Variationally Learning Grover’s Quantum Search Algorithm

Mauro E.S. Morales, Timur Tlyachev, and Jacob Biamonte

Deep Quantum Labs, Skolkovo Institute of Science and Technology, 3 Nobel Street, Moscow, Russia 121205
May 25, 2018

Given a parameterized quantum circuit such that a certain setting of these real-valued parameters corresponds to Grover’s celebrated search algorithm, can a variational algorithm recover these settings and hence learn Grover’s algorithm? We tried several constrained variations of this problem and answered this question in the affirmative, with some caveats. Grover’s quantum search algorithm is optimal up to a constant. The success probability of Grover’s algorithm goes from unity for two-qubits, decreases for three- and four-qubits and returns near unity for five-qubits then oscillates ever-so-close to unity, reaching unity in the infinite qubit limit. The variationally approach employed here found an experimentally discernible improvement of 5.77% and 3.95% for three- and four-qubits respectively. Our findings are interesting as an extreme example of variational search, and illustrate the promise of using hybrid quantum classical approaches to improve quantum algorithms.

1 Introduction

Grover’s algorithm [6] is one of the most celebrated quantum algorithms, enabling quantum computers to quadratically outperform classical computers at database search provided database access is restricted to a ‘black box’ – called the oracle model. In addition to the wide application scope of database search, Grover’s algorithm has further applications as a subroutine used in a variety of other quantum algorithms.

Variational hybrid quantum/classical algorithms have recently become an area of significant interest [4, 8, 10, 13, 14, 17, 19]. Here we consider a variational approach to the established problem of Grover’s search [6]. Note that Grover’s search was generalized to the setting of adiabatic quantum computing in [15, 16]. Grover’s quantum search algorithm has been shown to be asymptotically optimal [2, 3, 21] and hence provides a limiting test case to apply contemporary variational hybrid quantum/classical algorithms to.

We apply a variational algorithm to see if we can recover Grover’s algorithm under several constraining scenarios. We motivate our study by recalling that sequencing two Hermitian projectors (Hamiltonians) can be used to recover Grover’s search algorithm exactly. We then constrain the search space. For example, in one scenario we fix the oracle—as is standard—to apply a phase factor of −1 to the marked item when varying the time the diffusion generator is applied. In another scenario, we allow the oracle and the diffusion to take the same angle in all iterations. The main objective is to see if a variational algorithm is capable of recovering Grover’s algorithm given different restrictions. A peculiar finding is an experimentally discernible improvement of 5.77% and 3.95% for three- and four-qubits respectively (compared to Grover’s search algorithm).

2 Structure

In Section 3 we will overview the variational search algorithm, define the four different restrictions we will impose on the algorithm, and show this problem contains as one variational solution Grover’s original algorithm. Then we compare variational search and Grover’s search in Section 4. Finally the conclusion provides a detailed discussion about some of the more subtle points sur-
rounding this study.

3 Variational quantum search

In this section we will layout the notation and the different versions of the variational algorithm that we consider.

Let \( n \) be the number of qubits and let \( N = 2^n \) be the size of the search space. We are searching for a particular bitstring \( \omega = \omega_1, \omega_2, \omega_3, \ldots, \omega_n \).

We define a pair of rank-1 projectors.

\[
P_\omega = |\omega\rangle\langle\omega| \quad (1)
\]

\[
P_+ = |+\rangle\langle+|^n = |s\rangle\langle s| \quad (2)
\]

where \(|s\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle\). To find \(|\omega\rangle\), we consider a split-operator variational ansatz, formed by sequencing a pair of operators. These operators prepare a state \(|\varphi(\alpha, \beta)\rangle\), with vectors \(\alpha = \alpha_1, \alpha_2, \ldots, \alpha_p\) and \(\beta = \beta_1, \beta_2, \ldots, \beta_p\). We seek to minimize the orthogonal complement of the subspace for the searched string \(|\omega\rangle\).

\[
P_{\omega^\perp} = 1 - P_\omega \quad (3)
\]

We sometimes call (2) the driver Hamiltonian or diffusion operator. The state is varied to minimize this orthogonal component (4).

\[
\min_{\alpha, \beta} \langle \varphi(\alpha, \beta)|P_{\omega^\perp}|\varphi(\alpha, \beta)\rangle \geq \min \langle \phi|P_{\omega^\perp}|\phi\rangle \quad (4)
\]

To prepare the state we develop the sequence (5).

\[
|\varphi(\alpha, \beta)\rangle = K(\beta_p)\mathcal{V}(\alpha_p) \cdots K(\beta_1)\mathcal{V}(\alpha_1)|s\rangle. \quad (5)
\]

Where the operators are defined as (6) and (7).

\[
\mathcal{V}(\alpha) := e^{i\alpha P_\omega} \quad (6)
\]

\[
K(\beta) := e^{i\beta P_+} \quad (7)
\]

The length of the sequence is \(2p\), for integer \(p\). We consider now the following problems on which the variational algorithm will work.

**Problem 3.1 (Standard Oracle, Variational Diffusion).** Finding \(p\) angles \(\beta = (\beta_1, \ldots, \beta_p)\) and fixing \(\alpha = (\alpha_1 = \pi, \ldots, \alpha_p = \pi)\) to minimize (4) via the sequence (5), given the operators (6) and (7).

In this problem we have fixed the standard black-box oracle of Grover’s algorithm and the algorithm optimizes for the angles in the diffusion operator. We also consider a restricted variational problem where all the diffusion operators must apply the same variational angle.

**Problem 3.2 (Standard Oracle, Restricted Variational Diffusion).** Same as problem 3.1 but finding \(p\) angles \(\beta = (\beta_1, \ldots, \beta_p)\) and choosing \(\alpha = (\alpha_1 = \pi, \ldots, \alpha_p = \pi)\).

A third problem to which we will apply the variational algorithm is considering both the oracle and the diffusion angles as variational parameters. We consider in this case a phase matching condition, meaning that angles are restricted to be equal.

**Problem 3.3 (Restricted Variational Oracle and Diffusion).** Same as definition 3.1 but finding \(2p\) angles \((\alpha, \beta) = (\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_p)\) with the restriction \(\beta = \alpha = \alpha_1, \alpha_2, \ldots, \alpha_p\) and \(\alpha_1 = \alpha_2 = \ldots = \alpha_p\).

Finally we consider variations of the oracle angles of the oracle and the diffusion operator separately.

**Problem 3.4 (Variational Oracle and Diffusion).** Same as problem 3.1 but finding \(2p\) angles \((\alpha, \beta) = (\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_p)\).

We also call this last variation a two-level split operator ansatz. Note that the angles obtained in (4) only minimize the selected cost function for a particular number of qubits. Once the number of qubits change, the angles obtained in the minimization do not necessarily give the highest probability to find the searched item. Also its important to note that these angles are independent of \(\omega\), if we fix the number of qubits in the problem and run the algorithm with a particular set of angles, then these angles give the same probability no matter the \(\omega\) we are looking for. As stated earlier our objective in this work is to see if variational algorithms are able to recover Grover’s algorithm, for this we need a way of comparing both algorithms.

To compare these variational algorithms with Grover’s algorithm, consider the two-level split-operator ansatz case for \(p = 1\). Here we recover Grover’s operators as the optimal solution for finding a particular string. To prove this, first note that there is only one pair of angles \((\alpha, \beta)\), so we consider (6) and (7) directly. Since \(|\omega\rangle\langle\omega|\) is a projector we can expand (6).

\[
\mathcal{V}(\alpha) = e^{i\alpha}|\omega\rangle\langle\omega| = 1 + (e^{i\alpha} - 1)|\omega\rangle\langle\omega| = 1 - (e^{i\alpha} + 1)|\omega\rangle\langle\omega| \quad (8)
\]
Where in the last step we have defined $\tilde{\alpha} = \alpha - \pi$. Now we expand the unitary for the driver Hamiltonian (9).

$$K(\beta) = e^{i\beta}|s\rangle\langle s|$$

$$= H^{\otimes n}(1 + (e^{i\beta} - 1)|0\rangle\langle 0|)H^{\otimes n}$$

$$\sim H^{\otimes n}(-1 + (e^{i\beta} + 1)|0\rangle\langle 0|)H^{\otimes n}$$

$$= (e^{i\beta} + 1)|s\rangle\langle s| - 1$$

Where $\sim$ relates the equivalence class of operators indiscernible by a global phase, $H$ is the Hadamard gate and $\tilde{\beta} = \beta - \pi$. Notice that for $\tilde{\alpha} = \tilde{\beta} = 0$ Grover’s oracle and diffusion operators are recovered.

To see that the variational search includes Grover’s operators for the case $p > 1$, let us impose $\alpha_1 = \alpha_2 = \ldots = \alpha_p$ and $\beta_1 = \beta_2 = \ldots = \beta_p$. In Fig. 5a and Fig. 5b the circuits for the oracle and the diffusion operator respectively are shown. If $i$ pairs of operators (6) and (7) are applied to the initial state $|s\rangle$ as in (5), then we write the prepared state as (10).

$$|\varphi_i\rangle = A_i \frac{1}{\sqrt{N - 1}} \sum_{x \neq \omega} |x\rangle + B_i |\omega\rangle \quad (10)$$

We can relate the amplitudes of one step with the amplitudes of the next step with a recursion such as those that appear in (13) and (14); we express the effect of the operators for the variational search over the state as a matrix (11).

$$\begin{pmatrix}
1 + a(N-1) & -a(b+1) \frac{\sqrt{N-1}}{\sqrt{N}} \\
-a \frac{\sqrt{N-1}}{\sqrt{N}} & b+1 \left(1 + \frac{2}{N} \right)
\end{pmatrix} \quad (11)$$

Here $a = e^{i\alpha} - 1$ and $b = e^{i\beta} - 1$. Notice that for $a = b = -2$ the same relation between amplitudes at different steps in (13) and (14) up to a global phase in the definition of the Grover operators is obtained. Thus, the variational search space includes Grover’s original algorithm. From this matrix it is also possible to see that if the target state is changed, then the angles found through the variational algorithm will give the same probabilities.

An arbitrary phase applied by the oracle was first proposed in [20] although only remarks regarding the use of an arbitrary phase to get higher probabilities for the searched item were done, afterwards several studies regarding the validity of replacing Grover’s oracle and diffusion operator with an arbitrary phase version were made [7, 9, 11, 12]. The main conclusion is that a phase matching condition is required. This condition roughly stated requires the arbitrary angles in the oracle and the diffusion operator to be approximately equal. To address this, we consider also in this work the problem shown in definition 3.3, restricting the variational angles to be equal.

4 Comparison of Variational quantum search and Grover’s algorithm

In this section we show the main results of our study. We have compared the performance of the variational search algorithm to Grover’s for different number of qubits and for the problems 3.1, 3.2, 3.3 and 3.4. Surprisingly in problems 3.1, 3.3 and 3.4 it was found that for the first qubits and for the same number of operator applications (or oracle calls) $p$ on which Grover obtains the greatest probability, the variational algorithm achieves greater probabilities for finding the searched string. Comparison for the first steps is found for 3 and 4 qubits are shown in Fig. 1. The same plot is obtained for the variational algorithm defined for problems 3.1, 3.3 and 3.4. In Fig. 2 we show the probability for the searched item for 3 and 4 qubits in the case of problem 3.2. It is possible to see that in this case the advantage over Grover’s algorithm is lost. We also show in table 1, for the variational problem 3.3, the percentage increase between the variational algorithm and Grover’s for the probabilities at the number of oracle calls on which this probability is maximal from 2 to 6 qubits. For higher numbers of qubits this difference becomes negligible, although there are small oscillations. The same numbers are obtained (except the angle) for the algorithms in problems 3.1 and 3.4. We show in Fig. 3 the probability for finding the solution as a function of the only angle and number of qubits when considering the algorithm of problem 3.3. In case of problem 3.1 we recover the same probabilities for the marked state as in Grover’s algorithm, without the small improvement shown in Fig. 1. From the matrix in (11) and imposing $a = b$ it is possible to plot the probability as a function of the variational angle $\alpha$ and
the number of qubits for the algorithm in problem 3.3. We show this plot for 3 to 6 qubits in Fig. 3. The local maximum at \( \pi \) is clearly seen at \( n = 3 \) qubits but also at more qubits this angle is not the global maximum. The variational search manages to find these global maxima if a basin hopping method \[18\] for optimization (the search space of the angle is bounded since we restrict to \( \alpha \in [0, \pi] \)) is used. The difference of the probabilities to find the solution between the original Grover’s algorithm and the variational search does not diminish monotonically with the number of qubits, this is shown in Fig. 4. The same results are obtained for problems 3.1, 3.3, 3.4. In the case of problem 3.2, the difference is negligible.

For low \( N = 2^n \), where \( n \) is the number of qubits in the search, the variational search provides sequences that are more likely to succeed in finding the solution than Grover’s algorithm.

Grover’s algorithm has been proven to be optimal. This slight advantage of the variational algorithm over Grover’s is possible since the proofs have considered a large number of qubits \[2, 3, 21\]. We show in the following that this advantage disappears for large \( N \).

To prove this we first consider the following theorem.

**Theorem 4.1.** The maximum probability achievable for the target state in Grover \( \to 1 \) as \( N \to \infty \).

Before proving this we give proof of a proposition proved in \[21\].

**Proposition 4.2.** For \( N \gg 1 \) the probability of measuring the target state \( |\omega\rangle \) after making \( p \) oracle calls in Grover’s algorithm is \( P_p = \sin^2(p\phi + \phi/2) \).

**Proof of proposition 4.2.** We call the state of the system for step \( i \) of Grover’s algorithm \( |\psi_i\rangle \) and the target state is denoted \( |\omega\rangle \). As an initial state for the algorithm we have \( |\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \).

Following \[21\] we write the state of the system in the \( i \)th state (12) with (13) and (14).

\[
|\psi_i\rangle = A_i \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle + B_i |\omega\rangle \quad (12)
\]

\[
A_{i+1} = (1 - \frac{2}{N}) A_i - 2 \frac{\sqrt{N-1}}{N} B_i \quad (13)
\]

\[
B_{i+1} = 2 \frac{\sqrt{N-1}}{N} A_i - (1 - \frac{2}{N}) B_i \quad (14)
\]

This can be written as the result of applying a rotation \[21\] with \( \cos(\phi) = 1 - \frac{2}{N} \) and \( \sin(\phi) = 2 \frac{\sqrt{N-1}}{N} \). For the proof of the theorem we are interested in the large \( N \) limit. Let us consider then \( N \gg 1 \), thus \( \phi \approx \sin \phi \approx \frac{2}{\sqrt{N}} \). The initial state can be written in terms of this angle.

\[
|\psi_0\rangle = \cos(\phi/2) \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle + \sin(\phi/2) |\omega\rangle
\]

After applying a rotation with angle \( \phi \), \( p \) times (equivalent to applying both operators \( p \) times), if \( N \gg 1 \) then

\[
|\psi_i\rangle = \cos(\phi/2 + p\phi) \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle \\
+ \sin(\phi/2 + p\phi) |\omega\rangle
\]

Hence, the probability of measuring \( |\omega\rangle \) after \( p \) steps is (15).

\[
P_p = \sin^2(p\phi + \phi/2) \quad (15)
\]

With this, now we prove theorem 4.1.

**Proof of theorem 4.1.** From (15) we can calculate the maximum for the probability in the segment \([0, \pi]\). What we actually need is to calculate \( p_{\max} \) for which the probability is maximum in said segment. We know there is a maximum at \( \pi/2 \), thus

\[
p_{\max} + \phi/2 = \frac{\pi}{2} \implies p_{\max} = \frac{\pi}{2\phi} - \frac{1}{2}
\]

Then, for \( N \gg 1 \) we have

\[
p_{\max} = \frac{\pi \sqrt{N}}{4} - \frac{1}{2} \quad (16)
\]

Recall that \( p \) represents the oracle calls, thus it must be an integer. Then the maximum must be either (17) or (18).

\[
p_{\max} = \left| \frac{\pi \sqrt{N}}{4} - \frac{1}{2} \right| + 1 \quad (18)
\]
We want to prove that as $N \to \infty$ then the maximum probability goes to one. That is, we want to prove $\lim_{N \to \infty} (p\phi + \phi/2) = \pi/2$. We prove this with the following limit (19) — we can replace (17) with (18) and the result follows anyway.

$$\lim_{N \to \infty} \left( \frac{\pi \sqrt{N}}{4} - \frac{1}{2} \right) = \frac{2}{\sqrt{N}} + \frac{1}{\sqrt{N}} = \frac{\pi}{2}$$

Hence, $\sin^2(p\phi + \phi/2) \to 1$. \hfill \Box

With these results then its clear that the advantage is at best negligible for large $N$.

5 Conclusion

Let us reflect on several features relating to the most promising results of this study and contrast these with some of the more peculiar shortcomings.

An unusual feature of Grover was the small oscillation in the success probability going form unity for two-qubits and then decreasing for three- and four-qubits. This provided some slack for our variational approach to remove. In fact, with one angle (shared by both the oracle as well as the diffusion operator), we don’t always match the performance of Grover (for five or more qubits). Additional angles however add more degrees of freedom for the optimization procedure to succeed. When considering variational angles for the diffusion operator but not for the oracle operator, there is still the same advantage as in the case of the variational algorithm with only one angle shared between oracle and diffusion operator. The advantage disappears when only one variational angle is considered for the diffusion operator and the standard oracle of Grover’s algorithm is used.

We have presented a transfer matrix (11), interestingly, the optimization procedure is general in the sense that if we restrict to this transfer matrix, this defines the angle(s) for any search item. In other words, if we find the corresponding angle(s) for a given number of items to search in, we can use this same angle again and again for different search items. Nonetheless it must be noted that the angle(s) obtained through the variational algorithm will only give optimal probabilities for a given number of qubits $n$ in the search problem. For a different $n$, the algorithm needs to be rerun.

References

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. Divincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. Physical Review A, 52:3457–3467, November 1995.

[2] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. SIAM Journal on Computing, 26(5):1510–1523, 1997.

[3] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight Bounds on Quantum Searching. Fortschritte der Physik, 46:493–505, 1998.

[4] E. Farhi, J. Goldstone, and S. Gutmann. A Quantum Approximate Optimization Algorithm. ArXiv e-prints, November 2014.

[5] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, and C. Monroe. Complete 3-Qubit Grover search on a programmable quantum computer. Nature Communications, 8:1918, December 2017.

[6] L. K. Grover. A fast quantum mechanical algorithm for database search. eprint arXiv:quant-ph/9605043, May 1996.

[7] Long GuiLu, Zhang WeiLin, Li YanSong, and Niu Li. Arbitrary phase rotation of the marked state cannot be used for grover’s quantum search algorithm. Communications in Theoretical Physics, 32(3):335, 1999.

[8] S. Hadfield, Z. Wang, B. O’Gorman, E. G. Rieffel, D. Venturelli, and R. Biswas. From the Quantum Approximate Optimization Algorithm to a Quantum Alternating Operator Ansatz. ArXiv e-prints, September 2017.
[9] Peter Høyer. Arbitrary phases in quantum amplitude amplification. *Phys. Rev. A*, 62:052304, Oct 2000.

[10] Z. Jiang, E. G. Rieffel, and Z. Wang. Near-optimal quantum circuit for Grover’s unstructured search using a transverse field. *PRA*, 95(6):062317, June 2017.

[11] Che-Ming Li, Chi-Chuan Hwang, Jin-Yuan Hsieh, and Kuo-Shiong Wang. General phase-matching condition for a quantum searching algorithm. *Phys. Rev. A*, 65:034305, Feb 2002.

[12] X. Li, K. Song, N. Sun, and C. Zhao. Phase matching in grover’s algorithm. In *Proceedings of the 32nd Chinese Control Conference*, pages 7939–7942, July 2013.

[13] N. Moll, P. Barkoutsos, L. S. Bishop, J. M. Chow, A. Cross, D. J. Egger, S. Filipp, A. Fuhrer, J. M. Gambetta, M. Ganzhorn, A. Kandala, A. Mezzacapo, P. Müller, W. Riess, G. Salis, J. Smolin, I. Tavernelli, and K. Temme. Quantum optimization using variational algorithms on near-term quantum devices. *ArXiv e-prints*, October 2017.

[14] J. S. Otterbach, R. Manenti, N. Alidoust, A. Bestwick, M. Block, B. Bloom, S. Caldwell, N. Didier, E. Schuyler Fried, S. Hong, P. Karalekas, C. B. Osborn, A. Papageorge, E. C. Peterson, G. Prawiroatmodjo, N. Rubin, C. A. Ryan, D. Scarabelli, M. Scheer, E. A. Sete, P. Sivarajah, R. S. Smith, A. Staley, N. Tezak, W. J. Zeng, A. Hudson, B. R. Johnson, M. Reagor, M. P. da Silva, and C. Rigetti. Unsupervised Machine Learning on a Hybrid Quantum Computer. *ArXiv e-prints*, December 2017.

[15] J. Roland and N. J. Cerf. Quantum search by local adiabatic evolution. *Physical Review A*, 65 (4):042308, April 2002.

[16] W. van Dam, M. Mosca, and U. Vazirani. How Powerful is Adiabatic Quantum Computation? *eprint arXiv:quant-ph/0206003*, May 2002.

[17] G. Verdon, M. Broughton, and J. Biamonte. A quantum algorithm to train neural networks using low-depth circuits. *ArXiv e-prints*, December 2017.

[18] David J. Wales and Jonathan P. K. Doye. Global optimization by basin-hopping and the lowest energy structures of lemmard-jones clusters containing up to 110 atoms. *The Journal of Physical Chemistry A*, 101(28):5111–5116, 1997.

[19] Z. Wang, S. Hadfield, Z. Jiang, and E. G. Rieffel. Quantum approximate optimization algorithm for MaxCut: A fermionic view. *PRA*, 97(2):022304, February 2018.

[20] C. Zalka. A Grover-based quantum search of optimal order for an unknown number of marked elements. *eprint arXiv:quant-ph/9902049*, February 1999.

[21] Christof Zalka. Grover’s quantum searching algorithm is optimal. *Phys. Rev. A*, 60:2746–2751, Oct 1999.
Figure 1: Probability of measuring the solution to the search problem as a function of the number of oracle calls or equivalently, the number of applications of the Grover operators $p$ for 3 and 4 qubits. The same data is obtained using algorithms in definitions 3.1, 3.3 and 3.4. At the points of highest probability for the marked item, the variational algorithm obtains a slight advantage.

Figure 2: Probability of measuring the solution to the search problem as a function of the number of oracle calls or equivalently, the number of applications of the Grover operators $p$ for 3 and 4 qubits. The data was obtained using the algorithm in definition 3.2. At the points of highest probability for the searched item the advantage with Grover is lost.
Figure 3: (color online) (right) Grover’s algorithm takes a saddle point between two hills. Variational search recovers the hill peaks. Note that the valley becomes increasingly less pronounced past four qubits, providing negligible range for improvement. (left) Probability as a function of the variational angle for the 3 qubit case. Grover’s algorithm is recovered in the case $\alpha = \pi$, the variational algorithm obtains angles $\tilde{\alpha}_1 = 2.12^{\text{rad}}$ and $\tilde{\alpha}_2 = 2\pi - \tilde{\alpha}_1$

Table 1: Percentage increase between the highest probability for finding the solution after measurement obtained in Grover and the two-level variational ansatz. Percent given as a function of $N = 2^n$ where $n$ is the number of qubits and at step $p_{\text{max}}$ on which the probability of finding the solution string is maximum. The same table is obtained for the two-level split-operator ansatz with one angle or with $2p$ angles. Both the diffusion and oracle use the same angle.
Figure 4: Difference between variational and Grover. As the number of qubits grows there are exponentially diminishing oscillations in this difference. Each probability is defined for the optimal step in Grover’s algorithm for the number of qubits.

Figure 5: Circuit realization of diffusion and oracle circuits. Oracle and diffusion operators can be rewritten via $n$-body control gates $V(\alpha) = \bigotimes_{i=1}^{n} X_{i}^{1-\omega_{i}} \left( \mathbb{1}_{2^n-1} \oplus e^{i\alpha} \right) \bigotimes_{i=1}^{n} X_{i}^{1-\omega_{i}}$ and $K(\beta) = H^{\otimes n} X^{\otimes n} \left( \mathbb{1}_{2^n-1} \oplus e^{i\beta} \right) X^{\otimes n} H^{\otimes n}$ and therefore can be realized using $O(n^2)$ basic gates [1], here operator $\mathbb{1}_{2^n-1}$ is the $(2^n - 1) \times (2^n - 1)$ identity matrix. (See also the gate realizations in [5] which can be readily bootstrapped to realize (a) and (b) above).