I_n (3). The other one is local diffusion operator I_m (5). Diffusion operators are independent on oracle. Global diffusion operator I_n is also single-qubit gate equivalent with 6-qubit Toffoli gate $\Lambda_5(X)$:



(9)

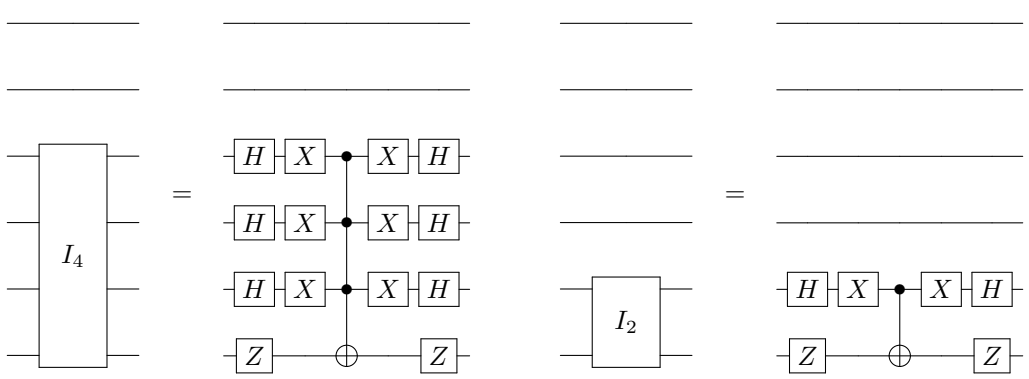
Then we have the depth

$$\mathrm{d}(I_6) = \mathrm{d}(\Lambda_5(X)) + 2 = 63. \tag{10}$$

In experiments, we can see that diffusion operator is realized by comparable depth to oracle. Although Grover's algorithm is optimal in number of oracle, depth can be optimized.

Note that local diffusion operator $I_{6,5}$ (short as I_5) is a 5-qubit gates instead of 6. And I_4 is a 4-qubit gate

and so forth. We give examples on I_4 and I_2:



(11)

The subspace where I_4 and I_2 are acting on can be chosen arbitrarily, such as qubits with high connectivity. According to [4], we have the depth of 4-qubit Toffoli gate: $\mathrm{d}(\Lambda_3(X)) = 13$, and 2-qubit CNOT gate: $\mathrm{d}(\Lambda_1(X)) = 1$. Therefore, we have

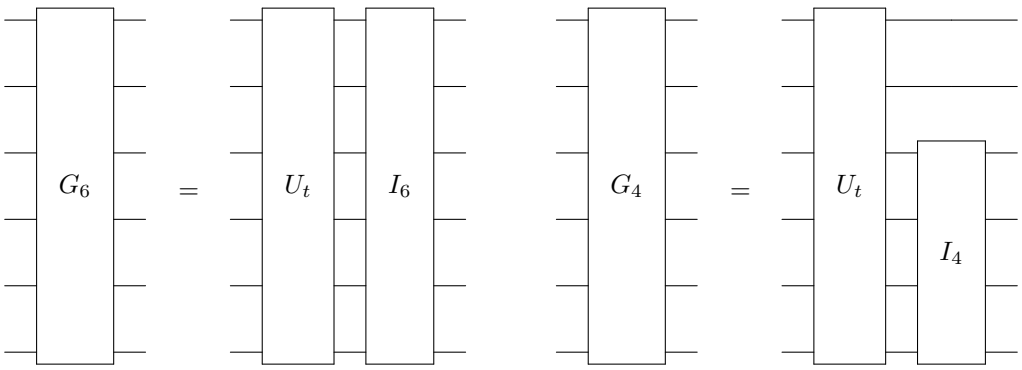
$$\mathrm{d}(I_4) = \mathrm{d}(\Lambda_3(X)) + 2 = 15, \qquad \mathrm{d}(I_2) = \mathrm{d}(\Lambda_1(X)) + 2 = 3. \tag{12}$$

Obviously, for any quantum computers, we will have

$$\mathrm{d}(I_n) < \mathrm{d}(I_m), \qquad m < n. \tag{13}$$

2.3 Grover operators

Global Grover operator G_n (4) is operation combined with oracle and global diffusion operator I_n (3). Local Grover operator G_m (6) is operation combined with oracle and local diffusion operator I_m (5). As examples on $n = 6$, we have



(14)

The depth of Grover operators can be simply counted:

$$\mathrm{d}(G_6) = \mathrm{d}(U_t) + \mathrm{d}(I_6) = 126, \qquad \mathrm{d}(G_4) = \mathrm{d}(U_t) + \mathrm{d}(I_4) = 78. \tag{15}$$

Obviously, for any quantum computers, we will have

$$\mathrm{d}(G_n) < \mathrm{d}(G_m), \qquad m < n. \tag{16}$$

3 Search algorithm with depth optimizations

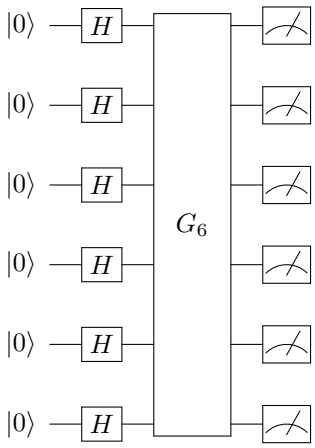
Near-term quantum computers are subjected to limited coherence time. We have to design low depth algorithm, or divide long circuit into shorter pieces. In $n = 6$ search algorithm, the probability finding the target state reaches maximal after 6 iterations of G_6:

$$|\langle t|G_6^6|s_6\rangle|^2 \approx 99.66\% \tag{17}$$

However, the operation G_6^6 is too long in practice. Besides, it is not optimal neither in depth nor success probability. We will show a better way for 6 iterations. For practice, we will concentrate on the circuit with one or two Grover iterations.

3.1 One oracle

- Grover's algorithm. The one iteration Grover's algorithm gives:



(18)

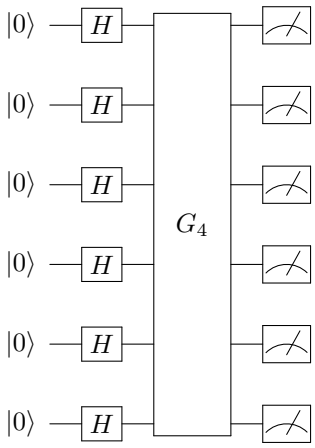
The whole circuit has depth $\mathrm{d}(G_6) = 126$ (we can incorporate the initial Hadamard gates into G_6.). The success probability finding the target state is

$$|\langle t|G_6|s_6\rangle|^2 \approx 13.48\%. \tag{19}$$

The result is better than classical algorithm. Optimal classical search has success probability 3.15%: single query followed by a random guess if the query fails ($1/64 + 1/63 \approx 3.15\%$). To evaluate the efficiency, we can calculate the *expected depth*:

$$\frac{\mathrm{d}(G_6)}{|\langle t|G_6|s_6\rangle|^2} \approx 935. \tag{20}$$

- Optimized algorithm. In order to lower the depth, we can apply one iteration with local diffusion operator: G_4 operator for example. The one iteration local Grover operator gives:



(21)

Note that G_4 is still a 6-qubit gate, although I_4 is a 4-qubit gate. The whole circuit has depth $\mathrm{d}(G_4) = 78$. The depth is lower compared with G_6. The success probability finding the target state is

$$|\langle t|G_4|s_6\rangle|^2 \approx 11.81\%. \tag{22}$$

The success probability decreases a little bit, but still outperforms the classical case. The expected depth is:

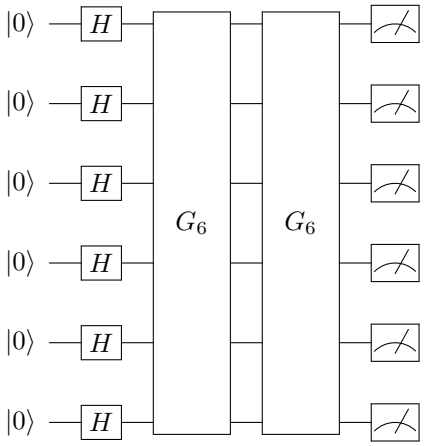
$$\frac{\mathrm{d}(G_4)}{|\langle t|G_4|s_6\rangle|^2} \approx 660. \tag{23}$$

The circuit is 38% shorter than one G_6 iteration. The expected depth is 29% lower! Local diffusion operator may decrease the success probability, but it saves depth.

3.2 Two oracles

We can apply same strategy for two iterations search algorithm: design circuit with local diffusion operators and find the optimal one with least expected depth. There is something new for local diffusion operators. We can apply *divided and conquer* strategy for search algorithm.

- Grover's algorithm. Two iterations Grover's algorithm gives:



(24)

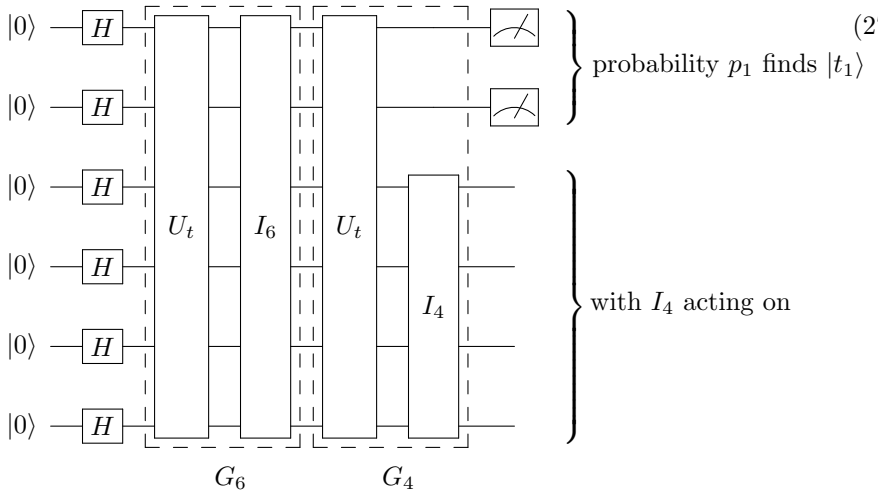
The whole circuit has depth $\mathrm{d}(G_6^2) = 252$. The success probability finding the target state is

$$|\langle t|G_6^2|s_6\rangle|^2 \approx 34.39\%. \tag{25}$$

And the expected depth is

$$\frac{\mathrm{d}(G_6^2)}{|\langle t|G_6^2|s_6\rangle|^2} \approx 733. \tag{26}$$

- Divided and conquer. We suppose that the target state is $|t\rangle = |000000\rangle$. We can divide the target state into two parts: $|t_1\rangle = |00\rangle$ and $|t_2\rangle = |0000\rangle$ ($|t\rangle = |t_1\rangle \otimes |t_2\rangle$). Accordingly, we can design the search algorithm which has two steps: the first step finds $|t_1\rangle$ and the second step finds $|t_2\rangle$. And each step, we only have two Grover operators (local or global Grover operators).
  - The first step has the circuit (G_4G_6 sequence):



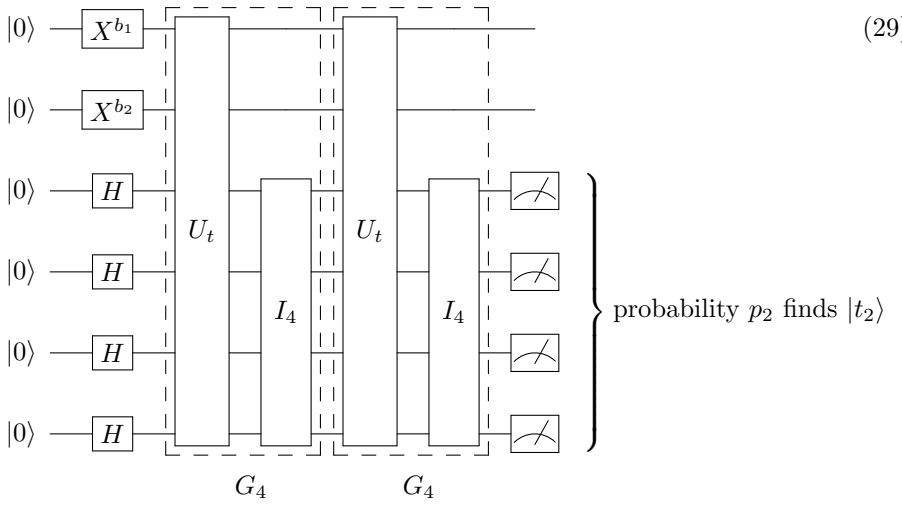
(27)

We only measure the qubit which does *not* have I_4 performed. The probability finding $|t_1\rangle$ is p_1:

$$p_1 \approx 56.04\% \tag{28}$$

The whole circuit has depth $\mathrm{d}(G_4G_6) = 204$. We can suppose the measurement results are $|b_1\rangle$ and $|b_2\rangle$ ($b_1, b_2 \in \{0, 1\}$). Note that we can not verify the partial bits b_1 and b_2. Since $p_1 > 1/2$, the majority vote can be applied.

– The second step has the circuit (G_4G_4 sequence):



(29)

The initial state is renormalized database. For example, the first step we find $|01\rangle$, then we prepare the input $|01\rangle \otimes H^{\otimes 4}|0\rangle^{\otimes 4}$. The probability finding $|t_2\rangle$ is p_2:

$$p_2 \approx 90.84\%. \tag{30}$$

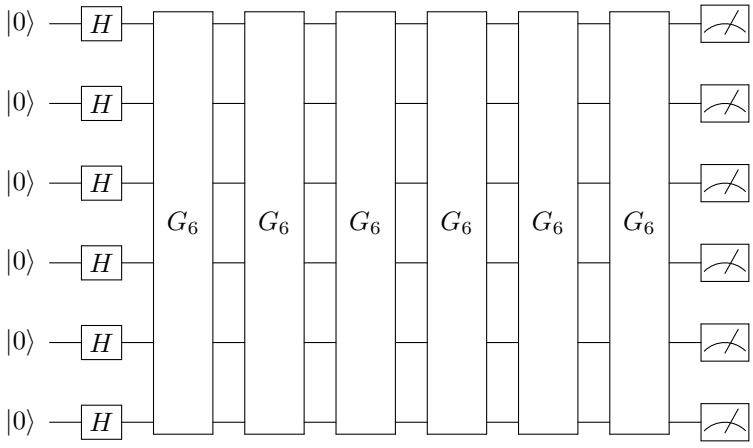
The whole circuit has depth $\mathrm{d}(G_4^2) = 156$. We have the expected depth

$$\frac{\mathrm{d}(G_6G_4) + \mathrm{d}(G_4^2)}{p_1 p_2} \approx 707. \tag{31}$$

The expected depth is still lower than two iteration Grover's algorithm. Besides, the divided and conquer method is subjected to half less errors from measurements.

3.3 Six oracles

- Grover's algorithm. In $n = 6$ search algorithm, six global Grover iterations gives the maximal success probability:



(32)

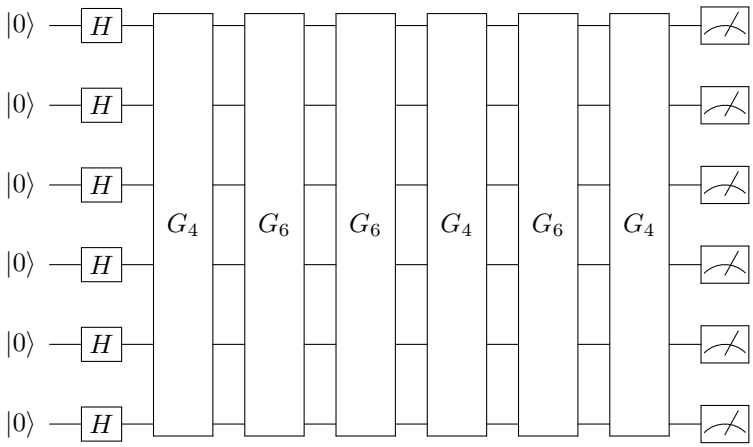
The success probability is

$$|\langle t|G_6^6|s_6\rangle|^2 \approx 99.66\%. \tag{33}$$

The whole circuit has depth $\mathrm{d}(G_6^6) = 756$.

- Optimized algorithm. It is very surprising that we can replace global diffusion operators by local diffusion

operators without decreasing the probability! We have the circuit:



(34)

We have replaced three global diffusion operator I_6 by three local diffusion operators I_4. Note that G_6 and G_4 does not commute. Such sequence does not unique. The success probability is

$$|\langle t|G_4G_6G_4G_6^2G_4|s_6\rangle|^2 \approx 99.86\%. \tag{35}$$

The whole circuit has depth $\mathrm{d}(G_4G_6G_4G_6^2G_4) = 612$. The whole circuit has decreased depths 19.05%. And the success probability does not decrease. It suggests that the maximal probability Grover's algorithm is neither optimal in depth nor in probability.

4 Conclusions

We have shown that quantum search algorithms can be optimized in depth by local diffusion operators. And the local diffusion operators can be applied to:

- decrease the expected depth of the circuit;
- divided and conquer strategy;
- decrease the depth for maximal success probability search algorithms.

References

[1] Lov K Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 79(2):325, 1997.

[2] Kun Zhang and Vladimir E Korepin. Low depth quantum search algorithm. *arXiv preprint arXiv:1908.04171*, 2019.

[3] Caroline Figgatt, Dmitri Maslov, KA Landsman, Norbert M Linke, S Debnath, and C Monroe. Complete 3-qubit grover search on a programmable quantum computer. *Nature communications*, 8(1):1918, 2017.

[4] Adriano Barenco, Charles H Bennett, Richard Cleve, David P DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical review A*, 52(5):3457, 1995.