

RANDOM GROVER SEARCH*

DEKUAN DONG[†], YINGZHOU LI[‡], AND JIAXIN MA[§]

Abstract. Grover’s algorithm achieves a quadratic speedup for unstructured search given a global oracle for the target set. In many applications, however, the target set is specified as the intersection of multiple constraint sets. Constructing a global oracle for the intersection can be costly, whereas the individual constraint oracles are often much simpler to implement.

We study a randomized Grover search algorithm that directly uses these constraint oracles. At each iteration, one of the corresponding Grover operators is selected at random. For the two-operator case with uniform sampling, we prove that the success probability approaches one after

$$\Theta\left(\frac{\pi}{4}\sqrt{\frac{N}{r}}\right)$$

iterations, where r is the size of the intersection. Thus, the algorithm achieves the same asymptotic query complexity as standard Grover search but without requiring a global oracle. We then generalize the analysis to arbitrary sampling distributions and an arbitrary number of Grover operators through an auxiliary operator that approximates the expected Grover evolution, while retaining the same asymptotic complexity. We further show that highly biased sampling distributions can still achieve near-unit success probability, enabling cheaper Grover operators to be used more frequently. Finally, we prove asymptotic optimality and support the theoretical results with numerical simulations.

Key words. Grover search, randomized quantum algorithms, quantum search

MSC codes. 81P68, 68Q12, 68W20

1. Introduction. Grover’s algorithm [9] is a fundamental quantum algorithm that achieves a quadratic speedup for unstructured search. Given oracle access to a Boolean function $f : [N] \rightarrow \{0, 1\}$, it finds a marked item using $\mathcal{O}(\sqrt{N})$ queries, which is optimal in the black-box model [1].

The standard formulation assumes a single oracle defining the solution space. In many applications, however, the solution is specified implicitly as the intersection of multiple constraints. Such settings arise naturally in constraint satisfaction, combinatorial search [11, 5, 14], and database filtering tasks [17]. Related work on quantum set operations has been studied in [16, 7], but existing Grover-based approaches are restricted to two-set intersections and rely on problem-specific spectral analyses that do not generalize easily. More recent structured or partial-search methods [2] suggest potential improvements but typically require stronger oracle assumptions or specialized settings. Randomized or dynamic variants of Grover search have also been considered [14, 4, 8], highlighting the potential of stochastic modifications.

*Submitted to the editors DATE.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant Nos. 12271109 and 12526211; by the Shanghai Pilot Program for Basic Research-Fudan University under Grant No. 21TQ1400100 (22TQ017); by the Scientific Research Innovation Capability Support Project for Young Faculty under Grant No. SRICSPYF-ZY2025159; and by the Xuemin Institute of Advanced Studies, Fudan University.

[†]School of Mathematical Sciences, Fudan University, Shanghai, 200433 China (dkdong21@m.fudan.edu.cn). These authors contributed equally to this work.

[‡]School of Mathematical Sciences, Fudan University, Shanghai, 200433 China, and Shanghai Key Laboratory for Contemporary Applied Mathematics, Shanghai, China (Corresponding author: yingzhouli@fudan.edu.cn).

[§]School of Mathematical Sciences, Fudan University, Shanghai, 200433 China (majx23@m.fudan.edu.cn). These authors contributed equally to this work.

Formally, suppose the solution set is

$$\mathcal{A} = \bigcap_{i=0}^{k-1} \mathcal{A}_i$$

where each $\mathcal{A}_i$ can be checked by an efficient oracle. While one may construct a global oracle for $\mathcal{A}$ and apply Grover's algorithm directly [14], this is often inefficient, as combining constraint oracles into a single unitary can incur substantial overhead and circuit complexity [12]. This motivates the question:

Can we solve the intersection search problem by directly using the simpler subproblem oracles, without explicitly constructing the global oracle?

A natural idea is to associate each subset $\mathcal{A}_i$ with its corresponding Grover operator G_i , and attempt to combine them to amplify the amplitude of the intersection $\bigcap_i \mathcal{A}_i$. However, this approach faces an immediate difficulty: unlike the standard Grover operator, different G_i generally do not commute, and their composition does not preserve the two-dimensional invariant subspace structure that underlies standard Grover algorithm. As a result, deterministic compositions of these operators are difficult to analyze and do not admit rigorous performance guarantees for coherent amplitude amplification toward the desired solution space.

In this work, we analyze a different approach based on randomization. Instead of deterministically composing Grover operators, we consider a stochastic process in which, at each step, a Grover operator G_i is selected at random and applied to the current state. This leads to a randomized sequence of unitary transformations, whose collective behavior is nontrivial but analyzable. Similar ideas of randomized unitary compositions have been successfully used in Hamiltonian simulation, where random product formulas can approximate target dynamics efficiently (e.g., qDRIFT and its higher order variants such as qSWIFT [15, 3], random permutation of the product formula terms [6, 18]). However, in contrast to prior work that focuses on simulation accuracy, our goal is to understand whether such randomized dynamics can serve as a search mechanism.

The main contributions of this paper are summarized as follows.

- We analyze the randomized Grover algorithm with two operators under uniform sampling. Exploiting the special structure of the expected Grover operator, we show that after

$$\Theta\left(\frac{\pi}{4}\sqrt{\frac{N}{r}}\right)$$

iterations, the success probability reaches $1 - \mathcal{O}(1/\sqrt{N})$, where $r := |\mathcal{A}_0 \cap \mathcal{A}_1|$. Thus, the proposed algorithm achieves the same asymptotic performance as standard Grover search without requiring a global oracle that marks elements in $\mathcal{A}_0 \cap \mathcal{A}_1$.

- We extend the analysis of the uniform two-operator setting to the general case of multiple Grover operators sampled according to an arbitrary probability distribution. The key ingredient is an auxiliary operator that approximates the expected Grover evolution in the relevant subspace while preserving the essential dynamics of the uniform two-operator case. Using this construction, we establish the same asymptotic performance guarantee in the general setting.

- We show that a high success probability can be achieved using a highly biased sampling distribution. This is particularly advantageous when the implementation costs of the Grover operators differ significantly, as it allows the less expensive operators to be sampled more frequently.
- We prove that the proposed algorithm is asymptotically optimal: any deterministic sequence of Grover operators that achieves a comparable success probability must use the same asymptotic number of Grover iterations.
- We provide numerical simulations that verify the theoretical results.

The remainder of this paper is organized as follows. In Section 2, we briefly review the standard Grover algorithm. Section 3 develops the randomized Grover framework. Specifically, Subsection 3.1 analyzes the two-operator and uniform sampling case, Subsection 3.2 extends the analysis to multiple operators with non-uniform sampling distribution; Subsection 3.3 studies biased sampling distributions, and Subsection 3.4 establishes the asymptotic optimality of the proposed algorithm. Numerical results are presented in Section 4. Finally, Section 5 concludes the paper. Additional technical details and omitted calculations are deferred to the Appendix.

2. Preliminaries.

2.1. Grover's algorithm. Grover's algorithm [9] is a quantum search procedure for finding a marked element in an unstructured database of size $N = 2^n$, providing a quadratic speedup over classical methods. Let $\mathcal{M} \subseteq \{0, \dots, N-1\}$ denote the set of marked items with $|\mathcal{M}| = r$. The algorithm initializes the uniform superposition

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

and applies the Grover operator $G = DO$, where O is the phase oracle marking elements in $\mathcal{M}$ and $D = 2|\psi\rangle\langle\psi| - I$ is the diffusion operator.

A standard fact is that the dynamics are confined to the two-dimensional subspace spanned by the normalized marked and unmarked states

$$|\alpha\rangle = \frac{1}{\sqrt{r}} \sum_{x \in \mathcal{M}} |x\rangle, \quad |\beta\rangle = \frac{1}{\sqrt{N-r}} \sum_{x \notin \mathcal{M}} |x\rangle.$$

In this basis, the evolution reduces to a rotation by a fixed angle determined by $\sin \theta = \sqrt{r/N}$, so that after t iterations the state is

$$|\psi_t\rangle = \sin((2t+1)\theta) |\alpha\rangle + \cos((2t+1)\theta) |\beta\rangle.$$

As a consequence, the success probability is maximized after $\mathcal{O}(\sqrt{N/r})$ iterations.

2.2. Notations. Given a search space $\mathcal{S}$ of size $N = 2^n$, let $\mathcal{A}_0, \mathcal{A}_1, \dots, \mathcal{A}_{k-1} \subset \mathcal{S}$ be k distinct subsets, and let $G_0, G_1, \dots, G_{k-1}$ denote the corresponding Grover operators. Define

$$|\mathcal{A}_i\rangle = \frac{1}{\sqrt{|\mathcal{A}_i|}} \sum_{x \in \mathcal{A}_i} |x\rangle, \quad \text{and} \quad |\mathcal{A}_i^c\rangle = \frac{1}{\sqrt{|\mathcal{A}_i^c|}} \sum_{x \notin \mathcal{A}_i} |x\rangle, \quad i = 0, 1, \dots, k-1.$$

Then each G_i acts as a rotation in the two-dimensional subspace spanned by $|\mathcal{A}_i\rangle$ and $|\mathcal{A}_i^c\rangle$. For any integer $j \in [0, 2^k - 1]$ with binary representation $(j_{k-1} \dots j_1 j_0)_2$, define

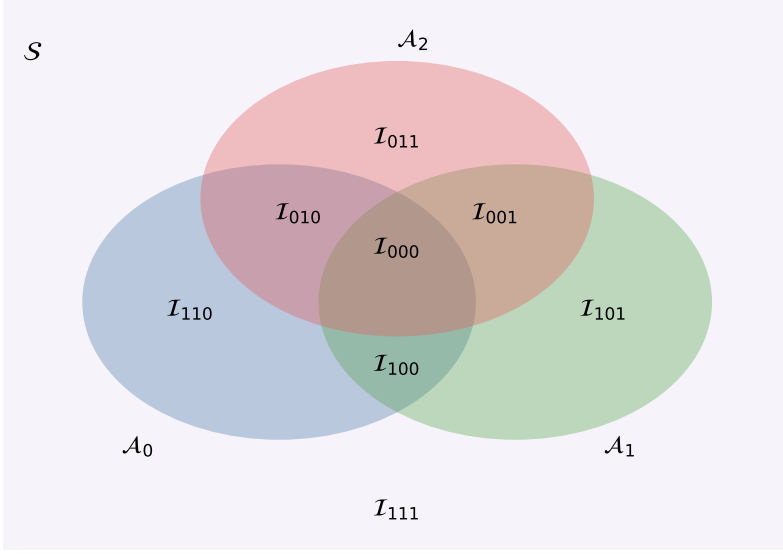


Fig. 1: Partition of the search space into the regions $\mathcal{I}_j$ induced by $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2$.

$$(2.1) \quad \mathcal{I}_j := \left(\bigcap_{i:j_i=0} \mathcal{A}_i \right) \cap \left(\bigcap_{i:j_i=1} \mathcal{A}_i^c \right).$$

The relation between $\mathcal{A}_i$ and $\mathcal{I}_j$ is illustrated by the $k = 3$ case in Figure 1. The corresponding normalized quantum state is

$$|\mathcal{I}_j\rangle := \frac{1}{\sqrt{|\mathcal{I}_j|}} \sum_{x \in \mathcal{I}_j} |x\rangle.$$

By construction, the sets $\mathcal{I}_i$ and $\mathcal{I}_j$ are disjoint for $i \neq j$, and hence $\langle \mathcal{I}_i | \mathcal{I}_j \rangle = 0$. The uniform superposition state $|\psi\rangle$ can be represented as

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{2^k-1} \sqrt{|\mathcal{I}_j|} |\mathcal{I}_j\rangle = \sum_{j=0}^{2^k-1} \sqrt{\frac{|\mathcal{I}_j|}{N}} |\mathcal{I}_j\rangle =: \sum_{j=0}^{2^k-1} \alpha_j |\mathcal{I}_j\rangle,$$

where $\alpha_j = \sqrt{|\mathcal{I}_j|/N}$.

Note that $G_i = DO_i$, where

$$D = 2|\psi\rangle\langle\psi| - I, \quad \text{and} \quad O_i|x\rangle = \begin{cases} -|x\rangle, & x \in \mathcal{A}_i, \\ |x\rangle, & x \in \mathcal{A}_i^c. \end{cases}$$

For any operator $M \in \mathbb{C}^{2^n \times 2^n}$, let $[M]_{\mathcal{I}}$ denote the restriction of M to the subspace

$$\text{span}\{|\mathcal{I}_j\rangle : j = 0, \dots, 2^k - 1\},$$

128 namely

$$129 \quad [M]_{\mathcal{I}} = \begin{bmatrix} \langle \mathcal{I}_0 | M | \mathcal{I}_0 \rangle & \cdots & \langle \mathcal{I}_0 | M | \mathcal{I}_{2^k-1} \rangle \\ \vdots & & \vdots \\ \langle \mathcal{I}_{2^k-1} | M | \mathcal{I}_0 \rangle & \cdots & \langle \mathcal{I}_{2^k-1} | M | \mathcal{I}_{2^k-1} \rangle \end{bmatrix} \in \mathbb{C}^{2^k \times 2^k}.$$

130 Under this notation, the diffusion operator D admits $[D]_{\mathcal{I}} = 2\alpha\alpha^\top - I$, where $\alpha =$
 131 $[\alpha_0, \dots, \alpha_{2^k-1}]^\top$. Moreover, for every $i = 0, \dots, k-1$ and every $j = 0, \dots, 2^k-1$, the
 132 set $\mathcal{I}_j$ is either entirely contained in $\mathcal{A}_i$ or entirely contained in its complement $\mathcal{A}_i^c$.
 133 Consequently,

$$134 \quad (2.2) \quad O_i |\mathcal{I}_j\rangle = \begin{cases} -|\mathcal{I}_j\rangle, & \mathcal{I}_j \subset \mathcal{A}_i, \\ |\mathcal{I}_j\rangle, & \mathcal{I}_j \subset \mathcal{A}_i^c. \end{cases}$$

135 Moreover, according to the definition of $\mathcal{I}_j$, we have

$$136 \quad (2.3) \quad O_i |\mathcal{I}_j\rangle = (-1)^{j_i+1} |\mathcal{I}_j\rangle,$$

137 so $[O_i]_{\mathcal{I}}$ is diagonal, whose j -th diagonal entry is $(-1)^{j_i+1}$, where j_i denotes the i -th
 138 bit in the binary representation of j .

139 Moreover, we denote $r := |\cap_{i=0}^{k-1} \mathcal{A}_i|$ and $m := |\cap_{i=0}^{k-1} \mathcal{A}_i^c|$ for notation simplification
 140 in this paper.

141 **3. Random Grover Search.** In this section, we sequentially apply randomly
 142 chosen operators from $\{G_0, G_1, \dots, G_{k-1}\}$ to $|\psi\rangle$, and denote by $|\psi(t)\rangle$ the state after
 143 t applications. Since the subspace spanned by $\{|\mathcal{I}_j\rangle : j = 0, \dots, 2^k-1\}$ is invariant
 144 under each G_i , there exists real coefficients $a_j(t)$ such that

$$145 \quad |\psi(t)\rangle = \sum_{j=0}^{2^k-1} a_j(t) |\mathcal{I}_j\rangle.$$

146 Note that the coefficients $a_j(t)$ are random variables, where the randomness arises
 147 from the random choice of Grover operators. For any fixed t , there are only finitely
 148 many possible Grover sequences, and hence each $a_j(t)$ takes values from a finite set
 149 $V_j(t)$. Measuring $|\psi(t)\rangle$ in the computational basis yields an outcome $x \in \mathcal{I}_0 = \cap_i \mathcal{A}_i$
 150 with probability

$$\begin{aligned} \mathbb{P}_{\text{succ}}(t) &= \sum_{s \in V_0(t)} \mathbb{P}(x \in \mathcal{I}_0 | a_0(t) = s) \mathbb{P}(a_0(t) = s) \\ 151 \quad &= \sum_{s \in V_0(t)} s^2 \cdot \mathbb{P}(a_0(t) = s) = \mathbb{E}[a_0^2(t)]. \end{aligned}$$

152 Here, the success probability incorporates both the randomness of the choice of Grover
 153 operators and the randomness of the final measurement. The above identity shows
 154 that $\mathbb{P}_{\text{succ}}(t)$ is equal to the expectation of $a_0^2(t)$, where the randomness comes solely
 155 from the choice of the Grover sequence.

156 **3.1. Two Grover operators.** First, we consider the simplest case, where $k = 2$
 157 and G_0, G_1 are selected with equal probability at each iteration. Restricting to the
 158 subspace spanned by $\{|\mathcal{I}_0\rangle, |\mathcal{I}_1\rangle, |\mathcal{I}_2\rangle, |\mathcal{I}_3\rangle\}$, the oracle operators take the form

$$159 \quad (3.1) \quad [O_0]_{\mathcal{I}} = \begin{bmatrix} -1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \quad [O_1]_{\mathcal{I}} = \begin{bmatrix} -1 & & & \\ & 1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix}.$$

The main result for this setting is stated below.

THEOREM 3.1. *Consider two distinct Grover operators G_0 and G_1 , and let the initial state be the uniform superposition state $|\psi\rangle$. At each step, independently apply either G_0 or G_1 with equal probability. Assume $N > (m+r)^2/r$, then after*

$$T = \Theta\left(\frac{\pi}{4}\sqrt{\frac{N}{r}}\right)$$

steps, measuring the resulting quantum state yields an element in $\mathcal{A}_0 \cap \mathcal{A}_1$ with probability

$$\mathbb{P}_{\text{succ}}(T) = \mathbb{E}[a_0^2(T)] \geq 1 - \left(\frac{2(m-r)}{\sqrt{Nr}} + \frac{4r}{N}\right).$$

Proof. By the Cauchy inequality, we have

$$(3.2) \quad \mathbb{E}[a_0^2(t)] \geq (\mathbb{E}[a_0(t)])^2.$$

Since the random choices are independent, it follows that

$$\begin{aligned} \mathbb{E}[a_0(t)] &= \mathbb{E}[\langle \mathcal{I}_0 | G_{i_t} G_{i_{t-1}} \cdots G_{i_1} | \psi \rangle] = \langle \mathcal{I}_0 | \mathbb{E}[G_{i_t} G_{i_{t-1}} \cdots G_{i_1}] | \psi \rangle \\ &= \langle \mathcal{I}_0 | \mathbb{E}[G_{i_t}] \mathbb{E}[G_{i_{t-1}}] \cdots \mathbb{E}[G_{i_1}] | \psi \rangle = \langle \mathcal{I}_0 | \mathbb{E}[G_{i_1}]^t | \psi \rangle \\ &= \langle \mathcal{I}_0 | \left(\frac{G_0 + G_1}{2}\right)^t | \psi \rangle. \end{aligned} \quad (3.3)$$

For convenience, we define

$$(3.4) \quad G := (G_0 + G_1)/2.$$

According to (3.1), in the subspace spanned by $\{|\mathcal{I}_0\rangle, |\mathcal{I}_1\rangle, |\mathcal{I}_2\rangle, |\mathcal{I}_3\rangle\}$, the operator G takes the form

$$[G]_{\mathcal{I}} = (2\alpha\alpha^\top - I) \left(\frac{[O_0]_{\mathcal{I}} + [O_1]_{\mathcal{I}}}{2} \right) = \begin{bmatrix} 1 - 2\alpha_0^2 & 0 & 0 & 2\alpha_0\alpha_3 \\ -2\alpha_0\alpha_1 & 0 & 0 & 2\alpha_1\alpha_3 \\ -2\alpha_0\alpha_2 & 0 & 0 & 2\alpha_2\alpha_3 \\ -2\alpha_0\alpha_3 & 0 & 0 & 2\alpha_3^2 - 1 \end{bmatrix}.$$

Next, suppose

$$G^t |\psi\rangle = \sum_{j=0}^3 \hat{a}_j(t) |\mathcal{I}_j\rangle.$$

Then the coefficients satisfy the recursion

$$(3.5) \quad \begin{bmatrix} \hat{a}_0(t) \\ \hat{a}_3(t) \end{bmatrix} = M \begin{bmatrix} \hat{a}_0(t-1) \\ \hat{a}_3(t-1) \end{bmatrix}, \quad \text{where} \quad M = \begin{bmatrix} 1 - 2\alpha_0^2 & 2\alpha_0\alpha_3 \\ -2\alpha_0\alpha_3 & 2\alpha_3^2 - 1 \end{bmatrix}, \quad \begin{bmatrix} \hat{a}_0(0) \\ \hat{a}_3(0) \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_3 \end{bmatrix}.$$

Here, $\alpha_0 = \sqrt{r/N}$ and $\alpha_3 = \sqrt{1 - m/N}$. Applying M^t to the initial vector $[\alpha_0, \alpha_3]^\top$ and extracting the first component yields

$$(3.6) \quad \hat{a}_0(t) = \frac{\alpha_0(1 - \alpha_0^2 + \alpha_3^2 + \Delta)(\alpha_3^2 - \alpha_0^2 + \Delta)^t + \alpha_0(\alpha_0^2 - \alpha_3^2 - 1 + \Delta)(\alpha_3^2 - \alpha_0^2 - \Delta)^t}{2\Delta},$$

where $\Delta = \sqrt{(1 - \alpha_0^2 - \alpha_3^2)^2 - 4\alpha_0^2\alpha_3^2}$. The derivation of the above expression is deferred to Subsection A.1. Since $N > (m + r)^2/r$, we have

$$(\alpha_0 + \alpha_3)^2 = \frac{N - m + r + 2\sqrt{r(N - m)}}{N} > \frac{N - m + r + 2\sqrt{m^2 + mr + r^2}}{N} > 1,$$

and thus $(1 - \alpha_0^2 - \alpha_3^2)^2 - 4\alpha_0^2\alpha_3^2 < 0$. Therefore, we write $\Delta = i\Gamma$, where $\Gamma = \sqrt{4\alpha_0^2\alpha_3^2 - (1 - \alpha_0^2 - \alpha_3^2)^2}$, and the expression for $\hat{a}_0(t)$ can be rewritten as

$$\hat{a}_0(t) = \frac{2\alpha_0\alpha_3e^{i\beta}\rho^te^{i\theta t} - 2\alpha_0\alpha_3e^{-i\beta}\rho^te^{-i\theta t}}{2i\Gamma} = \frac{2\alpha_0\alpha_3\rho^t\sin(t\theta + \beta)}{\Gamma},$$

where

$$\rho = \sqrt{2(\alpha_0^2 + \alpha_3^2) - 1}, \quad \sin\theta = \frac{\Gamma}{\rho}, \quad \sin\beta = \frac{\Gamma}{2\alpha_3}, \quad \theta, \beta \in [0, \frac{\pi}{2}].$$

Let

$$T = \left\lfloor \frac{\pi}{2\theta} - \frac{\beta}{\theta} \right\rfloor > \frac{\pi}{2\theta} - \frac{\beta}{\theta} - 1.$$

Then we have $T\theta + \beta \in (\pi/2 - \theta, \pi/2]$, and thus $\sin(T\theta + \beta) \geq \sin(\pi/2 - \theta) = \cos\theta$. Moreover, noting that $\Gamma \leq 2\alpha_0\alpha_3$, we obtain

$$\hat{a}_0(T_0) \geq \rho^{T_0} \cos\theta = \cos\theta (1 - 2(1 - \alpha_0^2 - \alpha_3^2))^{\frac{T_0}{2}} \geq \cos\theta (1 - (1 - \alpha_0^2 - \alpha_3^2)T_0),$$

where the last inequality follows from Bernoulli's inequality.

Consequently,

$$\begin{aligned} 0 &\leq 1 - \mathbb{E}[a_0^2(t)] \leq 1 - (\mathbb{E}[a_0(t)])^2 = 1 - \hat{a}_0^2(t) \\ &\leq 1 - \cos^2\theta (1 - (1 - \alpha_0^2 - \alpha_3^2)T)^2 \\ &\leq \sin^2\theta + 2\cos^2\theta(1 - \alpha_0^2 - \alpha_3^2)T_0 \\ &\leq \sin^2\theta + 2 \cdot \frac{m-r}{N} \cdot \frac{\pi}{2\theta} \leq \sin^2\theta + \frac{m-r}{N} \cdot \frac{\pi}{\sin\theta}. \end{aligned}$$

Here,

$$\sin\theta = \frac{\Gamma}{\rho} = \sqrt{\frac{\frac{4r(N-m)-(m-r)^2}{N^2}}{1 - \frac{2(m-r)}{N}}} = 2\sqrt{\frac{r}{N}} \sqrt{\frac{1 - (\frac{m+r}{2})^2 \frac{1}{Nr}}{1 - 2\frac{m-r}{N}}} \leq 2\sqrt{\frac{r}{N}}.$$

Moreover, since $N > (m + r)^2/r$, it follows that

$$\frac{1}{\sin\theta} \leq \frac{1}{2} \sqrt{\frac{N}{r}} \sqrt{\frac{4}{3}} = \frac{1}{\sqrt{3}} \sqrt{\frac{N}{r}}.$$

Substituting these bound into (3.8), we obtain

$$0 \leq 1 - \mathbb{E}[a_0^2(t)] \leq \frac{2(m-r)}{\sqrt{Nr}} + \frac{4r}{N}.$$

For the oracle complexity, consider the function

$$f(r) := \frac{\sin 2\beta}{\sin\theta} = \frac{(1 + \alpha_3^2 - \alpha_0^2)\sqrt{2(\alpha_0^2 + \alpha_3^2) - 1}}{2\alpha_3^2} = \frac{(2 - \frac{m+r}{N})\sqrt{1 - \frac{2(m-r)}{N}}}{2 - \frac{2m}{N}},$$

for $r \in (0, m]$. Using the assumption $N > (m + r)^2/r$, it follows that

$$f'(r) = \frac{N + m - 3r}{2N(N - m)\sqrt{1 - \frac{2(m-r)}{N}}} \geq \frac{3m - 2r}{2N^2} > 0, \quad \forall r \in (0, m].$$

Hence $f(r) \leq f(m) = 1$. Then we get $2\beta \leq \theta$, and thus $0 < \beta/\theta \leq 1/2$. Then, we have

$$T_0 \geq \frac{\pi}{2\theta} - 2 \geq \frac{\pi}{2(\sin\theta + \frac{\theta^3}{6})} - 2 \geq \frac{\pi}{2(\sin\theta + \frac{1}{6}(\frac{\pi}{2}\sin\theta)^3)} - 2 \geq \frac{\pi}{4}\sqrt{\frac{N}{r}}\frac{N}{N + 4r} - 2.$$

On the other hand, we have

$$T \leq \frac{\pi}{2\theta} \leq \frac{\pi}{2\sin\theta} \leq \frac{\pi}{4}\sqrt{\frac{N}{r}}\frac{1}{\sqrt{1 - \frac{(m+r)^2}{4Nr}}}.$$

Finally, we conclude that $T = \Theta(\pi/4\sqrt{N/r})$. $\square$

Remark 3.2. The operator M can be written as

$$M = \left(I - 2 \begin{bmatrix} \alpha_0 \\ \alpha_3 \end{bmatrix} \begin{bmatrix} \alpha_0 & \alpha_3 \end{bmatrix} \right) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

which closely resembles the Grover operator. However, since $\alpha_0^2 + \alpha_3^2 < 1$, this operator is not a perfect rotation and instead leads to leakage of amplitude outside the two-dimensional subspace during the evolution. Figure 2 shows the trajectory of $[\hat{a}_0(t), \hat{a}_3(t)]^\top$ in the two-dimensional plane under different parameters.

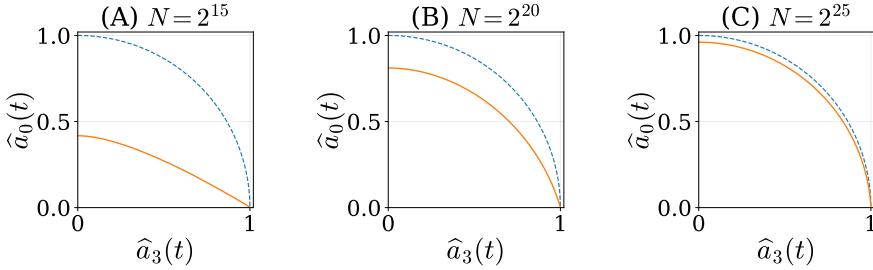


Fig. 2: Projected trajectories onto the $(\hat{a}_3(t), \hat{a}_0(t))$ -plane under the averaged evolution matrix M for different values of N , with fixed $r = 1$, $|\mathcal{A}_0| = 200$, and $|\mathcal{A}_1| = 100$. The dashed curves represent quarter circles of radius 1, while the solid curves denote the projected trajectories.

3.2. More than two Grover operators. In this section, we extend the analysis to the case of more than two Grover operators. Let $\{G_i : i = 0, \dots, k-1\}$ be selected independently at each step with probability $\{p_i\}_{i=0}^{k-1}$. As discussed earlier,

$$\mathbb{E}[a_0(t)] = \langle \mathcal{I}_0 | \left(\sum_{i=0}^{k-1} p_i G_i \right)^t | \psi \rangle.$$

226 Using the notations introduced in Subsection 2.2, we define

$$227 \quad G := \sum_{i=0}^{k-1} p_i G_i = D \sum_{i=0}^{k-1} p_i O_i.$$

228 Restricted to the subspace

$$229 \quad \text{span} \{ |\mathcal{I}_j\rangle : j = 0, \dots, 2^k - 1 \},$$

230 we have $[D]_{\mathcal{I}} = 2\alpha\alpha^\top - I$ and

$$231 \quad \left[\sum_{i=0}^{k-1} p_i O_i \right]_{\mathcal{I}} = \sum_{i=0}^{k-1} p_i [O_i]_{\mathcal{I}}.$$

232 According to (2.3), each $[O_i]_{\mathcal{I}}$ is diagonal, with j -th diagonal entry equal to $(-1)^{1+j_i}$.

233 Consequently, $\sum_{i=0}^{k-1} p_i [O_i]_{\mathcal{I}}$ is also diagonal, whose j -th diagonal entry is

$$234 \quad (3.9) \quad \sum_{i=0}^{k-1} p_i (-1)^{1+j_i} = \sum_{i:j_i=1} p_i - \sum_{i:j_i=0} p_i = 1 - 2 \sum_{i:j_i=0} p_i,$$

235 where we use the identity $\sum_{i=0}^{k-1} p_i = 1$.

236 Unlike the two-operator case with uniform sampling, the corresponding average
 237 evolution matrix G is no longer sparse in the relevant subspace, which makes its
 238 spectral analysis and the characterization of its powers considerably more challenging.
 239 To address this difficulty, we construct a sparse approximation $\tilde{G}$ by discarding entries
 240 whose contributions are asymptotically negligible. The following lemma provides the
 241 construction of $\tilde{G}$.

242 **LEMMA 3.3.** *Consider $k \geq 2$ distinct Grover operators $G_0, G_1, \dots, G_{k-1}$. Let*

$$243 \quad G = \sum_{i=0}^{k-1} p_i G_i, \quad \sum_{i=0}^{k-1} p_i = 1, \quad p_i > 0,$$

244 *define $\tilde{\alpha} := [\alpha_0, 0, \dots, 0, \alpha_{2^k-1}]^\top$, and let $\tilde{G}$ be an operator such that the subspace*

$$245 \quad \text{span} \{ |\mathcal{I}_j\rangle : j = 0, \dots, 2^k - 1 \}$$

246 *is invariant under $\tilde{G}$ and*

$$247 \quad [\tilde{G}]_{\mathcal{I}} := (2\alpha\tilde{\alpha}^\top - I) \sum_{i=0}^{k-1} p_i [O_i]_{\mathcal{I}}.$$

248 *Then, for all $n \in \mathbb{N}$,*

$$249 \quad (3.10) \quad \left\| [G^n]_{\mathcal{I}} - [\tilde{G}^n]_{\mathcal{I}} \right\|_2 \leq \frac{1}{p} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2} + \frac{2n}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2),$$

250 *where*

$$251 \quad p := \min_{0 \leq i \leq k-1} p_i.$$

Proof. First, observe that

$$[G]_{\mathcal{I}} - [\tilde{G}]_{\mathcal{I}} = 2\alpha(\alpha - \tilde{\alpha})^\top \sum_{i=0}^{k-1} p_i [O_i]_{\mathcal{I}} := 2\alpha\beta^\top.$$

Note that $\sum_{i=0}^{k-1} p_i [O_i]_{\mathcal{I}}$ is diagonal and its j -th diagonal entry is given by (3.9), we have

$$\beta_j = \begin{cases} 0, & j = 0, 2^k - 1, \\ \alpha_j \left(1 - 2 \sum_{i:j_i=0} p_i\right), & j = 1, \dots, 2^k - 2. \end{cases}$$

Since $\|[G]_{\mathcal{I}}\|_2 \leq \|G\|_2 = 1$, we have

$$\left\| [G]_{\mathcal{I}}^n - [\tilde{G}]_{\mathcal{I}}^n \right\|_2 = \left\| \sum_{l=0}^{n-1} [G]_{\mathcal{I}}^{n-1-l} ([G]_{\mathcal{I}} - [\tilde{G}]_{\mathcal{I}}) [\tilde{G}]_{\mathcal{I}}^l \right\|_2 \leq \sum_{l=0}^{n-1} \left\| ([G]_{\mathcal{I}} - [\tilde{G}]_{\mathcal{I}}) [\tilde{G}]_{\mathcal{I}}^l \right\|_2.$$

Moreover,

$$\left\| ([G]_{\mathcal{I}} - [\tilde{G}]_{\mathcal{I}}) [\tilde{G}]_{\mathcal{I}}^l \right\|_2 = 2 \left\| \alpha\beta^\top [\tilde{G}]_{\mathcal{I}}^l \right\|_2 = 2\|\alpha\|_2 \left\| \left([\tilde{G}]_{\mathcal{I}}^\top\right)^l \beta \right\|_2 = 2 \left\| \left([\tilde{G}]_{\mathcal{I}}^\top\right)^l \beta \right\|_2.$$

Denote

$$\left([\tilde{G}]_{\mathcal{I}}^\top\right)^l \beta = [b_0(l), b_1(l), \dots, b_{2^k-1}(l)]^\top.$$

By writing out the expression of $[\tilde{G}]_{\mathcal{I}}$ explicitly, we obtain the following recurrence relation:

$$(3.11) \quad \begin{bmatrix} b_0(l) \\ b_1(l) \\ \vdots \\ b_{2^k-2}(l) \\ b_{2^k-1}(l) \end{bmatrix} = \begin{bmatrix} 1 - 2\alpha_0^2 & -2\alpha_0\alpha_1 & \cdots & -2\alpha_0\alpha_{2^k-2} & -2\alpha_0\alpha_{2^k-1} \\ 0 & \gamma_1 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & \gamma_{2^k-2} & 0 \\ 2\alpha_{2^k-1}\alpha_0 & 2\alpha_{2^k-1}\alpha_1 & \cdots & 2\alpha_{2^k-1}\alpha_{2^k-2} & 2\alpha_{2^k-1}^2 - 1 \end{bmatrix} \begin{bmatrix} b_0(l-1) \\ b_1(l-1) \\ \vdots \\ b_{2^k-2}(l-1) \\ b_{2^k-1}(l-1) \end{bmatrix},$$

where

$$\gamma_j = 2 \sum_{i:j_i=0} p_i - 1, \quad j = 1, \dots, 2^k - 2.$$

Let $\gamma = \max_{2 \leq j \leq 2^k-2} |\gamma_j|$. It can be shown that

$$2p - 1 \leq \gamma_j \leq 1 - 2p, \quad \forall j = 1, \dots, 2^k - 2,$$

which implies $\gamma \leq 1 - 2p$.

From the recurrence (3.11), the first and last components satisfy

$$\begin{bmatrix} b_0(l) \\ b_{2^k-1}(l) \end{bmatrix} = M \begin{bmatrix} b_0(l-1) \\ b_{2^k-1}(l-1) \end{bmatrix} + v(l-1),$$

where

$$M = \begin{bmatrix} 1 - 2\alpha_0^2 & -2\alpha_0\alpha_{2^k-1} \\ 2\alpha_0\alpha_{2^k-1} & 2\alpha_{2^k-1}^2 - 1 \end{bmatrix}, \quad v(l-1) = \begin{bmatrix} -2\alpha_0 \left(\sum_{j=1}^{2^k-2} \alpha_j b_j(l-1) \right) \\ 2\alpha_{2^k-1} \left(\sum_{j=1}^{2^k-2} \alpha_j b_j(l-1) \right) \end{bmatrix}.$$

275 For the remaining components, we have

$$276 \quad b_j(l) = \gamma_j b_j(l-1) = \cdots = \gamma_j^l b_j(0) = \gamma_j^{l+1} \alpha_i, \quad \forall j = 1, \dots, 2^k - 2.$$

277 For the term $v(l-1)$, we have

(3.12)

$$278 \quad \|v(l-1)\|_2 = 2\sqrt{\alpha_0^2 + \alpha_{2^k-1}^2} \left| \sum_{j=1}^{2^k-2} \alpha_j b_j(l-1) \right| \leq 2 \left| \sum_{j=1}^{2^k-2} \alpha_j^2 \gamma_j^l \right| \leq 2\gamma^l (1 - \alpha_0^2 - \alpha_{2^k-1}^2).$$

279 Since $\|M\|_2 = 1$ and $b_0(0) = b_{2^k-1}(0) = 0$, it follows that

$$\begin{aligned} \sqrt{b_0(l)^2 + b_{2^k-1}(l)^2} &\leq \sqrt{b_0(l-1)^2 + b_{2^k-1}(l-1)^2} + 2\gamma^l (1 - \alpha_0^2 - \alpha_{2^k-1}^2) \\ &\leq 2 \left(\sum_{q=1}^l \gamma^q \right) (1 - \alpha_0^2 - \alpha_{2^k-1}^2) \\ 280 \quad (3.13) \quad &\leq \frac{2\gamma}{1-\gamma} (1 - \alpha_0^2 - \alpha_{2^k-1}^2) \\ &\leq \frac{1}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2), \end{aligned}$$

281 where we used $\gamma \leq 1 - 2p$ in the last inequality. Moreover, a direct computation gives

$$282 \quad \sqrt{\sum_{j=1}^{2^k-2} b_j(l)^2} \leq \gamma^{l+1} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2}.$$

283 Combining the above bounds and using the triangle inequality, we obtain

$$284 \quad \left\| \left([\tilde{G}]_{\mathcal{I}}^{\mathbb{T}} \right)^l \beta \right\|_2 \leq \frac{1}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2) + \gamma^{l+1} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2}.$$

285 Therefore,

$$\begin{aligned} \left\| [G]_{\mathcal{I}}^n - [\tilde{G}]_{\mathcal{I}}^n \right\|_2 &\leq \sum_{l=0}^{n-1} \left\| ([G]_{\mathcal{I}} - [\tilde{G}]_{\mathcal{I}}) [\tilde{G}]_{\mathcal{I}}^l \right\|_2 \\ 286 \quad (3.14) \quad &\leq \frac{2n}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2) + 2 \sum_{l=0}^{n-1} \gamma^{l+1} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2} \\ &\leq \frac{2n}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2) + \frac{1}{p} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2}. \end{aligned}$$

287 Finally, note that the subspace

$$288 \quad \text{span} \{ |\mathcal{I}_j\rangle : j = 0, \dots, 2^k - 1 \}$$

289 is invariant under both G and $\tilde{G}$, we have $[G^n]_{\mathcal{I}} = [G]_{\mathcal{I}}^n$ and $[\tilde{G}^n]_{\mathcal{I}} = [\tilde{G}]_{\mathcal{I}}^n$, and thus

$$\left\| [G^n]_{\mathcal{I}} - [\tilde{G}^n]_{\mathcal{I}} \right\|_2 = \left\| [G]_{\mathcal{I}}^n - [\tilde{G}]_{\mathcal{I}}^n \right\|_2 \leq \frac{1}{p} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2} + \frac{2n}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2).$$

290

□

Remark 3.4. Since $p \leq 1/k$, the right-hand side of (3.10) attains its minimum at $p = 1/k$, i.e., when all Grover operators are sampled with equal probability.

Using Lemma 3.3, we obtain the main result for the randomized Grover search algorithm with arbitrary number of operators and non-uniform sampling distribution.

THEOREM 3.5. *Consider $k \geq 2$ distinct Grover operators $G_0, G_1, \dots, G_{k-1}$, and let the initial state be the uniform superposition state $|\psi\rangle$. At each step, independently apply G_i with probability $p_i > 0$. Assume $N > (m+r)^2/r$, then after*

$$T = \Theta\left(\frac{\pi}{4}\sqrt{\frac{N}{r}}\right)$$

steps, measuring the resulting quantum state yields an element in $\cap_{i=0}^{k-1} \mathcal{A}_i$ with probability

$$\mathbb{P}_{\text{succ}}(T) = \mathbb{E}[a_0^2(T)] \geq 1 - \frac{4r}{N} - \left(2 + \frac{4}{p}\right) \frac{m-r}{\sqrt{rN}} - \frac{2}{p} \sqrt{\frac{m-r}{N}},$$

where $p = \min_{0 \leq i \leq k-1} p_i$.

Proof. Let $\tilde{G}$ be the operator constructed in Lemma 3.3. Observe that the evolution induced by $\tilde{G}$ on the invariant subspace $\text{span}\{|\mathcal{I}_0\rangle, |\mathcal{I}_{2^k-1}\rangle\}$ is identical to the evolution on the invariant subspace $\text{span}\{|\mathcal{I}_0\rangle, |\mathcal{I}_3\rangle\}$ considered in Theorem 3.1. Therefore, we choose

$$T_0 = \left\lfloor \frac{\pi}{2\theta} - \frac{\beta}{\theta} \right\rfloor = \Theta\left(\frac{\pi}{4}\sqrt{\frac{N}{r}}\right)$$

where θ and β are the same as in Theorem 3.1.

Using (3.7), together with the estimate in Lemma 3.3 and the triangle inequality, we obtain

$$\begin{aligned} & \mathbb{E}[a_0(T)] \\ &= \mathbb{E}[\langle \mathcal{I}_0 | G^{T_0} | \psi \rangle] \geq \mathbb{E}[\langle \mathcal{I}_0 | \tilde{G}^{T_0} | \psi \rangle] - \left\| [G^{T_0}]_{\mathcal{I}} - [\tilde{G}^{T_0}]_{\mathcal{I}} \right\|_2 \\ &\geq \cos \theta (1 - (1 - \alpha_0^2 - \alpha_{2^k-1}^2) T_0) - \frac{1}{p} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2} - \frac{2T_0}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2). \end{aligned}$$

Hence, the success probability satisfies

$$\begin{aligned} & \mathbb{P}_{\text{succ}}(T) = \mathbb{E}[a_0^2(T)] \geq (\mathbb{E}[a_0(T)])^2 \\ &\geq \cos^2 \theta (1 - (1 - \alpha_0^2 - \alpha_{2^k-1}^2) T)^2 - \frac{2}{p} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2} - \frac{4T_0}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2) \\ &\geq 1 - \sin^2 \theta - 2(1 - \alpha_0^2 - \alpha_{2^k-1}^2) T - \frac{2}{p} \sqrt{1 - \alpha_0^2 - \alpha_{2^k-1}^2} - \frac{4T_0}{p} (1 - \alpha_0^2 - \alpha_{2^k-1}^2) \\ &\geq 1 - \frac{4r}{N} - \left(2 + \frac{4}{p}\right) \frac{m-r}{\sqrt{rN}} - \frac{2}{p} \sqrt{\frac{m-r}{N}}, \end{aligned}$$

where we use the bound $\sin \theta \leq 2\sqrt{\frac{r}{N}}$ and $T \leq \sqrt{\frac{N}{r}}$ from Theorem 3.1. $\square$

According to Theorem 3.5, the randomized Grover search algorithm amplify the success probability approaching 1 if $1/p = o(\sqrt{N})$ under mild assumptions between m , r , and N . In contrast, a deterministic sequence of Grover operators does not

necessarily amplify the success probability to approach 1. To illustrate this, consider the sequence

$$(3.15) \quad G_0, G_1, G_0, G_0, G_1, G_0, G_0, \dots$$

Let $r_0 := |\mathcal{A}_0|$, $r_1 := |\mathcal{A}_1|$, and $r := |\mathcal{A}_0 \cap \mathcal{A}_1|$, and assume $N > \max\{4r_0, 4r_1\}$. The operator $G_0 G_0 G_1$ appears periodically in this sequence and can be rewritten as

$$\begin{aligned} G_0 G_0 G_1 &= G_0(2|\psi\rangle\langle\psi| - I)O_0(2|\psi\rangle\langle\psi| - I)O_1 \\ &= G_0(2|\psi\rangle\langle\psi| - I)G_0^\dagger O_1 \\ &= \left(2G_0|\psi\rangle\langle\psi|G_0^\dagger - I\right)O_1. \end{aligned}$$

Operators of this form were studied in [10], where the Walsh–Hadamard transform in the standard Grover algorithm is replaced by a general unitary operator. Following the same line of argument, we identify a two-dimensional invariant subspace of $G_0 G_0 G_1$, spanned by

$$|u\rangle = \frac{1}{\sqrt{|\mathcal{A}_1|}} \sum_{y \in \mathcal{A}_1} |y\rangle, \quad |v\rangle = G_0 |\psi\rangle.$$

Restricted $G_0 G_0 G_1$ to the subspace $\text{span}\{|u\rangle, |v\rangle\}$, and expressing it in the basis $\{|u\rangle, |v\rangle\}$, we obtain the matrix representation

$$(3.16) \quad W := \begin{bmatrix} 1 & 2\langle u|v\rangle \\ -2\langle v|u\rangle & 1 - 4|\langle u|v\rangle|^2 \end{bmatrix}.$$

Since $\text{Tr}(W) = 2 - 4|\langle u|v\rangle|^2$ and $\det(W) = 1$, the powers of W satisfy the recurrence

$$W^n = (2 - 4|\langle u|v\rangle|^2)W^{n-1} - W^{n-2}.$$

Solving this recurrence yields

$$W^n = \frac{1}{\sin\theta} \begin{bmatrix} \sin n\theta - \sin(n-1)\theta & 2\langle u|v\rangle \sin n\theta \\ -2\langle v|u\rangle \sin n\theta & (1 - 4|\langle u|v\rangle|^2) \sin n\theta - \sin(n-1)\theta \end{bmatrix},$$

where $\sin \frac{\theta}{2} := \langle u|v\rangle$. The derivation of the expression is deferred to Subsection A.2.

After one step of the Grover sequence, the quantum state becomes $G_0 |\psi\rangle$, which lies in the invariant subspace spanned by $|u\rangle$ and $|v\rangle$. After n applications of $G_0 G_0 G_1$, the success probability satisfies

$$\begin{aligned} (3.17) \quad \mathbb{P}_{\text{succ}}^{(n)} &= |\langle \mathcal{I}_0 | (G_0 G_0 G_1)^n G_0 |\psi\rangle|^2 \\ &= \left(\frac{2 \sin \frac{\theta}{2} \sin n\theta}{\sin \theta} \langle \mathcal{I}_0 | u \rangle + \frac{(1 - 4 \sin^2 \frac{\theta}{2}) \sin n\theta - \sin(n-1)\theta}{\sin \theta} \langle \mathcal{I}_0 | v \rangle \right)^2 \\ &= \left(\frac{2 \sin \frac{\theta}{2} \sin n\theta}{\sin \theta} \sqrt{\frac{r}{r_1}} + \left(3 - \frac{4r_0}{N}\right) \sqrt{\frac{r}{N}} \cdot \frac{(1 - 4 \sin^2 \frac{\theta}{2}) \sin n\theta - \sin(n-1)\theta}{\sin \theta} \right)^2 \\ &= \frac{4 \sin^2 \frac{\theta}{2}}{\sin^2 \theta} \left(\sin n\theta \sqrt{\frac{r}{r_1}} + 2 \left(3 - \frac{4r_0}{N}\right) \sqrt{\frac{r}{N}} \left(\cos \left(n - \frac{1}{2}\right) \theta - 2 \sin \frac{\theta}{2} \sin n\theta \right) \right)^2 \\ &\leq \frac{4 \sin^2 \frac{\theta}{2}}{\sin^2 \theta} \left(\sqrt{\frac{r}{b}} + 18 \sqrt{\frac{r}{N}} \right)^2. \end{aligned}$$

This upper bound can be significantly smaller than 1 when $r \ll r_1 < N$. Moreover, the success probabilities associated with the sequences $G_1(G_0G_0G_1)^nG_0$ and $G_0G_1(G_0G_0G_1)^nG_0$ can also be bounded far below 1. The corresponding analysis is presented in Subsection A.3. Therefore, the deterministic sequence (3.15) provides an example in which the success probability does not necessarily approach 1. Numerical experiments are conducted in Subsection 4.1 to verify the above analysis.

3.3. Biased sampling distribution. We now consider the scenario where G_0 is substantially cheaper to implement than the remaining Grover operators, and the goal is to minimize the number of queries to $G_i, i = 1, \dots, k-1$. A related problem was studied in [13], where the authors considered the two-operator setting and proposed a deterministic construction under the assumptions that $\mathcal{A}_1 \subset \mathcal{A}_0$ and $|\mathcal{A}_1| \ll |\mathcal{A}_0|$. Our framework requires neither of these restrictions.

By adopting a suitably biased sampling distribution, we can significantly reduce the expected number of applications of the remaining operators, while applying G_0 in the majority of iterations. The following corollary establishes the corresponding performance guarantee.

COROLLARY 3.6. *Let $\delta \in (0, 1/k)$, and suppose that*

$$(3.18) \quad p := \frac{1}{\delta - \frac{4r}{N} - \frac{2(m-r)}{\sqrt{rN}}} \left(\frac{4(m-r)}{\sqrt{rN}} + 2\sqrt{\frac{m-r}{N}} \right) < \frac{1}{k}.$$

At each step, independently apply an operator chosen from $\{G_0, G_1, \dots, G_{k-1}\}$ according to the probability distribution

$$p_0 = 1 - (k-1)p, \quad p_1 = p_2 = \dots = p_{k-1} = p.$$

Then, after

$$T = \Theta \left(\frac{\pi}{4} \sqrt{\frac{N}{r}} \right)$$

steps, measuring the resulting quantum state yields an element in $\cap_{i=0}^{k-1} \mathcal{A}_i$ with probability

$$\mathbb{P}_{\text{succ}}(T) = \mathbb{E}[a_0^2(T)] \geq 1 - \delta.$$

Moreover, the expected total number of applications of $G_1, \dots, G_{k-1}$ is

$$\mathcal{O} \left(\frac{k}{\delta} \cdot \frac{m}{r} \right).$$

Proof. According to Theorem 3.5, we have

$$(3.19) \quad \begin{aligned} 1 - \mathbb{E}[a_0^2(T)] &\leq \frac{4r}{N} + \left(2 + \frac{4}{p} \right) \frac{m-r}{\sqrt{rN}} - \frac{2}{p} \sqrt{\frac{m-r}{N}} \\ &= \frac{4r}{N} + \frac{2(m-r)}{\sqrt{rN}} + \frac{\frac{4(m-r)}{\sqrt{rN}} + 2\sqrt{\frac{m-r}{N}}}{p} = \delta. \end{aligned}$$

Therefore,

$$\mathbb{P}_{\text{succ}}(T) = \mathbb{E}[a_0^2(T)] \geq 1 - \delta.$$

The expected total number of applications of $G_1, \dots, G_{k-1}$ is

$$pT(k-1) = \mathcal{O} \left(\frac{k}{\delta} \cdot \frac{m}{r} \right).$$

□

3.4. Optimality of the random Grover search algorithm. In this section, we analyze the optimality of our approach in terms of query complexity

THEOREM 3.7 (Optimality of the random Grover search algorithm). *Consider $k \geq 1$ distinct Grover operators $G_0, G_1, \dots, G_{k-1}$. For any sequence $G_{i_1}, G_{i_2}, \dots, G_{i_t}$, suppose that the corresponding success probability satisfies*

$$\mathbb{P}_{\text{succ}}(t) = |\langle \mathcal{I}_0 | G_{i_t} G_{i_{t-1}} \cdots G_{i_1} | \psi \rangle|^2 \geq 1 - \delta,$$

where $\delta = \mathcal{O}(1/\sqrt{N})$. Then

$$t = \Omega\left(\frac{\pi}{4} \sqrt{\frac{N}{r}}\right).$$

Proof. Let

$$|\psi_t\rangle := G_{i_t} G_{i_{t-1}} \cdots G_{i_1} |\psi\rangle = \sum_{j=0}^{2^k-1} a_j(t) |\mathcal{I}_j\rangle,$$

and define

$$\sin \theta_t := |a_0(t)| = |\langle \mathcal{I}_0 | \psi_t \rangle|, \quad \theta_t \in \left[0, \frac{\pi}{2}\right].$$

In particular,

$$\sin \theta_0 = |a_0(0)| = \alpha_0.$$

Since

$$O_i |\mathcal{I}_j\rangle = (-1)^{1+j_i} |\mathcal{I}_j\rangle,$$

where we use the binary representation of $j = (j_{k-1} \cdots j_1 j_0)_2$, and

$$G_{i_t} = (2|\psi\rangle\langle\psi| - I)O_{i_t}, \quad |\psi\rangle = \sum_{j=0}^{2^k-1} \alpha_j |\mathcal{I}_j\rangle,$$

we obtain

$$\begin{aligned} a_0(t) &= \langle \mathcal{I}_0 | (2|\psi\rangle\langle\psi| - I)O_{i_t} |\psi_{t-1}\rangle = 2\langle \mathcal{I}_0 | \psi \rangle \langle \psi | O_{i_t} |\psi_{t-1}\rangle - \langle \mathcal{I}_0 | O_{i_t} |\psi_{t-1}\rangle \\ &= 2\alpha_0 \sum_{j=0}^{2^k-1} (-1)^{1+j_{i_t}} \alpha_j a_j(t-1) - (-1)^{1+0_{i_t}} a_0(t-1) \\ &= a_0(t-1) + 2\alpha_0 \sum_{j=0}^{2^k-1} (-1)^{1+j_{i_t}} \alpha_j a_j(t-1), \end{aligned}$$

where we use the fact that $0_i = 0$ for all $i = 0, \dots, k-1$ in the last inequality. Taking absolute values gives

$$\sin \theta_t = |a_0(t)| = \left| a_0(t-1) + 2\alpha_0 \sum_{j=0}^{2^k-1} (-1)^{1+j_{i_t}} \alpha_j a_j(t-1) \right|.$$

Therefore,

$$\begin{aligned}
\sin \theta_t &\leq (1 - 2\alpha_0^2)|a_0(t-1)| + 2\alpha_0 \sum_{j=1}^{2^k-1} \alpha_j |a_j(t-1)| \\
&\leq (1 - 2\alpha_0^2)|a_0(t-1)| + 2\alpha_0 \sqrt{\sum_{j=1}^{2^k-1} \alpha_j^2} \sqrt{\sum_{j=1}^{2^k-1} a_j(t-1)^2} \\
&\leq (1 - 2\alpha_0^2)|a_0(t-1)| + 2\alpha_0 \sqrt{1 - \alpha_0^2} \sqrt{1 - a_0(t-1)^2} \\
&= \cos(2\theta_0) \sin \theta_{t-1} + \sin(2\theta_0) \cos \theta_{t-1} \\
&= \sin(\theta_{t-1} + 2\theta_0).
\end{aligned}$$

It can be shown by induction that

$$(3.20) \quad \theta_t \leq (2t+1)\theta_0, \quad \forall t \leq \frac{\pi}{4\theta_0} - \frac{1}{2}.$$

The case $t = 0$ is immediate. If the relation holds for $t-1$, then for $t \leq \frac{\pi}{4\theta_0} - \frac{1}{2}$, we have

$$\theta_{t-1} + 2\theta_0 \leq (2t-1)\theta_0 + 2\theta_0 = (2t+1)\theta_0 \leq \frac{\pi}{2}.$$

By the monotonicity of the sine function on $(0, \frac{\pi}{2}]$ and $\sin \theta_t \leq \sin(\theta_{t-1} + 2\theta_0)$, we have

$$\theta_t \leq \theta_{t-1} + 2\theta_0 \leq (2t+1)\theta_0.$$

Consequently, the success probability at time t satisfies

$$\mathbb{P}_{\text{succ}}(t) = \sin^2 \theta_t \leq \sin^2((2t+1)\theta_0), \quad \forall t \leq \frac{\pi}{4\theta_0} - \frac{1}{2}.$$

Given $\sin^2((2t+1)\theta_0) \geq \mathbb{P}_{\text{succ}}(t) > 1 - \delta$, we further obtain

$$(3.21) \quad t \geq \frac{\arcsin \sqrt{1-\delta}}{2\theta_0} - \frac{1}{2} \geq \frac{\frac{\pi}{2} - \sqrt{2\delta}}{2(\sin \theta_0 + \sin^3 \theta_0)} - \frac{1}{2} \geq \left(\frac{\pi}{4} - \sqrt{\delta}\right) \cdot \sqrt{\frac{N}{r}} \cdot \frac{N}{N+r} - \frac{1}{2},$$

where we use the inequalities $\arcsin \sqrt{1-\delta} \geq \pi/2 - \sqrt{2\delta}$ and $\theta_0 \leq \sin \theta_0 + \sin^3 \theta_0$.

Let $\delta = \mathcal{O}(1/\sqrt{N})$, we have

$$t = \Omega\left(\frac{\pi}{4} \sqrt{\frac{N}{r}}\right).$$

□

4. Numerical Experiments. In this section, we present several numerical experiments to verify the theoretical results. The code for all simulations is publicly available¹.

4.1. Comparison between deterministic and random strategies. In this group of experiments, we compare a deterministic periodic sequence with the randomized strategy for two Grover operators. The deterministic sequence is

$$G_0, G_1, G_0, G_0, G_1, G_0, G_0, \dots$$

¹https://github.com/greenttt-cell/RGS_code

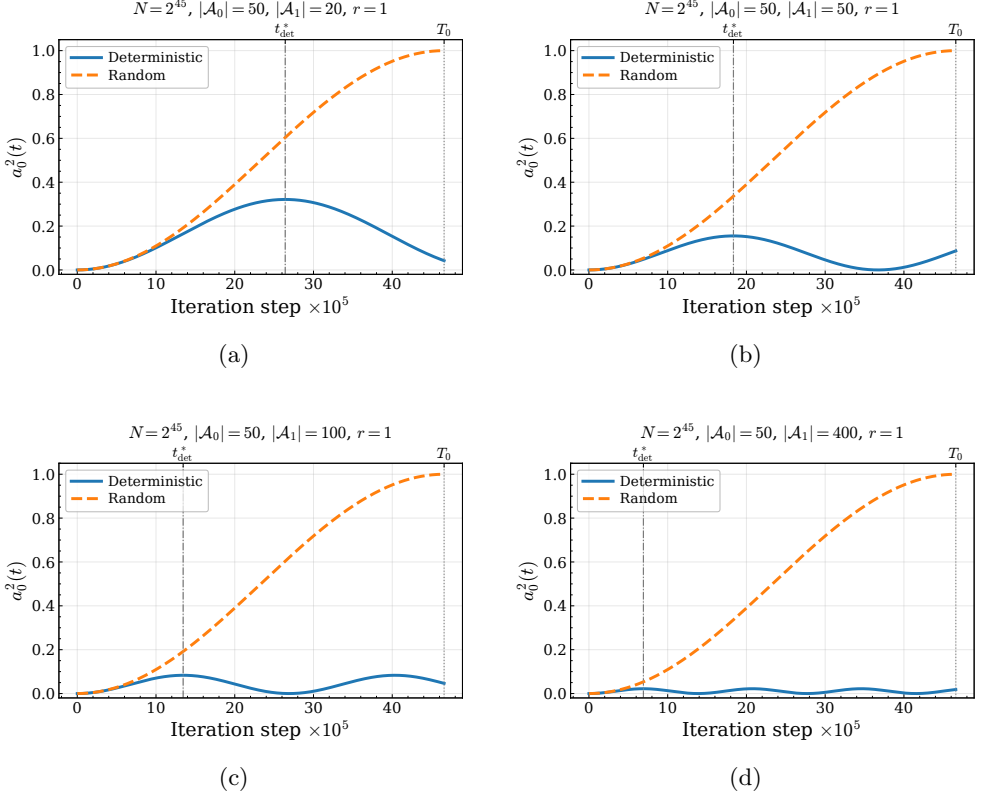


Fig. 3: Comparison between the deterministic periodic sequence and the corresponding randomized strategy under four parameter settings. In each panel, the solid curve represents the deterministic sequence, while the dashed curve shows the empirical mean over 50 independent randomized trials. The vertical dotted line marks the stopping time T , and the dash-dotted vertical line marks the first peak time t_{det}^* of the deterministic curve. The corresponding values of t_{det}^* are 2.6×10^6 , 1.8×10^6 , 1.3×10^6 , and 0.7×10^6 for the four panels, respectively.

so that G_0 and G_1 are applied with frequencies $2/3$ and $1/3$, respectively. In the randomized strategy, G_0 and G_1 are independently selected with probabilities $2/3$ and $1/3$. For each parameter setting, we perform 50 independent randomized trials and plot the empirical mean evolution of the target success probability $a_0^2(t)$.

Figure 3 compares the two approaches under four parameter settings. In all cases, the deterministic periodic sequence exhibits persistent oscillations and fails to amplify the success probability close to 1. By contrast, the randomized strategy yields a nearly monotone increase in the success probability and reaches a value close to 1 near the stopping time T . One may attempt to improve the deterministic approach by terminating the evolution at its first peak time t_{det}^* and boosting the overall success probability through repeated measurements. However, this strategy remains less efficient than the randomized scheme. For example, in Figure 3b

$$t_{\text{det}}^* > 1.8 \times 10^6, \quad a_0^2(t_{\text{det}}^*) < 0.2, \quad \text{and} \quad T < 5.0 \times 10^6.$$

Repeating the deterministic procedure three times yields a total cost exceeding 5.4×10^6 iterations, while the overall success probability remains below

$$1 - (1 - 0.2)^3 = 0.488.$$

Thus, even when combined with repetition, the deterministic strategy is unable to match the performance of the randomized approach.

The advantage of randomized strategy persists as $|\mathcal{A}_1|$ varies over 20, 50, 100, and 400 while the overlap size $|\mathcal{A}_0 \cap \mathcal{A}_1|$ is fixed. As $|\mathcal{A}_1|$ increases, the deterministic sequence becomes progressively less effective, with its maximum success probability decreasing substantially. By contrast, the randomized strategy consistently achieves a success probability close to one.

4.2. Sampling Grover operators with a biased distribution. We next validate Corollary 3.6, which shows that a suitably biased sampling distribution can maintain a high success probability while substantially reducing the use of expensive Grover operators. All simulations are implemented using the reduced matrix representations of the Grover operators in the basis $\{|\mathcal{I}_j\rangle : j = 0, \dots, 2^k - 1\}$. In all experiments, the evolution starts from the uniform superposition state and is run for

$$T = \left\lceil \frac{\pi}{4} \sqrt{\frac{N}{r}} \right\rceil$$

iterations. At each step, a Grover operator is sampled independently according to the distribution specified in Equation (3.18). For each parameter setting, we perform 50 independent trails and estimate the expected success probability

$$\mathbb{P}_{\text{succ}}(t) = \mathbb{E} [a_0^2(t)], \quad t = 1, \dots, T.$$

We first consider the two-operator setting. Fixing $N = 2^{40}$, $|\mathcal{A}_1| = 100$, and $r = 1$, we vary $|\mathcal{A}_0| \in \{100, 1000\}$ and the tolerance parameter $\delta \in \{0.1, 0.3, 0.5\}$. The results are shown in Figure 4. In all cases, the success probability increases steadily and reaches a value exceeding the theoretical guarantee $1 - \delta$ near the stopping time T . As expected, smaller values of δ lead to higher final success probabilities. For comparison, we also include the evolution obtained by repeatedly applying only G_0 . The resulting success probability remains substantially lower, indicating that even infrequent applications of G_1 play an essential role in the amplification process.

We next consider a three-operator setting with $N = 2^{40}$, $|\mathcal{A}_0| = 100$, $|\mathcal{A}_1| = 200$, $|\mathcal{A}_2| = 50$, and $r = 1$. The tolerance parameter δ is chosen from $\{0.005, 0.15, 0.4\}$. As shown in Figure 5a, the success probability again approaches one near T and consistently exceeds the lower bound $1 - \delta$, confirming the prediction of Corollary 3.6.

To examine the sampling distribution, Figure 5b reports the empirical usage ratios of the three Grover operators. In all tested cases, the inexpensive operator G_0 accounts for the overwhelming majority of iterations, while G_1 and G_2 are used only sparingly. Moreover, increasing δ further reduces the usage frequency of the expensive operators while maintaining a high success probability. These observations demonstrate that the proposed biased sampling strategy successfully concentrates queries on low-cost oracles without sacrificing the amplification performance.

5. Conclusion. In this work, we studied a randomized variant of Grover search for solving intersection problems defined by multiple constraints. Instead of constructing a global oracle, which can be costly, our approach directly exploits the

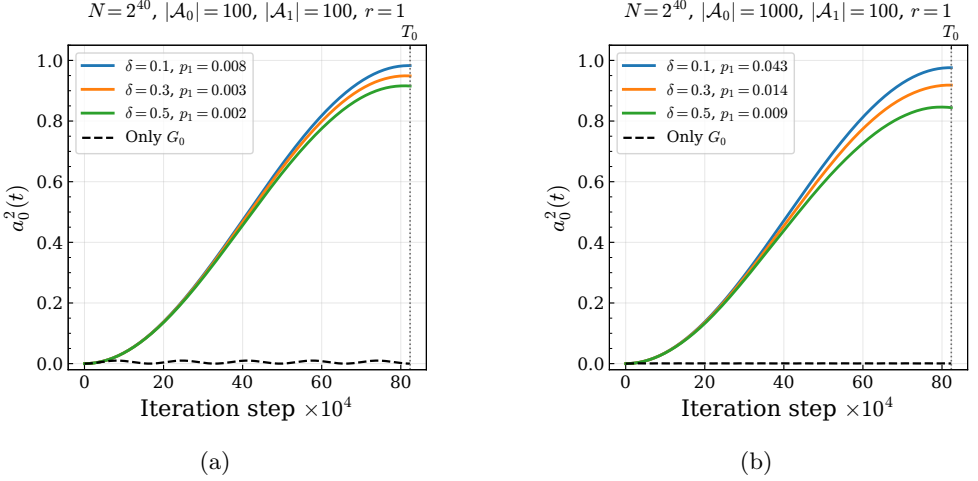


Fig. 4: Success-probability evolution for different values of δ , with fixed $N = 2^{40}$, $|\mathcal{A}_1| = 100$, and $r = 1$. The solid curves show the empirical averages over 50 independent trials, while the dashed curve corresponds to repeatedly applying only G_0 . The vertical dotted line marks the stopping time T .

Grover operators associated with the individual constraints. At each step, a Grover operator is selected according to a prescribed sampling distribution and applied to the quantum state.

Under mild assumptions, we proved that the expected success probability approaches one after

$$\Theta\left(\frac{\pi}{4}\sqrt{\frac{N}{r}}\right)$$

iterations by leveraging the special structure of the expected Grover operator. Furthermore, we showed that a highly biased sampling strategy is sufficient to achieve near-optimal performance, making the proposed framework particularly attractive when the implementation costs of different Grover operators vary significantly. We also established that the randomized algorithm is asymptotically optimal in query complexity: any deterministic sequence of Grover operators that achieves a comparable success probability must incur the same asymptotic complexity. Numerical simulations were conducted to validate the theoretical results and illustrate the effectiveness of the proposed approach across different parameter regimes.

These findings indicate that randomization provides an effective and analyzable mechanism for combining multiple Grover operators, offering a practical alternative when the construction of a global oracle is prohibitively expensive. An interesting direction for future work is to explore the random framework on estimating the number of solutions.

Appendix A. Supplementary Calculations.

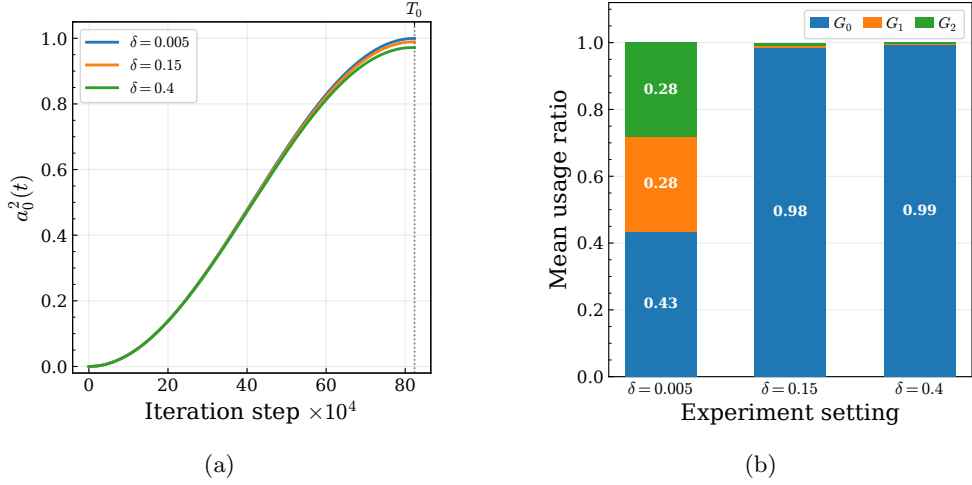


Fig. 5: Numerical results for $N = 2^{40}$, $|\mathcal{A}_0| = 100$, $|\mathcal{A}_1| = 200$, $|\mathcal{A}_2| = 50$, $r = 1$, and $\delta \in \{0.005, 0.15, 0.4\}$. (a) Empirical mean success probability for different values of δ . (b) Corresponding mean usage ratios of G_0 , G_1 , and G_2 .

A.1. Derivation of the expression of $\hat{a}_0(t)$. To compute $\hat{a}_0(t)$ explicitly, we diagonalize the matrix M . The characteristic polynomial of M is given by

$$\lambda^2 - 2(\alpha_3^2 - \alpha_0^2)\lambda + 1 = 0,$$

whose roots are $\lambda_{\pm} = (\alpha_3^2 - \alpha_0^2) \pm \Delta$, where

$$\Delta = \sqrt{(1 - \alpha_0^2 - \alpha_3^2)^2 - 4\alpha_0^2\alpha_3^2}.$$

Thus, M can be diagonalized as

$$M = P \begin{bmatrix} \lambda_+ & 0 \\ 0 & \lambda_- \end{bmatrix} P^{-1},$$

where

$$P = \begin{bmatrix} 2\alpha_0\alpha_3 & 2\alpha_0\alpha_3 \\ \alpha_0^2 + \alpha_3^2 - 1 + \Delta & \alpha_0^2 + \alpha_3^2 - 1 - \Delta \end{bmatrix},$$

and

$$P^{-1} = \frac{1}{4\alpha_0\alpha_3\Delta} \begin{bmatrix} -(\alpha_0^2 + \alpha_3^2 - 1 - \Delta) & 2\alpha_0\alpha_3 \\ \alpha_0^2 + \alpha_3^2 - 1 + \Delta & -2\alpha_0\alpha_3 \end{bmatrix}.$$

Using the fact that

$$M^t = P \begin{bmatrix} \lambda_+^t & 0 \\ 0 & \lambda_-^t \end{bmatrix} P^{-1},$$

we get

(A.1)

$$\hat{a}_0(t) = \frac{\alpha_0(1 - \alpha_0^2 + \alpha_3^2 + \Delta)(\alpha_3^2 - \alpha_0^2 + \Delta)^t + \alpha_0(\alpha_0^2 - \alpha_3^2 - 1 + \Delta)(\alpha_3^2 - \alpha_0^2 - \Delta)^t}{2\Delta}.$$

A.2. Derivation of the expression of W^n . Let $c = \langle u|v \rangle$. The matrix W defined in (3.16) is of the form

$$W = \begin{bmatrix} 1 & 2c \\ -2\bar{c} & 1 - 4|c|^2 \end{bmatrix},$$

and its characteristic polynomial is

$$\lambda^2 - (2 - 4|c|^2)\lambda + 1 = 0.$$

Define θ by $\cos \theta = 1 - 2|c|^2$ (so that $\sin^2(\theta/2) = |c|^2$), yielding eigenvalues $\lambda_{\pm} = e^{\pm i\theta}$. By the Cayley–Hamilton theorem,

$$W^2 - 2\cos \theta W + I = 0,$$

which implies the recurrence

$$W^n = 2\cos \theta W^{n-1} - W^{n-2}, \quad n \geq 2, \quad W^0 = I, \quad W^1 = W.$$

Solving it gives

$$W^n = \frac{\sin(n\theta)}{\sin \theta} W - \frac{\sin((n-1)\theta)}{\sin \theta} I.$$

Substituting W yields

$$W^n = \frac{1}{\sin \theta} \begin{bmatrix} \sin(n\theta) - \sin((n-1)\theta) & 2c \sin(n\theta) \\ -2\bar{c} \sin(n\theta) & (1 - 4|c|^2) \sin(n\theta) - \sin((n-1)\theta) \end{bmatrix}.$$

Therefore,

$$W^n = \frac{1}{\sin \theta} \begin{bmatrix} \sin(n\theta) - \sin((n-1)\theta) & 2\langle u|v \rangle \sin(n\theta) \\ -2\langle v|u \rangle \sin(n\theta) & (1 - 4|\langle u|v \rangle|^2) \sin(n\theta) - \sin((n-1)\theta) \end{bmatrix}$$

A.3. Additional estimates for deterministic prefix variations. In main text, we consider the quantum state

$$(G_0 G_1)^n G_0 |\psi\rangle, \quad \forall n = 0, 1, \dots,$$

and show that the success probability $\mathbb{P}_{\text{succ}}^{(n)} := |\langle \mathcal{I}_0 | (G_0 G_1)^n G_0 |\psi\rangle|^2$ can be significantly smaller than 1 for all n . Here we consider the following two variant sequences

$$G_1 (G_0 G_1)^n G_0 |\psi\rangle \quad \text{and} \quad G_0 G_1 (G_0 G_1)^n G_0 |\psi\rangle.$$

First, since $G_1^\dagger = O_1(2|\psi\rangle\langle\psi| - I)$, we have

$$\|G_1^\dagger |\mathcal{I}_0\rangle - |\mathcal{I}_0\rangle\|_2 = \left\| O_1 \left(2\sqrt{\frac{r}{N}} |\psi\rangle - |\mathcal{I}_0\rangle \right) - |\mathcal{I}_0\rangle \right\|_2 = 2\sqrt{\frac{r}{N}} \|O_1 |\psi\rangle\|_2 \leq 2\sqrt{\frac{r}{N}}.$$

Similarly,

$$\|G_0^\dagger |\mathcal{I}_0\rangle - |\mathcal{I}_0\rangle\|_2 \leq 2\sqrt{\frac{r}{N}}.$$

Consequently,

$$\begin{aligned} \|G_1^\dagger G_0^\dagger |\mathcal{I}_0\rangle - |\mathcal{I}_0\rangle\|_2 &= \|(G_0(G_1 - I) + (G_0 - I))^\dagger |\mathcal{I}_0\rangle\|_2 \\ &\leq \|G_0\|_2 \cdot \|(G_1 - I)^\dagger |\mathcal{I}_0\rangle\|_2 + \|(G_0 - I)^\dagger |\mathcal{I}_0\rangle\|_2 \leq 4\sqrt{\frac{r}{N}}. \end{aligned}$$

For the first prefix variation, we have

$$\begin{aligned}
& |\langle \mathcal{I}_0 | G_1 (G_0 G_0 G_1)^n G_0 | \psi \rangle|^2 \\
& \leq (|\langle \mathcal{I}_0 | (G_1 - I) (G_0 G_0 G_1)^n G_0 | \psi \rangle| + |\langle \mathcal{I}_0 | (G_0 G_0 G_1)^n G_0 | \psi \rangle|)^2 \\
& \leq \left(\|(G_1 - I)^\dagger | \mathcal{I}_0 \rangle\|_2 \cdot \|(G_0 G_0 G_1)^n G_0 | \psi \rangle\|_2 + \sqrt{\mathbb{P}_{\text{succ}}^{(n)}} \right)^2 \\
& \leq \left(2\sqrt{\frac{r}{N}} + \sqrt{\mathbb{P}_{\text{succ}}^{(n)}} \right)^2.
\end{aligned}$$

For the second prefix variation, we similarly have

$$\begin{aligned}
& |\langle \mathcal{I}_0 | G_0 G_1 (G_0 G_0 G_1)^n G_0 | \psi \rangle|^2 \\
& \leq (|\langle \mathcal{I}_0 | (G_0 G_1 - I) (G_0 G_0 G_1)^n G_0 | \psi \rangle| + |\langle \mathcal{I}_0 | (G_0 G_0 G_1)^n G_0 | \psi \rangle|)^2 \\
& \leq \left(\|(G_0 G_1 - I)^\dagger | \mathcal{I}_0 \rangle\|_2 \cdot \|(G_0 G_0 G_1)^n G_0 | \psi \rangle\|_2 + \sqrt{\mathbb{P}_{\text{succ}}} \right)^2 \\
& \leq \left(4\sqrt{\frac{r}{N}} + \sqrt{\mathbb{P}_{\text{succ}}} \right)^2.
\end{aligned}$$

Therefore, both variations are controlled by the base-sequence success probability, up to an additional error of order $\mathcal{O}(\sqrt{r/N})$. Together with the upper bound of $\mathbb{P}_{\text{succ}}^{(n)}$, it shows that the two variations also fail to amplify the success probability close to 1 in the regime $r \ll r_1 < N$.

REFERENCES

- [1] C. H. BENNETT, E. BERNSTEIN, G. BRASSARD, AND U. VAZIRANI, *Strengths and weaknesses of quantum computing*, SIAM Journal on Computing, 26 (1997), pp. 1510–1523, <https://doi.org/10.1137/S0097539796300933>, <https://doi.org/10.1137/S0097539796300933>, <https://arxiv.org/abs/https://doi.org/10.1137/S0097539796300933>.
- [2] F. M. BOLTON, *Accelerated quantum search using partial oracles and grover’s algorithm*, 2024, <https://doi.org/10.48550/arXiv.2403.13035>. arXiv:2403.13035.
- [3] E. CAMPBELL, *A random compiler for fast hamiltonian simulation*, Physical Review Letters, 123 (2019), p. 070503, <https://doi.org/10.1103/PhysRevLett.123.070503>.
- [4] I. CHAKRABARTY, S. KHAN, AND V. SINGH, *Dynamic grover search: Applications in recommendation systems and optimization problems*, Quantum Information Processing, 16 (2017), p. 153, <https://doi.org/10.1007/s11128-017-1600-4>.
- [5] Y.-A. CHEN AND X.-S. GAO, *Quantum algorithm for boolean equation solving and quantum algebraic attack on cryptosystems*, Journal of Systems Science and Complexity, 35 (2022), pp. 373–412, <https://doi.org/10.1007/s11424-020-0028-6>, <https://doi.org/10.1007/s11424-020-0028-6>.
- [6] A. M. CHILDS AND Y. SU, *Faster quantum simulation by randomization*, Physical Review Letters, 123 (2019), p. 050503, <https://doi.org/10.1103/PhysRevLett.123.050503>, <https://arxiv.org/abs/1811.06606>.
- [7] R. ELGENDY, S. KAMEL, AND A. FAROUK, *Efficient quantum algorithms for set operations*, Scientific Reports, 14 (2024), p. 18182, <https://doi.org/10.1038/s41598-024-68230-7>.
- [8] A. GILLIAM, S. WOERNER, AND C. GONCIULEA, *Grover adaptive search for constrained polynomial binary optimization*, Quantum, 5 (2021), p. 428, <https://doi.org/10.22331/q-2021-04-08-428>, <https://arxiv.org/abs/1912.04088>.
- [9] L. K. GROVER, *A fast quantum mechanical algorithm for database search*, in Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC ’96, New York, NY, USA, 1996, Association for Computing Machinery, p. 212–219, <https://doi.org/10.1145/237814.237866>, <https://doi.org/10.1145/237814.237866>.
- [10] L. K. GROVER, *Quantum computers can search rapidly by using almost any transformation*, Physical Review Letters, 80 (1998), pp. 4329–4332, <https://doi.org/10.1103/PhysRevLett.80.4329>.

- [11] T. HOGG, *Adiabatic quantum computing for random satisfiability problems*, Phys. Rev. A, 67 (2003), p. 022314, <https://doi.org/10.1103/PhysRevA.67.022314>, <https://link.aps.org/doi/10.1103/PhysRevA.67.022314>.
- [12] S. JAKES, M. NAEHRIG, M. ROETTELER, AND F. VIRDIA, *Implementing grover oracles for quantum key search on aes and lowmc*, 2019, <https://arxiv.org/abs/1910.01700>, <https://arxiv.org/abs/1910.01700>.
- [13] K. KHADIEV AND E. KRENDELEVA, *Quantum algorithm for searching of two sets intersection*, (2023). arXiv:2312.16897.
- [14] X. LI, H. SHEN, W. GAO, AND Y. LI, *Resource Efficient Boolean Function Solver on Quantum Computer*, Quantum, 8 (2024), p. 1500, <https://doi.org/10.22331/q-2024-10-10-1500>, <https://doi.org/10.22331/q-2024-10-10-1500>.
- [15] K. NAKAJI, M. BAGHERIMEHRAB, AND A. ASPURU-GUZI, *High-order randomized compiler for fast hamiltonian simulation*, arXiv preprint arXiv:2302.14811, (2023).
- [16] C.-Y. PANG, R. ZHOU, C.-B. DING, AND B.-Q. HU, *Quantum search algorithm for set operation*, Quantum Information Processing, 12 (2013), pp. 481–492, <https://doi.org/10.1007/s11128-012-0396-1>.
- [17] T. SALMAN AND Y. BARAM, *Quantum set intersection and its application to associative memory*, Journal of Machine Learning Research, 13 (2012), pp. 3177–3206, <https://jmlr.org/papers/v13/salman12a.html>.
- [18] C. ZHANG, *Randomized algorithms for hamiltonian simulation*, in Monte Carlo and Quasi-Monte Carlo Methods 2010, L. Plaskota and H. Woźniakowski, eds., Springer Berlin Heidelberg, 2012, pp. 709–719, https://doi.org/10.1007/978-3-642-27440-4_42.