Quantum Information Processing (2024) 23:356
https://doi.org/10.1007/s11128-024-04548-x

Simple exact quantum search

Raj Alexandru Guţoiu [1] · Andrei Tănăsescu [1] · Pantelimon George Popescu [1]

Received: 23 May 2024 / Accepted: 24 September 2024

Abstract
While Grover's search algorithm is asymptotically optimal, it does not always result in a real solution. If the search fails, the algorithm must be ran again from the beginning, conditionally doubling the effective number of oracle calls. Previous research attempted to fix this issue by modifying the oracle or alternating between numerically optimized reflectors. In this paper, we present an optimal initial state and reflector that produce an exact search with Grover's algorithm at the cost of at most one additional oracle call beyond the optimum, a cost which can be nullified if we know a non-solution. We do this without modifying the oracle, without changing the diffuser at each step and even without any numerical optimization procedure required.

Keywords Grover algorithm · Quantum search · Restricted oracle · Success rate

1 Introduction

Grover's search algorithm is one of the most important quantum algorithms showing a complexity advantage over classical search, providing a quadratic speedup in searching unstructured data [1, 2]. However, its success probability is not always 100%, which can sometimes make it less efficient than even guessing a solution, especially if there are particularly many. Prior research worked around this issue by changing the diffuser or even the oracle, which would have it change the phase of the solutions by a controllable angle as given in [3]. Such modifications allow for numerical optimization of the diffuser and oracle phase choice at each iteration, a technique known as phase matching [4] and commonly used in making quantum search algorithms [5, 6].

However, having the oracle be controllable by the user is a big assumption. A quantum random access memory (QRAM) can serve as an oracle, enabling access to data stored in an unstructured classical or quantum database [7, 8]. This led to the development of algorithms that only change the diffusion operator, such as the D2p [9], which arrives at a solution with 100% probability, at the performance cost of at most

✉ Pantelimon George Popescu
pgpopescu@upb.ro

[1] Computer Science and Engineering Department, National University of Science and Technology POLITEHNICA Bucharest, Splaiul Independeţei 313, (6), Bucharest, Romania

Published online: 18 October 2024

one more oracle call beyond Grover's original algorithm, with the added complexity that it uses two diffusers, continuously alternating between them. Although the D2p algorithm always finds real solutions, the equations determining its phase parameters are not always solvable. The D2p algorithm was also improved in the presence of phase noise [10], especially relevant when implemented on real quantum hardware [11].

If the oracle rotates the solution at an arbitrary angle instead of flipping it, other deterministic phase-matching algorithms can be implemented, such as FXR [12]. The FXR algorithm provides phases that can always be numerically calculated. However, as the phases are numerically calculated, there can be errors in implementing the correct angle on real hardware, decreasing actual success probability [13]. It was also proved that there is a lower bound of oracle calls for a deterministic quantum search [14].

While having two diffusers may be unappealing, the cost of one more oracle call is required in order to have 100% success probability [15]. Another requirement that is key to obtaining a quadratic speedup is knowledge of the ratio of solutions to candidates [3]. If unknown, the number of solution can be determined using quantum counting [16], which can also be simplified [17, 18], but this has its cost.

In this paper, we propose an algorithm that finds a solution of the search problem with 100% probability using at most one more oracle call beyond the optimum, but without modifying the oracle, without changing the diffuser at each step and even without any numerical optimization procedure required.

2 Preliminaries

Grover's unstructured database search problem involves finding one of M solutions among N candidate entries. Given a function $f : \{0, 1, \ldots, N-1\} \to \{0, 1\}$ and the number of inputs mapping to the desired target value $\left|f^{-1}(\{1\})\right| = M$, we are asked to find any one of these inputs $x \in f^{-1}(\{1\})$.

To adapt this problem to the context of quantum computation, we are given access to this database in the form of a quantum oracle gate, a unitary operator $\mathbf{U}_f \in \mathcal{B}\left(\mathbb{C}^N\right)$ such that $U_f|x\rangle = (-1)^{f(x)}|x\rangle$ for all $x \in \{0, 1, \ldots, N-1\}$.

The algorithm then begins by preparing the starting state

$$|s_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sin\frac{\theta_0}{2}|t_0\rangle + \cos\frac{\theta_0}{2}|r_0\rangle,$$

where the target state $|t_0\rangle = \frac{1}{\sqrt{M}} \sum_{x \in f^{-1}(1)} |x\rangle$ is a superposition of the solutions and the rest of the candidates are grouped into the state $|r_0\rangle = \frac{1}{\sqrt{M}} \sum_{x \in f^{-1}(0)} |x\rangle$; hence, $\theta_0 = 2 \arcsin \sqrt{M/N}$. Then, for τ_0 iterations it proceeds to first apply the Grover oracle $\mathbf{U}_f = \mathbf{I}_N - 2|t_0\rangle\langle t_0|$ and then a diffusion operator $\mathbf{D}_0 = 2|s_0\rangle\langle s_0| - \mathbf{I}_N$. After these τ iterations, the state of the system becomes

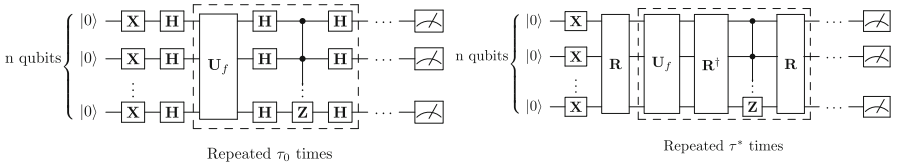

Fig. 1 Quantum circuit for the original Grover algorithm, where τ_0 is the optimal number of iterations given by Eq. 1 (left) and for our simple exact quantum search algorithm, where τ^* is the optimal number of iterations given by Eq. 2 (right)

$$|\psi_\tau\rangle = \sin\frac{(2\tau+1)\theta_0}{2}|t_0\rangle + \cos\frac{(2\tau+1)\theta_0}{2}|r_0\rangle,$$

which can be measured in the computational basis to yield a solution with probability $\sin^2\frac{(2\tau+1)\theta_0}{2}$, with the first maximum encountered at $\tau = \frac{\pi}{4\arcsin\sqrt{M/N}} - 1/2$, which, however, is not an integer. For this reason, Grover's algorithm is usually stopped whenever it reaches the closest integer (e.g. $CI(3.4) = 3$ and $CI(3.6) = 4$) to this number [19], which we denote

$$\tau_0 = CI\left(\frac{\pi}{4\arcsin\sqrt{M/N}} - \frac{1}{2}\right). \tag{1}$$

Consequently, the probability that Grover's algorithm finds a true solution is $\sin^2\frac{(2\tau_0+1)\theta_0}{2}$ which is actually only ever 100% if $M/N = 1/4$ [19]. In fact, as M/N increases from 0 to 1 this number oscillates, and for $M/N \geq 0.5$, the probability that Grover's algorithm provides a true solution is less than the probability to guess a solution. Also, for every value of the optimal number of iterations τ_0, there is only one value of the ratio M/N such that Grover's algorithm has a 0% failure rate, and this value of the ratio M/N is not always rational, as shown in Fig. 3 left.

3 Simple exact quantum search with a hint

In this section, we present our main result, a simple exact quantum search algorithm with at most one additional oracle call beyond the optimum.

To begin, we ask for a hint about a non-solution, i.e. to know of an $y \in f^{-1}(0)$. Such a hint can be obtained for example by checking whether $f(0)$ is a solution, at the cost of one oracle call.

Now, we start Grover's algorithm with a perturbed initial state

$$\begin{aligned}|\psi_0\rangle = &|s\rangle = \epsilon|y\rangle + \frac{\sqrt{1-\epsilon^2}}{\sqrt{N-1}}\sum_{x\neq y}|x\rangle \\ &= \cos\varphi\cos\frac{\theta}{2}|y\rangle + \sin\varphi\cos\frac{\theta}{2}|r\rangle + \sin\frac{\theta}{2}|t_0\rangle,\end{aligned}$$

where $\sin\frac{\theta}{2} = \eta\sqrt{M}$, $\sin\varphi = \eta\frac{\sqrt{N-M}}{\sqrt{1-M\eta^2}}$, and $\eta = \frac{\sqrt{1-\epsilon^2}}{\sqrt{N-1}}$.

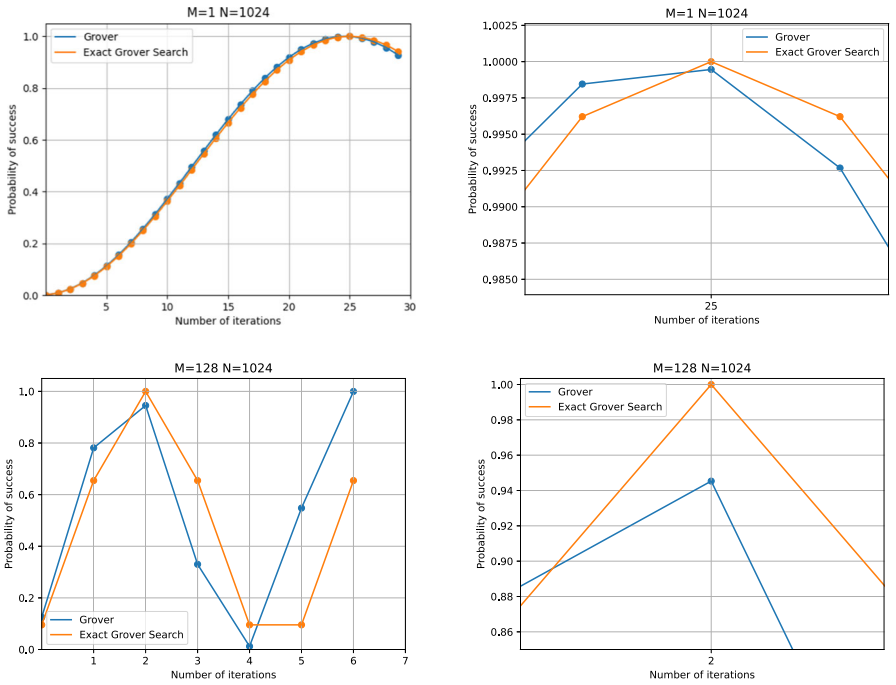

Fig. 2 Probability of finding a solution by measuring the system state after each number of iterations for $M = 1$ or $M = 128$ solutions out of $N = 1024$ candidates (left), zoomed in around the first peak (right)

The key insight of our method is that applying the modified diffuser $\mathbf{D} = 2|s\rangle\langle s| - \mathbf{I}_N$ produces a sequence of quantum states that allows us to stop the algorithm at a known time such that we always obtain a true solution. Notably, the matrix of this diffuser $\mathbf{D}$ is similar to the multi-controlled $\mathbf{Z}$ gate. Indeed, given a matrix $\mathbf{R}$ rotating $|1 \ldots 1\rangle$ into $|s\rangle$ we find that $\mathbf{D} = -\mathbf{R}(\mathbf{C} \ldots \mathbf{C})\mathbf{Z}\mathbf{R}^\dagger$, hence leading to the circuit implementation in Fig. 1.

Notice that if at the start of iteration τ the system has state

$$|\psi_\tau\rangle = \cos\varphi \cos\frac{(2\tau+1)\theta}{2}|y\rangle + \sin\varphi \cos\frac{(2\tau+1)\theta}{2}|r\rangle + \sin\frac{(2\tau+1)\theta}{2}|t_0\rangle$$

then, after the oracle call, it will be in state

$$\mathbf{U}_f|\psi_\tau\rangle = \cos\varphi \cos\frac{(2\tau+1)\theta}{2}|y\rangle + \sin\varphi \cos\frac{(2\tau+1)\theta}{2}|r\rangle - \sin\frac{(2\tau+1)\theta}{2}|t_0\rangle$$

so

$$\begin{aligned}\langle s|\mathbf{U}_f|\psi_\tau\rangle = \cos^2\varphi \cos\frac{\theta}{2}\cos\frac{(2\tau+1)\theta}{2} + \sin^2\varphi \cos\frac{\theta}{2}\cos\frac{(2\tau+1)\theta}{2} \\ - \sin\frac{\theta}{2}\sin\frac{(2\tau+1)\theta}{2} = \cos((\tau+1)\theta),\end{aligned}$$

where we used the identities $\cos^2\varphi + \sin^2\varphi = 1$ and $\cos x \cos y - \sin x \sin y = \cos(x+y)$.

Thus, after the reflection with respect to $|s\rangle$ the system is in state

$$\begin{aligned}
\mathbf{D}\mathbf{U}_f|\psi_\tau\rangle =& 2|s\rangle\langle s|\mathbf{U}_f|\psi_\tau\rangle - |\psi_\tau\rangle = 2\cos((\tau+1)\theta)|s\rangle - |\psi_\tau\rangle \\
=& 2\cos((\tau+1)\theta)\cos\varphi\cos\frac{\theta}{2}|y\rangle - \cos\varphi\cos\frac{(2\tau+1)\theta}{2}|y\rangle \\
&+ 2\cos((\tau+1)\theta)\sin\varphi\cos\frac{\theta}{2}|r\rangle - \sin\varphi\cos\frac{(2\tau+1)\theta}{2}|r\rangle \\
&+ 2\cos((\tau+1)\theta)\sin\frac{\theta}{2}|t_0\rangle - \sin\frac{(2\tau+1)\theta}{2}|t_0\rangle \\
=& \cos\varphi\cos\frac{(2\tau+3)\theta}{2}|y\rangle + \sin\varphi\cos\frac{(2\tau+3)\theta}{2}|r\rangle + \sin\frac{(2\tau+3)\theta}{2}|t_0\rangle \\
=& |\psi_{\tau+1}\rangle,
\end{aligned}$$

where we used the identities $2\cos x\cos y = \cos(x-y)+\cos(x+y)$ and $2\cos x\sin y = \sin(x+y) - \sin(x-y)$.

For the algorithm to produce a solution with 100% probability, we require that $1 = |\langle\psi_\tau \mid t_0\rangle|^2 = \sin^2\frac{(2\tau+1)\theta}{2}$. We thus require $(2\tau+1)\arcsin\eta\sqrt{M} = \frac{\pi}{2}$, where we can pick any $\eta \leq \frac{1}{\sqrt{N-1}}$ so $\tau \geq \frac{\pi}{4\arcsin\sqrt{\frac{M}{N-1}}} - \frac{1}{2}$, and thus, the optimal oracle call count is

$$\tau^* = \left\lceil \frac{\pi}{4\arcsin\sqrt{\frac{M}{N-1}}} - \frac{1}{2} \right\rceil, \tag{2}$$

obtained when $\epsilon = \sqrt{1 - \frac{N-1}{M}\sin^2\frac{\pi}{4\tau^*+2}}$.

Notice that the oracle call count τ^* is optimal for exact quantum search, but in order to achieve it, we needed a hint about the non-solution y. As discussed, y can be obtained by checking one of the solutions, potentially at the cost of one additional oracle call. Sometimes, this hint requires no additional oracle calls, e.g. when we are implementing the Grover algorithm for $N \neq 2^n$ using multi-qubit circuits, and in such cases, we do indeed achieve the optimal oracle call count.

For numerical validation, in Fig. 2 we plot the probability of successfully finding a solution when measuring the system state after τ iterations using the original Grover algorithm and our simple exact search algorithm. As we can see on the left, the success probability curve for our algorithm closely follows that of Grover's original algorithm, but, as we can see on the right, our method has the benefit that the first peak now corresponds to a 100% probability of obtaining a true solution. Finally, in Fig. 3 we plot the probability of not finding a solution for both Grover's algorithm (left) and our simple exact quantum search algorithm (right), noting the abundance of zero values.

Moreover, when comparing with previous approaches to exact quantum search, we find that our algorithm is indeed simpler. Unlike [3, 12], we use the same black box oracle as the original Grover algorithm, we do not need numerical optimization as in [4–6, 12], we do not need two different diffusers as in [9], and we still maintain the optimal oracle call count bound [14, 15]. Moreover, we not only obtained the

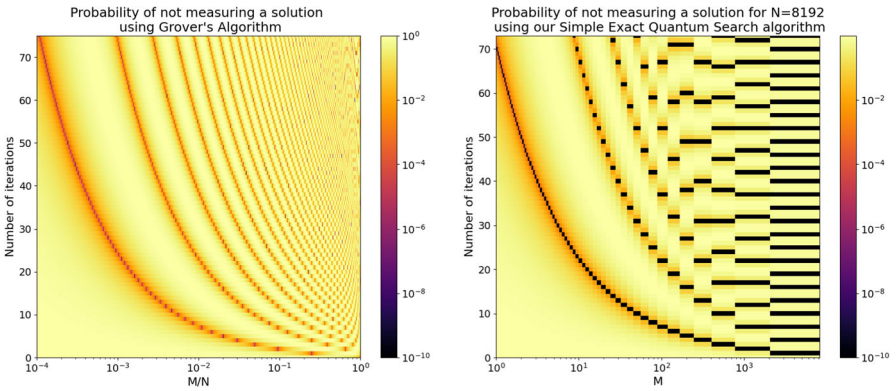

Fig. 3 Probability of not finding a solution using Grover's algorithm, as a function of the solution ratio M/N and number of iterations (left) and for our simple exact quantum search algorithm for a database with $N = 8192$ elements, as a function of number of iterations and number of solutions M (right)

optimal query complexity, but also the optimal constant factor, while providing a simple quantum circuit.

4 Conclusions

In this paper, we proposed an algorithm that solves the search problem with 100% probability using at most one more oracle call beyond the optimum. Our proposed algorithm does not need numerical optimization processes and its parameters can always be analytically determined. We did this by perturbing the initial state to take advantage of a hint about a known non-solution. A hint is sometimes available at no computational expense, such as when implementing Grover search with $N \neq 2^n$ on multi-qubit systems. We showed that our algorithm can be implemented using a small variation of the Grover circuit requiring only a few more rotation gates.

Acknowledgements This work is dedicated to Prof. Nicolae Tapus, on his 75th birthday. This work has been partially supported by RoNaQCI, part of EuroQCI, DIGITAL-2021-QCI-01-DEPLOY-NATIONAL, 101091562.

Author Contributions RAG, AT and PGP were involved in conceptualization, validation, writing—original draft preparation, and writing—review and editing; AT and PGP were responsible for methodology; PGP took part in supervision; and all authors have read and agreed to the published version of the manuscript.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Grover, L.K.: A fast quantum mechanical algorithm for database search. Phys. Rev. Lett. **79**, 325 (1997)
2. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, pp. 212–219. ACM, New York (1996)
3. Long, G.-L.: Grover algorithm with zero theoretical failure rate. Phys. Rev. A **64**(2), 022307 (2001)
4. Long, G.L., Li, Y.S., Zhang, W.L., Niu, L.: Phase matching in quantum searching. Phys. Lett. A **262**(1), 27–34 (1999)
5. Li, P., Li, S.: Phase matching in Grover's algorithm. Phys. Lett. A **366**(1), 42–46 (2007)
6. Toyama, F.M., Dijk, W., Nogami, Y., Tabuchi, M., Kimura, Y.: Multiphase matching in the Grover algorithm. Phys. Rev. A **77**, 042324 (2008)
7. Giovannetti, V., Lloyd, S., Maccone, L.: Architectures for a quantum random access memory. Phys. Rev. A **78**, 052310 (2008)
8. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum random access memory. Phys. Rev. Lett. **100**, 160501 (2008)
9. Roy, T., Jiang, L., Schuster, D.I.: Deterministic Grover search with a restricted oracle. Phys. Rev. Res **4**(2), 022013 (2022)
10. Leng, J., Yang, F., Wang, X.-B.: Improving d2p Grover's algorithm to reach performance upper bound under phase noise. Phys. Rev. Res. **5**(2), 023202 (2023)
11. Li, Z.-H., Yu, G.-F., Wang, Y.-X., Xing, Z.-Y., Kong, L.-W., Zhou, X.-Q.: Experimental demonstration of deterministic quantum search algorithms on a programmable silicon photonic chip. Sci. China Phys. Mech. Astron. **66**(9), 290311 (2023)
12. Li, G., Li, L.: Deterministic quantum search with adjustable parameters: implementations and applications. Inf. Comput. **292**, 105042 (2023)
13. Tonchev, H., Danev, P.: Robustness of different modifications of Grover's algorithm based on generalized householder reflections with different phases. Results Phys. **59**, 107595 (2024)
14. Beals, R., Buhrman, H., Cleve, R., Mosca, M., De Wolf, R.: Quantum lower bounds by polynomials. J. ACM **48**(4), 778–797 (2001)
15. Huang, Y., Pang, S.: Optimization of a probabilistic quantum search algorithm with a priori information. Phys. Rev. A **108**(2), 022417 (2023)
16. Brassard, G., Høyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. In: Lomonaco, S.J. (ed.) Quantum Computation and Quantum Information: A Millennium Volume. Contemporary Mathematics, vol. 305, pp. 53–74. American Mathematical Society, Providence (2002)
17. Aaronson, S., Rall, P.: Quantum approximate counting, simplified. In: Symposium on Simplicity in Algorithms, pp. 24–32. SIAM (2020)
18. Suzuki, Y., Uno, S., Raymond, R., Tanaka, T., Onodera, T., Yamamoto, N.: Amplitude estimation without phase estimation. Quantum Inf. Process. **19**, 75 (2020)
19. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition, 10th edn. Cambridge University Press, New York (2011)