Supplementary Material for the Paper 'Grover's algorithm on two-way quantum computer' by Grzegorz Czelusta

Bartosz Tomsia *

July 2024

Appendix: Extended Grover's Oracle

In this appendix, we detail the creation of an extended Grover's Oracle for solving quantum search problems without prior knowledge of the solutions. A concise summary is provided at the end of this appendix.

Let $f : \{0,1\}^n \to \{0,1\}$ be a boolean function, and $B \subset S \subseteq \{0,1\}^n$ the set of solutions in search space S such that:

$$f(x) = \begin{cases} 1 & \text{if } x \in B \\ 0 & \text{if } x \notin B \end{cases} \tag{1}$$

The search space S includes all database elements to search, labeled by binary integers.

Define $|B\rangle = \sum_{x \in B} |x\rangle$ as the sum of Z-basis states where $f(x) = 1$ and let $|S \setminus B\rangle$ be the sum of Z-basis states where $f(x) = 0$, so that $|S\rangle = |B\rangle + |S \setminus B\rangle$.

The state $|S\rangle$ is initially created in the U_f register. Without loss of generality, let's assume the initial state $|S\rangle = H^{\otimes n}|0\rangle = |+\rangle^{\otimes n}$ (encoding all possible labels in the database).

Grover's Oracle can be formulated using the function f as follows:

$$U_f = \mathbb{1}^{\otimes n} - 2\sum_{x \in B} |x\rangle\langle x| \tag{2}$$

$$= \sum_{x \in B} |x\rangle\langle x| - \sum_{x \in S \setminus B} |x\rangle\langle x| \tag{3}$$

$$= \sum_{x \in S} (-1)^{f(x)} |x\rangle\langle x| \tag{4}$$

The oracle U_f is extended by adding an ancillary qubit a and replacing each Z-gate with a controlled-X gate. The ancillary qubit a serves as the target, and the controls are in the U_f register, equipped with an additional control C_Z in place of the Z gate.

$$\begin{aligned} Z_{U_f} &\to C_Z X_{U_f,a} \\ CZ_{U_f} &\to CC_Z X_{U_f,a} \\ CCZ_{U_f} &\to CCC_Z X_{U_f,a} \\ &\dots \\ C^{n-1}Z_{U_f} &\to C^{n-1}C_Z X_{U_f,a} \end{aligned} \tag{5}$$

This is equivalent to:

$$\begin{aligned} U_\omega &= \sum_{i=0}^{2^n-1} (-1)^{f(i)} |i\rangle_n \langle i|_n \otimes (-X)^{f(i)} \\ &= \sum_{i=0}^{2^n-1} |i\rangle_n \langle i|_n \otimes X^{f(i)}. \end{aligned} \tag{6}$$

From the matrix representation perspective of U_f, the process (6) is as follows:

1. Double the size of Grover's Oracle matrix by the tensor product with identity matrix:

$$U_f \otimes \mathbb{1} = \sum_{x \in S} (-1)^{f(x)} |x\rangle\langle x| \otimes \mathbb{1} = \tag{7}$$

$$= \begin{bmatrix} (-\mathbb{1})^{f(0)} & 0 & \cdots & 0 & 0 \\ 0 & (-\mathbb{1})^{f(1)} & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & (-\mathbb{1})^{f(2^n-2)} & 0 \\ 0 & 0 & \cdots & 0 & (-\mathbb{1})^{f(2^n-1)} \end{bmatrix}_{2^{2n} \times 2^{2n}}$$

2. Replace $-\mathbb{1}$ with X gates on the diagonal of the new matrix, leaving $\mathbb{1}$ blocks unchanged:

$$\to \begin{bmatrix} X^{f(0)} & 0 & \cdots & 0 & 0 \\ 0 & X^{f(1)} & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & X^{f(2^n-2)} & 0 \\ 0 & 0 & \cdots & 0 & X^{f(2^n-1)} \end{bmatrix} \tag{8}$$

Note: The $-X$ gate is applied only to states $|x\rangle$ where $f(x) = 1$; otherwise, the identity $\mathbb{1}$ (which is equivalent to $(-X)^0$) is applied. Explicitly performing steps (7-8) would require identifying the

*email:bartosz.tomsia@gmail.com

diagonal positions where $-\mathbb{1}$ is applied, thereby revealing the solution states. Instead, we use information about the Z-gates to be replaced in U_f from the circuit using n qubits.

Next, we apply the extended Oracle U_ω to the initial state $|S\rangle$ in the U_f register, where $|S\rangle = |+\rangle^{\otimes n}$, and to the target state $|0\rangle_a$, initialized on the ancillary qubit a:

$$\begin{aligned} &U_\omega(|S\rangle \otimes |0\rangle_a) = \\ &= \left(\sum_{j=0}^{2^n-1} |j\rangle_n \langle j|_n \frac{1}{2^{\frac{n}{2}}} \sum_{i=0}^{2^n-1} |i\rangle_n\right) \otimes X^{f(j)} \\ &= \frac{1}{2^{\frac{n}{2}}} \left(\sum_{j=0}^{2^n-1} \sum_{i=0}^{2^n-1} |j\rangle_n \langle j|i\rangle_n\right) \otimes X^{f(j)} \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{i=0}^{2^n-1} |i\rangle_n \otimes X^{f(j)} = |+\rangle^{\otimes n} \otimes X^{f(S)} \\ &= |S\rangle \otimes X^{f(S)}. \end{aligned} \tag{9}$$

Consider that:

$$\begin{aligned} X^{f(x)} &= (|1\rangle\langle 0| + |0\rangle\langle 1|)^{f(x)} \\ &= |f(x)\rangle\langle 0| + |1 - f(x)\rangle\langle 1|, x \in S \end{aligned} \tag{10}$$

From equations (9) and (10), we express the state in the ancillary register as a superposition depending on the values of the function f:

$$\begin{aligned} U_\omega(|S\rangle \otimes |0\rangle_a) &= |S\rangle \otimes X^{f(S)} \\ &= |S\rangle \otimes (|f(S)\rangle\langle 0| + |1 - f(S)\rangle\langle 1|). \end{aligned}$$

Knowing that $f(S) = 1$ if and only if $S = B$, we finally postselect the state where the ancillary qubit is in state 1, which is achieved by means of the projection operator $|1\rangle\langle 1|_a$:

$$\begin{aligned} &(|1\rangle\langle 1|)_a U_\omega(H^{\otimes n}|0\rangle \otimes |0\rangle_a) = \\ &= |S\rangle \otimes (|1\rangle\langle 1|)_a (|f(S)\rangle\langle 0| + |1 - f(S)\rangle\langle 1|)_a \\ &= (|B\rangle + |S \setminus B\rangle) \otimes |1\rangle\langle 1|f(S)\rangle\langle 0| + |1\rangle\langle 1|1 - f(S)\rangle\langle 1|) \\ &= \langle 1|f(S)\rangle|B\rangle \otimes |1\rangle\langle 0| + \langle 1|1 - f(S)\rangle|S \setminus B\rangle \otimes |1\rangle\langle 1| \\ &= |B\rangle \otimes |1\rangle\langle 0|. \end{aligned}$$

In brief, the quantum search algorithm with postselection is the following:

Algorithm 1 Quantum Search Algorithm with Postselection

Input: Grover's Oracle U_f circuit, encoding solutions $x \in B \subset S$, where $f(x) = 1$.

Steps:

1. Prepare the initial state $|S\rangle$ in the U_f register as a superposition of Z-basis states, each representing a potential solution.
2. Add an ancillary qubit a: $U_f \otimes \mathbb{1}_a$
3. Create U_ω by replacing each $Z, CZ, \ldots, C^{n-1}Z$ gate in U_f with corresponding $C_Z X_{U_f,a}, CC_Z X_{U_f,a}, \ldots, C^{n-1}C_Z X_{U_f,a}$ gates, using the ancillary qubit as target.
4. Postselect the ancillary qubit to state $|1\rangle$: $(|1\rangle\langle 1|)_a U_\omega(|S\rangle|0\rangle \otimes |0\rangle_a) = |B\rangle_{U_f} \otimes (|1\rangle\langle 0|)_a$.
5. Measure the U_f register.

Output: The most probable states $|x\rangle$ in the U_f register represent solutions of $f(x) = 1$.