Understanding mathematics of Grover's algorithm

Paweł J. Szablowski¹

Received: 12 January 2021 / Accepted: 7 May 2021 / Published online: 26 May 2021
© The Author(s) 2021

Abstract

We analyze the mathematical structure of the classical Grover's algorithm and put it within the framework of linear algebra over the complex numbers. We also generalize it in the sense, that we are seeking not the one 'chosen' element (sometimes called a 'solution') of the dataset, but a set of m such 'chosen' elements (out of $n > m$). Besides, we do not assume that the so-called initial superposition is uniform. We assume also that we have at our disposal an oracle that 'marks,' by a suitable phase change φ , all these 'chosen' elements. In the first part of the paper, we construct a unique unitary operator that selects all 'chosen' elements in one step. The constructed operator is uniquely defined by the numbers φ and α which is a certain function of the coefficients of the initial superposition. Moreover, it is in the form of a composition of two so-called reflections. The result is purely theoretical since the phase change required to reach this heavily depends on α . In the second part, we construct unitary operators having a form of composition of two or more reflections (generalizing the constructed operator) given the set of orthogonal versors. We find properties of these operations, in particular, their compositions. Further, by considering a fixed, 'convenient' phase change φ , and by sequentially applying the so-constructed operator, we find the number of steps to find these 'chosen' elements with great probability. We apply this knowledge to study the generalizations of Grover's algorithm ($m = 1$, $\phi = \pi$), which are of the form, the found previously, unitary operators.

Keywords Quantum computation · Grover's algorithm · Unitary operations

Mathematics Subject Classification Primary 68Q12 · 15A04; Secondary 81P68 · 15B10

The author is very grateful to an unknown referee for pointing out the important positions of the letter overlooked in the first version of the paper.

✉ Paweł J. Szablowski
pawel.szablowski@gmail.com

¹ Emeritus in Department of Mathematics and Information Sciences, Warsaw University of Technology, ul. Koszykowa 75, 00-662 Warsaw, Poland

1 Introduction

Let us note at the beginning that we will avail a notation very commonly used in quantum physics, i.e., the Dirac notation. We will deal with finite- or infinite-dimensional Hilbert spaces $\mathbb{H}$ over the complex numbers. $|x\rangle$ will denote an element of this space (column vector in the case of the finite-dimensional linear space over the complex numbers), $\langle x|$ will denote the dual conjugate of $|x\rangle$, i.e., row vector in the finite-dimensional case, with entries that are conjugates of the entries of the vector $|x\rangle$. $\langle a|b\rangle$ will denote the inner (scalar) product in the space $\mathbb{H}$, while $|a\rangle\langle b|$ will denote the so-called outer product that is explained below.

Namely, the outer product of vectors two $|x\rangle$, $|y\rangle$ denoted by $|x\rangle\langle y|$ means a projection on the one-dimensional space $\text{span}(|x\rangle)$. More precisely

$$|x\rangle\langle y| : \mathbb{H} \ni |z\rangle \rightarrow |x\rangle\langle y|z\rangle \in \mathbb{H}.$$

Let $A : \mathbb{H} \rightarrow \mathbb{H}$ be a unitary operator (matrix in the case of finite-dimensional $\mathbb{H}$) of the form $A = I - 2|1\rangle\langle 1|$, with I denoting identity operator matrix and $|1\rangle$ being the vector of unit length and in the case of $\mathbb{H}$ being n -dimensional, having all identical entries equal to $1/\sqrt{n}$.

By $|b_j\rangle$ let us denote, here, versors having all but j -th entries equal to 0 and the j -th one equal to 1. In terms of quantum mechanics the versors $|b_j\rangle$ are the so-called pure states and the vector $|1\rangle$ is, in fact, certain superposition of the pure states $\{|b_j\rangle\}_{j=1}^n$.

The basis of the famous Grover's algorithm (see, e.g., [1], [4] or [6]) is the following remarkable property of the operator A for $n = 4$. Namely, if we consider versors $|j\rangle$, $j = 1 \dots, 4$ having all entries except for the j -th equal to $1/2$ and the j -th equal to $-1/2$, then $A|j\rangle = -|b_j\rangle$ for all $j = 1, \dots, 4$.

To appreciate this property more, let us imagine that one has a database consisting of 4 elements. We are looking for a particular, 'chosen' element of this base. Suppose that a certain function (an oracle) can be evaluated at every element of this base. In the considered situation, the oracle assigns the value 1 (in fact multiplies by 1, since the action of the oracle must be a unitary operation) to all except for the 'chosen' element of the base and the value -1 to the 'chosen' one. Then, using operator A it is possible to regain this 'chosen' element just in one step.

We will generalize the problem discussed above and construct an algorithm that finds m 'chosen' (or 'special') elements of the database of the size $n > m$. The generalization is also in the sense that the marking of 'selected' elements by an oracle is done by the so-called phase change φ . In the discussed above example, φ was equal to π .

It has to be clearly stated that the problem of finding all m chosen elements of n -element database in one step by suitable choice of phase changing oracle is by no means not new. One has to mention a sequence of papers of Long and his associates such as [7], [8], [9], [12], [13], [14], or [10], [11] or the summarizing and putting in the linear algebraic context, the paper [15].

In the sequel, we are repeating most of the results of these papers, but from the broader and general purely linear algebraic perspective. Moreover, we show that the

structure of Grover's algorithm that has a form of the composition of two the so-called reflection operators (for the definition and properties of such operators see Sect. 3) is uniquely defined. We also slightly generalize the original statement of the algorithm, assuming that the initial superposition is not uniform. In the sequel, we develop a small theory of analysis of generalized reflection operators.

We will construct a unitary operator that finds all chosen m elements of the database of size n in just one step by properly choosing the phase $\varphi = 2 \arcsin \sqrt{\frac{n}{4m}}$, with which the oracle marks chosen elements, provided $n/m \leq 4$. We will also show that so-constructed unitary operator must be of the form:

$$ie^{-i\varphi/2}(\mathbf{I} - (1 - e^{i\varphi})|\mathbf{1}\rangle\langle\mathbf{1}|),$$

with $|\mathbf{1}\rangle$ as described above. Hence, the form of the operator is unique. More precise development of this thought will be presented in Sect. 2.1, however, now we can state, that one cannot find any other finite-dimensional unitary operator in n -dimensional Hilbert space over complex numbers that would find all 'marked elements in the database' in one step. Thus, Grover's algorithm is unique and the 'only one' that does it. The result is purely theoretical (see also Remark 2), however, in the author's belief, it adds to a better understanding of Grover's algorithm.

In particular, it will turn out that if $n/m = 4$ then in just one step, one can find all 'chosen' elements when the phase change is $\varphi = \pi$ like in the classical Grover's algorithm. To complete the list of simple cases, we find also unitary operators that 'find the "chosen" element in one step' when $n/m = 3$, then $\varphi = 2\pi/3$ and when $n/m = 2$ then $\varphi = \pi/2$.

In fact, we generalize Grover's algorithm even further. Namely, we assume that a 'database' is given in the form of the vector $|\mathbf{y}\rangle = \sum_{k=1}^n \sigma_k |b_k\rangle$, with $\sum_{k=1}^n |\sigma_k|^2 = 1$, $\forall k = 1, \dots, n$ $\sigma_k \neq 0$, and we are interested in getting all elements of this database, i.e., say all the elements of the set $\{|b_k\rangle\}_{k \in S}$ for some subset S of the set $\{1, \dots, n\}$ that are 'marked' by an oracle. In quantum mechanical terms, the state $|\mathbf{y}\rangle$ is a superposition of states $\{|b_k\rangle\}_{k=1}^n$ with weights $\{\sigma_k\}_{k=1}^n$. The results similar to the ones described above are presented in Theorem 1.

One has to remark that, obviously, if one makes a measurement (the so-called collapse of the superposition) after applying our unitary operator A , one would get only one of those 'selected' elements. A similar situation would happen if we would have made a measurement on the database itself.

Generally, we can use the outcome of operator A in at least two ways. Firstly, if the phase change φ is exactly equal to $2 \arcsin \sqrt{\frac{n}{4m}}$, we can treat it as the smaller new database, of the size m . That is the outcome is now the superposition of m chosen elements.

Secondly, if the phase change φ is not exactly equal to $2 \arcsin \sqrt{\frac{n}{4m}}$, then one can apply the composition of the operator A . That is to consider A^k and find k such, that the probability of observing elements from the set of 'marked' elements, be equal say greater than, say, .99999. How to find such k is given, below, e.g., by Formula (3.15). Notice that estimating the probability of the outcome is particularly important

in the case of quantum systems because of their random nature. Let us remark that the classical Grover's algorithm works the same way with $m = 1$ and $\varphi = \pi$.

To find such k and generally how to analyze and deal with the composition of reflection operators (the operator A itself and A^k are examples of such composition) is shown in Sect. 3, where the mathematical foundations of our mathematical analysis of the generalized Grover's algorithm are presented in the general setting. More specifically, we will define a certain class of unitary operators, so to say generated by a system of orthonormal versors. Then, to prove certain properties of this class of operators, in particular, to show that the operators of this class constitute a non-commutative, multiplicative ring over complex numbers. As stated above, the operator considered in the literature and known under the name of the Grover's algorithm belongs to this class. Finally, we will make use of the properties of this class of unitary operators and we will analyze the Grover's algorithm and will prove known properties of this algorithm in a different way, in particular, we will estimate the number of its iterations to get the probability of getting the 'chosen' element very close to one. See Subsection 3.1.

Returning to the exact choice of the phase change mentioned above, the outcome of operator A , as the new, smaller database can be used in various ways. The simplest way seems to be speeding up Grover's algorithm at least in some special cases.

To see what we mean and how this idea of speeding up Grover's algorithm would work, let us imagine that we have a database of the size 64 and that we are interested in finding a chosen element. Imagine that the elements of this base are assigned labels ' $i_1 i_2 i_3$ ' where $i_j \in \{1, 2, 3, 4\}$, $j = 1, 2, 3$. Suppose that the 'chosen' element has label ' 111 '. So now, first we apply oracle that marks all elements with $i_1 = 1$. Hence, by applying operator A (with $\varphi = \pi$ as in the Grover's algorithm case) we will get the 'new' database (of the size 16) with elements labeled ' $1i_2 i_3$ '. We apply new oracle that marks all elements with $i_2 = 1$, and then the operator A (again with $\varphi = \pi$) getting the new database of size 4 with elements labeled ' $11i_3$ '. And finally we apply oracle and the operator A (again with $\varphi = \pi$) likewise, for the last time getting our element with label ' 111 '. Notice, that we obtained our 'chosen element' in 3 steps not in $\lfloor 8\pi/4 + 1 \rfloor = 7$ as it would be in the case of the classical Grover's algorithm! This idea can be easily generalized, and we could see that in the case of $n = 4^k$ we could get chosen element in k steps not in $\lfloor \pi 2^{k-2} + 1 \rfloor$ as the results of Grover's algorithm would suggest.

Another possible way of 'speeding up' Grover's algorithm using the results of the paper, although less spectacular than the example above, could be reducing the number of iterations in order to get the 'chosen' element of the base with very high probability. Namely, if, say, the size of the base is $n = n_1 n_2$. Then, direct application of the Grover's algorithm would require $\lfloor \pi \sqrt{n_1 n_2}/4 + 1 \rfloor$ iterates, while the two-stage application of Grover's algorithm firstly with $m = n_1$ and then with $m = 1$ and the vector $|1\rangle$ in the original Grover's algorithm substituted by the outcome of the Grover's algorithm applied in the first stage as the second stage. One can notice that then with such two-stage algorithm would require only $\lfloor \pi \sqrt{n_2}/4 + 1 \rfloor + \lfloor \pi \sqrt{n_1}/4 + 1 \rfloor$ iterations. That is why we needed generalization of the Grover's algorithm presented in Theorem 1. Of course, such reduction was possible under the assumption that we have some partial

knowledge about the 'chosen' item, i.e., that this item is an element of the dataset of size n_1 .

The reduction of the number of iterates was possible, since, according to Remark 8, the necessary number of iterates to find the set of chosen elements with probability close to 1 is $\left\lfloor \frac{\pi}{4} \sqrt{\frac{n}{m}} + 1 \right\rfloor$.

Another purpose of this note is to show that this feature is specific (for the classical Grover's algorithm) only when the ratio $n/m \leq 4$ and $\varphi \in [0, \pi]$. The Grover's algorithm apart from being a source of other important algorithms (to mention only one [3]) was one of the algorithms pointing out the great difference between classical (so to say sequential) computers and quantum ones (at least partially parallel).

The paper consists of three sections. The next one (number 2, below) solves the problem of finding a unitary operator that finds all m 'chosen' elements of the data of size n in one step.

The second Sect. 3 presents, as mentioned above, a generalization of the operator A , mentioned above, in the sense that we consider $k \geq 1$, mutually orthogonal vectors $|x_j\rangle$, $j = 1, \dots, k$ that are used in the construction. We do not confine here ourselves to the fact that we deal with a finite-dimensional situation. The selected vectors $|x_j\rangle$ can be 'chosen' from any Hilbert space. We show how to briefly describe an operator of this kind and what is more we show how to compose such operators. The detailed analysis of the generalization of Grover's algorithm is performed, as stated above, in Subsection 3.1.

The last Sect. 4 contains less important properties of the unitary operator, analyzed in the first section, as well as some less interesting or longer proofs.

2 The choice of all marked elements

In all formulae in the sequel by i , we will denote imaginary unit, i.e., $i = \sqrt{-1}$.

Let us consider a state space $\mathbb{H}$ of dimension n . Let $\{|b_k\rangle\}_{k=1}^n$ constitute the n elements of its orthonormal basis. That is $\langle b_j | b_k \rangle = 1$ if $k = j$ and 0 otherwise.

We start with the following auxiliary problem. Let us imagine that a system is in the state $|y\rangle = \sum_{k=1}^n \sigma_k |b_k\rangle$, where $\sum_{k=1}^n |\sigma_k|^2 = 1$. Let us also assume that $\forall k = 1, \dots, n : \sigma_k \neq 0$ in order to avoid unnecessary confusion. Let us assume that some of the (pure) states of $\{|b_k\rangle\}_{k=1}^n$ for example $\{|b_k\rangle\}_{k \in S}$, where S is a subset of $\{1, \dots, n\}$, are 'chosen,' meaning that there exists a unitary operation J_S (an oracle) that maps say all $|b_j\rangle$, $j = \{1, \dots, n\} \setminus S$ into themselves but $|b_k\rangle$ into $e^{i\varphi} |b_k\rangle$, for $k \in S$, for some $\varphi \in (0, 2\pi)$. Assume that the cardinality of S is m . Let us further denote

$$\alpha = \sqrt{\sum_{k \in S} |\sigma_k|^2}, \quad |y_S\rangle = \frac{1}{\alpha} \sum_{k \in S} \sigma_k |b_k\rangle$$

$$\text{and } |z_S\rangle = \frac{1}{\sqrt{1 - \alpha^2}} \sum_{k \notin S} \sigma_k |b_k\rangle.$$

Hence, $|x_S\rangle$ and $|z_S\rangle$ are mutually orthogonal and we have

$$|y\rangle = \alpha |y_S\rangle + \sqrt{1 - \alpha^2} |z_S\rangle.$$

Let us also define the following vector:

$$\begin{aligned} |v_S\rangle &= \sum_{k \notin S} \sigma_k |b_k\rangle + e^{i\varphi} \sum_{k \in S} \sigma_k |b_k\rangle \\ &= \sqrt{1 - \alpha^2} |z_S\rangle + e^{i\varphi} \alpha |y_S\rangle. \end{aligned}$$

Now, notice that the action of the oracle can be described in terms of unitary operations as an operation defined by an operator

$$J_S = I - (1 - e^{i\varphi}) |y_S\rangle \langle y_S|, \quad (2.1)$$

that has the property that $J_S |y\rangle = |v_S\rangle$.

We want to find a unitary operator $\mathcal{A}$ that maps every vector $|v_S\rangle$ into vector $|y_S\rangle$ for every $S \subset \{1, \dots, n\}$ of cardinality m . Or, in other words, using operator J_S , that for every subset $S \subset \{1, \dots, n\}$ of cardinality m

$$\mathcal{A} J_S |y\rangle = |y_S\rangle. \quad (2.2)$$

Now let us denote by $\varphi = 2 \arcsin \frac{1}{2\alpha}$. By construction, we have $\alpha \in (0, 1)$.

Theorem 1 *The only unitary operator $\mathcal{A}$ satisfying relationship (2.2) for every $S \subset \{1, \dots, n\}$ is when $\frac{1}{2} \leq \alpha < 1$ or equivalently $\pi/3 < \varphi \leq \pi$, and $\mathcal{A}$ has the following form:*

$$\mathcal{A} = -ie^{-i\varphi/2} (I - (1 - e^{i\varphi}) |y\rangle \langle y|). \quad (2.3)$$

In particular, we have:

if $\alpha = 1/2$, then $\varphi = \pi$ and

$$\mathcal{A} = -I + 2 |y\rangle \langle y|,$$

if $\alpha = 1/\sqrt{3}$, then $\varphi = 2\pi/3$ and

$$\mathcal{A} = e^{-i5\pi/6} \left(I - \left(1 - e^{2i\pi/3} \right) |y\rangle \langle y| \right),$$

if $\alpha = 1/\sqrt{2}$, then $\varphi = \pi/2$ and

$$\mathcal{A} = e^{-3i\pi/4} \left(I - \left(1 - e^{i\pi/2} \right) |y\rangle \langle y| \right).$$

Proof Is shifted to Sect. 4.

2.1 The miracle can happen only for $n/m \leq 4$

Now, let us apply the above-mentioned result to the following setting that is, in fact, a generalization of situation met in a famous Grover's algorithm.

Let $|\mathbf{1}\rangle$ denote the vector having all entries equal to $1/\sqrt{n}$. Hence, formally, $|\mathbf{1}\rangle = \frac{1}{\sqrt{n}} \sum_{j=1}^n |b_j\rangle$. $|\mathbf{1}\rangle$ is a state vector (versor) of some quantum system.

Let us define vectors $|V_S\rangle$, by the formula:

$$|V_S\rangle = \frac{1}{\sqrt{n}} \sum_{j \notin S} |b_j\rangle + \frac{e^{i\varphi}}{\sqrt{n}} \sum_{j \in S} |b_j\rangle.$$

Let us denote, as before, $|U_S\rangle = \frac{1}{\sqrt{n-m}} \sum_{j \notin S} |b_j\rangle$ and $|E_S\rangle = \frac{1}{\sqrt{m}} \sum_{j \in S} |b_j\rangle$. Thus, utilizing notation from above we have $\sigma_k = 1/\sqrt{n}$, $k = 1, \dots, n$, $\alpha = \sqrt{m/n}$ and so on.

Hence, we have

$$|V_S\rangle = \sqrt{\frac{n-m}{n}} |U_S\rangle + e^{i\varphi} \sqrt{\frac{m}{n}} |E_S\rangle. \quad (2.4)$$

We have the following result.

Theorem 2 *The only unitary operator $\mathcal{A}$ satisfying relationship (2.2) for every $S \subset \{1, \dots, n\}$ of cardinality m is when $\frac{n}{m} \leq 4$ (equivalently $\frac{1}{2} \leq \alpha < 1$ or $\pi/3 < \varphi \leq \pi$) and $\mathcal{A}$ has the following form:*

$$\mathcal{A} = -ie^{-i\varphi/2} \left(\mathbf{I} - \left(1 - e^{i\varphi} \right) |\mathbf{1}\rangle \langle \mathbf{1}| \right). \quad (2.5)$$

In particular, we have:

if $n/m = 4$, then $\varphi = \pi$ and

$$\mathcal{A} = -\mathbf{I} + 2 |\mathbf{1}\rangle \langle \mathbf{1}|,$$

if $n/m = 3$, then $\varphi = 2\pi/3$ and

$$\mathcal{A} = e^{-i5\pi/6} \left(\mathbf{I} - \left(1 - e^{2i\pi/3} \right) |\mathbf{1}\rangle \langle \mathbf{1}| \right),$$

if $n/m = 2$, then $\varphi = \pi/2$ and

$$\mathcal{A} = e^{-3i\pi/4} \left(\mathbf{I} - \left(1 - e^{i\pi/2} \right) |\mathbf{1}\rangle \langle \mathbf{1}| \right).$$

Proof For the proof, let us notice that in the setting of Theorem 1 we take $\sigma_k = 1/\sqrt{n}$, $k = 1, \dots, n$. Then, consequently we have $\alpha = \sqrt{m/n}$, $|\mathbf{y}\rangle = |\mathbf{1}\rangle$, $|\mathbf{y}_S\rangle = |E_S\rangle$, $|\mathbf{z}_S\rangle = |U_S\rangle$, $|\mathbf{v}_S\rangle = |V_S\rangle$. Then, the result follows immediately. $\square$

Remark 1 Let us note, that the assertion of the theorem states that any proportion $\frac{m}{n}$ of chosen elements of the database of the size n can be found in just one step provided $m/n \geq 1/4$. Moreover, that operator $\mathcal{A}$ must have a form of generalized reflection ‘in the direction $|1\rangle$ ’ and then oracle applied. Since the action of the oracle can also be described as a generalized reflection (compare Formula (2.1)), we see that any algorithm for finding a set of ‘chosen’ elements has to have a form of the composition of two reflections. Hence, we need a new definition.

Definition 1 Let $|x\rangle$ be any versor in $\mathbb{H}$ and φ any real number from the segment $[0, 2\pi)$. Then, the operator

$$\begin{aligned} R(|x\rangle, \varphi) &= I - (1 - e^{i\varphi}) |x\rangle \langle x| \\ &= I + 2ie^{i\varphi/2} \sin(\varphi/2) |x\rangle \langle x|, \end{aligned}$$

will be called a generalized reflection (in brief reflection).

Remark 2 Notice also that, if we could subtract (in the sense of the theory of sets but of course with the help of some unitary operator) from the whole database the set of ‘chosen’ elements, then theoretically by the proper choice of the phase φ we could identify just one chosen element in two steps regardless of the size of the base. Namely, first finding the number $1/\alpha^2 = \frac{n}{n-1}$ and then applying an oracle with the phase change $\varphi = 2 \arcsin(\frac{1}{2\alpha})$. Now following the argument proceeding the theorem we can find just in one step all elements that are not ‘chosen.’ Then, subtracting from the whole base the whole set of ‘unchosen’ elements we can find the ‘chosen’ one. Of course, this is only theory since function $2 \arcsin(\frac{1}{2\alpha})$ is highly nonlinear, so one cannot precisely find the phase φ and another problem is with is the oracle marking all not chosen elements by the precise phase change φ .

3 General unitary operator generated by the ‘chosen’ elements of the base

Keeping in mind that the versor $|1\rangle$ is a linear combination of two orthogonal versors $|U_S\rangle$ and $|E_S\rangle$ and that, in fact, we deal with the composition of operators

$$\begin{aligned} \mathcal{G} = \mathcal{A}J_S &= -ie^{-i\varphi/2} \left(I - \left(1 - e^{i\varphi} \right) \left(\sqrt{1 - \alpha^2} |U_S\rangle + \alpha |E_S\rangle \right) \right) \\ &\times \left(\sqrt{1 - \alpha^2} \langle U_S| + \alpha \langle E_S| \right) \left(I - \left(1 - e^{i\varphi} \right) |E_S\rangle \langle E_S| \right), \end{aligned} \quad (3.1)$$

which, after some algebra, leads to the conclusion that the product is of the general form (3.2) considered below. So first let us analyze the unitary operators of the form (3.2).

Let k be such a natural number that is less or equal than the dimension of $\mathbb{H}$. Finally, let $\{|x_j\rangle\}_{j=1}^k$ be a collection of orthonormal, unit vectors (versors) of $\mathbb{H}$. Let us define

operator $A_k : \mathbb{H} \rightarrow \mathbb{H}$ in the following way:

$$A_k = I - \sum_{j=1}^k \beta_j |x_j\rangle\langle x_j| - \sum_{j \neq l}^k \alpha_{jl} |x_j\rangle\langle x_l|, \quad (3.2)$$

where $\beta_j, \alpha_{jl} \in \mathbb{C}$, $j, l = 1, \dots, k$ and I denotes an identity operator on $\mathbb{H}$.

We will develop, now, tools to deal with the operators given by (3.2).

Let us denote by $\mathbb{H}_k$ the subspace of $\mathbb{H}$ that is spanned by the elements $\{|x_j\rangle\}_{j=1}^k$. Further, let $\mathbb{U}_k$ denote the orthogonal complement of $\mathbb{H}_k$ in $\mathbb{H}$. Now we have $\mathbb{H} = \mathbb{H}_k \oplus \mathbb{U}_k$. Notice that the operator $\sum_{j=1}^k |x_j\rangle\langle x_j|$ is the projection on $\mathbb{H}_k$. Hence, $I - \sum_{j=1}^k |x_j\rangle\langle x_j|$ is the projection on $\mathbb{U}_k$. Now, let consider also a finite-dimensional, involutive algebra over the complex numbers generated by the column vectors y_j with an element $\langle x_j|$ being its j -th entry and 0 being all others. Let the involution $*$ be defined by the rule that y_j^* is a row vector having all entries equal to zero and the j -being equal to $\langle x_j|$. Let $\mathbb{K}_k$ denote a space spanned by elements y_j , $j = 1, \dots, k$. Obviously and naturally $\mathbb{K}_k$ is isomorphic with the subspace $\mathbb{H}_k$ of the space $\mathbb{H}$. Let us denote $Y = \sum_{j=1}^k y_j$. Notice that $Y^* Y = \sum_{j=1}^k |x_j\rangle\langle x_j|$, and $Y Y^* = I_k$ - the identity matrix in $\mathbb{K}_k$.

Remark 3 Further, let's define matrix G_k such that its (j, l) -th entry is given by

$$(G_k)_{jl} = \begin{cases} (1 - \beta_j) & \text{if } j = l \\ -\alpha_{jl} & \text{if } j \neq l \end{cases}. \quad (3.3)$$

Notice that in our notation $Y^* = [|x_1\rangle \dots |x_j\rangle \dots |x_k\rangle]$. Notice that using our notation we have the following equality:

$$Y^* G_k Y = \sum_{j=1}^k |x_j\rangle\langle x_j| - \sum_{j=1}^k \beta_j |x_j\rangle\langle x_j| - \sum_{j \neq l}^k \alpha_{jl} |x_j\rangle\langle x_l|.$$

Hence, operator A_k can be decomposed as follows:

$$A_k = I - \sum_{j=1}^k |x_j\rangle\langle x_j| + Y^* G_k Y. \quad (3.4)$$

As noticed above, the operator $I - \sum_{j=1}^k |x_j\rangle\langle x_j|$ is the projection on the space $\mathbb{U}_k$. Notice also that the operator A_k is completely defined by the set $\{|x_j\rangle\}_{j=1}^k$ and the matrix G_k . Matrix G_k will be called an associated matrix of an operator A_k . We will use simplified notation $O(\{|x_j\rangle\}_{j=1}^k, G_k)$ to denote the operator of the form (3.2) defined by the set $\{|x_j\rangle\}_{j=1}^k$ and the matrix G_k .

We have the following result.

Theorem 3 Let us consider two operators $O_1(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k^{(1)})$ and $O_2(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k^{(2)})$, then their composition, i.e., of the operator $O_1(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k^{(1)})$ and of the operator $O_2(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k^{(2)})$, is of the same class and is equal to $O_3(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k^{(1)} \mathbf{G}_k^{(2)})$. That is the composition operator has its associated matrix being equal to the product of the matrices $\mathbf{G}_k^{(1)}$ and $\mathbf{G}_k^{(2)}$.

Proof Is shifted to Sect. 4. $\square$

Theorem 4 Let us consider an operator $O(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k)$. The following statements are equivalent:

a) The constants $\beta_j, \alpha_{jl} \in \mathbb{C}$, $l, j = 1, \dots, k$ are selected in such a way that

$$-2 \operatorname{Re} \beta_j + |\beta_j|^2 + \sum_{j \neq l} |\alpha_{jl}|^2 = 0, \quad (3.5)$$

$$-\left(\alpha_{jl} + \alpha_{lj}^*\right) + \beta_j^* \alpha_{jl} + \alpha_{lj}^* \beta_l + \sum_{m \neq j, m \neq l} \alpha_{jm}^* \alpha_{ml} = 0, \quad (3.6)$$

for $l, j = 1, \dots, k$.

b) Matrix $\mathbf{G}_k$ associated with O (defined by Formula (3.3)) is unitary.

If one of these conditions is satisfied, then the operator $\mathbf{A}_k$ is unitary.

Proof Is shifted to Sect. 4. $\square$

Remark 4 It can be useful to view $\mathbf{A}_k |y\rangle$ in the following way

$$\mathbf{A}_k |y\rangle = |y\rangle - \sum_{j=1}^k \chi_j(y) |x_j\rangle,$$

where

$$\chi_j(y) = \left(\beta_j \langle x_j | y \rangle + \sum_{l=1, l \neq j}^k \alpha_{jl} \langle x_l | \langle x_l | y \rangle \right). \quad (3.7)$$

Proposition 1 k eigenvalues of the operator $\mathbf{A}_k = O(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k)$ are equal to the eigenvalues of the $k \times k$ unitary matrix $\mathbf{G}_k$ associated with $\mathbf{A}_k$. Moreover, the first k eigenvectors of the operator $\mathbf{A}_k$ are linear combinations of the vectors $|x_j\rangle$. More precisely, suppose that the vector $\boldsymbol{\gamma}^T = (\gamma_1, \dots, \gamma_k)$ is the eigenvector of the matrix $\mathbf{G}_k$ related to the eigenvalue λ . Then, $\mathbf{Y}^* \boldsymbol{\gamma} = \sum_{j=1}^k \gamma_j |x_j\rangle$ is the eigenvector of the operator $\mathbf{A}_k$ related to the eigenvalue λ .

Proof We have

$$\begin{aligned} \mathbf{A}_k \sum_{j=1}^k \gamma_j |x_j\rangle &= \left(\mathbf{I} - \sum_{j=1}^k |x_j\rangle \langle x_j| + \mathbf{Y}^* \mathbf{G}_k \mathbf{Y} \right) \mathbf{Y}^* \boldsymbol{\gamma} \\ &= \mathbf{Y}^* \mathbf{G}_k \mathbf{Y} \mathbf{Y}^* \boldsymbol{\gamma} = \mathbf{Y}^* \mathbf{G}_k \boldsymbol{\gamma} = \lambda \mathbf{Y}^* \boldsymbol{\gamma}. \end{aligned}$$

□

In particular, for any $n \geq 1$ and sets of orthonormal vectors $\{|x_j\rangle\}_{j=1}^n$ and n reals $\{\alpha_j\}_{j=1}^n$ such that $\alpha_j \in (-\pi, \pi]$ the operator

$$A_n = I - \sum_{j=1}^n \left(1 + e^{i\alpha_j}\right) |x_j\rangle\langle x_j|,$$

is unitary. Moreover, its first n eigenvectors are vectors $|x_j\rangle$, $j = 1, \dots, n$ and eigenvalues are numbers $e^{i\alpha_j}$.

Corollary 1 Let A_k be the unitary operator defined by vectors $\{|x_j\rangle\}_{j=1}^k$ given by Formula (3.2) with associated matrix G_k according to (3.3). For any natural m , we have

$$A_k^m = I - \sum_{j=1}^k \beta_j^{(m)} |x_j\rangle\langle x_j| - \sum_{l \neq j}^k \alpha_{jl}^{(m)} |x_j\rangle\langle x_l|,$$

where the matrix $G_k^{(m)}$ defined in the following way

$$\left(G_k^{(m)}\right)_{jl} = \begin{cases} \left(1 - \beta_j^{(m)}\right) & \text{if } j = l \\ -\alpha_{jl}^{(m)} & \text{if } j \neq l \end{cases}$$

is the m -th power of the matrix G_k defined by (3.3) or equivalently

$$A_k^m = I - \sum_{j=1}^k |x_j\rangle\langle x_j| + Y^* G_k^m Y.$$

Proof Follows directly from Theorem 3 and Formula (3.4). □

Corollary 2 Let $A_k = O(\{|x_j\rangle\}_{j=1}^k, G_k)$ be given by Formula (3.2) with the associated matrix G_k according to (3.3) and let us consider vector $|t\rangle = \sum_{j=1}^k \chi_j |x_j\rangle =$

$Y^* \chi$, where $\chi = \begin{bmatrix} \chi_1 \\ \dots \\ \chi_k \end{bmatrix}$ and $\chi_j \in \mathbb{C}$, then

$$A_k |t\rangle = Y^* G_k \chi.$$

In particular,

$$A_k^m |t\rangle = Y^* B_k \Lambda_k^m B_k^{-1} \chi,$$

where $\mathbf{B}_k$ is a $k \times k$ matrix composed of eigenvectors of the matrix $\mathbf{G}_k$ (i.e., for which we have $\mathbf{B}_k^{-1} \mathbf{G}_k \mathbf{B}_k = \mathbf{\Lambda}_k$) and $\mathbf{\Lambda}_k$ is a diagonal matrix with eigenvalues of $\mathbf{G}_k$ on its diagonal.

3.1 Analysis of the generalization of the Grover's algorithm

Let us return to the generalization of the Grover's algorithm presented by Formula (3.1). As remarked above, it is a composition of two reflections. So to analyze it, we will make use of Theorem 3 in order to find the associated matrix of an operator $\mathcal{A}J_S$. Let us select vector $\mathbf{Y}^*$ to be $(|U_S\rangle, |E_S\rangle)$. So operator

$$\mathbf{I} - \left(1 - e^{i\varphi}\right) \left(\sqrt{1 - \alpha^2} |U_S\rangle + \alpha |E_S\rangle\right) \left(\sqrt{1 - \alpha^2} \langle U_S| + \alpha \langle E_S|\right)$$

has associated matrix equal to (after some elementary algebra)

$$\mathbf{G}_1 = \begin{bmatrix} e^{i\varphi} + \alpha^2 (1 - e^{i\varphi}) & -(1 - e^{i\varphi}) \alpha \sqrt{1 - \alpha^2} \\ -(1 - e^{i\varphi}) \alpha \sqrt{1 - \alpha^2} & (1 - e^{i\varphi}) \alpha^2 \end{bmatrix},$$

while the operator

$$\left(\mathbf{I} - \left(1 - e^{i\varphi}\right) |E_S\rangle \langle E_S|\right),$$

has associated matrix given by (also after some elementary algebra)

$$\mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}.$$

Theorem 5 Operator $\mathcal{G} = \mathcal{A}J_S$ has the following associated matrix:

$$\mathbf{G}_S = \begin{bmatrix} -ie^{i\varphi/2} - 2\alpha^2 \sin(\varphi/2) & 2\alpha\sqrt{1 - \alpha^2} e^{i\varphi} \sin(\varphi/2) \\ 2\alpha\sqrt{1 - \alpha^2} \sin(\varphi/2) & -ie^{i\varphi/2} + 2\alpha^2 e^{i\varphi} \sin(\varphi/2) \end{bmatrix}.$$

(a) $\det(\mathbf{G}_S) = -e^{i\varphi}$, $\text{tr}(\mathbf{G}_S) = -2ie^{i\varphi/2}(1 - 2\alpha^2 \sin^2(\varphi/2))$ and the characteristic polynomial of $\mathbf{G}_S$ is given by

$$\lambda^2 + 2\lambda i e^{i\varphi/2} (1 - 2\alpha^2 \sin^2(\varphi/2)) - e^{i\varphi} = 0.$$

(b) Consequently, we get two eigenvalues of the matrix $\mathbf{G}_S$

$$\lambda_1 = -ie^{i\varphi/2} e^{i\theta}, \lambda_2 = -ie^{i\varphi/2} e^{-i\theta}. \quad (3.8)$$

where we denoted by $\theta(\alpha, \varphi) \in [-\pi/2, 0]$ (or θ if it will be not confusing) the positive angle such that

$$e^{i\theta} = (1 - 2\alpha^2 \sin^2(\varphi/2)) + 2i\alpha \sin(\varphi/2)\sqrt{1 - \alpha^2 \sin^2(\varphi/2)}. \quad (3.9)$$

(c) Eigenvectors of $\mathbf{G}_S$ are the columns of the following matrix

$$\mathcal{B} = \begin{bmatrix} e^{i\varphi/2} \sin \gamma & -e^{i\varphi/2} \cos \gamma \\ \cos \gamma & \sin \gamma \end{bmatrix}. \quad (3.10)$$

where angle γ is defined by

$$e^{i\gamma} = \frac{1}{\sqrt{b^2 + 1}} + i \frac{b}{\sqrt{b^2 + 1}},$$

and where we denoted

$$b = \frac{\sqrt{1 - \alpha^2 \sin^2(\varphi/2)} - \alpha \cos(\varphi/2)}{\sqrt{1 - \alpha^2}}. \quad (3.11)$$

Proof Is shifted to Sect. 4. $\square$

Remark 5 Notice that both extreme values of θ are reached since we see that for $\varphi = 0$ we have $\theta = 0$, while for α and φ satisfying $\sin(\varphi/2) = -\frac{\sqrt{2}}{2\alpha}$ we have $\theta = -\pi/2$.

As a corollary, we get the following expression for the result of k -iterations of the operator $\mathcal{G}$ acting on the overseer $|\mathbf{1}\rangle$.

Corollary 3

$$\begin{aligned} (\mathcal{G})^k |\mathbf{1}\rangle &= (|U_S\rangle, |E_S\rangle) \\ &\left[\begin{array}{l} (-ie^{i\varphi})^k (\cos \delta (-i \cos(2\gamma) \sin(k\theta) + \cos(k\theta)) + ie^{i\varphi/2} \sin(k\theta) \sin(2\gamma) \sin \delta) \\ (-ie^{i\varphi})^k (ie^{-i\varphi/2} \sin(k\theta) \sin 2\gamma \cos \delta + \sin \delta (i \cos(2\gamma) \sin(k\theta) + \cos(k\theta))) \end{array} \right], \end{aligned} \quad (3.12)$$

$$(3.13)$$

where we denoted for simplicity by δ the angle defined by the relationship

$$e^{i\delta} = \sqrt{1 - \alpha^2} + i\alpha. \quad (3.14)$$

Consequently,

$$\Pr \left((\mathcal{G})^k |\mathbf{1}\rangle = E_S \right) = \left| ie^{-i\varphi/2} \sin(k\theta) \sin 2\gamma \cos \delta + \sin \delta (i \cos(2\gamma) \sin(k\theta) + \cos(k\theta)) \right|^2. \quad (3.15)$$

Proof Is shifted to Sect. 4. $\square$

One can simplify this expression further by noticing that

$$\begin{aligned}\sin(2\gamma) &= \frac{2b}{b^2 + 1} = \sqrt{\frac{1 - \alpha^2}{1 - \alpha^2 \sin(\varphi/2)^2}}, \\ \cos(2\gamma) &= \frac{b^2 - 1}{b^2 + 1} = \frac{\alpha \cos(\varphi/2)}{\sqrt{1 - \alpha^2 \sin(\varphi/2)^2}},\end{aligned}$$

and recalling definitions of the Chebyshev polynomials of the first and second kind, namely that:

$$T_m(\cos x) = \cos(mx) \text{ and } U_m(\cos x) = \frac{\sin((m+1)x)}{\sin x}.$$

Thus, we could express $\Pr((\mathcal{G})^k | \mathbf{1}) = E_S$ as a function of φ , α and k only, to study what is the smallest number of iterates k , to ensure, for a given α and φ , that this probability is, say, greater than .999. We could also construct tables of $\Pr((\mathcal{G})^k | \mathbf{1}) = E_S$ for given φ , α and k .

Since intention of this paper is to give a theoretical outlook for the Grover's algorithm, we will skip those calculations. We will make use of Chebyshev polynomials in the following subsection when we will apply the obtained formulae to the classical Grover's algorithm.

Remark 6 Notice that the properties of the matrix $\mathbf{G}_S$, essential in finding the desired properties of the output vector, depend only on parameters α and φ . Hence, we can treat the output of, say, k iterates of the operator $\mathbf{A}_n$ as the input of the similar operation with the other oracle to refine the search. Just as described in the introductory section.

3.1.1 Analysis of the classical Grover's algorithm

Returning to the first section and the definition of the Grover's algorithm (see, e.g., [4] or [6]) we see that we deal with the classical case when $\varphi = \pi$. Then, notice that parameter b (defined by (3.11)) is equal to 1 which means that angle $\gamma = \pi/4$. More precisely in classical Grover's algorithm α was equal to $1/\sqrt{n}$, where n is size of the database. We will extend the definition of the Grover's algorithm by assuming that $\alpha \in (0, \frac{1}{2}]$. In this subsection, we are going to derive known properties of the Grover's algorithm from the general considerations and formulae presented above.

Following considerations above, we see that the associated matrix $\mathbf{G}_S$ of the operator where matrix $\mathbf{G}$ has a form:

$$\mathbf{G}_S = \begin{bmatrix} 1 - 2\alpha^2 & -2\alpha\sqrt{1 - \alpha^2} \\ 2\alpha\sqrt{1 - \alpha^2} & 1 - 2\alpha^2 \end{bmatrix}.$$

The eigenvalues of the matrix G_S are (following (3.8))

$$\xi_1 = i \frac{n - 2m + 2i\sqrt{m(n-m)}}{n} \stackrel{df}{=} ie^{i\theta_{m,n}},$$

$$\text{and } \xi_2 = i \frac{n - 2m - 2i\sqrt{m(n-m)}}{n} = ie^{-i\theta_{m,n}}$$

and the related eigenvectors compose the following matrix B is equal to (by (3.10))

$$B = \begin{bmatrix} \frac{i}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

Although almost all the results of the following assertion can be derived directly from the results of the previous section, for the sake of clarity and importance we will present them in the form of the theorem.

Theorem 6

$$\begin{aligned} G^k |1\rangle &= (i)^k (|U_S\rangle \cos(k\theta_{m,n} + \delta) + |E_S\rangle \sin(k\theta_{m,n} + \delta)), \\ \Pr(\Gamma_S^k | Y_S) = E_S) &= (\sin(k\theta_{m,n} + \delta))^2. \end{aligned}$$

where δ is defined by (3.14). We have also

$$\Pr(\Gamma_S^k | Y_S) = E_S) \stackrel{df}{=} F_k(\alpha) = (\alpha T_{2k}(\alpha) + (1 - \alpha^2) U_{2k-1}(\alpha))^2, \quad (3.16)$$

where T_n and U_n denote Chebyshev polynomials of the first and second type, respectively. Besides for small values of x for $l \geq 0$ and $k \cong \frac{\pi(2l+1)}{4\alpha} - 1$, we get $\Pr(\Gamma_S^k | Y_S) = E_S) \cong 1$.

In the simplification of Formula (3.16), we have used the following well-known properties of Chebyshev polynomials: for $n \geq 0$ and $x \in \mathbb{R}$:

$$\begin{aligned} T_n(-x) &= (-1)^{n-1} T_n(x), \quad T_n(2x^2 - 1) = T_{2n}(x), \\ 2xU_n(1 - 2x^2) &= (-1)^n U_{2n+1}(x). \end{aligned}$$

Corollary 4 Now notice that to have the element of the set S to be ‘chosen’ for sure we have to have $|\sin(k\theta_{m,n} + \delta)| = 1$, that is

$$k\theta_{m,n} + \delta = l\pi, \quad (3.17)$$

for some integers m, n, k and l . The simplest case is when $k = 1$ and $l = 0$. Then, this equation reduces to $\theta_{m,n} = \delta$ which leads to the equation

$$1 - 2\alpha^2 = \alpha.$$

The only positive solution of this equation is $\alpha = 1/2$, which refers to the well-known property of the Grover's algorithm that if $n/m = 4$ then all 'chosen' elements can be chosen in one step. Thus, quantum computers can find all elements of the set consisting of the quarter of the population in one step! Of course the state collapse will produce only one state of the set S . However, the system is in E_S after just one iteration.

Remark 7 We have $\forall k \geq 1 : F_k(\frac{\sqrt{2}}{2}x)^2 = 1/2$. In other words, the set of the size of half of the population can be identified by algorithm Γ_S only with probability $1/2$. However, as it follows from the first part of the paper, we can obtain all 'chosen' elements in just one step, provided that the oracle marked chosen elements by the phase change $\pi/2$ not π as in the case of the classical Grover's algorithm.

Further, using Mathematica, we get $F_1(\frac{\sqrt{3}}{3}) = .92$, $F_6(\frac{\sqrt{3}}{3}) = .978$ and $F_{11}(\frac{\sqrt{3}}{3}) = .99982$. That is by iterating Γ_S only 11 times, we can identify a subset of 'chosen' elements of the size of $1/3$ of the population with very big probability. As shown above, we have $F_1(1/2) = 1$. Again, as it follows from the considerations presented in the first part of the paper, this selection of $1/3$ of the population can be done in just one step provided the oracle would mark all chosen elements by changing their phase change by $2\pi/3$.

Again using Mathematica, we have $F_8(\frac{\sqrt{5}}{5}) = .999214$, $F_{20}(\frac{\sqrt{6}}{6}) = .99864$, $F_{38}(\frac{\sqrt{7}}{7}) = .999999965$.

Remark 8 Notice also that if m is fixed and n is very large then the optimal number of iterations to get the probability of selecting the set S with probability close to 1 is approximately $\frac{\pi}{4} \sqrt{\frac{n}{m}}$. This result is known for $m = 1$ and firstly noted in [2].

4 Proofs and auxiliary remarks

Proof of Theorem 1 First of all notice, that $|v_S\rangle = |y\rangle + \alpha(e^{i\varphi} - 1)|y_S\rangle$. Hence, we are looking for a unitary operator that satisfies n equations

$$\mathcal{A}(|y\rangle + \alpha(e^{i\varphi} - 1)|y_S\rangle) = |y_S\rangle$$

for every $S \subset \{1, \dots, n\}$ of cardinality m . Multiplying both sides by $\mathcal{A}^*$, we get

$$|y\rangle = (\mathcal{A}^* - \alpha(e^{i\varphi} - 1)\mathbf{I})|y_S\rangle, \quad (4.1)$$

for every $S \subset \{1, \dots, n\}$ of cardinality m . The above-mentioned equality implies that the matrix $(\mathcal{A}^* - \alpha(e^{i\varphi} - 1)\mathbf{I})$ is of rank 1. Thus, we must have

$$(\mathcal{A}^* - \alpha(e^{i\varphi} - 1)\mathbf{I}) = |x_1\rangle\langle x_2|,$$

for some vectors $|\mathbf{x}_1\rangle$ and $|\mathbf{x}_2\rangle$. To get to know vectors $|\mathbf{x}_1\rangle$ and $|\mathbf{x}_2\rangle$ better, let us write

$$\begin{aligned}\mathcal{A}^* &= \alpha \left(e^{i\varphi} - 1 \right) \mathbf{I} + |\mathbf{x}_1\rangle \langle \mathbf{x}_2|, \\ \mathcal{A} &= \alpha \left(e^{-i\varphi} - 1 \right) \mathbf{I} + |\mathbf{x}_2\rangle \langle \mathbf{x}_1|,\end{aligned}$$

and multiply these equations side by side getting:

$$\begin{aligned}\mathbf{I} &= \mathcal{A}^* \mathcal{A} = 2\alpha^2 (1 - \cos \varphi) \mathbf{I} + \langle \mathbf{x}_2 | \mathbf{x}_2 \rangle |\mathbf{x}_1\rangle \langle \mathbf{x}_1| \\ &\quad + \alpha \left(e^{i\varphi} - 1 \right) |\mathbf{x}_2\rangle \langle \mathbf{x}_1| + \alpha \left(e^{-i\varphi} - 1 \right) |\mathbf{x}_1\rangle \langle \mathbf{x}_2| \\ &= \mathcal{A} \mathcal{A}^* = 2\alpha^2 (1 - \cos \varphi) \mathbf{I} + \langle \mathbf{x}_1 | \mathbf{x}_1 \rangle |\mathbf{x}_2\rangle \langle \mathbf{x}_2| \\ &\quad + \alpha \left(e^{i\varphi} - 1 \right) |\mathbf{x}_2\rangle \langle \mathbf{x}_1| + \alpha \left(e^{-i\varphi} - 1 \right) |\mathbf{x}_1\rangle \langle \mathbf{x}_2|.\end{aligned}$$

Hence, we see that

$$\frac{|\mathbf{x}_1\rangle \langle \mathbf{x}_1|}{\langle \mathbf{x}_1 | \mathbf{x}_1 \rangle} = \frac{|\mathbf{x}_2\rangle \langle \mathbf{x}_2|}{\langle \mathbf{x}_2 | \mathbf{x}_2 \rangle}.$$

Thus, we deduce that $|\mathbf{x}_1\rangle$ and $|\mathbf{x}_2\rangle$ are parallel. Consequently, let $|\mathbf{x}_1\rangle \langle \mathbf{x}_2| = \gamma |\mathbf{x}_1\rangle \langle \mathbf{x}_1|$. Besides, let us select $|\mathbf{x}_1\rangle$ to be normalized, i.e., $\langle \mathbf{x}_1 | \mathbf{x}_1 \rangle = 1$. Relationship (4.1) implies that $|\mathbf{x}_1\rangle$ must be parallel to $|\mathbf{y}\rangle$ so since it is assumed to be a versor we must have $|\mathbf{x}_1\rangle = |\mathbf{y}\rangle$. Now notice that $\langle \mathbf{y} | \mathbf{y}_S \rangle = \alpha$. Consequently, parameter γ must satisfy

$$1 = \gamma \alpha, \quad (4.2)$$

or $\gamma = 1/\alpha$. Further, we have

$$\mathbf{I} = 2\alpha^2 (1 - \cos \varphi) \mathbf{I} + |\gamma|^2 |\mathbf{x}_1\rangle \langle \mathbf{x}_1| + 2\alpha \operatorname{Re}(\gamma^* \left((e^{i\varphi} - 1) \right)^2 |\mathbf{x}_1\rangle \langle \mathbf{x}_1|).$$

Consequently, the following system of two equations must be satisfied:

$$2\alpha^2 (1 - \cos \varphi) = 1, \quad (4.3)$$

$$\frac{1}{\alpha^2} + 2\alpha \frac{1}{\alpha} \operatorname{Re} \left(e^{i\varphi} - 1 \right) = \frac{1}{\alpha^2} + 2(\cos \varphi - 1) = 0. \quad (4.4)$$

From the first one, we get

$$1 - \cos \varphi = 2 \sin^2(\varphi/2) = \frac{1}{2\alpha^2},$$

from which it follows that the smallest α^2 , for which we can get equality (4.1) is $1/4$ and that it can happen only when $\varphi = \pi$. Notice also that if $\varphi = 2 \arcsin \frac{1}{2\alpha}$, then not

only the first (i.e., (4.3)) but also the second equation (i.e., (4.4)) is satisfied. So the operator in question is given by the following formula:

$$\mathcal{A} = \alpha \left(e^{-i\varphi} - 1 \right) \mathbf{I} + \frac{1}{\alpha} |\mathbf{y}\rangle \langle \mathbf{y}|.$$

Now notice that

$$\begin{aligned} \alpha \left(e^{-i\varphi} - 1 \right) &= \frac{\cos \varphi - 1 - i \sin \varphi}{2 \sin(\varphi/2)} = \frac{-2 \sin^2(\varphi/2) - 2i \sin(\varphi/2) \cos(\varphi/2)}{2 \sin(\varphi/2)} \\ &= -\sin(\varphi/2) - i \cos(\varphi/2) = -ie^{-i\varphi/2}. \end{aligned}$$

Secondly, notice that

$$\begin{aligned} ae^{i\varphi/2} &= 2 \sin(\varphi/2)(\cos(\varphi/2) + i \sin(\varphi/2)) \\ &= \sin \varphi + i(1 - \cos \varphi) = i(1 - \cos \varphi - i \sin \varphi) \\ &= i(1 - e^{i\varphi}). \end{aligned}$$

This formula can be nicely transformed to

$$\mathcal{A} = -ie^{-i\varphi/2} \left(\mathbf{I} - \left(1 - e^{i\varphi} \right) |\mathbf{y}\rangle \langle \mathbf{y}| \right).$$

Now if $\alpha = 1/2$, then $\varphi = \pi$ and we have

$$\mathcal{A} = -\mathbf{I} + 2|\mathbf{y}\rangle \langle \mathbf{y}|,$$

if $\alpha = 1/\sqrt{3}$, then $\varphi = 2\pi/3$ and we have

$$\mathcal{A} = e^{-i5\pi/6} \left(\mathbf{I} - \left(1 - e^{2i\pi/3} \right) |\mathbf{y}\rangle \langle \mathbf{y}| \right),$$

if $\alpha = 1/\sqrt{2}$, then $\varphi = \pi/2$ and we have:

$$\mathcal{A} = e^{-3i\pi/4} \left(\mathbf{I} - \left(1 - e^{i\pi/2} \right) |\mathbf{y}\rangle \langle \mathbf{y}| \right).$$

□

Proof of Theorem 3 We will use the form (3.4). We have

$$\begin{aligned} &O_1(\{|x_j|\}_{j=1}^k, \mathbf{G}_k^{(1)}) O_2(\{|x_j|\}_{j=1}^k, \mathbf{G}_k^{(2)}) \\ &= \left(\mathbf{I} - \sum_{j=1}^k |x_j\rangle \langle x_j| + \mathbf{Y}^* \mathbf{G}_k^{(1)} \mathbf{Y} \right) \left(\mathbf{I} - \sum_{j=1}^k |x_j\rangle \langle x_j| + \mathbf{Y}^* \mathbf{G}_k^{(2)} \mathbf{Y} \right) \\ &= \mathbf{I} - \sum_{j=1}^k |x_j\rangle \langle x_j| + \mathbf{Y}^* \mathbf{G}_k^{(1)} \mathbf{Y} \mathbf{Y}^* \mathbf{G}_k^{(2)} \mathbf{Y} = \mathbf{I} - \sum_{j=1}^k |x_j\rangle \langle x_j| + \mathbf{Y}^* \mathbf{G}_k^{(1)} \mathbf{G}_k^{(2)} \mathbf{Y}. \end{aligned}$$

□

Proof of Theorem 4 By Theorem 3, we know that given two operators $O_1(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k^{(1)})$ and $O_2(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k^{(2)})$, whose associated matrices satisfy

$$\mathbf{G}_k^{(1)} \mathbf{G}_k^{(2)} = \mathbf{I}_k,$$

we deduce that the composition of these two operators is equal to

$$\mathbf{I} - \sum_{j=1}^k |x_j\rangle \langle x_j| + \sum_{j=1}^k |x_j\rangle \langle x_j| = \mathbf{I}.$$

In other words, an operator $O(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k^{-1})$ is an inverse of the operator $O(\{|x_j\rangle\}_{j=1}^k, \mathbf{G}_k)$. Now notice

$$\mathbf{G}_k^* = \begin{cases} (1 - \beta_j^*) & \text{if } j = l \\ -\alpha_{lj}^* & \text{if } j \neq l \end{cases}.$$

Consequently, we have

$$(\mathbf{G}_k^* \mathbf{G}_k)_{jl} = \begin{cases} |1 - \beta_j|^2 + \sum_{m \neq j} |\alpha_{jm}|^2 & \text{if } j = l \\ (1 - \beta_j) \alpha_{jl}^* + (1 - \beta_l^*) \alpha_{lj} + \sum_{m \neq j, m \neq l} \alpha_{jm} \alpha_{ml}^* & \text{if } j \neq l \end{cases},$$

which together with the requirement that $\mathbf{G}_k^* \mathbf{G}_k$ is the identity matrix lead to equations (3.5) and (3.6). $\square$

Proof of Theorem 5 We have $\mathbf{G}_S = \mathbf{G}_2 \mathbf{G}_1$. Now we get expressions for the determinant and the trace of the matrix $\mathbf{G}_S$ by direct calculations. Using the well-known formula expressing characteristic polynomial of the 2×2 matrix by its determinant and the trace, we get the characteristic polynomial of $\mathbf{G}_S$. We solve it directly and obtain:

$$\begin{aligned} \lambda_1 &= -ie^{i\varphi/2} \left(\left(1 - 2\alpha^2 \sin^2(\varphi/2) \right) + 2i\alpha \sin(\varphi/2) \sqrt{1 - \alpha^2 \sin^2(\varphi/2)} \right), \\ \lambda_2 &= -ie^{i\varphi/2} \left(\left(1 - 2\alpha^2 \sin^2(\varphi/2) \right) - 2i\alpha \sin(\varphi/2) \sqrt{1 - \alpha^2 \sin^2(\varphi/2)} \right), \end{aligned}$$

for the eigenvalues. Further, we get

$$\begin{aligned} v_1^T &= \left(e^{i\varphi/2} \frac{-\alpha \cos(\varphi/2) + \sqrt{1 - \alpha^2 \sin^2(\varphi/2)}}{\sqrt{1 - \alpha^2}}, 1 \right) = \left(e^{i\varphi/2} b, 1 \right) \\ v_2^T &= \left(-e^{i\varphi/2} \frac{\alpha \cos(\varphi/2) + \sqrt{1 - \alpha^2 \sin^2(\varphi/2)}}{\sqrt{1 - \alpha^2}}, 1 \right) = \left(-e^{i\varphi/2} \frac{1}{b}, 1 \right), \end{aligned}$$

for the eigenvectors. Now, it is a matter of little algebra to normalize them and to form matrix $\mathbf{B}$ out of coefficients of the so obtained vectors. $\square$

Proof of Corollary 3 By Proposition 1, we deduce that the eigenvectors of the operator $\mathcal{G}$ are given by the relationship

$$\begin{bmatrix} |g_1\rangle \\ |g_2\rangle \end{bmatrix} = \mathcal{B} \begin{bmatrix} |U_S\rangle \\ |E_S\rangle \end{bmatrix}.$$

Consequently, we have

$$\mathcal{B}^{-1} \begin{bmatrix} |g_1\rangle \\ |g_2\rangle \end{bmatrix} = \begin{bmatrix} |U_S\rangle \\ |E_S\rangle \end{bmatrix},$$

Now recall Formula (2.4). We see that vector $|\mathbf{1}\rangle$ is given by

$$|\mathbf{1}\rangle = (|U_S\rangle, |E_S\rangle) \begin{bmatrix} \sqrt{1-\alpha^2} \\ \alpha \end{bmatrix},$$

We have

$$\begin{aligned} (\mathcal{G})^k |\mathbf{1}\rangle &= (\mathcal{G})^k |\mathbf{1}\rangle = \mathcal{B} \mathcal{B}^{-1} (\mathcal{G})^k \mathcal{B} \mathcal{B}^{-1} |\mathbf{1}\rangle \\ &= \begin{bmatrix} e^{i\varphi/2} \sin \gamma & -e^{i\varphi/2} \cos \gamma \\ \cos \gamma & \sin \gamma \end{bmatrix} \begin{bmatrix} e^{ik\theta} & 0 \\ 0 & e^{-ik\theta} \end{bmatrix} \\ &\quad \times \begin{bmatrix} e^{-i\varphi/2} \sin \gamma & \cos \gamma \\ -e^{-i\varphi/2} \cos \gamma & \sin \gamma \end{bmatrix} \begin{bmatrix} \cos \delta \\ \sin \delta \end{bmatrix} \\ &= (-i)^k e^{ik\varphi/2} \begin{bmatrix} e^{i\varphi/2} \sin \gamma & -e^{i\varphi/2} \cos \gamma \\ \cos \gamma & \sin \gamma \end{bmatrix} \\ &\quad \times \begin{bmatrix} e^{ik\theta} (e^{-i\varphi/2} \sin \gamma \cos \delta + \cos \gamma \sin \delta) \\ e^{-ik\theta} (-e^{-i\varphi/2} \cos \gamma \cos \delta + \sin \gamma \sin \delta) \end{bmatrix} \\ &= \begin{bmatrix} e^{ik\theta} (e^{ik\varphi/2} \sin^2 \gamma \cos \delta + e^{i(k+1)\varphi/2} \cos \gamma \sin \gamma \sin \delta) \\ +e^{-ik\theta} (e^{ik\varphi/2} \cos^2 \gamma \cos \delta + e^{i(k+1)\varphi/2} \cos \gamma \sin \gamma \sin \delta) \\ e^{ik\theta} (e^{i(k-1)\varphi/2} \sin \gamma \cos \gamma \cos \delta + e^{ik\varphi/2} \cos^2 \gamma \sin \delta) \\ +e^{-ik\theta} (-e^{i(k-1)\varphi/2} \cos \gamma \sin \gamma \cos \delta + e^{ik\varphi/2} \sin^2 \gamma \sin \delta) \end{bmatrix}. \end{aligned}$$

□

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Grover, Lov K.: Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Phys. Rev. Lett.* **79**(2), 325 (1997)
2. Zalka, Cristof: Grover's quantum searching algorithm is optimal. *Phys. Rev. A* **60**, 2746–2751 (1999)
3. Baritomp, W.P., Bulger, D.W., Wood, G.R.: Grover's Quantum Algorithm Applied to Global Optimization. *SIAM J. Opt.* **15**(4), 1170–1184 (2005)
4. Emma Strubell.: An Introduction to Quantum Algorithms, COS498-Chawathe, (2011)
5. Diao, Zijian: Exactness of the original Grover search Algorithm. *Physical Review A* **82**, 044301 (2010)
6. Chappell, James M., Iqbal, Azhar; Lohe, M. A., von Smekal, Lorenz, Abbott, Derek.: An improved formalism for quantum computation based on geometric algebra—case study: Grover's search algorithm. *Quantum Inf. Process.* **12**(4), 1719–1735 (2013)
7. Long GuiLu, Zhang WeiLin, Li YanSong, NIU L.: Arbitrary phase rotation of the marked state cannot be used for Grover's quantum search algorithm., *Commun. Theor. Phys. (Beijing, China)* **32**, pp 335–3388 (1999)
8. Long, Gui, Lu, Li, Yan, Song, Zhang, Wei, Lin, Niu, Li.: Phase matching in quantum searching. *Phys. Lett. A* **262**(1), 27–34 (1999)
9. Long, Gui-Lu, Li, Xiao, Sun, Yang: Phase matching condition for quantum search with a generalized initial state. *Phys. Lett. A* **294**(3–4), 143–152 (2002)
10. Li, Dafa, et al.: Invariants of Grover's algorithm and the rotation in space. *Physical Review A* **66**.4: 044304 (2002)
11. Li, Dafa, Li, Xinxin: More general quantum search algorithm $Q = I - \gamma V - \tau U$ and the precise formula for the amplitude and the non-symmetric effects of different rotating angles. *Phys. Lett. A* **287**(5–6), 304–316 (2001)
12. Long, Gui, Lu, Tu, Chang, Cun, Li, Yan, Song, Zhang, Wei, Lin, Yan, Hai, Yang.: An $SO(3)$ picture for quantum searching. *J. Phys. A* **34**(4), 861–866 (2001)
13. Long, Gui-Lu: Grover algorithm with zero theoretical failure rate. *Physical Review A* **64**(2), 022307 (2001)
14. Long, Gui-lu, Liu, Yang: Search an unsorted database with quantum mechanics. *Frontiers of Computer Science in China* **1**(3), 247–271 (2007)
15. Toyama, F.M., van Dijk, W., Nogami, Y.: Quantum search with certainty based on modified Grover algorithms: optimum choice of parameters. *Quantum Inf. Process.* **12**(5), 1897–1914 (2013)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.