QAOA for the Grover problem with multiple marked items

Aniruddha Bapat

1 Introduction

We consider the analog version of Grover's algorithm for a number of marked items m that is unknown. The goal is to achieve a generalization of the work done in [2, 3] on analog Grover algorithm with one marked item. In the analog version, we use a *Hamiltonian* oracle C which is diagonal in the item basis and assigns energies of -1 to marked items and 0 to unmarked items:

$$C = -\sum_{i=0}^{m-1} |\mathbf{x_i}\rangle\langle\mathbf{x_i}| \tag{1}$$

where $\mathbf{x_i}$ are bitstrings labeling the marked items. In standard Grover, the other unitary operator used is reflection about the equal superposition state $|\psi\rangle$. A direct analog analogue would be to use the Hamiltonian that generates this unitary under a π rotation,

$$H = \mathbb{1} - |\psi\rangle\langle\psi| \tag{2}$$

In the past, (2) has been used as the mixing operator for analog Grover, e.g. in [1, 4]. However, this operator is not local and practical implementations which decompose one application of it into two-qubit gates will considerably increase the gate depth of the circuit. Therefore, the use of a local mixing operator, such as the transverse field Ising Hamiltonian used in [2, 3], is practically well-motivated. While this does not guarantee an efficient gate decomposition for the oracle, it removes additional overheads in gate complexity from the part of the circuit outside the black box. Therefore, we will this mixer, up to an energy shift of n:

$$B = n\mathbb{1} - \sum_{i=1}^{n} X_i \tag{3}$$

Perhaps surprisingly, the Grover speed-up can be shown in this restricted computational model of using the Hamiltonian oracle and only 1-local operations in addition, in the case where there is only one marked item. For the case of multiple marked items, both [2, 3] observed that the performance of QAOA seemed to depend on the Hamming distances between the marked items. In this work, we provide a concrete theoretical characterization of this dependence, and, by understanding how it affects the QAOA protocol, provide a way to make QAOA with the 1-local mixer succeed on multple-marked item instances.

2 Background and notation

Before starting calculations for the multiple marked item case, here are some additional notes on notation and lemmas to be used:

1. For any positive integer n, we use the shorthand $[n] := \{0, 1, \ldots, n\}$. Replacing the left or right bracket by a parenthesis will correspond to excluding either 0 or n from the set, so that $(n] = \{1, \ldots, n\}$. In particular, $[1] = \{0, 1\}$, and $[1]^n$ is the set of all n-length bitstrings.

2. We will always denote bitstrings by boldface variables, such as $\mathbf{x}, \mathbf{z}$ etc. The bits in a given bitstring will be denoted by the corresponding plain variable indexed by the position of the bit. So, we have $\mathbf{x} = x_1 x_2 \cdots x_n$, $\mathbf{x} = z_1 z_2 \cdots z_n$, etc., with $x_i, z_i \in [1]$. The all-zero and all-one bitstrings will be denoted by $\mathbf{0} = 00 \cdots 0$ and $\mathbf{1} = 11 \cdots 1$, respectively. Lastly, the *Hamming weight* of a bitstring $\mathbf{z}$ is the 1-norm of $\mathbf{z}$, or, the number of ones in $\mathbf{z}$. It will be denoted by $|\mathbf{z}|$, or simply z when clear from context.

3. It will be convenient to introduce the following notation: for any bitstring $\mathbf{z} \in [1]^n$, the corresponding *bit flip operator* will be denoted $X^{\mathbf{z}} := \bigotimes_{i=1}^{n} X^{z_i}$. So,

$$X^{\mathbf{z}} |\mathbf{y}\rangle = |\mathbf{y} \oplus \mathbf{z}\rangle$$

   and in particular, $|\mathbf{z}\rangle = X^{\mathbf{z}} |\mathbf{0}\rangle$. Finally, for the Grover problem with m marked items labelled $\mathbf{x_0}, \mathbf{x_1}, \ldots, \mathbf{x_{m-1}}$, define $\bar{X} := \sum\limits_{i=0}^{m-1} X^{\mathbf{x_i}}$. (Note that each of the $\mathbf{x_i}$ are bitstrings, not bits.)

4. In the bit shift notation, the Hamiltonian oracle and corresponding unitary can be expressed

$$C = -\sum_{i=0}^{m-1} X^{\mathbf{x_i}} |\mathbf{0}\rangle\langle\mathbf{0}| X^{\mathbf{x_i}} \tag{4}$$

$$e^{-i\gamma C} = \mathbb{1} - \omega_\gamma \sum_{i=0}^{m-1} X^{\mathbf{x_i}} |\mathbf{0}\rangle\langle\mathbf{0}| X^{\mathbf{x_i}} \tag{5}$$

   where we set $\omega_\gamma := 1 - e^{i\gamma}$.

5. We will use the shorthand $\mathcal{C}(\gamma) = e^{-i\gamma C}$, and $\mathcal{B}(\beta) = e^{-i\beta B}$. Further, $\mathcal{C} \equiv \mathcal{C}(\pi) \equiv \mathcal{C}(-\pi)$.

6. The two unitaries $\mathcal{B}, \mathcal{C}$ act on the equal superposition in the following manner:

$$\mathcal{B}(\beta) |\psi\rangle = |\psi\rangle \tag{6}$$

$$\mathcal{C}(\gamma) |\psi\rangle = |\psi\rangle - \frac{\omega_\gamma}{\sqrt{N}} \sum_{i=0}^{m-1} |\mathbf{x_i}\rangle = |\psi\rangle - \frac{\omega_\gamma}{\sqrt{N}} \bar{X} |\mathbf{0}\rangle \tag{7}$$

$$\text{In particular, } \mathcal{C}|\psi\rangle = |\psi\rangle - \frac{2}{\sqrt{N}} \bar{X} |\mathbf{0}\rangle \tag{8}$$

7. It will be useful to know how $\mathcal{B}(\beta)$ acts on the $|\mathbf{0}\rangle$ state. While the exact form is derived in appendix B, we first observe that the diffusion operator preserves *Hamming symmetry*: if the initial state is invariant under bit permutations, then so is the final state. Since $|\mathbf{0}\rangle$ is a Hamming symmetric state, it must be possible to write $\mathcal{B}(\beta) |\mathbf{0}\rangle$ as a sum over symmetrized states of Hamming weight w given by

$$|w\rangle := \frac{1}{\sqrt{\binom{n}{w}}} \sum_{|\mathbf{x}|=w} |\mathbf{x}\rangle \tag{9}$$

Therefore,

$$\mathcal{B}\left(\beta\right)|\mathbf{0}\rangle = \sum_{w=0}^{n} f(w)|w\rangle \tag{10}$$

for some function f which, as mentioned, is derived in Appendix B.

8. Finally,

$$\mathcal{B}\left(\beta\right)\mathcal{C}\left(\gamma\right)|\psi\rangle = |\psi\rangle - \frac{\omega_\gamma}{\sqrt{N}}\bar{X}\sum_{w=0}^{n} f(w)|w\rangle \tag{11}$$

where $f(w)$ is as defined in the previous point, and we implicitly used the fact that $\mathcal{B}$ and $\bar{X}$ are diagonal in the Pauli X basis, and there mutually commute. Next, we write this expression in a more suggestive form. Noting that the equal superposition state is invariant under the $\bar{X}$ operator up to a factor of m,

$$|\psi\rangle = \frac{1}{m}\bar{X}|\psi\rangle$$

we have in the symmetric basis

$$|\psi\rangle = \bar{X}\sum_{w=0}^{n}\frac{\sqrt{\binom{n}{w}}}{m\sqrt{N}}|w\rangle$$

Then, collecting terms in Eq. 11,

$$\mathcal{B}\left(\beta\right)\mathcal{C}\left(\gamma\right)|\psi\rangle = \bar{X}\sum_{w=0}^{n} g(w)|w\rangle \tag{12}$$

where

$$g(w) = \frac{1}{\sqrt{N}}\left(\frac{\sqrt{\binom{n}{w}}}{m} - \omega_\gamma f(w)\right)$$

Therefore, we see that after one QAOA iteration, the support of the state is on what we may call the *displaced symmetric subspace* (DSS) spanned by the states $\{X^{\mathbf{x_i}}|w\rangle : i \in [m], w \in [n]\}$. A total of $m(n+1)$ states span the DSS, and its dimension is therefore much smaller than the full Hilbert space dimension N, when $m \ll N$. This is a key observation, and is discussed further in Sec. 3.1. We will call the form of writing the state as in Eq. 12 the canonical form.

Lastly, we give a quick review of the single-marked item QAOA protocol used in [2].

- Start in the equal superposition state $|\psi\rangle \equiv |+\rangle^{\otimes n}$.
- Apply the unitary $W\left(\beta,\gamma\right) = e^{-i\beta B}e^{i\gamma C}e^{-i\beta B}e^{-i\gamma C}$ for a total of $O(\sqrt{N})$ iterations.
- Measure in the computational basis. The expected success probability is (asymptotically) 0.5.

So, there are $O(\sqrt{N})$ rounds, each consisting of four unitary gates $e^{-i\gamma C}, e^{-i\beta B}, e^{i\gamma C}, e^{-i\beta B}$ (to be applied in that order). While β, γ are parameters to be optimized, the choice $\gamma = \pi, \beta = \pi/n$ is shown to be successful at finding the marked state. The same protocol is not guaranteed to succeed for the case of multiple marked items, since the analysis becomes considerably harder and involves the knowledge of the Hamming distances between the marked items. In the following work, we make this dependence precise [WELL, NOT 100% THERE YET], and argue that it can be made sufficiently "tame", allowing the single-marked item protocol to apply to the general case. And now, we now present the main ideas that make this generalization possible, without further ado.

3 QAOA for multiple marked item Grover

In the last section, it was observed that after one QAOA iteration, the state can be written in the canonical form of Eq. 12. It would be nice if this statement could hold for further QAOA iterations as well. In that case, we could keep track of the state overlap on the support subspace efficiently in n, and compute the success probability at the end of T iterations, for an arbitrary T. For a successful Grover protocol, $T \sim O(\sqrt{N})$, so the entire computation would have the same time complexity as the query complexity of Grover, up to log factors. This "one-time cost" would hopefully guide the QAOA parameter setting for all future Grover instances.

Unfortunately, this hope is squandered in the very next step of QAOA, for a general problem instance. We have

$$\mathcal{C}\left(\gamma'\right)\mathcal{B}\left(\beta\right)\mathcal{C}\left(\gamma\right)|\psi\rangle = \mathcal{C}\left(\gamma'\right)\bar{X}\sum_{w=0}^{n} g(w)|w\rangle \tag{13}$$

In order to evaluate this expression further, note that the operator $\mathcal{C}\left(\gamma'\right)$ applies a trivial phase of 1 to all un-marked item states, and a phase of $e^{i\gamma'}$ to all marked item states. Therefore, we only need to isolate the marked states in the expression, and then we can write

$$\mathcal{C}\left(\gamma'\right)\mathcal{B}\left(\beta\right)\mathcal{C}\left(\gamma\right)|\psi\rangle = \bar{X}\sum_{w=0}^{n} g(w)|w\rangle - \omega_{\gamma'}\cdot\left[\bar{X}\sum_{w=0}^{n} g(w)|w\rangle\right]_{\text{marked only}} \tag{14}$$

Now, the expression $\bar{X}\sum\limits_{w=0}^{n} g(w)|w\rangle$ can be expressed as a sum over the bitstrings $|\mathbf{z}\oplus\mathbf{x_i}\rangle$ for all $\mathbf{z}\in[1]^n$, and for all $i = 0,\ldots,m-1$. Explicitly,

$$\bar{X}\sum_{w=0}^{n} g(w)|w\rangle = \sum_{i=0}^{m-1}\sum_{\mathbf{z}\in[1]^n}\frac{g\left(z\right)}{\sqrt{\binom{n}{z}}}|\mathbf{z}\oplus\mathbf{x_i}\rangle$$

From the above sum, we wish to look at bitstrings that correspond to marked states. In other words, we are interested in strings $\mathbf{z}$ s.t. $\mathbf{z}\oplus\mathbf{x_i} = \mathbf{x_j}$ for some i, j. Since bitwise addition is involutive, the set of such strings $\mathbf{z}$ is precisely $\{\mathbf{d_{ij}} := \mathbf{x_i} \oplus \mathbf{x_j} : i, j \in [m)\}$. Therefore, Eq. 14 becomes

$$\mathcal{C}\left(\gamma'\right)\mathcal{B}\left(\beta\right)\mathcal{C}\left(\gamma\right)|\psi\rangle = \bar{X}\sum_{w=0}^{n} g(w)|w\rangle - \omega_\gamma \sum_{i,j} \frac{g\left(d_{ij}\right)}{\sqrt{\binom{n}{d_{ij}}}}|\mathbf{x_j}\rangle \tag{15}$$

$$= \bar{X}\sum_{w=0}^{n} g(w)|w\rangle - \omega_\gamma \underbrace{\left(\sum_{i,j} \frac{g\left(d_{ij}\right)}{\sqrt{\binom{n}{d_{ij}}}} X^{\mathbf{x_j}}\right)}_{\tilde{X}}|\mathbf{0}\rangle \tag{16}$$

Now we see the problem: if the operator $\tilde{X}$ (marked by the underbrace) is proportional to $\bar{X}$, then the above state is expressible in the canonical form, since the state $|\mathbf{0}\rangle \propto |w = 0\rangle$ is already a symmetric state. However, if $\tilde{X}$ is not proportional to $\bar{X}$ (which it isn't in general), the state has different amplitudes on different $X^{\mathbf{x_j}}$, and can no longer be written in the canonical form.

However, notice that the state still has support only on the displaced symmetric states $X^{\mathbf{x_i}}|w\rangle$. In fact, the next step of applying $\mathcal{B}(\beta)$ (and indeed all future QAOA steps) will preserve this property of the state. While this form isn't as compact as Eq. 12, it is indeed a low-rank description of the state when $m \ll N$. In the coming section, we will describe the QAOA dynamics in this reduced state description. Later in Sec. 3.2, we will argue that the canonical form can in fact be recovered if we impose a condition known as *homogeneity* for the marked item distribution.

3.1 Reduction to the Displaced Symmetric Subspace (DSS)

Let us introduce a slightly overloaded but helpful notation for the displaced symmetric state,

$$X^{\mathbf{x}}|w\rangle := |w \oplus \mathbf{x}\rangle, \quad \text{for some Hamming weight } w\text{, and string } \mathbf{x}. \tag{17}$$

To recap, the DSS is the space spanned by the above states, i.e.,

$$\mathrm{DSS} = \mathrm{span}\left\{|w \oplus \mathbf{x_i}\rangle : w \in [n], i \in [m)\right\} \tag{18}$$

Since we know that a general QAOA protocol has a low-rank description on the DSS, we will constrain our notation to reflect this fact. At step t of the QAOA protocol (where each step is an application of $\mathcal{C}$ followed by an application of $\mathcal{B}$), let the state be given by

$$|\psi_t\rangle = \sum_{w\in[n], i\in[m)} A^{(t)}_{wi}|w \oplus \mathbf{x_i}\rangle \tag{19}$$

After "t and a half" steps, i.e., after t full steps of QAOA and an additional application of $\mathcal{C}$, call the state

$$|\psi_{t.5}\rangle = \sum_{w\in[n], i\in[m)} A^{(t.5)}_{wi}|w \oplus \mathbf{x_i}\rangle \tag{20}$$

So, we now have to keep track of how the rank-2 tensor A_{wi} of dimension $m(n+1)$ evolves during QAOA. Under $\mathcal{C}\,(\gamma)$ and $\mathcal{B}\,(\beta)$, we have

$$A_{wi} \xrightarrow[\mathcal{C}(\gamma)]{} \begin{cases} A_{0i} - \omega_\gamma \sum\limits_{j\in[m]} \frac{A_{a_{ij}j}}{\sqrt{\binom{n}{a_{ij}}}}, & \text{if } w = 0 \\ A_{wi}, & \text{if } w > 0. \end{cases} \tag{21}$$

$$A_{wi} \xrightarrow[\mathcal{B}(\beta)]{} \sum_{v\in[n]} \mathcal{D}(\beta)_{wv} A_{vi}. \tag{22}$$

where $\mathcal{D}(\beta)$ is the diffusion operator on the symmetric subspace (see Appendix B). So, we see that the DSS dynamics depend on the distribution of the Hamming distances of all marked states from one another, i.e. the distances d_{ij} for $i, j \in [m]$.

Now, we write the action of operators $\mathcal{B}, \mathcal{C}$ in terms of matrices acting on the representation of the state in the DSS, taking directly from Eq. 22 and 21. We label the corresponding matrices $\tilde{\mathcal{B}}, \tilde{\mathcal{C}}$. First, let χ^w be an $(n+1)\times(n+1)$ matrix with $\frac{1}{\sqrt{\binom{n}{w}}}$ in the $(0,i)$-th entry, and zeros elsewhere, i.e.,

$$\chi^w := \begin{pmatrix} 0 & \overbrace{\cdots}^{w} & \frac{1}{\sqrt{\binom{n}{w}}} & \overbrace{\cdots}^{n-w} & 0 \\ 0 & \ddots & \cdots & \cdots & 0 \\ \vdots & \cdots & 0 & \cdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \tag{23}$$

Recall that $\mathcal{D}$ is the diffusion matrix on the symmetric subspace spanned by $\{|w\rangle : w \in [n]\}$. With these auxiliary matrices, we can write

$$\tilde{\mathcal{B}}(\beta) = \begin{pmatrix} e^{-i\beta\mathcal{D}} & & & \\ & e^{-i\beta\mathcal{D}} & & \\ & & \ddots & \\ & & & e^{-i\beta\mathcal{D}} \end{pmatrix} \tag{24}$$

$$\tilde{\mathcal{C}}(\gamma) = \mathbb{1} - \omega_\gamma \begin{pmatrix} \chi^{d_{00}} & \chi^{d_{01}} & \cdots & \chi^{d_{0(m-1)}} \\ \chi^{d_{10}} & \chi^{d_{11}} & \cdots & \chi^{d_{1(m-1)}} \\ \vdots & \cdots & \ddots & \vdots \\ \chi^{d_{(m-1)0}} & \chi^{d_{(m-1)1}} & \cdots & \chi^{d_{(m-1)(m-1)}} \end{pmatrix} \tag{25}$$

$$=: \mathbb{1} - \omega_\gamma \mathcal{P} \tag{26}$$

where there are m blocks in each row an column of the above matrices, and each block is of dimensions $(n+1)\times(n+1)$. So, we see that both matrices have sparse structure. Finally, we will show that $\mathcal{P}$, defined above, is in fact an idempotent operator, i.e., $\mathcal{P}^2 = \mathcal{P}$. This will allow us to write $\tilde{\mathcal{C}}(\gamma) = e^{-i\gamma\mathcal{P}}$. [NOT SURE IF THIS IS USEFUL; OH WELL, SEEMS LIKE A NICE PROPERTY.]

Lemma 1. *The matrix $\mathcal{P}$, defined in Eq. 26, is idempotent, i.e., $\mathcal{P}^2 = \mathcal{P}$.*

Proof. The (i,j)-th entry of the product $\mathcal{P}^2$ may be expressed as

$$[\mathcal{P}^2]_{ij} = \sum_k \chi^{d_{ik}}\chi^{d_{kj}} \tag{27}$$

So, we need to know the form of the product $\chi^w\chi^v$ for two arbitrary weights $w, v \in [n]$. However, the sparseness of the χ matrices yields the simple expression

$$[\chi^w\chi^v]_{ij} = \delta_{i0}\delta_{jv}\delta_{w0}\frac{1}{\sqrt{\binom{n}{w}}}\frac{1}{\sqrt{\binom{n}{v}}} \implies \chi^w\chi^v = \delta_{w0}\chi^v \tag{28}$$

Secondly, we use the property that two marked items indexed i, k have Hamming distance $d_{ik} = 0$ if and only if $i = k$ (that is, iff they are in fact the same item). Then, we have

$$[\mathcal{P}^2]_{ij} = \sum_k \chi^{d_{ik}}\chi^{d_{kl}} = \chi^0\chi^{d_{ij}} = \chi^{d_{ij}} = [\mathcal{P}]_{ij} \tag{29}$$

for all marked indices i, j. Therefore, $\mathcal{P}^2 = \mathcal{P}$ and the proof is complete. □

We point out that in the special case where we fix $\beta_t = \beta$ and $\gamma_t = \gamma$ for all steps t, the full Grover operator becomes $\left(\mathcal{B}\left(\beta\right)\mathcal{C}\left(\gamma\right)\right)^T$, which can be computed in time $O(\text{poly}(n))$ by exact diagonalization. This simplification is well-motivated, since the original one-marked item QAOA protocol involves identical β, γ at each step.

Looking at Eq. 21, 22, we see that if all the marked items were distributed identically w.r.t any given marked item, then the dynamics of A_{wi} would be identical for all i. This property would then allow us to "collapse" the state description even further, and we would essentially recover the canonical form of Eq. 12. We call this property homogeneity, and discuss it in the next section.

3.2 Marked items are mutually homogeneous

In this simplification, we assume that for any marked string $\mathbf{x_i}$, there is a distribution $p_w, w \in [n]$ such that the number of strings $\mathbf{x}_j$ at a distance w from $\mathbf{x_i}$ is p_w, and $p_0 = 1$ by default. Therefore, the distribution of the marked strings is "homogeneous" in that it appears identical from the perspective of any marked string. In other words, $\{d_{ij} : j \in [m)\}$ is the same set for every i. Note that homogeneity is not exactly a special case of the previous section, since m can be large here.

While it may seem artificial, homogeneity (or at least, approximate homogeneity) is well-motivated. This is because asymptotically in n, the distance between two randomly chosen bit-strings is sharply peaked around $n/2$ and follows a binomial distribution. When $m \ll N$, and the marked items are distributed typically (or pre-permuted so as to have a typical distribution), every distance d_{ij} can be assumed to be an independent sample of the same binomial distribution. For each i, the m samples d_{ij}, for $j \in [m)$, will then trace out the same sharply peaked binomial distribution, and we expect approximate homogeneity to hold across all i.

Homogeneity ensures that the canonical form is preserved at every step of QAOA. This allows us to track the state evolution efficiently in n for an arbitrary number of marked items (as long as they are mutually homogeneous). Previously, the coefficient tensor A depended on the the weight

w as well as the marked item index i. Now, we have $A_{w0} = A_{w1} = \cdots = A_{w(m-1)} =: A_w$. So, the state can be expressed via the rank-1 tensor A_w,

$$|\psi_t\rangle = \bar{X} \sum_{w \in [n]} A_w^{(t)} |w\rangle \tag{30}$$

and similarly for the intermediary half-steps. The tensor evolves under $\mathcal{C}, \mathcal{B}$ as follows:

$$A_w \underset{\mathcal{C}(\gamma)}{\longrightarrow} \begin{cases} A_0 - \sum_{v \in [n]} p_v \frac{A_v}{\sqrt{\binom{n}{v}}}, & \text{if } w = 0. \\ A_w, & \text{if } w > 0 \end{cases} \tag{31}$$

$$A_w \underset{\mathcal{B}(\beta)}{\longrightarrow} \sum_{v \in [n]} \mathcal{D}(\beta)_{wv} A_v \tag{32}$$

3.3 Success Probability

The success probability for the state at time T is given by the squared sum of amplitudes on marked item states. Each marked item state $|\mathbf{x_i}\rangle$ has amplitude contributions from displaced states of the form $|d_{ij} \oplus \mathbf{x_j}\rangle$ for all j. The sum then goes over all such states,

$$P(\text{success}) = \sum_{i \in [m)} \left(\sum_{j \in [m)} \frac{A_{d_{ij}j}^{(T)}}{\sqrt{\binom{n}{d_{ij}}}} \right)^2 \tag{33}$$

When homogeneity holds, the probability can be expressed as

$$P(\text{success}) = \sum_{i \in [m)} \left(\sum_{w \in [n]} p_w \frac{A_w^{(T)}}{\sqrt{\binom{n}{w}}} \right)^2 \tag{34}$$

4 Impurity band model

Now, we work towards generalizing the above methods to other cost functions. Here, we will look at the impurity band model (name subject to change). Here, we assume that instead of m marked items, we now have m "impurity" configurations for which the potential is non-zero, and zero for all other bitstring configuration. So, for every impure string $\mathbf{x_i}$, there is an associated potential c_i (which is -1 for Grover). Naturally, we may defined a *phased* bitshift operator

$$\bar{X}(\gamma) := \sum_{i \in [m)} e^{-i\gamma c_i} X^{\mathbf{x_i}} \tag{35}$$

Note that $\bar{X}(0) \equiv \bar{X}$ from the previous sections, so the new notation is consistent. Also, the impurity band model is capable of describing any potential landscape, since we could just call each bitstring $\mathbf{x}$ an impurity and assign a potential $c_{\mathbf{x}}$ to it. In that case, there would be 2^n impurity configurations. Therefore, keeping m arbitrary allows us to talk about a general problem instance.

Now, the transformations of an intermediate amplitude A_{wi} under $\mathcal{B}, \mathcal{C}$ can be written as

$$A_{wi} \xrightarrow[\mathcal{C}(\gamma)]{} \begin{cases} A_{0i} - \sum\limits_{j \in [m)} e^{-i\gamma c_j} \frac{A_{a_{ji} i}}{\sqrt{\binom{n}{a_{ji}}}}, & \text{if } w = 0 \\ A_{wi}, & \text{if } w > 0. \end{cases} \tag{36}$$

$$A_{wi} \xrightarrow[\mathcal{B}(\beta)]{} \sum_{v \in [n]} \mathcal{D}(\beta)_{wv} A_{vi}. \tag{37}$$

Finally, the state we "care about" is the global minimum, i.e., the impurity i^* for which the cost c_{i^*} is the smallest.

5 Some rough work

Here, I will explore a recent idea: in general for a random multiple item instance, one can say that the Hamming distances between strings will be sampled from a Binomial distribution centered at $n/2$, with a spread of $\sim \sqrt{n}$. However, there is no promise on the minimum distance between any two distinct marked items, which could be anywhere between 1 and n.

Suppose we had such a promise on the minimum distance. Could a sufficiently high lower bound guarantee the success of QAOA Grover on the m-item instance?

This question seems well-motivated by empirics, where we have observed that instances where strings are close to one another behave "irregularly", in the sense that the final probability time curve shows multi-period sinusoidal behaviour, and the peak success is often lower. In the worst case, when two strings are at a distance $d = 1$ from each other, the protocol seems to fail to produce a constant success probability.

Apart from empirical motivation, there is some mathematical motivation to impose a lower bound on d_{ij}: the contributions of marked item j on the amplitude on marked item i is via the diffusion operator $\mathcal{B}(\beta)$. When the separation between i, j is $d_{ij} = d$, and the evolution angle $\beta \ll 1$, the matrix term is of order

$$\mathcal{B}(j \to i) \sim (\cos\beta)^d (i \sin\beta)^{n-d} \sim \beta^d \tag{38}$$

Note that in the above, the combinatorial factor $1/\sqrt{\binom{n}{d}}$ has been ignored. The reason for this will become clear shortly.

So, a lower bound on d implies an upper bound on the cross terms between two marked items, and we sohuld expect the items to evolve more or less independently. To be more precise, when $\beta = \pi/n$, we have

$$\mathcal{B}(j \to i) \sim \beta^d \sim 2^{-d \log n} \tag{39}$$

and a distance lower bound of $d > n/\log n$ implies an upper bound of $O(1/\text{poly}(N))$ on the matrix terms, which could be sufficient to show convergence between the one-marked item protocol and the m-marked item protocol, over a total of $\sqrt{N}$ rounds of Grover. This will be the goal of this section. In particular, we [TRY TO] show that

Theorem 1. *Let $\{\mathbf{x_1}, \mathbf{x_1}, \ldots, \mathbf{x_m}\}$ be the marked item labels of an m-item Grover instance. Then, there is a minimum distance $d_0(n, m)$, $0 < d_0 < n/2$, such that $d_{ij} = |\mathbf{x_i} \oplus \mathbf{x_j}| > d_0$ implies that QAOA on the m-item instance, with angle parameters $(\beta, \gamma) = (\pi/n, \pi)$, succeeds with constant probability in $O(\sqrt{N})$ rounds of QAOA.*

Proof. As a first order of business, we will massage the DSS description into a form more amenable to analysis. Recall that the DSS is spanned by the states $\{|w \oplus \mathbf{x_i}\rangle : w \in [n], i \in [m)\}$. We will use the double-index wi to denote the basis state $|w \oplus \mathbf{x_i}\rangle$, so that a state is given by the amplitude vector A_{wi}, and an operator $\mathcal{O}$ by entries $\mathcal{O}_{wi,vj}$. Define the following normalization matrix

$$N_{wi,vj} = \delta_{wv}\delta_{ij}\frac{1}{\sqrt{\binom{n}{w}}} \equiv N_{ww} \tag{40}$$

So, N is a diagonal matrix of combinatorial factors. Now, given a QAOA protocol as an alternating application of DSS operators $\tilde{\mathcal{C}}, \tilde{\mathcal{B}}$ on the initial state $|\tilde{\psi}_0\rangle$ (also in DSS representation), we may normalize using N as follows

$$N|\tilde{\psi}_T\rangle = N\mathcal{B}\tilde{(}\beta)\mathcal{C}\tilde{(}\gamma)\cdots\mathcal{B}\tilde{(}\beta)\mathcal{C}\tilde{(}\gamma)\mathcal{B}\tilde{(}\beta)\mathcal{C}\tilde{(}\gamma)|\tilde{\psi}_0\rangle \tag{41}$$

$$= \left(N\tilde{\mathcal{B}}\tilde{\mathcal{C}}N^{-1}\right)\cdots\left(N\tilde{\mathcal{B}}\tilde{\mathcal{C}}N^{-1}\right)\left(N\tilde{\mathcal{B}}\tilde{\mathcal{C}}N^{-1}\right)\left(N|\tilde{\psi}_0\rangle\right) \tag{42}$$

For the normalized version of the final state (which we also denote $|\tilde{\psi}_T\rangle$ by abuse of notation), the success probability is given by

$$P(\text{success}) = \sum_{i\in[m)}\left|\left(\sum_{j\in[m)} A^{(T)}_{d_{ij}j}\right)\right|^2 \tag{43}$$

Under normalization, the initial state becomes the □

6 QAOA succeeds for m item Grover

In this section, we prove that a QAOA protocol successfully finds marked items in order $\sqrt{N/m}$ times for instances that satisfy a certain *well-distributedness* criterion.

Definition 1. *We call a Grover search instance, specified by m marked item locations $\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_m$, well-distributed, if any two marked items i, j are separated by Hamming distance $|\mathbf{z}_i \oplus \mathbf{z}_j| \geq \bar{d}$, where $d = \frac{n+\log m}{2\log(n/\pi)}$.*

From

Appendices

Appendix A Diffusion on the all-zero string

Here, we explicitly compute the function f, where

$$e^{-i\beta B}|\mathbf{0}\rangle = \sum_{w=0}^{n} f(w)|w\rangle$$

$$e^{-i\beta B}|\mathbf{0}\rangle = e^{-i\beta n}e^{-i\beta\sum_i X_i}|\mathbf{0}\rangle = e^{-i\beta n}\bigotimes_{i=1}^{n}\left(\cos\beta\mathbb{1} + i\sin\beta X_i\right)|\mathbf{0}\rangle$$

$$= e^{-i\beta n}\sum_{\mathbf{x}\in[1]^n}\left(\cos\beta\right)^{(n-x)}\left(i\sin\beta\right)^{x}|\mathbf{x}\rangle = e^{-i\beta n}\sum_{w=0}^{n}\left(\cos\beta\right)^{(n-w)}\left(i\sin\beta\right)^{w}\sqrt{\binom{n}{w}}|w\rangle$$

where in the last step we grouped terms with the same Hamming weight. Therefore, $f(w) = e^{-i\beta n}\left(\cos\beta\right)^{(n-w)}\left(i\sin\beta\right)^{w}\sqrt{\binom{n}{w}}$.

Appendix B Diffusion on a string of Hamming weight w

Now, we are interested in evaluating the expression

$$e^{-i\beta B}|w\rangle$$

This is a harder case to analyze, since any X string operator appearing in the expansion of $e^{-i\beta B}$ can either decrease or increase the Hamming weight depending on the location of the X flips. However, recall that the diffusion operator preserves Hamming symmetry - we will use this fact in the counting argument. Consider a bistring $|\mathbf{x}\rangle$ with w ones on the left followed by $n-w$ zeros. This is one of the weight w states appearing in the symmetrized state $|w\rangle$. First, only look at terms in $e^{-i\beta B}$ which have a total weight of v for some $v = 0, 1, \ldots, n$. In other words, terms of the form $\left(\cos\beta\right)^{(n-v)}\left(i\sin\beta\right)^{v}X^{\mathbf{z}}$ where $|\mathbf{z}| = v$. WLOG, let k of the X operators overlap with the one substring of $|\mathbf{x}\rangle$ and $v-k$ overlap with the zero substring. Note that range of k is $k = \max\left(0, w+v-n\right), \ldots, \min\left(v, w\right)$. The state after the X string operator acts on $|\mathbf{x}\rangle$ has weight $w+v-2k$. Now consider the following counting:

- The number of weight w states $|\mathbf{x}\rangle$ is $\binom{n}{w}$.
- For each weight w state $|\mathbf{x}\rangle$, there are $\binom{w}{k}\binom{n-w}{v-k}$ X string operators with total weight v and an overlap of k with the one region of $|\mathbf{x}\rangle$.
- Therefore, there are $\binom{n}{w}\cdot\binom{w}{k}\binom{n-w}{v-k}$ states (with multiplicity) of weight $w+v-2k$ that arise from the diffusion operator acting on a weight w state.
- Since there are $\binom{n}{w+v-2k}$ states of weight $w+v-2k$, and we expect the final state to have Hamming symmetry, there must be a multiplicity of $\binom{n}{w}\binom{w}{k}\binom{n-w}{v-k}/\binom{n}{w+v-2k}$. So the (unnormalized) state $|w\rangle$ yields $\binom{n}{w}\binom{w}{k}\binom{n-w}{v-k}/\binom{n}{w+v-2k}$ copies of the (unnormalized) state $|w+v-2k\rangle$.
- The initial state has normalization denominator $\sqrt{\binom{n}{w}}$ and the final state has normalization $\sqrt{\binom{n}{w+v-2k}}$. Moreover, the X string operator of weight v has a coefficient of $\left(\cos\beta\right)^{(n-v)}\left(i\sin\beta\right)^{v}$.
- Putting the combinatorial factors and normalization coefficients together, we get that

$$e^{-i\beta B}|w\rangle \to \left(\cos\beta\right)^{(n-v)}\left(i\sin\beta\right)^{v}\binom{n-w}{v-k}\binom{w}{k}\sqrt{\frac{\binom{n}{w}}{\binom{n}{w+v-2k}}}|w+v-2k\rangle$$

Finally, we have

$$e^{-i\beta B}|w\rangle = \sum_{v=0}^{n}\sum_{k=\max(0,w+v-n)}^{\min(w,v)} (\cos\beta)^{(n-v)} (i\sin\beta)^{v} \binom{n-w}{v-k}\binom{w}{k}\sqrt{\frac{\binom{n}{w}}{\binom{n}{w+v-2k}}}|w+v-2k\rangle$$

We will write the above action using a diffusion operator $\mathcal{D}(\beta)$, with $\mathcal{D}(\beta)_{uv} := \langle u|\mathcal{D}(\beta)|v\rangle$ for any two Hamming-symmetric states $|u\rangle, |v\rangle$.

Appendix C Some results on the DSS

In Eq. 40, we introduced a normalization matrix. Now, we will explicitly write the form of the normalized matrices $\bar{\mathcal{B}}$ and $\bar{\mathcal{C}}$. First, the matrices $\tilde{\mathcal{B}}$ and $\tilde{\mathcal{C}}$ are

$$\tilde{\mathcal{B}}(\beta)_{wi,vj} = \delta_{ij}\mathcal{D}(\beta)_{wv}, \quad \tilde{\mathcal{C}}(\gamma)_{wi,vj} = \delta_{wv}\delta_{ij} - \frac{\omega_\gamma}{\sqrt{\binom{n}{v}}}\delta_{w0}\delta_{vd_{ij}} \tag{44}$$

and the matrix N is

$$N_{wi,vj} = \delta_{wv}\delta_{ij}\frac{1}{\sqrt{\binom{n}{w}}} \equiv N_{ww} \tag{45}$$

Therefore, the normalized matrices may be written as

$$\bar{\mathcal{B}}(\beta)_{wi,vj} = N_{ww}\tilde{\mathcal{B}}(\beta)_{wi,vj}N_{vv}^{-1} = \sqrt{\frac{\binom{n}{v}}{\binom{n}{w}}}\mathcal{D}(\beta)_{wv}\delta_{ij} \tag{46}$$

$$\bar{\mathcal{C}}(\gamma)_{wi,vj} = \delta_{wv}\delta_{ij} - N_{ww}\frac{\omega_\gamma}{\sqrt{\binom{n}{v}}}\delta_{w0}\delta_{vd_{ij}}N_{vv}^{-1} = \delta_{wv}\delta_{ij} - \omega_\gamma\delta_{w0}\delta_{vd_{ij}} \tag{47}$$

For any state with (normalized) DSS amplitudes A_{wi}, the success probability is given by $\sum_{i\in[m]}\left|\left(\sum_{j\in[m]} A_{d_{ij}j}\right)\right|^2$. This can also be written as

References

[1] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Quantum Computation by Adiabatic Evolution. jan 2000.

[2] Zhang Jiang, Eleanor G. Rieffel, and Zhihui Wang. Near-optimal quantum circuit for Grover's unstructured search using a transverse field. feb 2017.

[3] G. Kato. Grover-algorithm-like operator using only single-qubit gates. *Phys. Rev. A*, 72:032319, Sep 2005.

[4] Jérémie Roland and Nicolas J Cerf. Quantum circuit implementation of the Hamiltonian versions of Grover's algorithm. 2003.