Approximate Phase Search and Eigen-Estimation using Modified Grover’s Algorithm

Sayantan Pramanik, M Girish Chandra, Shampa Sarkar and Manoj Nambiar

TCS Research and Innovation, India

{sayantan.pramanik, m.gchandra, shampa.sarkar, m.nambiar}@tcs.com

Abstract—An attempt has been made in this paper to modify Grover’s Algorithm to find the binary string solutions approximating a target cost value. In that direction, new Controlled Oracle and the Local Diffusion Operator are suggested, apart from incorporating suitable ancilla qubits. A possible strategy to estimate eigenvalues and eigenstates of a given cost Hamiltonian, extending the reasoning of the methodology, is also pointed out. Typical results and relevant discussions are captured to support the propositions.

Index Terms—Grover’s algorithm, approximate search, phase oracle, global diffusion operator, local diffusion

I. INTRODUCTION

Grover’s Algorithm was one of the flagship algorithms that demonstrated a quantum advantage over its classical counter-part. Right from its proposition more than two decades ago, it has attracted undiminished interest and explorations from the Quantum Information Processing research community [2–[10], [15]. Many interesting extensions and modifications resulted out of this focus. In this paper, we considered the possibility of working out different (all) possible solutions of binary strings approximating the target cost of a function to varied degrees, within the context of combinatorial optimization setting. The idea is to pick up the solutions which satisfy the cost more closely with greater probability than others. In this direction, we propose a simple extension in terms of nonbinary phase oracles that append phases to the states based on the cost of the state, compared to the traditional binary marking in the original Grover’s Algorithm. Two more tricks appeared to be necessary to solve the problem- expansion of the search space using suitable number of ancilla qubits and a novel definition of what we refer as Local Diffusion Operator. As in other Grover- based algorithms, applying suggested nonbinary phase oracle (which is a controlled oracle) and the Diffusion operators successively, we obtained the useful amplitude amplification of the approximate states by measuring the requisite qubits in the computational bases, leaving out the ancillae. Another spin off this extension is to further parametrize the Control Oracle to estimate the eigenvalues and the corresponding eigenstates of the cost Hamiltonian.

The paper is organized as follows: In Section II necessary points on Grover’s Algorithm required as a base for our work are captured. Section III discusses at length the proposed method, including Control Oracle and Local Diffusion Operator. Some observations on the number of iterations required is also brought out. Section IV contains details about the eigen-estimation. The results achieved so far, relevant remarks and possible further examinations are discussed in Section V.

II. GROVER’S ALGORITHM

Grover’s Algorithm [1] addresses the problem of finding the needle in a haystack, i.e., searching for an element in an unstructured database. It provides a quadratic speedup over classical search algorithms, with a complexity of $O(\sqrt{N})$, where $N$ is the size of the database.

Given a database with $N$ entries, a set $\Omega$ of $k$ target states denoted by $\omega_j$, and an oracle that has the capability to identify and mark them, the algorithm finds and returns the marked elements with near-certain probability, with approximately $\sqrt{\frac{N}{k}}$ calls to the oracle.

Steps to follow in Grover’s algorithm:

1) Application of the Hadamard gate to place all the qubits in an equal superposition state $|s\rangle$.

2) Applying the oracle $O_G$ on the qubits:

$$O_G = I - (1 - e^{-i\alpha}) \sum_{j=1}^{k} |\omega_j\rangle \langle \omega_j|$$

3) Applying the diffusion operator $D$ to selectively increase the probability of obtaining the marked states through amplitude amplification:

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

4) Performing $r$ repetitions of steps 2 and 3, where $r$ is a function of $\alpha$, $\beta$, $k$, and $N$, and is in the order of $\sqrt{\frac{N}{k}}$.

It was identified by Long, et al. in [3], that the search algorithm is feasible only when $\alpha = \beta$, and the condition is known as phase-matching.

III. APPROXIMATE PHASE SEARCH

In this paper, we endeavour to solve the search problem spelt out in Section II which we also refer to as Approximate Phase Search using a modified version of Grover’s search algorithm. In literature there exists a technique named fuzzy string searching, also called the Approximate String Matching Algorithm (ASMA). As the name suggests, ASMA tries to find strings that are approximately related to a given string, which are found through insertion, deletion, substitution or transposition of certain characters within the original string. For instance, the words paste, past, part, pass, etc., can all be derived from the word past through the use of said operations.
Similar to its string counterpart, the approximate phase search algorithm attempts to solve an equivalent problem in the combinatorial regime. Given a set of bitstrings \( X = \{ x_j \} \), a function \( c(x_j) \) to calculate the cost of each bitstring, and a target cost \( c_0 \), the goal is to find the bitstring with cost closest to \( c_0 \) with the highest probability. More generally, the probability of measuring \( x_j \) after the algorithm, \( P(x_j) \) should be inversely proportional to \( |c(x_j) - c_0| \).

In [5], the authors talk about a variation of Grover’s algorithm where the target states are weighted. The method was devised so that the “probability of getting each target can be approximated to the corresponding weight coefficient \( w_j \).” With \( |q\rangle = \sum b_j |\omega_j\rangle \) being the weighted superposition of all the states, their oracle was defined as \( O_W = I - 2 |q\rangle \langle q| \), where:

\[
b_j = \begin{cases} \sqrt{w_j}, & \text{if } \omega_j \in \Omega \\ 0, & \text{otherwise} \end{cases}
\]  

However, there appear to be two major flaws in this approach. The first being that the oracle should have been \( O_W = I - 2 \sum |b_j|^2 |\omega_j\rangle \langle \omega_j| \). Even with the corrected oracle, it is not unitary if \( b_j \) is not a complex number with unit modulus.

Finally, it is worth mentioning that approximate phase search is principally different from the Grover-based optimization algorithms discussed in [6]–[8]. The optimization algorithms aim at obtaining the target states (having minimum cost, or equivalently, having cost \( c_0 \)) with as high a probability as possible, while effectively reducing the probability amplitudes of all the other states to zero. If a state with cost \( c_0 \) does not exist, then the optimization algorithms tend to fail. On the contrary, all the states in approximate phase search are potential solutions to the problem with varying measures of accuracy which are defined by their absolute deviation from the target cost. Higher the deviation, lower should be the probability of measuring the corresponding state. As a result, even if a state with the target cost does not exist, the closest possible match may be obtained from the algorithm.

A. Non-Binary Phase Oracles

Grover’s algorithm uses an oracle \( O_G \) that identifies and marks the elements being searched for with a negative sign. In the phase-matched version of the algorithm, the corresponding states are appended with a phase of \( \alpha \). Essentially, a binary-phase oracle is used which has the following effect:

\[
O_G(x) |x\rangle = e^{i\Pi(x)} |x\rangle
\]  

where \( \Pi(x) = 0 \) when \( x \notin \Omega \), or \( \Pi(x) = \alpha \) when \( x \in \Omega \). When \( \alpha = \pi \), we recover Grover’s original algorithm.

In the case of Approximate Search, we propose the use of non-binary phase oracles that append phases to the states based on their cost:

\[
O |x\rangle = e^{i\Phi(x)} |x\rangle
\]  

where \( \Phi(x) = f(c(x)) \) is a function which is designed in such a way that it depends on the cost of the state \( x \), and is scaled appropriately to append the phase \( \pi \) to the best solution states.

B. Expansion of Search Space

Grover’s algorithm acts by amplifying the amplitude of the states with phase \( \pi \). The amplification works by reducing the amplitudes of the non-targeted states, which reduces the probability of measuring them. In the context of search, most of the states are expected to have a non-zero phase and are potential solutions to the problem. This makes the redistribution of amplitude a formidable difficult task to accomplish. The difficulty can be overcome by expanding the search space through the use of ancilla qubits, which is unintuitive from the perspective of a search problem, but as demonstrated later, does not increase the order of complexity of the problem.

The ancillae are appended to the system and are ignored at the time of measurement, which acts as a form of marginalisation. In the light of the expanded search space, the oracle is converted into a controlled gate which acts on the work qubits only when all the ancillae are in the state \( |1\rangle \). The action of the controlled oracle \( O_C \) on a state \( |x\rangle \) in a system with \( m \) ancilla qubits, which are in the uniform superposition state \( |+\rangle_m \), can be represented as:

\[
O_C |x\rangle |+\rangle_m = \sum_{j=0}^{2^{m-2}} |x\rangle |j\rangle + e^{i\Phi(x)} |x\rangle |1\rangle_m
\]  

C. Local Diffusion Operator

The diffusion operator \( D \), defined by Grover, acts on all of the work-qubits to perform inversion about the mean. It has a global view of the system in the sense that it acts on all the states at the same time to perform the reflection operation. In a similar manner, we define a local diffusion operator \( D_L \) that has a local view of the system. If there are \( m \) ancilla qubits, then the local diffusion operator acts on \( 2^m - 1 \) states that do not have a phase, and only one state with a phase associated with it. Thus, it works only in the locality of the superposition states of the ancilla qubits for a given state of the work qubits. The local diffusion operator being proposed here is not the same as the partial diffusion operator discussed in [9].

The local diffusion operator is a block-diagonal, \( 2^{m+n} \times 2^{m+n} \) unitary matrix with \( 2^n \times 2^m \) dimensional diffusion operators forming its diagonal elements, when the ancilla qubits are present at the end of the system.
\[ D_L = 2 \sum_{j=0}^{2^n-1} |j\rangle + \rangle_m \langle +_m |j\rangle - I \]
\[ = 2 \sum |j\rangle + \rangle_m \langle +_m |j\rangle - \sum_{j=0}^{2^n-1} \sum_{j'=0}^{2^n-1} |j\rangle |j'\rangle \langle j'\rangle \langle j| \]
\[ = 2 \sum |j\rangle \langle j| \otimes |+\rangle_m \langle +_m - \sum |j\rangle \langle j| \otimes \sum |j'\rangle \langle j'| \]
\[ = 2^{n-1} \sum |j\rangle \langle j| \otimes (2^0 + \rangle_m \langle +_m - I) \]
\[ = I \otimes (2^0 + \rangle_m \langle +_m - I) \]

From Equation (7) it is clear that the local diffusion operator is analogous to its global counterpart working on just the ancilla qubits on the system. Since the local diffuser acts on groups of \(2^m\) states, it is imperative to have at least two ancillae, as it is known that performing diffusion on only one qubit does not provide any measurable advantage in the computational basis. Application of operators \(O_C\) and \(D_L\) in succession \(\lceil \frac{n}{4} \sqrt{2^m} \rceil\) times acts as a preprocessing step. It increases the amplitude of the states with phase \(\pi\) (i.e., the solution states) from \(\frac{1}{\sqrt{2^m+\pi}}\) (in the equal superposition state at the start of the algorithm) to nearly \(\frac{1}{\sqrt{2^m}}\). Parallely, it also amplifies the states in which the ancilla qubits are in \(|1\rangle_m\) at the cost of others.

**D. Overview of the Approximate Phase Search Algorithm**

Having discussed about all the components required by the approximate phase search algorithm, it might now be ideal to list down the requisite steps for a complete overview of the algorithm:

1) Initialization of a quantum circuit with two quantum registers, one with \(n\) work qubits and the other with \(m\) ancilla qubits, along with a classical register containing \(n\) classical bits.
2) Bringing the system to equal superposition through the use of \(H\) gates on all of the qubits.
3) Repetition of the following steps \(\lceil \frac{n}{4} \sqrt{2^m} \rceil\) times, which carries out the requisite preprocessing:
   a) Application of the controlled-oracle with the ancillae as control and the work qubits as the target.
   b) Followed by the application of the local diffusion operator.
4) Looping over the following two steps \(N_{iter}\) times:
   a) Again, applying the oracle as discussed in the previous point.
   b) Application of the global diffusion operator, this time, on all the qubits in the system.
5) Measurement of the \(n\) work qubits into the \(n\) classical bits.

The ideal number of ancillae, \(m\), and iterations, \(N_{iter}\), required for the optimal performance of the algorithm is subject to further research. As there are \(2^n\) possible phases appended by the oracle, as opposed to just two in Grover’s traditional algorithm, that interfere with each other, it is suspected that the ideal number of iterations may not have a closed-form solution. Additionally, the degeneracy of the system need to be considered to find \(N_{iter}\). To that extent, a generalized version of the Quantum Counting Algorithm [10] for multiple phases needs to be designed, and is beyond the scope of this work. To simplify the application and to demonstrate the feasibility of the algorithm, we empirically set \(m = n\), and \(N_{iter} = \sqrt{2^m}\), which yields consumable, if not the best, results.

The circuit for the complete scheme for \(n = m = 2\) qubits can be found in Figure [1]

**E. Kullback-Leibler Divergence as a Performance Metric**

Kullback-Leibler Divergence (in short, KLD) is a metric used to compare two probability distributions, i.e., the extent to which the given distributions differ from each other. Its value ranges between 0 and \(\infty\), 0 when the two distributions are exactly identical. Given two distributions, \(P(x)\) and \(Q(x)\), the KLD between them is specified by:

\[ D_{KL} = \sum_j P(x_j) \log \left( \frac{P(x_j)}{Q(x_j)} \right) \]

After running Grover’s algorithm for multiple shots, the final, normalised histogram of measurements can be treated as a probability distribution, \(P(x)\). The other distribution in question, \(Q(x)\), is the histogram obtained from an equal superposition of all the the states, and is basically an uniform distribution. The reason behind selecting the uniform distribution to compare \(P(x)\) against is that the performance of any variant of Grover’s algorithm relies on the ability of the oracle to properly mark the target states (with various phases, in our case). Failing to appropriately mark the states will result in none of them getting selectively amplified, yielding the uniform distribution as a result. This allows us to use \(D_{KL}\) as a measure of success of the algorithm, provided that the state achieved with highest probability is one of the targeted states.

It must also be noted that the KLD metric reduces with the introduction of degeneracy into the system. As a general rule, higher the degeneracy, lower is the value of KLD.

**IV. Eigen-Estimation Using the Proposed Approximate Phase Search**

Given a cost Hamiltonian, \(H_C\), we attempt to find its eigenvalues and corresponding eigenvectors (for ground and excited states) by leveraging the approximate phase search algorithm that has been described thus far. To accomplish that, a parameterized oracle with parameter \(\lambda\) is defined as:

\[ O_{H_C} = e^{i\pi H_C / \lambda} \]

If the Hamiltonian \(H_C\) is Hermitian, then the oracle \(O_{H_C}\) is guaranteed to be unitary for real values of \(\lambda\). The oracle can be converted to a controlled one as discussed in subsection [II-B]. If the eigenvalues and eigenvectors of \(H_C\) are given by \(\lambda_j\) and \(|\psi_j\rangle\), then \(O_{H_C}\) can be written in the form:
A. Construction of Local Diffuser

As discussed in section III-C and as evident from Equation (7), the local diffusion operation, on a system of $n$ work qubits and $m$ ancilla qubits alone.

Figure 2 shows the gate-circuit implementation for a simple system with six qubits, three of them used to encode the problem, and the other three to increase the dimension of the search space, formulated in Section III-B. The $H$ and $X$ gates can be merged for a more efficient circuit with lesser depth, as suggested in [15]. Also, the $U1$ gate has a parameter of $\pi$.

B. A Variation of Subset-Sum Problem

Given a set of $n$ real numbers, $\xi = \{s_0, s_2, \ldots, s_{n-1}\}$, the problem is to find $\zeta \subseteq \xi$ such that the sum of elements in $\zeta$ is as close as possible to a given real number $S$. Trivially, $2^n$ subsets of $\xi$, can be represented by the binary strings $\{0, 1\}^n$, where each bitstring $x_j = y_0 \ldots y_{n-1}$; $y_i = 1$ if the element $s_i$ is present in the $j^{th}$ subset, and $y_i = 0$ otherwise. The cost $c(x_j)$ of the bitstring $x_j$ is given by $c(x_j) = \sum_{l=0}^{n-1} s_l y_l$.

To construct the oracle for this problem, the function $\Phi(x_j)$ in Equation (12) is chosen such that it linearly scales the cost to map $c(x_j) = S$ to the phase $\pi$. It has the disadvantage that if $c(x_j)$ is an odd multiple of $S$, the effective phase evaluates to $\pi$. As a simple example, let $\xi = \{2, 3, 4, 8\}$ and $S = 9$. The oracle and results have been portrayed in Figures 34 and 35 respectively. It can be seen that state $|1110\rangle$ with the highest probability has a cost of 9, and the second and third most probable states have costs of 10 and 8, each. It is evident that our new algorithm is able to search the approximate solutions.

$$\Phi(x_j) = \pi \frac{c(x_j)}{S}$$ (12)

C. Max-cut Problem

The max-cut problem starts with an undirected graph $G(V, E)$ with a set of vertices $V$ and a set of edges $E$ between the vertices. The weight $w_{jl}$ of an edge between vertices $j$ and $l$, is a positive real number, with $w_{jl} = 0$ if there is no edge between them. A cut is a set of edges that separates the vertices $V$ into two disjoint sets $V_1$ and $V_2$, such that $V_1 \subseteq V$ and $V_2 = V \setminus V_1$, and the cost of a cut is defined as the sum of all weights of edges connecting vertices in $V_1$ with vertices in $V_2$. One define a cut for the graph by labelling
the vertices with $s_j$ such that $s_j = 1$ suggesting that node $j$ belongs to $V_1$ and $s_j = 0$ corresponds to $V_2$ (of course, $V_1$ and $V_2$ can be interchanged). The cost Hamiltonian for the max-cut problem is specified as [20]:

$$H_C = \sum_{jl} w_{jl} (I - \sigma^z_j \sigma^z_l).$$

The aim is to partition the nodes in such a way that the cost of the resulting cut is maximized. The cost Hamiltonian can be used to construct the oracle by leveraging Equation (9). This step is tricky for problems like max-cut where the cost of the best cut is not known beforehand. If the max-cost is known and is equal to $C_{\text{max}}$, then $\lambda$ is set equal to $C_{\text{max}}$. Otherwise, the strategy to circumvent this barrier is to start with the observation that bipartite graphs have the highest possible max-cut cost, which is equal to the sum of all the weights of the edges in the graph. Then setting $\lambda = \sum_{jl} w_{jl}$, there is a hope that the state with highest cost is amplified to a greater extent towards higher probability of occurrence. Of course, one can expect the deterioration of performance with increasing difference between $\lambda$ and the highest cost. For max-cut, too, the graph structure, oracle, and results for $\lambda = 6$ are demonstrated for a toy problem (due to size constraints on the quantum circuit) in Figures 4a, 4b and 5, respectively. The results do show the possibility of identifying the correct states in this toy example.

**D. Finding Eigenvalues**

For the eigen-estimation, we return to the subset-sum problem where we attempted to find the eigenvalues for the corresponding problem Hamiltonian in Equation (14):

$$H_C = \sum_j s_j Z_j$$

where $s_j$ is the $j^{th}$ element in $\xi$, $Z = (I - \sigma^z)/2$ and $Z_j$ is the appropriate tensor product of $I$ and $Z$. A set $\xi = \{1, 1, 1, 1, 1, 1\}$ was considered, and it is trivial to see that the set of eigenvalues are $\Lambda = \{0, 1, 2, 3, 4, 5, 6, 7\}$, with each eigenvalue $\lambda_j$ having a degeneracy of $k_j = \binom{7}{j}$. The plot for Kullback-Leibler Divergence against $\lambda$ has been shown
Fig. 5: Histogram of max-cut results for the graph in 4a

Fig. 6: Plot of KLD against $\lambda$, where peaks can be seen when the value of $\lambda$ becomes equal to an eigenvalue of the system. In Figure 6, which was obtained on looping over values of $\lambda$ with a small step-size $\epsilon$, the number of global iterations were set to $\sqrt{N/k} \pm 1$ and the best values were captured in the plot. Additional measures had to be taken to curtail the effects of higher harmonics, as discussed in Section V-B. Some anomalies still appear in the plot, such as the abnormally high peak for $\lambda_j = 2$, and the decaying values for $\lambda_j = 6$ and $\lambda_j = 7$. Finally, it needs to be mentioned that comparably good results for eigen-estimation were obtained when all the elements in the set $\xi$ were equal. With arbitrary values, the effect of interference dominated the plot and the algorithm needs to be investigated further for improvements.

VI. CONCLUSION

An effort has been made in this paper to arrive at suitable modifications to the standard Grover’s Algorithm to get different possible binary strings as solutions for approximating the target cost of a function within the context of combinatorial optimization; they approximate the cost to different extents. The relevant results of the proposal for subset-sum and max-cut demonstrate the applicability and usefulness of the research. The methodology also facilitates the estimation of eigenvalues and eigenstates of the cost Hamiltonian, but needs additional examination towards obtaining good results in different scenarios. Further study is also underway to strengthen the present empirical suggestion for the number of iterations.

VII. ACKNOWLEDGEMENT

The authors sincerely thank Dr. Gautam Shroff, Head, TCS Research, for his encouragement and support.

REFERENCES

[1] L.K. Grover, “A fast quantum mechanical algorithm for database search,” Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212.
[2] L. GuiLi, Z. WeiLin, L. YanSong and N. Li, “Arbitrary phase rotation of the marked state cannot be used for grover’s quantum search algorithm,” 1999 Commun. Theor. Phys. 32 335.
[3] G.L. Long, Y.S. Li, W.L. Zhang, L. Niu, “Phase matching in quantum searching,” Physics Letters A, vol. 262, 1999.
[4] F.M. Toyama, W. van Dijk, Y. Nogami, M. Tabuchi, Y. Kimura, “Multi-phase matching in the grover algorithm,” Physical Review A, (Apr 2008), vol. 77.
[5] L. Panchi and L. Shiyong, “Grover quantum searching algorithm based on weighted targets,” in Journal of Systems Engineering and Electronics, vol. 19, no. 2, pp. 363-369, April 2008, doi: 10.1016/S1004-4132(08)60093-6.
[6] W. P. Baritompa, D. W. Bulger, and G. R. Wood, “Grover’s quantum algorithm applied to global optimiza- tion,” SIAM J. on Optimization 15, 1170–1184 (2005).
[7] D. Bulger, W. P. Baritompa, and G. R. Wood, “Im- plementing pure adaptive search with grover’s quantum algorithm,” Journal of Optimization Theory and Appli- cations 116, 517–529 (2003).
[8] A. Gilliam, S. Woerner, C. Gonciulea, “Grover adaptive search for constrained polynomial binary optimization,” [arXiv:1912.04088] [quant-ph]
[9] A. Younes, J. Rowe, and J. Miller, “Quantum search algorithm with more reliable behaviour using partial diffusion,” AIP Conference Proceedings 734, 171 (2004).
[10] G. Brassard, P. Hoyer, A. Tapp, “Quantum Counting,” Lecture Notes in Computer Science (1998), Springer Berlin Heidelberg, p. 820–831.
[11] A. Peruzzo, J. McClean et al., “A variational eigenvalue solver on a photonic quantum processor”. Nature Communications 5, 4213 (2014).
[12] E. Farhi, J. Goldstone, S. Gutmann, “A quantum approximate optimization algorithm”. [arXiv:1411.4028] [quant-ph].
[13] O. Higgott, D. Wang, S. Brierley, “Variational quantum computation of excited states”. Quantum, vol. 3, (July 2019), p. 156.
[14] H. Abraham et. al., “Qiskit: an open-source frame- work for quantum computing,” (2019).
[15] A. Gilliam, M. Pistoia, C. Gonciulea, “Optimizing quantum search using a generalized version of grover’s algorithm,” [arXiv:2005.06468] [quant-ph].
[16] L. Tse, P. Mountney, P. Klein, S. Severini, “Graph Cut Segmentation Methods Revisited with a Quantum Algorithm,” [arXiv:1812.03050]