A Quantum Algorithm for Finding Common Matches between Databases with Reliable Behavior

Khaled El-Wazan

Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Egypt

Problem Statement

Definition

Consider having a set $\mathcal{Z}$ of $\kappa \geq 2$ lists, $\mathcal{Z} = \{L_0, \cdots, L_{\kappa-1}\}$. Each list $L_j \in \mathcal{Z}$ is of $N = 2^n$ unstructured entries, which has an oracle U_j that is being used to access those entries in L_j. Each entry $i \in L_j = \{0, 1, \cdots, N-1\}$ in the list L_j is mapped to either 0 or 1 according to any certain property satisfied by i in L_j, *i.e.* $f_j : L_j \to \{0, 1\}$. The common elements problem is stated as follows: find the entry $i \in L_j$ such that $\forall L_j \in \mathcal{Z},\ f_j(i) = 1$.

Example

$f_0(x_0, x_1, x_2) = x_0 x_1, \quad solns = \{110, 111\}$
$f_1(x_0, x_1, x_2) = x_0 x_1 x_2, \ solns = \{111\}$

Literature Review

- In 1998, Burhman *et al.* introduced a quantum algorithm [1] find common entries between remotely separated lists in $\mathcal{O}(p\sqrt{N})$, with p trials and $N = 2^n$.
- In 2012, Tulsi provided a quantum algorithm [2] to find a single common entry between two lists using Grover algorithm, in $\mathcal{O}(\sqrt{N})$.
- In 2013, Pang *et al.* proposed a quantum algorithm [3] to find common entries between two sets stored in classical memory, in $\mathcal{O}(\sqrt{N^2/C})$, where C is the number of common entries.

Amplitude Amplification

- In 1996, Grover proposed a unique approach [4] to find a single item in a database, in $\mathcal{O}(\sqrt{N})$.
- Boyer *et al.* later generalized Grover's quantum search algorithm [5, 6] to fit the purpose of finding multiple solutions M to the oracle, in $\mathcal{O}(\sqrt{N/M})$.
- Grover's algorithm amplifies solutions to an extend, *i.e.* $1 \leq M \leq 3N/4$ [5, 6].
- Younes *et al*'s algorithm [7] is reliable in case of multiple matches, *i.e.* $1 \leq M \leq N$.
- Both run in $\mathcal{O}(\sqrt{N/M})$.

Algorithm 1 Younes quantum search algorithm.

1: Prepare a quantum register of $n+1$ qubits to the state $|0\rangle^{n+1}$.
2: Apply the Hadamard gates on the register to create a uniform superposition $\frac{1}{\sqrt{N}}\sum_{l=0}^{N-1}|l\rangle$.
3: Iterate over the following $q = \frac{\pi}{2\sqrt{2}}\sqrt{\frac{N}{M}}$ steps:

   1. Apply the function U_f, to mark the solutions with entanglement.
   2. Apply the diffusion operator

$$Y = (H^{\otimes n} \otimes I)(2|0\rangle\langle 0| - I_{n+1})(H^{\otimes n} \otimes I).$$

4: Measure the output.

Common Entries Oracle Construction: Two Oracles

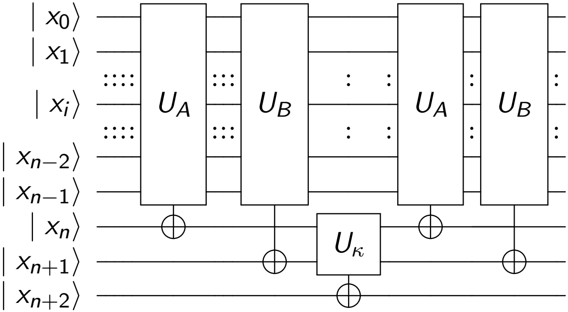

Figure 1: A quantum circuit for the proposed oracle $U_\hbar$ for $\kappa = 2$ databases, where $f_\kappa = x_n x_{n+1}$.

Common Entries Oracle Construction: κ Oracles

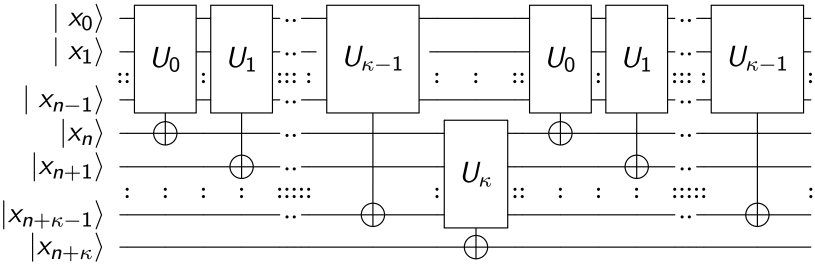

Figure 2: A quantum circuit for the proposed oracle $U_\hbar$ for κ functions, where $f_\kappa = x_n x_{n+1} \cdots x_{n+\kappa}$.

The Proposed Algorithm I

The Proposed Algorithm II

Algorithm 2 The Proposed Algorithm.

1: Construct the oracle $U_\hbar$.
2: Set the quantum register to $|0\rangle^{\otimes n}$ and the extra $\kappa+1$ qubits to $|0\rangle$.
3: Apply the Hadamard gates to the first n qubits to create the uniform superposition $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\otimes|0\rangle^{\otimes\kappa+1}$.
4: Iterate over the following $q_c = \frac{\pi}{2\sqrt{2}}\sqrt{\frac{N}{C}}$ steps:
   1. Apply the oracle $U_\hbar$.
   2. Apply the diffusion operator Y.
5: Measure the output.

The Proposed Algorithm III

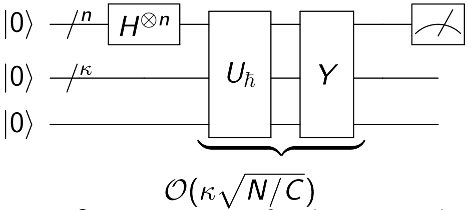

Figure 3: Quantum circuit for the proposed algorithm.

Analysis of the Proposed Algorithm

- *In case of known number of common matches C between κ databases.* The proposed algorithm requires $\mathcal{O}(\kappa\sqrt{N/C})$, where $1 \leq C \leq N$.
- *In case of unknown number of common matches between databases.*
  - An algorithm [8] for estimating the number of matches was presented by Brassard *et al.*, known as quantum counting.
  - Another algorithm [7] was presented by Younes *et al.* to search for a match in a database, with unknown number of matches.

Comparison with other Literature

	Tulsi [2]	Proposed Algorithm
Number of common entries C	$1 \leq C \leq 3N/4$	$1 \leq C \leq N$
Number of databases κ	$\kappa = 2$	$\kappa \geq 2$
Query calls: $\kappa = 2, \; C = 1$	$\mathcal{O}(\sqrt{N})$	$\mathcal{O}(\sqrt{N})$
Query calls: $\kappa = 2, C \geq 2$	$\mathcal{O}(\sqrt{N/C})$	$\mathcal{O}(\sqrt{N/C})$
Query calls: $\kappa > 2, C \geq 1$	NA	$\mathcal{O}(\kappa\sqrt{N/C})$

Table 1: Comparison between the proposed algorithm and relevant literature.

Conclusion I

- Proposed a quantum algorithm to find the common entries between κ databases.
- Each database uses an oracle to access its entries.
- Using the given oracles, we constructed another oracle that exhibits the behavior of finding only the common entries between those databases, using entanglement.
- Amplitude amplification algorithm is followed to increase the success probability of finding the common entries.
- The proposed algorithm requires $\mathcal{O}(\kappa\sqrt{N/C})$ to find the common matches, such that $1 \leq C \leq N$.

Conclusion II

- The proposed oracle can be extended using [8] to count the number of common entries between any given oracles, or find a match as in [5, 7], when the number of common entries C is unknown.
- The proposed algorithm can be used to solve a system of binary equations with no constraints on the form of the equations contrary to [9].
- Utilizing the proposed oracle with quantum counting, it can be used to measure the Hamming distance between oracles similar to [10, 11].

Bibliography

[1] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. Classical Communication and Computation," pp. 63–68, 1998. [Online]. Available: http://arxiv.org/abs/quant-ph/9802040

[2] A. Tulsi, "Optimal quantum searching to find a common element of two sets," pp. 1–5, 2012. [Online]. Available: http://arxiv.org/abs/1210.4648

[3] C. Y. Pang, R. G. Zhou, C. B. Ding, and B. Q. Hu, "Quantum search algorithm for set operation," *Quantum Information Processing*, vol. 12, no. 1, pp. 481–492, 2013.

[4] L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack," *Physical Review Letters*, vol. 79, p. 325, 1997. [Online]. Available: http://arxiv.org/abs/quant-ph/9706033

[5] M. Boyer, G. Brassard, P. Hoeyer, and A. Tapp, "Tight bounds on quantum searching," *arXiv preprint quant-ph/9605034*, vol. 46, no. May, p. 8, 1996. [Online]. Available: http://arxiv.org/abs/quantph/9605034{%}5Cnhttp://arxiv.org/abs/quant-ph/9605034

[6] A. Younes, "Strength and Weakness in Grover's Quantum Search Algorithm," *Arxiv preprint arXiv:0811.4481*, p. 15, 2008. [Online]. Available: http://arxiv.org/pdf/0811.4481{%}5Cnhttp://arxiv.org/abs/0811.4481

[7] A. Younes, J. Rowe, and J. Miller, "Enhanced quantum searching via entanglement and partial diffusion," *Physica D: Nonlinear Phenomena*, vol. 237, no. 8, pp. 1074–1078, 2008.

[8] G. Brassard, P. Hoyer, and A. Tapp, "Quantum Counting," vol. 20244, no. 20244, 1998. [Online]. Available: http://arxiv.org/abs/quant-ph/9805082{%}0Ahttp://dx.doi.org/10.1007/BFb0055105

[9] P. Schwabe and B. Westerbaan, "Solving binary $\mathcal{MQ}$ with grovers algorithm," *International Conference on Security, Privacy, and Applied Cryptography Engineering*, 2017.

[10] Z. Xie, D. Qiu, and G. Cai, "Quantum algorithms on walsh transform and hamming distance for boolean functions," *Quantum Information Processing*, vol. 17, pp. 1–17, 2018.

[11] K. El-Wazan, "Measuring hamming distance between boolean functions via entanglement measure," 2019. [Online]. Available: https://arxiv.org/abs/1903.04762v1