Quantum Inf Process
DOI 10.1007/s11128-011-0355-6

From orthogonal projections to a generalized quantum search

César Bautista-Ramos · Carlos Guillén-Galván · Alejandro Rangel-Huerta

Received: 5 May 2011 / Accepted: 29 December 2011

Abstract A quantum algorithm with certainty is introduced in order to find a marked pre-image of an element which is known to be in the image domain of an orthogonal projection operator. The analysis of our algorithm is made by using properties of the Moebius transformations acting on the complex projective line. This new algorithm closely resembles the quantum amplitude amplification algorithm, however it is proven that our algorithm is a proper generalization of the latter (with generalized phases), in such a way that the quantum search engine of the main operator of quantum amplification is included as a particular case. In order to show that there exist search problems that can be solved by our proposal but cannot be by applying the quantum amplitude amplification algorithm, we modify our algorithm as a cryptographic authentification protocol. This protocol results to be robust enough against attacks based on the quantum amplitude amplification algorithm. As a byproduct, we show a condition where it is impossible to find exactly a pre-image of an orthoghonal projection. This result generalizes the fact that, it is impossible to find a target state exactly by using quantum amplification on a three dimensional invariant subspace.

Keywords Grover algorithm · Quantum amplitude amplification algorithm · Orthogonal projection · Moebius transformations

C. Bautista-Ramos (✉) · C. Guillén-Galván · A. Rangel-Huerta
Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla, 14 Sur y Av. San Claudio, Edif. 104C, Ciudad Universitaria, Puebla, Pue 72570, Mexico
e-mail: bautista@cs.buap.mx

C. Guillén-Galván
e-mail: cguillen@cs.buap.mx

A. Rangel-Huerta
e-mail: arangel@cs.buap.mx

Published online: 06 January 2012

1 Introduction

Generalizations of concepts, theorems or algorithms are, most of the time, important because they help us to understand the fundamental facts about the theory. Goguen argues in Ref. [1] that "sufficiently abstract formulations can reveal surprising connections". This is particularly true in Quantum Computation. For instance, the quantum amplitude amplification algorithm [2] is a generalization of the Grover algorithm [3] which recognizes the use of the Walsh-Hadamard transformation as a non-fundamental matter (this is also recognized in Ref. [4]): what really matters is the existence of a quantum algorithm that can be used to quadratically amplify the success probability. Furthermore, the phase shifts by angle π, that mark the good and initial states, are also non-fundamental: the important fact is that they must match in order to gain quadratic speed up [5,6]. Besides, by allowing phase shifts other than π, improvement to certainty can be achieved [2,7,8]. Additional generalizations in a different direction, dealing with the initial state of the Grover algorithm, are studied in Refs. [9,10]; while in Refs. [11,12] the case of three dimensional invariant subspaces is analyzed. In Ref. [13] a four dimensional invariant subspace case is studied.

In order to get a better understanding of all these generalizations, it has been proposed to separate the initial state (or database) from the quantum search engine [6,14]. From our point of view, this separation is possible because it is just one aspect of a more general phenomenon: using quantum algorithms for finding a unique *marked* (by a quantum oracle) solution of an equation of the type

$$P|X\rangle = |b\rangle \tag{1}$$

where P is an orthogonal projection, $|X\rangle$ is an unknown unit vector and $|b\rangle$ is a known vector of constant terms. We prove that the problem of finding a good state, as specified in the quantum amplitude amplification techniques, is a particular case of solving Eq. 1 where the unknown $|X\rangle$ is the normalized vector of good states and the algorithm that solves the problem is the iteration of two operators: an oracle that distinguishes (marks) the solution $|X\rangle$ and a generalization of the diffusion operator used by Grover in his original algorithm [3]. So, in general, we need two different algorithms to solve Eq. 1: one quantum algorithm that allows us to put the known vector $|b\rangle$ (the database in the case of Grover's algorithm) inside the quantum computer and another algorithm for "inverting" P in Eq. 1 (even though P is not an invertible matrix unless P is the identity matrix). In these lines we propose a quantum algorithm for finding a marked solution to Eq. 1 that succeed with certainty. It turns out that our setting is a proper generalization of the above mentioned quantum amplification techniques, aside from Ref. [13], since all these solve Eq. 1, where the projection P has rank one (see Theorem 1), even in the three dimensional case [11,12]; while our generalization doesn't have such constrain. As a consequence, our proposal includes a generalized diffusion operator that doesn't depend on the initial state. This is explained at Sect. 7 in the framework of a cryptographic identification protocol.

We cannot say that our framework is a generalization of Ref. [13]; neither the other way around. This follows from the fact that, in the formulation of Ref. [13], the generalized Grover operator needs the initial state; unlike our proposal which is independent from such initial state. Both are generalizations of the Grover algorithm but into different directions. The precise statement about the relationship between orthogonal projections and Ref. [13] is given in Sect. 3, Proposition 2 and Theorem 2.

In our setting, just as in the Grover algorithm and quantum amplitude amplification algorithm, a two-dimensional invariant subspace arises, hence the analysis of our proposed algorithm is reduced to studying the powers of a 2×2 invertible matrix on the initial state. Recalling the relationship between the general linear group of 2×2 matrices and Moebius transformations (fractional linear transformations) we can go further in reducing the analysis to the iteration of a Moebius transformation of elliptic type on a fixed complex number.

Moebius transformations enable the geometry of complex numbers that we use to our advantage. However, although they are part of the elemental tools of Complex Analysis [15–17] and that they are also useful in some branches of theoretical physics (see discussion in Ref. [18]), their use has been largely ignored by the Quantum Computing community. There is a pair of exceptions: the relationship between Moebius transformations and Quantum Computing was first pointed out in Ref. [18]; while in Ref. [19] they were used for analyzing the quantum amplitude amplification algorithm with generalized phases.

We end up with a generalization of a modified version of Grover's algorithm [8] that can find the solution $|X\rangle$ with certainty, if the vector $|b\rangle$ on the right hand side of Eq. 1, can be introduced in the quantum computer without any error. Otherwise an additional one dimensional subspace appears which makes impossible to find $|X\rangle$ with certainty. See Corollary 2. This result generalizes the main one of Ref. [11] in a simpler way. See Eqs. 11 and 12.

It is worth noting that equations of the type of Eq. 1 appear in several branches of Computer Science:

1. Relational databases: The model of structured databases most widely used is the so called *relational model* (originally proposed by Codd [20]). Its formal setting is an algebra called *relational algebra* [21,22] which has several operators, one of which is the *selector operator* which is an abstraction of an algorithm that finds pre-images of a projection. In this paper we address an analogous selection problem for a quantum computer.
2. Computer graphics: Equations of the type of Eq. 1 appear in computer graphics and robotics as an *object reconstruction problem* where P is a parallel projection [23–25]. Despite the common practice of using local coordinates of the range of P for the vector $|b\rangle$ this is not the case in Eq. 1: $|X\rangle$ and $|b\rangle$ belong to the same Hilbert space.
3. Cryptography: The orthogonal projection P can be interpreted as a trapdoor one-way function [26] because finding a particular marked solution of Eq. 1 is not trivial. The naive approach to solving Eq. 1 would be Gaussian elimination. However the solutions have the form

$$\sqrt{\frac{1-a}{\langle w|w\rangle}}|w\rangle + |b\rangle$$

with $|w\rangle$ in the null space of P and $a = \langle b|b\rangle$, i.e., the solutions form a sphere S^{k-1} of dimension $k-1$, where k is the nullity of P. Thus, finding a single element of S^{k-1} is not feasible by using only Gaussian elimination. The trapdoor information, within the framework of quantum computing, is developed in this paper.

2 The problem

In this section the main problem is stated, the necessary definitions are given and the notation that will be used through all this paper is fixed.

We try to find a solution of Eq. 1 under the following assumptions:

1. The operator P is a not null orthogonal projection: $P \neq 0$, $P^2 = P$ and $P^* = P$, where P^* is the conjugate transpose of P.
2. There exists a unit vector $|X\rangle$ which is solution of Eq. 1.
3. The solution $|X\rangle$ is distinguishable by the quantum oracle $\mathcal{S}(\varphi) = I - (1 - e^{i\varphi})|X\rangle\langle X|$, where $0 < \varphi < 2\pi$.
4. There is a quantum algorithm $\mathcal{A}$ without measurement with *initial state* $|\mathbf{s}\rangle$ such that $\mathcal{A}|\mathbf{s}\rangle$ is an eigenvector of P.
5. The number $a = \langle b|b\rangle$ is known and holds $0 < a < 1$.
6. For some angle ϕ with $0 < \phi < 2\pi$, the matrix P is *ϕ-known*, meaning that $\exp(i\phi P)$ can be implemented efficiently on a quantum computer.

Our definition of *knowledge* of P may seem counterintuitive and out of place. It is introduced here because the operators $\exp(i\phi P)$ are "near" to P and have the advantage of being unitary. In fact, we are going to show that $\exp(i\phi P)$ helps to invert the projector P. The basic idea is that P and a are classical data (which can be written in a piece of paper), while $|b\rangle$ and $\exp(i\phi P)$ are quantum data: $|b\rangle$ can be introduced to the quantum computer by the quantum algorithm $\mathcal{A}$ and $\exp(i\phi P)$ is a quantum oracle.

Definition 1 We call $\exp(i\phi P)$ the *diffusion operator* of P. The vector $|b\rangle$ is said *known exactly by $\mathcal{A}$* if

$$\mathcal{A}|\mathbf{s}\rangle = \frac{1}{\sqrt{a}}|b\rangle. \tag{2}$$

Thus, the orthogonal projection P is ϕ-known if its diffusion operator can be efficiently implemented on a quantum computer. The diffusion operator is used in the quantum algorithm defined by the quantum circuit of Fig. 1. We are going to prove below that, if the vector $|b\rangle$ is not known exactly, then it is imposible to solve Eq. 1 with certainly. While, in contrast, if $|b\rangle$ is known exactly, then, for a convenient choice of ϕ and φ, the quantum algorithm of Fig. 1 solves the stated problem with certainty.

Note that the quantum oracle $S(\varphi)$ is a diffusion operator of the projector $|X\rangle\langle X|$. Also, we can write

$$\exp(i\varphi P) = I - (1 - e^{i\varphi})P \tag{3}$$

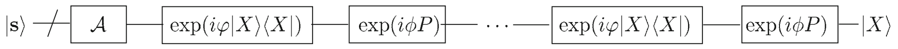

Fig. 1 Proposed quantum algorithm, without measurements, for finding $|X\rangle$. The number of iterations, as well as the angles ϕ and φ are given in Theorem 4. The output state is $|X\rangle$ up to a global phase

since P is idempotent.

3 Quantum amplitude amplification and diffusion

In this Section we prove that the quantum amplitude amplification with generalized phases techniques are a particular case of our framework. Besides we establish the relationship with Ref. [13].

Let $Z : \mathbb{C}P^1 \to \mathbb{C}$ be the affine coordinate map $Z[z_0 : z_1] = z_0/z_1$, where $\mathbb{C}P^1$ is the complex projective line.

Definition 2 Let $[x : y]$ be any point in $\mathbb{C}P^1$ with affine coordinate $-\sqrt{a}$. Define $|\delta\rangle = x|X\rangle + \frac{y}{\sqrt{a}}|b\rangle$.

This point $[x : y]$ helps to define the orthogonal vector $|\delta\rangle$ to the solution $|X\rangle$: from

$$x + \frac{y}{\sqrt{a}}\langle X|b\rangle = 0$$

it follows that $|X\rangle$ and $|\delta\rangle$ are orthogonal states. Besides

$$|b\rangle = a|X\rangle + \frac{\sqrt{a}}{y}|\delta\rangle. \tag{4}$$

So, if $|b\rangle$ is known exactly by $\mathcal{A}$, then

$$\mathcal{A}|\mathbf{s}\rangle = \sqrt{a}|X\rangle + \frac{1}{y}|\delta\rangle. \tag{5}$$

Therefore, $\mathcal{A}$ is a quantum algorithm which produces $|X\rangle$ with measurement probability a. Thus, we can use quantum amplitude amplification in order to amplify this success probability to $\sqrt{a}$. This algorithm has quantum circuit given in Fig. 2 where $A = \mathcal{A}$ and $S_{\mathbf{s}}(\phi) = I - (1 - \exp(i\phi))|\mathbf{s}\rangle\langle\mathbf{s}|$.

We can notice that quantum algorithm proposed in Fig. 1 looks like the quantum amplitude amplification in Fig. 2. Actually, quantum amplitude amplification is an

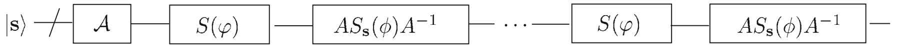

Fig. 2 The quantum amplitude amplification with generalized phases algorithm (without measurements). The usual quantum amplitude amplification is when $\varphi = \phi = \pi$. The number of times that $\mathcal{A}$ is used in our case is $\Theta(1/\sqrt{a})$. Now, compare Figs. 1 and 2. Note that $S(\varphi) = \exp(i\varphi|X\rangle\langle X|)\rangle$. However, Theorem 1 and Proposition 1 ensure that, in general, $\exp(i\phi P) \neq AS_{\mathbf{s}}(\phi)A^{-1}$

instance of our quantum algorithm with generalized diffusion operator. Indeed, let A be an arbitrary quantum algorithm that uses no measurement such that

$$A|\mathbf{s}\rangle = |\Psi_1\rangle + |\Psi_0\rangle \tag{6}$$

where $|\Psi_1\rangle$, $|\Psi_0\rangle$ are superpositions of good states and bad states, respectively, such that $\langle\Psi_1|\Psi_0\rangle = 0$ [2]. The following theorem puts quantum amplification in the frame of solving Eq. 1.

Theorem 1 *There exists a projector P' of rank one such that its diffusion operator holds* $\exp(i\phi P') = AS_{\mathbf{s}}(\phi)A^{-1}$. *Furthermore, the normalized vector of the good states is a pre-image, under P', of a vector $|b\rangle$ such that it is known exactly by A and $\langle b|b\rangle = \langle\Psi_1|\Psi_1\rangle$.*

Proof By defining

$$P' = \frac{1}{1-e^{i\phi}}(I - AS_{\mathbf{s}}(\phi)A^{-1})$$

the relation

$$P' = \frac{1}{1-e^{i\phi}}A(I - S_{\mathbf{s}}(\phi))A^{-1}$$

is fulfilled. But $I - S_{\mathbf{s}}(\phi) = (1-e^{i\phi})|\mathbf{s}\rangle\langle\mathbf{s}|$ then P' is similar to the orthogonal projection $|\mathbf{s}\rangle\langle\mathbf{s}|$ with unitary similarity matrix A: $P' = A|\mathbf{s}\rangle\langle\mathbf{s}|A^{-1}$. It follows that P' is an orthogonal projection that holds

$$\exp(i\phi P') = I - (1-e^{i\phi})P' = AS_{\mathbf{s}}(\phi)A^{-1}. \tag{7}$$

Also, quantum amplitude amplification finds an element in a fiber, i.e, solves an equation of the type Eq. 1: assume that $a = \langle\Psi_1|\Psi_1\rangle$ then, from Eq. 6 we get that,

$$\begin{aligned} P'|\Psi_1\rangle &= A|\mathbf{s}\rangle\langle\mathbf{s}|A^{-1}|\Psi_1\rangle \\ &= A|\mathbf{s}\rangle(\langle\Psi_1| + \langle\Psi_0|)|\Psi_1\rangle \\ &= aA|\mathbf{s}\rangle \\ &= a|\Psi_1\rangle + a|\Psi_0\rangle \end{aligned}$$

then $|X\rangle = \frac{1}{\sqrt{a}}|\Psi_1\rangle$ holds $P'|X\rangle = |b\rangle$ where $|b\rangle = \sqrt{a}|\Psi_1\rangle + \sqrt{a}|\Psi_0\rangle$ and $\langle b|b\rangle = a$.

Furthermore, A is a quantum algorithm producing $|b\rangle$ in the sense of Eq. 2. So, according to our previous definitions, $|b\rangle$ is known exactly. Meanwhile, from Eq. 7, we can say that P' is ϕ-known, if A can be implemented efficiently. □

However, in the general case of our main problem, the orthogonal projection P could have rank greater than one, in which case P is not even similar to the orthogonal projection P' since the rank of P' is always one.

Proposition 1 *If the orthogonal projection P has rank k then its diffusion operator* $\exp(i\phi P)$ *has eigenvalue $e^{i\phi}$ with algebraic multiplicity k.*

Proof There exists an invertible matrix B such that

$$P = B\left(\sum_{j=0}^{k-1} |j\rangle\langle j|\right)B^{-1}$$

so

$$\exp(i\phi P) = I - (1 - e^{i\phi})P = B\left(\sum_{j=0}^{k-1} e^{i\phi}|j\rangle\langle j| + \sum_{j=k}^{m-1} |j\rangle\langle j|\right)B^{-1}$$

from which it follows that the characteristic polynomial of $\exp(i\phi P)$ is the same as the diagonal matrix $\sum_{j=0}^{k-1} e^{i\phi}|j\rangle\langle j| + \sum_{j=k}^{m} |j\rangle\langle j|$ where the eigenvalue $e^{i\phi}$ has algebraic multiplicity k. □

The following Proposition will help us to characterize the relationship between Eq. 1 and the framework of Ref. [13].

Proposition 2 *Let U, V be a pair of unitary matrices such that VU is a Hermitian matrix. Let* $0 < \phi < 2\pi$ *and define*

$$P_0 = (1 - e^{i\phi})^{-1}(I - US_{\mathbf{s}}(\phi)V).$$

The following conditions are equivalent.

1. $VU = I$ *or* ($\phi = \pi$ *and* $VU|\mathbf{s}\rangle = \pm|\mathbf{s}\rangle$).
2. $P_0^* = P_0$.
3. $P_0^2 = P_0$.

Proof We can write $P_0 = (1 - e^{i\phi})^{-1}(I - UV) + U|\mathbf{s}\rangle\langle\mathbf{s}|$. Then, carrying out the algebra, we get that $P_0^* = P_0$ is equivalent to

$$|\mathbf{s}\rangle\langle\mathbf{s}| - VU|\mathbf{s}\rangle\langle\mathbf{s}|VU = \frac{2i\ \sin(\phi)}{|1 - e^{i\phi}|^2}(VU - I). \tag{8}$$

Multiplying both sides of Eq. 8 by $|\mathbf{s}\rangle$ on the right we obtain that

$$\frac{|1 - e^{i\phi}|^2 + 2i\ \sin(\phi)}{|1 - e^{i\phi}|^2\langle\mathbf{s}|VU|\mathbf{s}\rangle + 2i\ \sin(\phi)} \tag{9}$$

is an eigenvalue of VU. Since VU is a unitary Hermitian matrix, then the expression (9) equals ±1. If expression (9) equals 1 then $VU|\mathbf{s}\rangle = |\mathbf{s}\rangle$. It follows, from Eq. 8 that $VU = I$ or $\phi = \pi$ and $VU|\mathbf{s}\rangle = |\mathbf{s}\rangle$. If expression (9) equals -1, it follows immediately that $\phi = \pi$ and $VU|\mathbf{s}\rangle = -|\mathbf{s}\rangle$.

Reciprocally, if $VU = I$, then $P_0 = U|\mathbf{s}\rangle\langle\mathbf{s}|U^{-1}$. Thus, P_0 is a Hermitian matrix. While, if $\phi = \pi$ and $VU\mathbf{s} = \pm|\mathbf{s}\rangle$, then Eq. 8 holds. It follows again that P_0 is Hermitian.

Similarly, it can be shown that condition 1 is equivalent to condition 3. □

Proposition 2 gives us conditions under which our point of view coincides with the one of Ref. [13]. We have dealt with the case $VU = I$ of Ref. [13] in Theorem 1. The remaining case $\phi = \pi$ and $VU|\mathbf{s}\rangle = \pm|\mathbf{s}\rangle$ is the following.

Theorem 2 *Let U, V be a pair of unitary matrices such that VU is a Hermitian matrix such that $VU|\mathbf{s}\rangle = \pm|\mathbf{s}\rangle$. Then*

1. *There exists an orthogonal projector P_0 such that its diffusion operator holds $\exp(i\pi P_0) = US_{\mathbf{s}}(\pi)V$. Such projector P_0 has $U|\mathbf{s}\rangle$ as an eigenvector.*
2. *Let*

$$-1 < \langle\tau|UV|\tau\rangle - 2\langle\tau|U|\mathbf{s}\rangle\langle\mathbf{s}|V|\tau\rangle < 1.$$

Then, the target vector $|\tau\rangle$ satisfy $P_0|\tau\rangle = |b\rangle$ for some vector $|b\rangle$ such that $0 < \langle b|b\rangle < 1$.

Proof 1. We may combine the definition of P_0 in Proposition 2 with Eq. 3 to conclude that the diffusion operator of P_0 is $US_{\mathbf{s}}(\pi)V$. Besides, a direct calculations shows that

$$P_0U|\mathbf{s}\rangle = \begin{cases} 0, & \text{if } VU|\mathbf{s}\rangle = |\mathbf{s}\rangle; \\ U|\mathbf{s}\rangle, & \text{if } VU|\mathbf{s}\rangle = -|\mathbf{s}\rangle. \end{cases}$$

2. Define $|b\rangle = P_0|\tau\rangle$. Then, from $\langle b|b\rangle = \langle\tau|P_0|\tau\rangle = \frac{1}{2}(1 - \langle\tau|US_{\mathbf{s}}(\pi))V|\tau\rangle)$ and $\langle\tau|US_{\mathbf{s}}(\pi)V|\tau\rangle = \langle\tau|UV|\tau\rangle - 2\langle\tau|U|\mathbf{s}\rangle\langle\mathbf{s}|V|\tau\rangle$ it follows that $0 < \langle b|b\rangle < 1$. □

4 Analysis of the quantum algorithm with diffusion operator

In this Section we analyze the quantum algorithm given by the quantum circuit in Fig. 1. Just as in Grover's algorithm and the quantum amplitude amplification algorithm, a two dimensional invariant subspace arises. However, when $|b\rangle$ is not known exactly, an additional one dimensional invariant subspace appears. In such a case, we ended up with a three dimensional invariant subspace which is the direct sum of these invariant subspaces.

Theorem 3 *The subspace W spanned by $|X\rangle$ and $|\delta\rangle$ is an invariant subspace of $\exp(i\phi P)$. Moreover, let z be $1 - \exp(i\phi)$, then the matrix of $\exp(i\phi P)$ relative to the ordered basis $\big(|X\rangle, |\delta\rangle\big)$ is*

$$\begin{pmatrix} 1 - za & zx(1-a) \\ -\sqrt{a}\,\frac{z}{y} & 1 - z + za \end{pmatrix}.$$

Proof By straightforward calculations of $\exp(i\phi P)$ on the orthogonal basic elements $|X\rangle$, $|\delta\rangle$ and using Eq. 3, the Theorem follows. □

Corollary 1 *The matrix of* $\exp(i\phi P)\exp(i\varphi|X\rangle\langle X|)|_W$ *relative to the ordered basis* $(\,|X\rangle, |\delta\rangle\,)$ *is*

$$R_{\phi,\varphi} = \begin{pmatrix} a\, e^{i\,\varphi+i\,\phi} - a\, e^{i\,\varphi} + e^{i\,\varphi} & (1-a)\left(1-e^{i\phi}\right)x \\ \frac{\sqrt{a}}{y}\left(e^{i\,\varphi+i\,\phi} - e^{i\,\varphi}\right) & -e^{i\,\phi}\,a + a + e^{i\,\phi} \end{pmatrix}$$

and has determinant given by $e^{i\,(\varphi+\phi)}$.

The following result generalizes the main one of Ref. [11].

Corollary 2 *If* $|b\rangle$ *is not known exactly by* $\mathcal{A}$*, then the quantum algorithm given in Fig. 1 cannot find a solution to Eq. 1 with certainty.*

Proof By Eqs. 4 and 5 we have that the vectors $|X\rangle$, $|\delta\rangle$ and $\mathcal{A}|\mathbf{s}\rangle$ are linear independent. Using the Gram-Schmidt process we get a new vector $|e\rangle$ such that

$$\mathcal{A}|s\rangle = |e\rangle - \langle\mathbf{s}|\mathcal{A}^*|X\rangle|X\rangle - \frac{\langle\mathbf{s}|\mathcal{A}^*|\delta\rangle}{\langle\delta|\delta\rangle}|\delta\rangle \tag{10}$$

where $|X\rangle$, $|\delta\rangle$ and $|e\rangle$ are orthogonal vectors. From assumption 4, Section 2 and Eq. 3 we obtain that $\exp(i\phi P)\mathcal{A}|\mathbf{s}\rangle = e^{i\xi\phi}\mathcal{A}|\mathbf{s}\rangle$, where ξ is the eigenvalue corresponding to the eigenvector $\mathcal{A}|s\rangle$ of P. Hence by Theorem 3 we get

$$e^{i\phi P}|e\rangle = e^{i\xi\phi}\mathcal{A}|\mathbf{s}\rangle + \alpha|X\rangle + \beta|\delta\rangle$$

for some complex numbers α, β. Thus, by substitution of $\mathcal{A}|\mathbf{s}\rangle$ for the right hand side of Eq. 10 we get

$$e^{i\phi P}|e\rangle = e^{i\xi\phi}|e\rangle + \alpha'|X\rangle + \beta'|\delta\rangle$$

for some complex numbers α', β'. It follows that $\alpha' = \beta' = 0$. So the one-dimensional subspace spanned by $|e\rangle$ is $\exp(i\phi P)$-invariant.

By Corollary 1, on the ordered orthogonal base (not normalized) $(|X\rangle, |\delta\rangle, |e\rangle)$ we have that

$$\begin{aligned}&\exp(i\phi P)\exp(i\varphi|X\rangle\langle X|) \\ &\quad= \begin{pmatrix} a\, e^{i\,\varphi+i\,\phi} - a\, e^{i\,\varphi} + e^{i\,\varphi} & (1-a)\left(1-e^{i\phi}\right)x & 0 \\ \frac{\sqrt{a}}{y}\left(e^{i\,\varphi+i\,\phi} - e^{i\,\varphi}\right) & -e^{i\,\phi}\,a + a + e^{i\,\phi} & 0 \\ 0 & 0 & e^{i\xi\phi} \end{pmatrix}\end{aligned} \tag{11}$$

and by Eq. 10,

$$\mathcal{A}|\mathbf{s}\rangle = \begin{pmatrix} -\langle\mathbf{s}|\mathcal{A}^*|X\rangle \\ -\langle\mathbf{s}|A^*|\delta\rangle\langle\delta|\delta\rangle^{-1} \\ 1 \end{pmatrix}.$$

Hence, for any positive integer n we get

$$\big(\exp(i\phi P)\exp(i\varphi|X\rangle\langle X|)\big)^n\mathcal{A}|\mathbf{s}\rangle = \alpha_n|X\rangle + \beta_n|\delta\rangle + e^{in\xi\phi}|e\rangle \tag{12}$$

for some complex numbers α_n, β_n. Then, the error probability is always, at least $\langle e|e\rangle > 0$. □

5 From unitary matrices to Moebius transformations

Therefore, the analysis of the quantum algorithm given by Fig. 1 is reduced to studying the matrix powers of $R_{\varphi,\phi}$ on the vector $(\sqrt{a}, 1/y)^t$ (see Eq. 5).

We can study the powers of $R_{\phi,\varphi}$ by means of the canonical group epimorphism $\mu : GL(2,\mathbb{C}) \to \Gamma$ from the general linear group onto Γ, the group of Moebius transformations:

$$\begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \overset{\mu}{\mapsto} \frac{c_{11}z + c_{12}}{c_{21}z + c_{22}}.$$

The evaluation of a two by two invertible matrix C as a linear transformation is naturally related to the evaluation of its Moebius transformation $\mu(C)(z)$, in the category theory sense of natural transformation (see the commutative diagram (2) in Ref. [19]), meaning that the following rule holds:

$$C\begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} w_0 \\ w_1 \end{pmatrix} \text{ implies } \mu(C)(z_0/z_1) = w_0/w_1. \tag{13}$$

The Moebius transformations are classified in elliptic, parabolic, hyperbolic and loxodromic [15,27]. Such type can be identified by the trace when we have normalized Moebius transformations. The normalized form of $\mu(R_{\phi,\varphi})$ is $\mu(N_{\phi,\varphi})$ where

$$\begin{aligned} N_{\phi,\varphi} &= e^{-i(\varphi+\phi)/2}R_{\phi,\varphi} \\ &= \begin{pmatrix} f + i\,g & -2ix(1-a)\sin\left(\frac{\phi}{2}\right)\,e^{-i\varphi/2} \\ \frac{2i\sqrt{a}\sin\left(\frac{\phi}{2}\right)}{y}\,e^{i\varphi/2} & f - i\,g \end{pmatrix} \end{aligned} \tag{14}$$

$$f = f(\varphi,\phi) = a\cos\left(\frac{\varphi+\phi}{2}\right) + (1-a)\cos\left(\frac{\varphi-\phi}{2}\right) \tag{15}$$

and

$$g = g(\varphi,\phi) = a\sin\left(\frac{\varphi+\phi}{2}\right) + (1-a)\sin\left(\frac{\varphi-\phi}{2}\right). \tag{16}$$

As the trace of $N_{\phi,\varphi}$ is $2f(\varphi,\phi)$ then $\mu(N_{\phi,\varphi})$ is an elliptic transformation, since $-1 < f(\varphi,\phi) < 1$. Such trace is important because will give the behavoir of the iterations of $\mu(R_{\phi,\varphi})$.

Thus, the analysis of our algorithm is reduced to a problem of Moebius transformation iteration: In fact, to analyzing the powers of a complex number, thanks to the following Lemma [28,29]:

Lemma 1 *Let $M(z) = (c_{11}z + c_{12})/(c_{21}z + c_{22})$ be a Moebius transformation with two different fixed points $\gamma_1, \gamma_2 \in \mathbb{C}$. Let $S(z) = (z - \gamma_2)/(z - \gamma_1)$. Then,*

$$M = S^{-1} \circ H \circ S$$

where $H(z) = kz$ for some $k \in \mathbb{C}$. Such k is called the multiplier of M.

Lemma 1 tells us that the iterations of $\exp(i\varphi P)\exp(i\varphi|X\rangle\langle X|)$ are reduced to the powers of the multiplier of $\mu(N_{\phi,\varphi})$. These can be calculated with the help of the so called *character* and *co-character* of $R_{\phi,\varphi}$.

Definition 3 We call the number $f = f(\varphi,\phi)$ defined by Eq. 15 the *character* of the matrix $R_{\phi,\varphi}$ and the number $g = g(\varphi,\phi)$ defined by Eq. 16 the *co-character*.

The character and co-character are related by the equation

$$f^2 + g^2 = 1 - 4a(1-a)\sin^2(\phi/2). \tag{17}$$

Let f and g be the character and co-character of $R_{\phi,\varphi}$ respectively. From Lemma 1 for $M = \mu(N_{\phi,\varphi})$, the normalized Moebius transformation of $\mu(R_{\phi,\varphi})$, we get that its multiplier is

$$k = \left(f + i\sqrt{1-f^2}\right)^2 \tag{18}$$

and

$$\mu(R_{\phi,\varphi}) = \mu(N_{\phi,\varphi}) = \mu(T)^{-1} \circ H \circ \mu(T) \tag{19}$$

where

$$T = \begin{pmatrix} 1 & -\gamma_2 \\ 1 & -\gamma_1 \end{pmatrix}, \quad \mu(T)^{-1}(z) = \frac{\gamma_1 z - \gamma_2}{z - 1}, \quad H(z) = kz$$

and γ_1, γ_2 are the fixed points of $\mu(R_{\phi,\varphi})$ defined by the following equations

$$\gamma_1 = \frac{g + \sqrt{1-f^2}}{2\sqrt{a}\sin(\phi/2)}\, e^{-i\varphi/2} y, \quad \gamma_2 = \frac{g - \sqrt{1-f^2}}{2\sqrt{a}\sin(\phi/2)}\, e^{-i\varphi/2} y. \tag{20}$$

All the above defined quantities can be managed by means of the geometry of complex numbers. Namely, by the following Lemmas, which are proven in the Appendix.

Lemma 2 *Let $M(z)=(c_{11}z+c_{12})/(c_{21}z+c_{22})$ be a Moebius transformation with two different fixed points $\gamma_1,\gamma_2\in\mathbb{C}$. Let $S(z)=(z-\gamma_2)/(z-\gamma_1)$. Assume that $M(z)$ is a normalized ($c_{11}c_{22}-c_{12}c_{21}=1$) elliptic transformation, α is the argument of the complex number c_{21} with $\pi/2\le\alpha\le\pi$, and $c_{11}-c_{22}$ is purely imaginary. Then $|S(1)|=1$ if and only if $2\operatorname{Im}c_{21}=|c_{11}-c_{22}|$. In such a case we can write $S(1)=\exp(-i\kappa)$ where*

$$\tan\left(\frac{\pi-\kappa}{2}\right)=\frac{|c_{21}|\,\sin(\alpha-\pi/2)}{\sqrt{1-(c_{11}+c_{22})^2/4}}.$$

Using Lemma 2 for $\mu(N_{\phi,\varphi})$, the normalized transformation of $\mu(R_{\phi,\varphi})$, we get:

Lemma 3

1. $|\mu(T)(-x)|=1$ *if and only if* $\phi=\varphi$. *In such a case* $\mu(T)(-x)=\exp(-i\kappa)$, *where* $\kappa=2\arccos(\sqrt{a}\sin(\phi/2))$;

2. $\sqrt{1-f(\phi,\phi)^2}=2\sin(\phi/2)\sqrt{a}\sqrt{1-a\sin^2(\phi/2)}$;

3. *Let*

$$h(z)=\frac{\arccos(z)}{\arcsin(2z\sqrt{1-z^2})}.$$

(a) If $0<z\le 1/\sqrt{2}$ *then* $h(z)=\pi/4\arcsin(z)-1/2$.
(b) If $1/\sqrt{2}\le z<1$ *then* $h(z)=1/2$.

6 Main results

From Eq. 18, notice that we can write the multiplier k as $e^{i\omega}$, where

$$\omega=2\arcsin\sqrt{1-f^2}, \tag{21}$$

and f is the character of $R_{\phi,\varphi}$. So, from Eq. 19, we get

$$\mu(R_{\phi,\varphi})^n(-x)=\mu(T)^{-1}\left(e^{in\omega}\mu(T)(-x)\right). \tag{22}$$

Theorem 4 *Let x be a complex number as in Definition 2 then*

$$\mu(R_{\phi,\varphi})^n(-x)=\infty$$

whenever $\varphi=\phi$,

$$\phi=2\arcsin\left(\frac{1}{\sqrt{a}}\sin\left(\frac{\pi}{4n+2}\right)\right)\ \text{and}\quad n=\left\lceil\frac{\arccos\sqrt{a}}{\arcsin(2\sqrt{a}\sqrt{1-a})}\right\rceil.$$

Besides if $1/2<a<1$, then the number of iterations n is equal to one.

Proof Let $h(z)$ be as in Lemma 3(3). For any fixed a holding $0 < a \leq 1/2$, the function $H_a(\phi) = h(\sqrt{a}\sin(\phi/2))$ is decreasing for $0 < \phi < \pi$. On other hand, for $1/2 \leq a < 1$ the function $H_a(\phi)$ is decreasing for $0 < \phi \leq 2\arcsin(1/\sqrt{2a})$ and takes the constant value of $1/2$ for $2\arcsin(1/\sqrt{2a}) \leq \phi \leq \pi$. However, in any case $\lim_{\phi\to 0^+} H_a(\phi) = \infty$. Then from $\lceil h(\sqrt{a})\rceil \geq h(\sqrt{a}) = H_a(\pi)$ and the Intermediate Value Theorem, it follows that there exist ϕ_0 such that

$$H_a(\phi_0) = \lceil h(\sqrt{a})\rceil = n. \tag{23}$$

Now, we put $\varphi_0 = \phi_0$ in Lemma 3(1) in order to get

$$\mu(T)(-x) = e^{-i\kappa}$$

where $\kappa = 2\arccos(\sqrt{a}\sin(\phi_0/2))$. Thus, for $\omega = 2\arcsin\sqrt{1 - f(\phi_0, \phi_0)^2}$, where $f(\phi_0, \phi_0)$ is the character of R_{ϕ_0,ϕ_0}, and with help of Lemma 3(2), we get $\kappa/\omega = H_a(\phi_0) = n$.

From Eq. 22, we get

$$\mu(R_{\phi_0,\phi_0})^n(-x) = \mu(T)^{-1}(e^{in\omega - i\kappa}) = \mu(T)^{-1}(1) = \infty.$$

The angle ϕ_0 is calculated in the following way: if $0 < a \leq 1/2$ then, from Lemma 3(3a), we get that Eq. 23 is equivalent to

$$\phi_0 = 2\arcsin\left(\frac{1}{\sqrt{a}}\sin\left(\frac{\pi}{4n+2}\right)\right).$$

While, if $1 > a > 1/2$, then, for any $\pi > \phi_0 \geq 2\arcsin(1/\sqrt{2a})$ we get $\sqrt{a}\sin(\phi_0/2) \geq 1/\sqrt{2}$, so from Lemma 3(3b), we obtain $H_a(\phi_0) = 1/2$ and $n = 1$. □

Returning to the usual vector state representation and unitary matrix evolution, we get:

Corollary 3 *Let n, ϕ and φ be as in Theorem 4. Then*

$$\big(\exp(i\phi P)\exp(i\phi|X\rangle\langle X|)\big)^n \mathcal{A}|\mathbf{s}\rangle = \begin{cases} e^{i\xi}|X\rangle, & \text{if } |b\rangle \text{ is known} \\ & \text{exactly by } \mathcal{A}; \\ \alpha|X\rangle + |e\rangle, & \text{otherwise,} \end{cases}$$

for some ξ, α a real number and a complex number, respectively. Besides $|e\rangle$ is defined in Eq. 10.

Proof Since Eq. 10 in the proof of Corollary 2 and Eq. 5 we have

$$\mathcal{A}|\mathbf{s}\rangle = \begin{cases} \sqrt{a}|X\rangle + \frac{1}{y}|\delta\rangle, & \text{if } |b\rangle \text{ is known exactly by } \mathcal{A}; \\ -\langle\mathbf{s}|\mathcal{A}^*|X\rangle|X\rangle - \frac{\langle\mathbf{s}|\mathcal{A}^*|\delta\rangle}{\langle\delta|\delta\rangle}|\delta\rangle + |e\rangle, & \text{otherwise.} \end{cases}$$

Thus, in view of Theorem 3 and Eq. 12 in the proof of Corollary 2, we can write

$$\big(\exp(i\phi P)\exp(i\phi|X\rangle\langle X|)\big)^n\mathcal{A}|\mathbf{0}\rangle = \alpha_n|X\rangle + \beta_n|\delta\rangle + \epsilon_n|e\rangle$$

for some complex numbers α_n, β_n, ϵ_n such that

$$\begin{pmatrix}\alpha_n\\ \beta_n\end{pmatrix} = \begin{cases} R^n_{\phi,\varphi}\begin{pmatrix}\sqrt{a}\\ 1/y\end{pmatrix}, & \text{if } |b\rangle \text{ is known exactly by } \mathcal{A};\\ R^n_{\phi,\varphi}\begin{pmatrix}-\langle\mathbf{s}|\mathcal{A}^*|X\rangle\\ -\langle\mathbf{s}|\mathcal{A}^*|\delta\rangle\langle\delta|\delta\rangle^{-1}\end{pmatrix}, & \text{otherwise,}\end{cases}$$

where $R_{\phi,\varphi}$ is defined in Corollary 1.

Let $y = -\frac{\langle s|A^*|X\rangle\langle\delta|\delta\rangle}{\sqrt{a}\langle\mathbf{s}|A^*|\delta\rangle}$ in Definition 2. Then, in any case,

$$\frac{\alpha_n}{\beta_n} = \mu\big(\exp(i\phi P)\exp(i\phi|X\rangle\langle X|)\big)^n(-x) = \infty$$

since (13) and Theorem 4 hold. Thus $\beta_n = 0$. □

Therefore, if we put $\phi = \varphi$ and n as in Theorem 4 in the quantum circuit of Fig. 1; and besides $|b\rangle$ is known exactly, we get $|X\rangle$ up to a global phase.

7 An interactive proof system

In this section we interpreted our algorithm as a quantum interactive proof system in order to prove that our proposal is a proper generalization of the quantum amplitude amplification algorithm. We take advantage of the following properties of the orthogonal projection P. Assume that P has rank two. Let $|b_0\rangle$, $|b_1\rangle$ be a couple of orthogonal vectors in the range of P such that there exist two unit vectors $|X_0\rangle$, $|X_1\rangle$ which are solutions of an equation of type Eq. 1:

$$P|X_0\rangle = |b_0\rangle \text{ and } P|X_1\rangle = |b_1\rangle. \tag{24}$$

Assume that $a = \langle b_0|b_0\rangle = \langle b_1|b_1\rangle$ and $|b_0\rangle$, $|b_1\rangle$ are known exactly by using the same unitary matrix $\mathcal{A}$, i.e.,

$$\mathcal{A}|\mathbf{s_0}\rangle = \frac{1}{\sqrt{a}}|b_0\rangle \text{ and } \mathcal{A}|\mathbf{s_1}\rangle = \frac{1}{\sqrt{a}}|b_1\rangle$$

where $|\mathbf{s_0}\rangle$, $|\mathbf{s_1}\rangle$ is a pair of orthonormal initial states. The Corollary 3 ensures that

$$\big(\exp(i\phi P)\exp(i\phi|X_0\rangle\langle X_0|)\big)^n\mathcal{A}|\mathbf{s_0}\rangle = e^{i\xi_0}|X_0\rangle \tag{25}$$

and

$$\big(\exp(i\phi P)\exp(i\phi|X_1\rangle\langle X_1|)\big)^n\mathcal{A}|\mathbf{s_1}\rangle = e^{i\xi_1}|X_1\rangle \tag{26}$$

for some angles ξ_0, ξ_1 and where n and ϕ are defined in Theorem 4. Note that in Eqs. 25 and 26 the diffusion operator of P remains unaltered, unlike quantum amplification which needs the initial state for its diffusion operator. See Fig. 2.

Let us consider two parties: Alice as a prover and Bob as a verifier. Both have quantum computers and a quantum channel for message exchange. The prover's secret is the knowledge of an orthogonal projector P of rank two. Bob chooses unit solutions to equations of type (24), where $a = \langle b_0|b_0\rangle = \langle b_1|b_1\rangle$, then challenges Alice to find these.

While the number a, the set $S = \{\mathbf{s_0}, \mathbf{s_1}\}$ of possible initial states and the operator $\mathcal{A}$ are made public, the orthogonal projection P is kept secret by Alice and Bob. Furthermore, we are assuming that P is ϕ-known by both Alice and Bob, where $\phi = \phi(a)$ is given in Theorem 4. The basic idea is that Alice must show to Bob that she knows P sufficiently enough, even the quantum information related to this operator, meaning that Alice must be able to implement the operator $\exp(i\phi P)$ on a quantum computer. We are assuming that Bob knows the vectors $|b_0\rangle$, $|b_1\rangle$ classically, i.e., he can write them on a piece of paper or on a classical computer and choose solutions $|X_j\rangle$, $j = 0, 1$ of $P|X_j\rangle = |b_j\rangle$. An additional assumption is that Bob can mark these solutions by using the quantum oracle $\exp(i\phi|X_j\rangle\langle X_j|)$, $j = 0, 1$.

1. Bob chooses at random a unit vector $|\mathbf{s}_j\rangle$ in S, then he computes the normalized vector $(1/\sqrt{a})|b_j\rangle = \mathcal{A}|\mathbf{s}_j\rangle$. Using such a vector, Bob also chooses a unit pre-image $|X_j\rangle$ of $|b_j\rangle$ under the projection P. Bob makes sure of being able to identify such a pre-image by using the quantum oracle $\exp(i\phi|X_j\rangle\langle X_j|)$. So, Bob sends to Alice the state $|\chi_1\rangle = \exp\left(i\phi|X_j\rangle\langle X_j|\right)(1/\sqrt{a})|b_j\rangle$ where $\phi = \phi(a)$ is given in Theorem 4.
2. Alice applies the diffusion operator $\exp(i\phi P)$ to the state she received. The resulting state $|\chi_2\rangle = \exp(i\phi P)|\chi_1\rangle$ is sent back to Bob.
3. Bob marks with $\exp(i\varphi|X_j\rangle\langle X_j|)$ the state received; this new marked state $|\chi_3\rangle = \exp(i\varphi|X_j\rangle\langle X_j|)|\chi_2\rangle$ is sent back to Alice.
4. Let $|\chi_1\rangle$ be $|\chi_3\rangle$.
5. Steps 2 through 4 are repeated $n-1$ times, where n is defined in Theorem 4.
6. Alice applies the difussion operator $\exp(i\phi P)$ one more time to the state received and the resulting state $|\chi_4\rangle = \exp(i\phi P)|\chi_3\rangle$ is sent back to Bob.
7. Bob measures using the projective measurement operators $|X_j\rangle\langle X_j|$ and $I - |X_j\rangle\langle X_j|$. He accepts if he gets the state $|X_j\rangle$.

7.1 Completeness condition

Equations 25 and 26 ensure that if Alice follows the protocol, her identity will be accepted by Bob.

7.2 Partial soundness condition

In order to prove soundness we should consider arbitrary attacks by the impersonator Eve. However, since we want only to prove that our proposed algorithm is a generalization of quantum amplitude amplification, we consider only attacks by the latter. This means that Eve, since she lacks the knowledge of the projection P, instead of applying the generalized diffusion operator $\exp(i\phi P)$, she uses, at Step 2 of the protocol, a particular diffusion operator of the form $\mathcal{A}S_{\mathbf{s}'}(\varphi)\mathcal{A}^{-1}$ given by quantum amplitude amplification, but first she has to guess what the initial state chosen by Bob was. Assume that $|\mathbf{s}'\rangle$ is Eve's guess state, where $|\mathbf{s}'\rangle \in S$. If $|\mathbf{s}'\rangle = |\mathbf{s}\rangle$ then Bob will accept Eve as Alice. Otherwise $|\mathbf{s}'\rangle \neq |\mathbf{s}\rangle$, then

$$\langle X_{\mathbf{s}}|A|\mathbf{s}'\rangle = \frac{1}{\sqrt{a}}\langle X_{\mathbf{s}}|P|b_{\mathbf{s}'}\rangle = \frac{1}{\sqrt{a}}\langle b_{\mathbf{s}}|b_{\mathbf{s}'}\rangle = 0$$

so, by definition of $|\delta_{\mathbf{s}}\rangle$,

$$\langle \delta_{\mathbf{s}}|A|\mathbf{s}'\rangle = \frac{1}{\sqrt{a}}\langle \delta_{\mathbf{s}}|b_{\mathbf{s}'}\rangle = \frac{x}{\sqrt{a}}\langle X_{\mathbf{s}}|b_{\mathbf{s}'}\rangle = 0.$$

It follows that $A|\mathbf{s}'\rangle$ belongs to the orthogonal complement $W^{\perp}$ of the Q-invariant subspace W spanned by $|X_{\mathbf{s}'}\rangle$ and $|\delta_{\mathbf{s}'}\rangle$. Then $Q^n A|\mathbf{s}'\rangle \in W^{\perp}$, since $W^{\perp}$ is also Q-invariant. Thus, in Step 4 of the protocol, Bob receives a state where the probability of measuring $|X_{\mathbf{s}}\rangle$ is null and Bob will reject Eve's identity for sure. Therefore, the probability of accepting Eve as Alice is the same as the probability of choosing the initial state at random: one half.

The probability of cheating might be decreased by increasing the rank of the projection P and then using a greater number of possible initial states or by repeating the basic protocol several times and independently, as usual.

8 Conclusions

We proposed a quantum algorithm with certainty for finding a marked solution of the equation $P|X\rangle = |b\rangle$ under the conditions given in Sect. 2. This framework generalizes the ones of quantum amplitude amplification algorithms with generalized phases of Brassard *et al.*, Høyer and Long, since all of these find pre-images of orthogonal projectors of rank one; while our proposed algorithm works for orthogonal projectors of arbitrary rank. We compared our algorithm with quantum amplification in an authentification protocol, in which our proposal succeeds with zero error probability, while quantum amplification succeeds with one half probability. This is so because the latter needs the initial state in its diffusion operator, while in the former the diffusion operator is independent of the initial state.

Appendix

Proof (Lema 2) There exist u, v real numbers such that $c_{11}+c_{22}=2u$ and $c_{11}-c_{22}=2iv$ where $|u|<1$, since $M(z)$ is elliptic. Thus, the fixed points are

$$\gamma_1=\frac{v+\sqrt{1-u^2}}{c_{21}/i}, \quad \gamma_2=\frac{v-\sqrt{1-u^2}}{c_{21}/i} \tag{27}$$

so γ_1 and γ_2 are in a line through the origin and they are symmetrical relative to the point $v/(c_{21}/i)$. Notice that ξ, the argument of c_{21}/i, is a non-negative real number lower than $\pi/2$. See Fig. 3. Therefore, point 1 is equidistant from the fixed points if and only if 1 belongs to the orthogonal line passing through the point $v/(c_{21}/i)$, which is equivalent to $\cos(\xi)=|v/c_{21}|$, i.e., $\operatorname{Im} c_{21}=\operatorname{Re}(c_{21}/i)=\cos(\xi)|c_{21}|=|v|$. Furthermore, from Fig. 3, we get

$$1=i\,\frac{v}{c_{21}}+\sin(\xi)\,i\exp(-i\xi)$$

leading to

$$S(1)=\frac{\sin(\xi)+c_{21}^{-1}\exp(i\xi)\sqrt{1-u^2}}{\sin(\xi)-c_{21}^{-1}\exp(i\xi)\sqrt{1-u^2}}$$

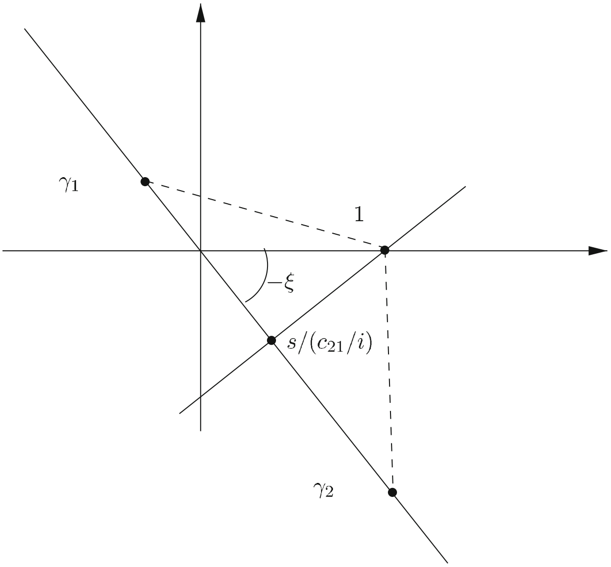

Fig. 3 Here γ_1, γ_2 are the fixed points of a Moebius transformation $M(z)$ as in Lemma 1. Point 1 is equidistant from the fixed points if and only if the line through $s/(c_{21}/i)$ and 1 is perpendicular to the line passing through the fixed points

with the help of Eq. 27. Additionally, $c_{21} = i\,|c_{21}|\exp(i\xi)$, so

$$S(1) = \frac{i\sin(\xi) + \sqrt{1-u^2}\,|c_{21}|^{-1}}{i\sin(\xi) - \sqrt{1-u^2}\,|c_{21}|^{-1}} = \exp(-i\kappa)$$

and

$$\tan\left(\frac{\pi-\kappa}{2}\right) = \frac{|c_{21}|\,\sin(\xi)}{\sqrt{1-u^2}}$$

because κ is the angle between the arguments of $i\sin(\xi) - \sqrt{1-u^2}\,|c_{21}|^{-1}$ and $i\sin(\xi) + \sqrt{1-u^2}\,|c_{21}|^{-1}$. □

Proof (Lema 3)

1. A straightforward calculation shows that $\mu(T)(y\sqrt{a}) = \mu(T_o)(1)$, where

$$T_0 = \begin{pmatrix} 1 & -\gamma_2' \\ 1 & -\gamma_1' \end{pmatrix}, \quad \gamma_1' = \frac{g+\sqrt{1-f^2}}{2a\sin(\phi/2)}\exp(i\varphi/2),$$

$$\gamma_2' = \frac{g-\sqrt{1-f^2}}{2a\sin(\phi/2)}\exp(i\varphi/2)$$

and γ_1', γ_2' are the fixed points of the normalized Moebius transformation $\mu(M_0)$; here

$$M_0 = \begin{pmatrix} f+ig & 2i(1-a)\exp(-i\varphi/2)\sin(\phi/2) \\ 2i\,a\,\exp(i\varphi/2)\sin(\phi/2) & f-ig \end{pmatrix}.$$

Using Lemma 2 for $\mu(M_0)$, we get that $|\mu(T)(y\sqrt{a})| = 1$ if and only if $2a\,\sin(\phi/2)\,\cos(\varphi/2) = g(\varphi,\phi)$, which in turn is equivalent to $\varphi = \phi$, since $g(\varphi,\phi) = \cos(\phi/2)\,\sin(\varphi/2) + (2a-1)\,\sin(\phi/2)\,\cos(\varphi/2)$. Also, from Lemma 2 for $\mu(M_0)$ we get $\mu(T)(y\sqrt{a}) = \exp(-i\kappa)$ where

$$\tan\left(\frac{\pi-\kappa}{2}\right) = \frac{2a\sin^2(\phi/2)}{\sqrt{1-f^2}}. \tag{28}$$

On one hand, from expression (17), Eq. 28 is equivalent to

$$\tan\left(\frac{\pi-\kappa}{2}\right) = \frac{\sqrt{a}\sin(\phi/2)}{\sqrt{1-a\sin^2(\phi/2)}}$$

on the other, $\tan[\arcsin(z)] = z/\sqrt{1-z^2}$. Therefore $(\pi-\kappa)/2 = \arcsin[\sqrt{a}\,\sin(\phi/2)]$, i.e., $\kappa = 2\arccos[\sqrt{a}\sin(\phi/2)]$.

2. Use Eq. 17.
3. We have that,

$$\arcsin(2z\sqrt{1-z^2}) = \begin{cases} 2\arcsin(z) & \text{if } 0 \le z \le 1/\sqrt{2}; \\ 2\arccos(z) & \text{if } 1/\sqrt{2} \le z \le 1. \end{cases}$$

Besides, $\arccos(z) = \pi/2 - \arcsin(z)$ if $-1 \le z \le 1$.

□

References

1. Goguen, J.A.: A categorical manifesto. Math. Struct. Comput. Sci. **1**, 49–67 (1991)
2. Brassard, G., Høyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. In: Lomonaco, J. S. J., Brandt, H.E. (eds.) Quantum Computation and Quantum Information: A Millennium Volume. AMS Contemporary Mathematics Series, vol. 305, pp. 53–74 (2002)
3. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**, 325 (1997)
4. Grover, L.K.: Quantum computers can search rapidly by using almost any transformation. Phys. Rev. Lett. **80**, 4329–4332 (1998)
5. Long, G.L., Zhang, W.L., Li, Y.S., Niu, L.: Arbitrary phase rotation can not be used in Grover's quantum search algorithm. Commun. Theor. Phys. **32**, 335–338 (1999)
6. Long, G.L., Li, X., Sun, Y.: Phase matching condition for quantum search with a generalized initial state. Phys. Lett. A **294**, 143–152 (2002)
7. Høyer, P.: Arbitrary phases in quantum amplitude amplification. Phys. Rev. A **62**, 052,304 (2000)
8. Long, G.L.: Grover algorithm with zero theoretical failure rate. Phys. Rev. A **64**, 022,307 (2001)
9. Biham, E., Biham, O., Biron, D., Grassl, M., Lidar, D.A.: Grover's quantum search algorithm for an arbitrary initial amplitude distribution. Phys. Rev. A **60**, 2742–2745 (1999)
10. Carlini, A., Hosoya, A.: Quantum computers and unstructured search: finding and counting items with an arbitrarily entangled initial state. Phys. Lett. A **280**, 114–120 (2001)
11. Jin, W.L., Chen, X.D.: A desired state can not be found with certainty for Grover's algorithm in a possible three-dimensional complex subspace. Quantum Inf. Process. **10**, 419–429 (2011)
12. Jin, W.: Quantum search in a possible three-dimensional complex subspace. Quantum Inf. Process. (2011). doi:10.1007/s11128-011-0230-5
13. Li, D.F., Li, X.X.: More general quantum search algorithm $Q = -I_\gamma V I_\tau U$ and the precise formula for the amplitude and the non-symmetric effects of different rotating angles. Phys. Lett. A **287**, 304–316 (2001)
14. Long, G.L., Yang, L.: Search an unsorted database with quantum mechanics. Front. Comput. Sci. China **1**(3), 247–271 (2007)
15. Ahlfors, L.V.: Complex Analysis. 3rd edn. McGraw-Hill, Tokyo (1979)
16. Conway, J.B.: Functions of One Complex Variable I. 2nd edn. Springer, New York (1995)
17. Needham, T.: Visual Complex Analysis. Oxford University Press, Oxford (2002)
18. Lee, J., Kim, C.H., Lee, E., Kim, J., Lee, S.: Qubit geometry and conformal mapping. Quantum Inf. Process. **1**(1/2), 129–134 (2002)
19. Bautista-Ramos, C., Castillo-Tepox, N.: Möbius transformations in quantum amplitude amplification with generalized phases. Int. J. Quantum Inf. **8**(6), 923–935 (2010)
20. Codd, E.F.: A relational model of data for large shared data banks. Commun. ACM **13**, 377–387 (1970)
21. Codd, E.F.: The Relational Model for Database Management: Version 2. Addison-Wesley, Reading Mass (1990)
22. Abiteboul, S., Hull, R., Vianu, V.: Foundations of Databases. Addison-Wesley, Reading Mass (1995)
23. Agoston, M.K.: Computer Graphics and Geometrical Modeling. Springer, London (2005)
24. Hartley, R., Zisserman, A.: Multiple View Geometry in Computer Vision. Cambrigde University Press, Cambridge (2003)
25. Xie, M.: Fundamentals of Robotics: linking perception to action. World Scientific, Singapore (2003)

26. Menezes, A., Oorschot, P.van , Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
27. Schwerdtfeger, H.: Geometry of Complex Numbers. Dover, New York (1979)
28. Schwerdtfeger, H.: Moebius transformations and continued fractions. Bull. Amer. Math. Soc. **52**, 307–309 (1946)
29. Lane, R.: The convergence and the values of periodic continued fractions. Bull. Amer. Math. Soc. **51**, 246–250 (1945)