Quantum Information Processing (2022) 21:274
https://doi.org/10.1007/s11128-022-03614-6

Quantum measurement detection algorithms

Guillermo Lugilde Fernández[1] · Elías F. Combarro[2] · Ignacio F. Rúa[1]

Received: 16 February 2022 / Accepted: 9 July 2022

Abstract
In this paper, we introduce and study the quantum measurement detection algorithms (QMDA), whose objective is to detect whether unwanted measurements are being taken in a quantum circuit or not by applying the Zeno effect. A QMDA is a quantum circuit that includes three unitary matrices, one of them being applied numerous times consecutively, and whose initial state is fixed when no foreign measurements occur. One example is the Elitzur–Vaidman bomb tester, which is generalized by the QMDA definition, allowing the detection of measurements that are taken in an unknown basis and in circuits with an arbitrary number of qubits. We prove some key properties and limitations of these algorithms, as well as studying the performance of the Elitzur–Vaidman bomb tester and its possible improvements. Some extensions of the definition would lead to algorithms such as the counterfactual communication one.

Keywords Quantum measurement detection algorithms · Quantum detection · Quantum measurements · Elitzur–Vaidman bomb tester · Zeno effect · Counterfactual communication

1 Introduction

Quantum computing is known for its potential to outperform classical computation in some specific tasks. The most popular quantum algorithms are Shor's factorization algorithm [1] and Grover's search algorithm [2], which provide exponential and quadratic time speedup, respectively, over the best known classical algorithms.

✉ Guillermo Lugilde Fernández
lugildeguillermo@uniovi.es

Elías F. Combarro
efernandezca@uniovi.es

Ignacio F. Rúa
rua@uniovi.es

[1] Mathematics Department, University of Oviedo, Oviedo, Spain

[2] Computer Science Department, University of Oviedo, Oviedo, Spain

Published online: 13 August 2022

However, other algorithms that show the potential of quantum computers have been proposed, such as the Elitzur–Vaidman bomb tester [3]. This algorithm is based on the Zeno effect [4], that is, the initial state of the circuit is slowly rotated to a different state unless measurements occur. On the other hand, in the presence of measurements, the final and initial states are the same with high probability. Zeno effect-based circuits, and mainly the Elitzur–Vaidman one, have proved to be useful in applications to multiple fields, such as cryptography or object mapping [5–9].

In this article, we introduce a framework for studying measurement detection in an unknown basis in circuits of the same kind. One of the aims of this work is to extend the scope of the Elitzur–Vaidman algorithm, and study its behaviour for unknown measurement bases and multiple qubits. So, we introduce quantum measurement detection algorithms (QMDA), which provide a generalization of the Zeno effect of the Elitzur–Vaidman algorithm.

A QMDA is a quantum circuit that includes three operators (U_0, U, U_1), one of them (U) being applied numerous times consecutively, and whose initial state is fixed when no foreign measurements (i.e. undesired measurements that are not expected during the execution of a circuit) occur.

Some properties of a QMDA are proved, including the detection of measurement probability of error of a QMDA for a given measurement basis and the corresponding optimal value. In addition, we find some bases that are likely to yield less accurate detections, although the probability bounds that we provide, decrease exponentially as the number of qubits increases. Such bases are given by a linear combination of eigenvectors of the operator U. This framework allows to compare the generalization of the Elitzur–Vaidman algorithm with the best possible QMDA. For more than one qubit, it can be proved to be outperformed by some rather difficult-to-describe QMDA.

Finally, we hint at some extensions of the definition of a QMDA that might overcome some problems derived from our study. Such extensions of the definition would also include algorithms such as the counterfactual communication [5] one. In addition, a QMDA might also be helpful to spot interferences that cause undesired measurements in a circuit.

The structure of this paper is as follows. In Sect. 2, we briefly describe the Elitzur–Vaidman bomb tester. In Sect. 3, we introduce the definition of QMDA, its associated detection scheme and we show the main properties of these circuits. In Sect. 4, we study the particular case of the Elitzur–Vaidman bomb tester, and finally, Sect. 6 contains the conclusions and future work.

2 Elitzur–Vaidman algorithm

This paper has been motivated by the Elitzur–Vaidman algorithm. It aims at determining whether foreign measurements have been applied to a circuit or not. Henceforth, by *foreign measurements*, we will mean undesired measurements that are not expected during the execution of a circuit, and they will be represented as an O in the circuits. In order to detect them, the Zeno effect is used, rotating the initial state slowly so that, if measurements are taken, the final state of the algorithm differs, with high probability, from the one when none of those measurements occur. We will briefly describe it next.

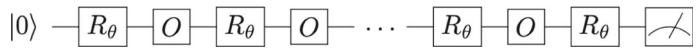


Fig. 1 Elitzur–Vaidman algorithm for one qubit

Elitzur–Vaidman bomb tester

The objective is to detect measurements in a 1-qubit quantum circuit. Such measurements represent a bomb in a quantum circuit, which explodes when $|1\rangle$ is measured. The algorithm is designed to minimize the probability of measuring $|1\rangle$, while detecting the presence of the measurements in the end, without triggering the bomb. As mentioned before, O will represent the place where a measurement may or may not occur.

The Elitzur–Vaidman circuit is shown in Fig. 1, where $\theta = \frac{\pi}{2k}$ for a given $k \in \mathbb{N}$, and the rotation R_θ, whose coordinate matrix with respect to the computational basis is $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, is applied k times. As we mentioned above, the rotation is applied multiple times in order to rotate the state slowly while the measurements may occur, so that an interruption of such rotation (a measurement) would cause different outcomes in the final measurement with high probability.

If there are no measurements on O (no bomb), the state $|0\rangle$ will be allowed to rotate to $|1\rangle$, which will be the result of the last measurement with certainty. (Since this measurement is not related to O, it does not affect the bomb.)

On the other hand, if there is actually a bomb, each O will take a measurement. This is the case when the rotation is constantly being interrupted, and consequently, the state will not be able to get to $|1\rangle$ and it is likely to stay in $|0\rangle$ for every O measurement. More precisely, the probability of outcome $|1\rangle$ (and so exploding the bomb) is $\sin^2\theta$ each time. Therefore, the probability of measuring $|0\rangle$ in every O, is $\cos^{2k}\theta \xrightarrow[k\to\infty]{} 1$. So, the probability of measuring $|0\rangle$ at the end can be as close to 1 as desired, meaning the detection of bomb in the circuit despite not having sparked any explosion.

As we see, the algorithm detects the existence of measurements in a circuit. A relevant question is its performance when the measurements basis is unknown and arbitrary. This is the problem that will be addressed in this article.

3 QMDA and their properties

As shown in the previous section, we know algorithms that are able to detect, with high probability, if measurements were taken during the circuit or not, and our aim is to generalize them taking the Elitzur–Vaidman algorithms as the main reference. We will provide the theoretical framework before focusing on the Elitzur–Vaidman bomb tester.

3.1 QMDA definition

The following definition is inspired by our previous work on Quantum Abstract Detecting Systems (QADS) [10]. These systems are able to detect whether there is a marked

Table 1 Comparison between QADS and QMDA

Algorithm	Trivial case	Implication	Expected outcome	Non-trivial case	Expected outcome
QADS with initial state $\|\psi_0\rangle$	$f \equiv 0$	$U_f\|\psi_0\rangle = \|\psi_0\rangle$	$\|\psi_0\rangle$	$f \not\equiv 0$	Different from $\|\psi_0\rangle$
QMDA with initial state $\|\psi_0\rangle$	$O \equiv I$	$U_1U^kU_0\|\psi_0\rangle = \|\psi_0\rangle$	$\|\psi_0\rangle$	$O \equiv$ *measurement*	Different from $\|\psi_0\rangle$

element in a given set. This is achieved by creating circuits that fix the initial state when there are no marked elements, so that the outcome is predictable in that case. Measuring any other state at the end of the circuit would inevitably mean that there are marked elements. Different subclasses, such as combinatorial or rotational QADS, have proved to be useful for a variety of problems [11].

Since the objective of QMDA is to detect whether there are measurements in our circuit, we can employ the same strategy as QADS: fixing the initial state when none of those measurements occur, so that a predictable outcome is forced for this case. Hence, the QMDA will be expected to fix the initial state when there are no measurements, so that any other state at the end of the circuit would confirm that measurements have happened. The similarities are illustrated in Table 1.

Definition 1 A quantum measurement detection algorithm of size n, henceforth QMDA$_n$, is a 5-tuple $(U_0, U, U_1, k, |\psi_0\rangle)$, where $|\psi_0\rangle \in \mathcal{H}$ represents the initial state, being $\mathcal{H}$ a Hilbert space of dimension $N = 2^n$; U_0, U, U_1 are unitary operators on $\mathcal{H}$ and $k > 0$ is a natural number such that $U_1U^kU_0|\psi_0\rangle = |\psi_0\rangle$.

As shown in Fig. 2, U_0 represents the sub-circuit before the first O (measurement or not), U the sub-circuit that will be repeated between each two O and U_1 the final sub-circuit before the last measurement. It is clear, then, that the circuit is prepared for $k + 1$ applications of O. If $O \equiv I$ (no measurement), then the gates are applied consecutively getting to the final state $|\psi_0\rangle$. If $O \equiv$ *measure*, we assume all of them measure in the same basis.

From this, the detection scheme for measurements is the following.

Algorithm 1 Detection scheme for a QMDA$_n$

Given a QMDA$_n$ $(U_0, U, U_1, k, |\psi_0\rangle)$:

1: Implement the circuit $\mathcal{C}$ starting on the initial state $|\psi_0\rangle$.
2: Measure the final state over any orthonormal basis that contains $|\psi_0\rangle$.
3: If the result is $|\psi_0\rangle$, output 'NO.' If the result is any other state different from $|\psi_0\rangle$, output 'YES.'

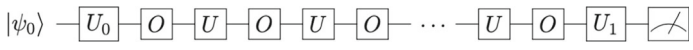


Fig. 2 Circuit of a QMDA

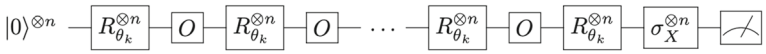


Fig. 3 Elitzur–Vaidman algorithm as a QMDA for n qubits

We would like to minimize the probability of error of the algorithm when the measurement basis is unknown. We should notice that the detection scheme does not provide a wrong answer when $O \equiv I$, but it might fail when $O \equiv$ *measure* when we obtain $|\psi_0\rangle$ at the end, so the probability of error is only related to this case.

Our definition allows us to introduce a family of Elitzur–Vaidman algorithms.

Definition 2 We define $\mathrm{EV}_{n,k}$ as the 5-tuple $(R_{\theta_k}^{\otimes n}, R_{\theta_k}^{\otimes n}, \sigma_X \cdot R_{\theta_k}^{\otimes n}, k, |0\rangle^{\otimes n})$, where $\theta_k = \frac{\pi}{2(k+2)}$. $\mathrm{EV}_{n,k}$ is a QMDA_n for all n and k natural numbers.

The circuit is shown in Fig. 3. The final NOT gate has the objective of fixing the initial state whenever $O \equiv I_N$.

3.2 Properties of a QMDA$_n$

We begin by studying the behaviour of the circuit when the measurements occur. Let us introduce some useful notation.

Definition 3 Given a QMDA_n $(U_0, U, U_1, k, |\psi_0\rangle)$ and an orthonormal basis $M = \{|m_i\rangle\}_{i=1}^N$, we define the auxiliary matrices

$$\hat{M}_0 := (|\langle m_i|U_0|\psi_0\rangle|^2)_{1\le i\le N} \text{ (column vector)},$$
$$\hat{M} := (|\langle m_i|U|m_j\rangle|^2)_{1\le i,j\le N},$$
$$\hat{M}_1 := (|\langle \psi_0|U_1|m_j\rangle|^2)_{1\le j\le N} = (|\langle m_j|U_1^\dagger|\psi_0\rangle|^2)_{1\le j\le N} \text{ (row vector)}.$$

$\hat{M}_0$ gathers the probability of the QMDA_n circuit collapsing into each $|m_i\rangle$ in the first O measurement, after starting in the state $|\psi_0\rangle$; $\hat{M}$ gathers its probability of collapsing into each $|m_i\rangle$ in the following O measurements, after starting each subcircuit in the corresponding $|m_j\rangle$ measured in the previous O; and $\hat{M}_1$ gathers its probability of collapsing into $|\psi_0\rangle$ at the end (which would mean a wrong detection), depending on the state $|m_j\rangle$ it started in after the final O measurement.

The auxiliary matrices are central in our study, due to the fact that they will allow us to calculate the probability of error of the detection scheme.

Theorem 1 *Given a QMDA$_n$ $(U_0, U, U_1, k, |\psi_0\rangle)$, and assuming that every O represents a measurement in an orthonormal basis $M = \{|m_i\rangle\}_{i=1}^N$, the probability of measuring the state $|\psi_0\rangle$ at the end of the algorithm is given by $\hat{M}_1\hat{M}^k\hat{M}_0$.*

The proof of every result of this section can be found in "Appendix A." This theorem theoretically allows us to calculate the probability of error of the algorithm for a given basis M. However, a practical computation of $\hat{M}^k$ might be difficult when $n >> 1$. In this sense, a useful property that we can use to calculate the three auxiliary matrices

is the fact that every row and column adds up to 1, and so some tricks to calculate $\hat{M}^k$ are used in subsequent proofs (gathered in the appendices).

Moreover, since there may be a high number of undesired measurements in the circuits that are out of our control and that might be conditioned by an interfering environment, it is reasonable to question the effect that noisy measurements would have on QMDA. We can obtain a first insight into this subject by considering that, for every measurement in O, the probability of measuring the state $|m_i\rangle$ when, in absence of noise, we would have measured $|m_j\rangle$, is given by $\langle m_i|E|m_j\rangle$, where E is a stochastic matrix. This type of noise has been used before to study measurement errors, for instance in [12].

Under these conditions, the formula for the probability of error changes, as the stochastic matrix gets represented once for each O measurement.

Theorem 2 *Given a QMDA$_n$ $(U_0, U, U_1, k, |\psi_0\rangle)$, and assuming that every O represents a noisy measurement in an orthonormal basis $M = \{|m_i\rangle\}_{i=1}^N$, being E the associated readout error stochastic matrix, the probability of measuring the state $|\psi_0\rangle$ at the end of the algorithm is given by $\hat{M}_1(\hat{E}\hat{M})^k\hat{E}\hat{M}_0$, where $\hat{E} := (\langle m_i|E|m_j\rangle)_{1\leq i,j\leq N}$.*

The effect of more complex types of noise is an interesting subject that would deserve a more thorough and independent study. For now, our aim is to find an algorithm capable of detecting whether measurements have taken place or not, but without knowing the basis in which they occur. To guide us, we will use the following natural definition for the worst behaviour of the detection scheme.

Definition 4 Let $\mathcal{M}$ be the set of orthonormal bases of a Hilbert space $\mathcal{H}$ of dimension N. Given a QMDA$_n$ $\mathcal{Q}$, we define $\delta(\mathcal{Q}) := \sup\{\hat{M}_1\hat{M}^k\hat{M}_0\}_{M\in\mathcal{M}}$, and we say that $\mathcal{Q}$ is a $\delta(\mathcal{Q})$-detector algorithm.

Obviously, we aim to find a QMDA whose $\delta(\mathcal{Q})$ is as low as possible.

It is time to prove some bounds to the probability of error and to $\delta(\mathcal{Q})$, some of them being related to the eigenvectors of U, due to their ability to skip the influence of every U gate.

Proposition 1 *Let $(U_0, U, U_1, k, |\psi_0\rangle)$ be a QMDA$_n$ and M an orthonormal basis of a Hilbert space of dimension N. Then*

$$\hat{M}_1\hat{M}^k\hat{M}_0 \geq \frac{1}{N^{2(k+1)}} > 0.$$

This immediately shows that it is impossible for a QMDA$_n$ to achieve a perfect accuracy for any basis we are measuring in, so our best option is to be able to decrease the probability of error as much as desired, which will always require an increment of k. Although this can be easily overcome, in the next theorems we identify measurement bases having particularly undesired properties.

Theorem 3 *Let $(U_0, U, U_1, k, |\psi_0\rangle)$ be a QMDA$_n$ and let $A = \{|a_i\rangle\}_{i=1}^N$ be an orthonormal basis of eigenvectors of U. Then $\hat{A} = I_N$, $\hat{A}_1^t = \hat{A}_0$ and*

$$\hat{A}_1 \hat{A}^k \hat{A}_0 = \hat{A}_1 \hat{A}_1^t = \hat{A}_0^t \hat{A}_0 \geq \frac{1}{N}.$$

Moreover,

$$\hat{A}_1 \hat{A}^k \hat{A}_0 = \frac{1}{N} \Leftrightarrow |\langle a_i|U_0|\psi_0\rangle|^2 = \frac{1}{N}, \ \forall i = 1, \ldots, N.$$

As we can see, when measurements occur in a basis of eigenvectors of U, the detection is immediately restricted to $\frac{1}{N}$. This property suggests that eigenvectors-related bases are worth studying and will be our main concern. Several conclusions can be deduced from it, mainly bounds for $\delta(\mathcal{Q})$ that warn us about the difficulty of dealing with these bases.

Corollary 1 *If $\mathcal{Q}$ is a QMDA$_n$, then $\delta(\mathcal{Q}) \geq \frac{1}{N}$.*

Corollary 2 *If $\mathcal{Q}$ is a QMDA$_n$, then $\delta(\mathcal{Q}) = \frac{1}{N}$ if and only if the maximum of $\hat{M}_1 \hat{M}^k \hat{M}_0$ is reached for any basis of eigenvectors of U and its value is $\frac{1}{N}$.*

Corollary 3 *If $\mathcal{Q}$ is a QMDA$_n$ and $\exists |a\rangle$ eigenvector of U such that $U_0|\psi_0\rangle = |a\rangle$, then $|\langle a|U_0|\psi_0\rangle|^2 = 1$, and hence, $\delta(\mathcal{Q}) = 1$.*

Although the first corollary is a lower bound for the probability of error, this bound decreases exponentially with n, so it is not as restrictive as expected. Additionally, it suggests the following definition.

Definition 5 We say that a QMDA$_n$ $\mathcal{Q}$ is optimal if $\delta(\mathcal{Q}) = \frac{1}{N}$.

Corollary 4 *If a QMDA$_n$ is optimal and A is a basis of eigenvectors of U, then $|\langle a_i|U_0|\psi_0\rangle|^2 = \frac{1}{N}$, $\forall i = 1, \ldots, N$.*

It is worth pointing out that this bound does not mean that the maximum of $\hat{M}_1 \hat{M}^k \hat{M}_0$ is always reached for a basis of eigenvectors of U. In fact, as we will see in the next section, the maximum probability of error in the case of any EV$_{1,k}$ is not reached for the basis of eigenvectors $\{|+i\rangle, |-i\rangle\}$, but for $\{|+\rangle, |-\rangle\}$. This means that no EV$_{n,k}$ is optimal. However, at least every EV$_{1,k}$ will satisfy the following definition, which is inspired by the properties proved in Proposition 1 and Theorem 3.

Definition 6 We say that an infinite family $\{\mathcal{Q}_p\}_{p=1}^{\infty}$ of QMDA$_n$, dependent on the parameter p, is asymptotically optimal if $\delta(\mathcal{Q}_p) \xrightarrow[p\to\infty]{} \frac{1}{N}$ and $\exists M \in \mathcal{M}$ such that $\hat{M}_{1,p} \hat{M}_p^{k(p)} \hat{M}_{0,p} \xrightarrow[p\to\infty]{} 0$.

If a family $\{\mathcal{Q}_p\}_{p=1}^{\infty}$ is asymptotically optimal, then we know from Proposition 1 that $p \to \infty \Rightarrow k(p) \to \infty$. After these two definitions, we aim at finding some

QMDA_n that verifies the conditions presented. As we already advanced, $\text{EV}_{1,k}$ does the job for $n = 1$, but as n increases, we need to consider QMDAs with clever combinations of eigenvectors of U. This is because, as we will prove, they tend to cause high probabilities of error if they are not treated correctly. We gather the bases of linear combinations of eigenvectors of U in the following definition.

Definition 7 For any basis $A = \{|a_i\rangle\}_{i=1}^{N}$ and any P divisor of N, we say the basis M is a P-combination of A if

$$|m_{Pd+i}\rangle = \frac{1}{\sqrt{P}} \sum_{j=1}^{P} \sigma_i(j)|a_{Pd+j}\rangle,$$

where $i = 1, \ldots, P$; $d = 0, \ldots, N/P - 1$ and each $\sigma_i(j)$ is either 1 or -1 (in other words, it just indicates the sign accompanying each $|a_j\rangle$ for the ith element of M). Moreover, M must verify the following properties:

$$\begin{aligned}
&1. \quad \sigma_1(j) = \sigma_i(1) = 1, \quad \forall i, j \\
&2a. \quad \sum_{j=1}^{P} \sigma_{i_1}(j)\sigma_{i_2}(j) = 0, \quad \forall i_1 \neq i_2 \\
&3a. \quad \forall i_1, i_2, \ \exists p \text{ such that } \ \sigma_{i_1}(j)\sigma_{i_2}(j) = \sigma_p(j), \quad \forall j \\
&3b. \quad \forall j_1, j_2, \ \exists q \text{ such that } \ \sigma_i(j_1)\sigma_i(j_2) = \sigma_i(q), \quad \forall i
\end{aligned}$$

This bases are just linear combinations of the vectors of A, but with every coefficient being $\pm 1/\sqrt{P}$. We will see how to construct one soon. Property 1 means that the first element of M is the sum of the first P elements of A. Property 2a ensures the orthonormality of the basis, and 3a means that the product of the signs of two different elements of M are the signs of another element of M. We will need all of them for proving the upcoming theorems. In addition, some extra properties can be deduced from these:

Proposition 2 *If M is a P-combination of the basis A, the following properties are a consequence of the properties 1 and 2a.*

$$\begin{aligned}
&2b. \quad \sum_{i=1}^{P} \sigma_i(j_1)\sigma_i(j_2) = 0, \quad \forall j_1 \neq j_2 \\
&2c. \quad \sum_{j=1}^{P} \sigma_i(j) = 0, \quad \forall i \neq 1 \\
&2d. \quad \sum_{i=1}^{P} \sigma_i(j) = 0, \quad \forall j \neq 1
\end{aligned}$$

We will also benefit from the property 3a and 3b to introduce some notation. Since 3a is a property of the signs 'by rows', and 3b is analogous 'by columns', we will use

the notation

$$(i_1, i_2)_r = p \ :\Leftrightarrow \ \sigma_{i_1}(j)\sigma_{i_2}(j) = \sigma_p(j),$$
$$(j_1, j_2)_c = q \ :\Leftrightarrow \ \sigma_i(j_1)\sigma_i(j_j) = \sigma_i(q).$$

In order to find an example of P-combination basis, we only have to choose a proper combination of signs. A way of doing it is by using the Sylvester matrices [13]. The Sylvester matrix $S(k)$ of order 2^k is

$$S(k) = \begin{pmatrix} + & + \\ + & - \end{pmatrix}^{\otimes k}.$$

These matrices offer an example of signs election that can be used for constructing P-combination bases, as we prove in the following proposition.

Proposition 3 *If $S(k)$ is a Sylvester matrix and $\sigma_i(j) := S(k)_{ij}$, then, for all k and any given a basis A,*

$$|m_{Pd+i}\rangle = \frac{1}{\sqrt{P}} \sum_{j=1}^{P} \sigma_i(j)|a_{Pd+j}\rangle$$

is a P-combination of the basis A for $P = 2^k$.

The first Sylvester matrices are:

$$S(1) = \begin{pmatrix} + & + \\ + & - \end{pmatrix}, \ S(2) = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}, \ S(3) = \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{pmatrix}.$$

So, given any basis A, an example of 2-combination basis of A for $n = 2$ is:

$$|m_1\rangle = \frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle) \qquad |m_3\rangle = \frac{1}{\sqrt{2}}(|a_3\rangle + |a_4\rangle)$$
$$|m_2\rangle = \frac{1}{\sqrt{2}}(|a_1\rangle - |a_2\rangle) \qquad |m_4\rangle = \frac{1}{\sqrt{2}}(|a_3\rangle - |a_4\rangle).$$

For $n = 3$, an example of 4-combination basis is

$$|m_1\rangle = \frac{1}{2}(|a_1\rangle + |a_2\rangle + |a_3\rangle + |a_4\rangle) \qquad |m_5\rangle = \frac{1}{2}(|a_5\rangle + |a_6\rangle + |a_7\rangle + |a_8\rangle)$$

$$|m_2\rangle = \frac{1}{2}\left(|a_1\rangle - |a_2\rangle + |a_3\rangle - |a_4\rangle\right) \qquad |m_6\rangle = \frac{1}{2}\left(|a_5\rangle - |a_6\rangle + |a_7\rangle - |a_8\rangle\right)$$
$$|m_3\rangle = \frac{1}{2}\left(|a_1\rangle + |a_2\rangle - |a_3\rangle - |a_4\rangle\right) \qquad |m_7\rangle = \frac{1}{2}\left(|a_5\rangle + |a_6\rangle - |a_7\rangle - |a_8\rangle\right)$$
$$|m_4\rangle = \frac{1}{2}\left(|a_1\rangle - |a_2\rangle - |a_3\rangle + |a_4\rangle\right) \qquad |m_8\rangle = \frac{1}{2}\left(|a_5\rangle - |a_6\rangle - |a_7\rangle + |a_8\rangle\right).$$

In this last example, we have combined elements 1-2-3-4 and 5-6-7-8 of A, but any other combination could be possible, for example, 1-5-7-8 and 2-3-4-6. For any A basis, and for any given n and P, there are

$$\binom{N}{P}\cdot\binom{N-P}{P}\cdot\binom{N-2P}{P}\cdot\ldots\cdot\binom{2P}{P} = \frac{N!}{(P!)^{N/P}}$$

different possible P-combination bases. Our theorems provide results for one of the P combination bases, but the optimality requires an acceptable behaviour for every possible basis.

We will focus on bases of eigenvectors of U. Their P-combination bases challenge the optimality of the algorithm and their properties simplify the calculations considerably.

Theorem 4 *Given a QMDA$_n$, A an orthonormal basis of eigenvectors of U and M a P-combination basis of A, then, if the eigenvalue associated with $|a_i\rangle$ is $\lambda_i = e^{i\varphi_i}$,*

$$\begin{aligned}\hat{M}_1\hat{M}^k\hat{M}_0 = &\sum_{d=0}^{N/P-1}\frac{1}{P}\left(\sum_{j=1}^{P}|\beta_{Pd+j}|^2\right)^2\\ &+\sum_{i=2}^{P}\left(\frac{1}{P}\sum_{j=1}^{P}\cos\varphi_{Pd+j,Pd+(i,j)_c}\right)^k\\ &\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_{Pd+j}||\beta_{Pd+(i,j)_c}|\cos\beta_{Pd+j,Pd+(i,j)_c}\right)\\ &\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_{Pd+j}||\beta_{Pd+(i,j)_c}|\cos(\beta_{Pd+j,Pd+(i,j)_c}+k\varphi_{Pd+j,Pd+(i,j)_c})\right),\end{aligned}$$

where $\varphi_{ij} = \varphi_i - \varphi_j$, and β_{ij} is the angle between $\beta_i := \langle a_i|U_0|\psi_0\rangle$ and $\beta_j := \langle a_j|U_0|\psi_0\rangle$.

The optimality of the QMDA$_n$ requires this probability not to exceed $\frac{1}{N}$. We can simplify the formula assuming that $|\beta_i|^2 = |\langle a_i|U_0|\psi_0\rangle|^2 = \frac{1}{N}$, which is a necessary condition for the optimality.

Theorem 5 *In the conditions of the previous theorem, if* $|\beta_i|^2 := |\langle a_i|U_0|\psi_0\rangle|^2 = \frac{1}{N}$ *and* $P = 2^q$*, then*

$$\hat{M}_1\hat{M}^k\hat{M}_0 = \frac{1}{2^n} + \frac{1}{2^{2n-q}}\sum_{d=0}^{N/P-1}\sum_{i=2}^{P}\left(\frac{1}{P}\sum_{j=1}^{P}\cos\varphi_{Pd+j,Pd+(i,j)_c}\right)^k \cdot\left(\frac{1}{P}\sum_{j=1}^{P}\cos\beta_{Pd+j,Pd+(i,j)_c}\right) \cdot\left(\frac{1}{P}\sum_{j=1}^{P}\cos(\beta_{Pd+j,Pd+(i,j)_c} + k\varphi_{Pd+j,Pd+(i,j)_c})\right).$$

This formula does not imply that $\hat{M}_1\hat{M}^k\hat{M}_0 \geq \frac{1}{N}$, due to the fact that the cosines may be negative. Unfortunately, making the cosines negative requires large angles, and since the number of angles increases exponentially with n, getting large ones becomes a problem of unclear solution. Moreover, we have to remember that the P combination can be done with any group of P eigenvectors of A, so the angles of the cosines can be combined however we desire to, and the summation must be negative (or 0) for all of them in order to achieve the optimality.

Minimizing the formula analytically is difficult in general, but in the case of $P = 2$ it can be cleverly done. The trick is based on the fact that 2-combination bases are the only ones in which there is no mixture of angles in the cosines, so that they can be treated independently.

Theorem 6 *Given a QMDA*$_n$*, A an orthonormal basis of eigenvectors of U, and M a 2-combination basis, then*

$$\hat{M}_1\hat{M}^k\hat{M}_0 = \frac{1}{2}\left[\sum_{i=1}^{N/2}\left(|\beta_{2i-1}|^2 + |\beta_{2i}|^2\right)^2 + 4\sum_{i=1}^{N/2}|\beta_{2i-1}|^2|\beta_{2i}|^2\cos^k\varphi_{2i-1,2i}\cos\beta_{2i-1,2i}\cos(\beta_{2i-1,2i} + k\varphi_{2i-1,2i})\right].$$

Moreover, defining $C_i := \cos^k\varphi_{2i-1,2i}\cos\beta_{2i-1,2i}\cos(\beta_{2i-1,2i} + k\varphi_{2i-1,2i})$*, the following bound is verified:*

$$\hat{M}_1\hat{M}^k\hat{M}_0 \geq \frac{1}{2\sum_{i=1}^{N/2}\frac{1}{C_i+1}}.$$

The equality is satisfied if and only if

$$\forall j = 1, \ldots, N/2,\ |\beta_{2j-1}|^2 + |\beta_{2j}|^2 = \frac{1}{\sum_{i=1}^{N/2} \frac{C_j + 1}{C_i + 1}},\ \textit{and, if } C_j \neq 0 \Rightarrow\ |\beta_{2j-1}|^2 = |\beta_{2j}|^2.$$

The condition for the equality is rather cumbersome. Consequently, since we aim at a minimization for every 2-combination basis, we focus on the case of independence of the constants, i.e. $|\beta_i|^2 = |\beta_j|^2 = \frac{1}{N}$, $\forall i, j$. This condition is convenient for a QMDA_n since it unifies the probability formulas for every P-combination basis for any given P and is a necessary condition for the optimality. Applied to a 2-combination basis, the probability under this condition is

$$\hat{M}_1 \hat{M}^k \hat{M}_0 = \frac{1}{2^n} + \frac{1}{2^{2n-1}} \sum_{i=1}^{N/2} \cos^k \varphi_{2i-1,2i} \cos \beta_{2i-1,2i} \cos(\beta_{2i-1,2i} + k\varphi_{2i-1,2i}) \quad (1)$$

However, being able to minimize the probability of error under one 2-combination basis does not provide a way of minimizing the probability of error under every 2-combination basis at the same time, especially for great values of n.

Finally, before getting into the study of $\text{EV}_{n,k}$, we will prove a very useful result for calculating probabilities of a QMDA_{n+m} constructed from other QMDA_n and QMDA_m of smaller size.

Theorem 7 *Let* $(U_0, U, U_1, k, |\psi_0\rangle)$ *be a* QMDA_n, $(V_0, V_1, V, k, |\varphi_0\rangle)$ *a* QMDA_m *and* X, Y *two orthonormal bases of dimension* 2^n *and* 2^m*, respectively. Then, given the* QMDA_{n+m} $(U_1 \otimes V_1, U \otimes V, U_0 \otimes V_0, k, |\psi_0\rangle \otimes |\varphi_0\rangle)$*, the basis* $Z = \{|x_i\rangle \otimes |y_j\rangle, \forall i = 1, \ldots, 2^n, \forall j = 1, \ldots, 2^m\}$ *verifies*

$$\hat{Z}_0 = \hat{X}_0 \otimes \hat{Y}_0,\ \hat{Z}_1 = \hat{X}_1 \otimes \hat{Y}_1, \textit{ and } \hat{Z} = \hat{X} \otimes \hat{Y}.$$

As a consequence, $\hat{Z}_1 \hat{Z}^k \hat{Z}_0 = \hat{X}_1 \hat{X}^k \hat{X}_0 \cdot \hat{Y}_1 \hat{Y}^k \hat{Y}_0$.

This intuitive property allows us to calculate probabilities associated to any basis that verifies the given conditions whenever we are working with a QMDA_n constructed from a tensor product, as it is the case of any $\text{EV}_{n,k} = \text{EV}_{1,k} \otimes \ldots \otimes \text{EV}_{1,k}$.

4 Study of the Elitzur–Vaidman algorithm

In this last section, we will analyse the behaviour of the Elitzur–Vaidman algorithm. We will prove that, for $n = 1$, $\text{EV}_{1,k}$ is an asymptotically optimal family of QMDA_n. However, this is not the case for $n > 1$, due to the P-combination bases, as the angles involved in the formula of Theorem 4 get smaller when $k \longrightarrow \infty$. We will suggest an adjustment that overcomes this for $n = 2$, but for greater n the solution in unclear. The main theorem of this section is the following.

Theorem 8 *Given k, we consider the QMDA$_1$ $EV_{1,k}$ and we define $c := \cos\theta_k$, $s := \sin\theta_k$. If every O is equivalent to a measurement in the basis M where $|m_1\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ and $|m_2\rangle = \sin\frac{\theta}{2}|0\rangle - e^{i\varphi}\cos\frac{\theta}{2}|1\rangle$, then*

$$\hat{M}_1\hat{M}^k\hat{M}_0 = \frac{1}{2} + \frac{(c^2 - s^2 + 2s^2\sin^2\theta\sin^2\varphi)^k(4c^2s^2\sin^2\theta\cos^2\varphi - (c^2 - s^2)^2\cos^2\theta)}{2}.$$

The proofs of the two main results of this section can be found in "Appendix B." As a consequence, when we measure in the basis of eigenvalues of $U = R_{\theta_k}$, which is $A = |+i\rangle, |-i\rangle$, we get $\hat{A}_1\hat{A}^k\hat{A}_0 = \frac{1}{2} = \frac{1}{N}$. Unfortunately, this does not imply its optimality, as we are about to prove.

Theorem 9 *Given k and $EV_{1,k}$, the critical points of the formula in Theorem 8 are reached for the bases $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ and $\{|+i\rangle, |-i\rangle\}$.*

Obviously, the basis $\{|0\rangle, |1\rangle\}$ corresponds to the minimum, and we need to confirm where the maximum is.

Corollary 5 *Given k and $EV_{1,k}$, if measurements occur in the basis $M = \{|0\rangle, |1\rangle\}$, then*

$$\hat{M}_1\hat{M}^k\hat{M}_0 = \frac{1 - (\cos\frac{\pi}{k+2})^{k+2}}{2}.$$

Proof We substitute directly in the formula of Theorem 8 taking into account that, for $|0\rangle$, $\theta = 0$, obtaining

$$\hat{M}_1\hat{M}^k\hat{M}_0 = \frac{1 - (c^2 - s^2)^{k+2}}{2} = \frac{1 - (\cos 2\theta_k)^{k+2}}{2}.$$ □

As expected, $\frac{1-(\cos\frac{\pi}{k+2})^{k+2}}{2} \xrightarrow[k\to\infty]{} 0$, so one of the conditions for the asymptotical optimality is verified. For the second one, we have the following result.

Corollary 6 *Given k and $EV_{1,k}$, if measurements occur in the basis $A = \{|+i\rangle, |-i\rangle\}$, then $\hat{A}_1\hat{A}^k\hat{A}_0 = \frac{1}{2}$. If measurements occur in the basis $M = \{|+\rangle, |-\rangle\}$, then*

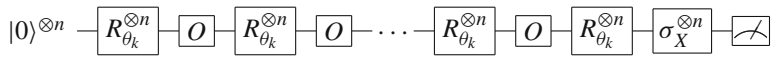
$$\hat{M}_1\hat{M}^k\hat{M}_0 = \frac{1}{2} + 2\cos^k\frac{\pi}{k+2}\cos^2\frac{\pi}{2(k+2)}\sin^2\frac{\pi}{2(k+2)} > \frac{1}{2}.$$

Proof We can substitute directly in the formula of Theorem 8 knowing that, for $|+i\rangle$, $\theta = \varphi = \frac{\pi}{2}$. The same applies for M, taking into account that for $|+\rangle$, $\theta = \frac{\pi}{2}$ and $\varphi = 0$. □

As we can see, the maximum is reached for $M = \{|+\rangle, |-\rangle\}$, for which $\hat{M}_1\hat{M}^k\hat{M}_0 > \frac{1}{2}$. However, the fact that $\hat{M}_1\hat{M}^k\hat{M}_0 \xrightarrow[k\to\infty]{} \frac{1}{2} = \frac{1}{N}$ allows us to conclude:

Theorem 10 *The family $EV_{1,k}$ of QMDA$_1$ is asymptotically optimal.*

This confirms that there exists a family of QMDA_1 with the desirable properties. For $n > 1$, the $\text{EV}_{n,k}$ circuit looks like:



Because $\text{EV}_{n,k} = \text{EV}_{1,k} \otimes \ldots \otimes \text{EV}_{1,k}$, Theorem 7 guarantees a good behaviour for any basis built from a tensor product of 1-qubit bases. The next step is to study entangled bases, as P-combination bases can be.

The eigenvectors of R_{θ_k} are $|+i\rangle, |-i\rangle$, with eigenvalues $e^{i\theta}, e^{-i\theta}$, respectively, so we can consider the basis A of eigenvectors of $R_{\theta_k}^{\otimes 2}$ as

$$|a_1\rangle = |+i\rangle|+i\rangle, \quad |a_2\rangle = |+i\rangle|-i\rangle, \quad |a_3\rangle = |-i\rangle|+i\rangle, \quad |a_4\rangle = |-i\rangle|-i\rangle.$$

Their eigenvalues would be, respectively, $e^{i2\theta}, e^{-i2\theta}, 1, 1$. Keeping this in mind, the following result is verified.

Theorem 11 *Given k and $EV_{2,k}$, we consider M a 2-combination basis of A. Then,*

$$\hat{M}_1 \hat{M}^k \hat{M}_0 = \frac{1}{4} + \frac{\cos^{k+2} \frac{2\pi}{k+2} + 1}{8}.$$

Proof Combining Theorem 6 with the fact that $|\langle a_i | R_\theta^{\otimes 2} | 00\rangle|^2 = \frac{1}{4}, \forall i = 1, 2, 3, 4$, we can substitute on formula (1) knowing that $n = 2$, $\theta_k = \frac{\pi}{2(k+2)}$, $\varphi_{12} = \beta_{12} = 4\theta$ and $\varphi_{34} = \beta_{34} = 0$. We should notice that $\beta_{12} + k\varphi_{12} = (k+1)4\theta = \frac{(k+1)2\pi}{k+2} = -\frac{2\pi}{k+2} = -4\theta_k$, and $\cos -4\theta_k = \cos 4\theta_k$. □

The important observation is that $\frac{1}{4} + \frac{\cos^{k+2} 4\theta_k + 1}{8} \xrightarrow[k\to\infty]{} \frac{1}{2}$. Moreover, $\frac{1}{4} + \frac{\cos^{k+2} 4\theta_k + 1}{8} < \frac{1}{2}$, which means that the probability of error increases as $k \longrightarrow \infty$! This leads us inevitably to the conclusion:

Theorem 12 *The family $EV_{n,k}$ of $QMDA_n$ is asymptotically optimal if and only if $n = 1$.*

The reason why the previous theorem prevents the optimality also for $n > 2$ is due to Theorem 7, which can be used to generate bases from the tensor product of this 2-combination basis and yield a probability of error higher than $\frac{1}{N}$.

A way of overcoming this issue with 2-combination bases is by adjusting the angles involved. For example, if $\{\varphi_i\}_{i=1}^4 = \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ and $\{\widetilde{\beta}_i\}_{i=1}^4 = \{\frac{\pi}{2}, 0, \pi, \frac{3\pi}{2}\}$, where $\widetilde{\beta}_i$ is the argument of $\beta_i = \langle a_i | U_0 | 00\rangle$. This means that $U := \sum_{j=1}^4 e^{i\varphi_j} |a_j\rangle\langle a_j|$. And, for example, we can define $U_0 := \sum_{j=1}^4 \beta_j |a_j\rangle\langle 00| + \sum_{j=1}^4 \beta_j |a_j\rangle\langle 11|$. The angles are chosen so that, no matters how the eigenvectors are paired in the 2-combination basis, the product of cosines is always equal to 0. Unfortunately, this alternative does not generalize for greater values of n.

However, the Elitzur–Vaidman circuit of any number of qubits can be adapted to any basis in which we desire to achieve maximum accuracy by adjusting the initial

state and the rotation axis of U. This is already suggesting a possibility for the future: mixing or nesting two different QMDA$_n$ so that one can fix the weaknesses of the other by providing high detecting probabilities over those bases where the other struggles.

5 Possible extensions of QMDA$_n$ and counterfactual communication

As mentioned throughout the article, there are some possible extensions of the QMDA$_n$ definition that can be considered in order to generalize their behaviour further, which we want to address in the future. Some extensions include the study when each O only measures on certain qubits (and not on all of them), or the study of properties of the QMDA$_n$ circuits having intentional, intermediate measurements. These extensions of our framework, along with some others, would lead to other well-known algorithms, such as the counterfactual communication [5] one.

The counterfactual communication algorithm works with three-qubit modelling photons, and the objective is to establish a communication between two parties, Alice and Bob, in such a way that Bob can communicate a decision (blocking Alice's photon or not) to Alice without any photon crossing the transmission channel. This means that Bob and Alice have communicated without actually sharing any information. The circuit is shown in Fig. 4.

A $|1\rangle$ in one of the arms means that Alice's photon is currently in that arm. The two upper arms belong to Alice's side and the lower one to Bob's side. This means that, whenever we have the state $|001\rangle$, the photon would have crossed the transmission channel. Here, BS_P stands for beam splitter with reflectivity $\cos^2\theta_P$, being $\theta_P = \frac{\pi}{2P}$. In other words, with respect to the computational basis,

$$BS_P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\theta_P & -\sin\theta_P & 0 \\ 0 & \sin\theta_P & \cos\theta_P & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

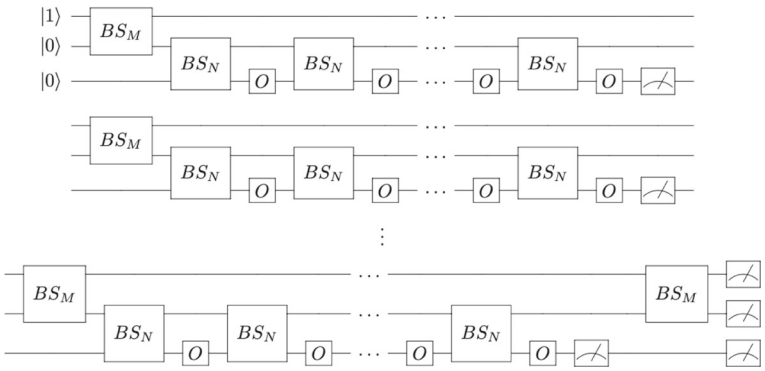


Fig. 4 Counterfactual communication algorithm

The BS_M gate will be applied M times to the two upper arms, and after each one (except the last one) a whole cycle of N applications of BS_N gates to the two lower arms. The natural numbers M and N can be chosen unrestrictedly. The algorithm ensures that Alice, based on the measured state at the end, will be able to infer Bob's choice with a probability as close to 1 as desired and without $|1\rangle$ being ever measured in the third qubit. (No photon has crossed the transmission channel.)

The similarities with QMDA$_n$ are clear, since the algorithm, from Alice's perspective, intends to detect whether measurements have been taken in every O (Bob has decided to block her photon) or not (Bob has decided to let her photon pass). However, the intermediate measurements, the nested loops of BS_M and BS_N and the measurements on a specific qubit instead of on all of them, prevents this algorithm from being a QMDA$_n$ yet, but makes its study interesting enough to deserve another work.

6 Conclusions and future work

In this paper, we have introduced a general framework to detect foreign measurements in circuits with respect to an unknown basis. The definition of quantum measurement detection algorithms generalizes the Elitzur–Vaidman bomb tester circuit.

Our results show the key properties and scope of QMDA. We have obtained the measurement detection probability error in terms of three matrices. In particular, for high number of qubits, we have derived explicit expressions of such a probability. Optimality of QMDA has been addressed, showing that bases that do not contain eigenvectors of the above-mentioned matrices yield better results. Finally, we study the performance of the Elitzur–Vaidman bomb tester and conclude its asymptotic optimality for the single-qubit circuit.

Future work includes the study when each O only measures on certain qubits (and not on all of them). Also, the study of properties of the QMDA circuits having internal measurements. Other extensions of our framework may include the counterfactual communication algorithm. Finally, we intend to provide a deeper insight into the effect of different types of noisy measurements on the detection power of QMDA.

Acknowledgements This work was supported in part by the MINECO under Grant MTM-2017-83506-C2-352 2-P, in part by the MICINN under Grant PID2020-119082RB-C22 and in part by Principado de Asturias under Grant FC-GRUPIN-IDI/2021/000047.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Data Availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Appendix A: Proofs of the results in Sect. 3

Before getting into the results, let us fix our notation. We will work with mixed states of the form $\sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i|$, where $\sum_{i=1}^{N} p_i = 1$. Here, the nonnegative real number p_i represents the probability of the circuit being in the pure state $|\psi_i\rangle$. If the current pure state is $|\psi\rangle\langle\psi|$, and we apply a measurement in the orthonormal basis $\{|m_i\rangle\}_{i=1}^{N}$, the state evolves to

$$\begin{aligned}\sum_{i=1}^{n} |m_i\rangle\langle m_i||\psi\rangle\langle\psi||m_i\rangle\langle m_i| &= \sum_{i=1}^{n} |m_i\rangle\langle m_i|\psi\rangle\langle\psi|m_i\rangle\langle m_i| \\ &= \sum_{i=1}^{n} |\langle\psi|m_i\rangle|^2 |m_i\rangle\langle m_i|.\end{aligned}$$

Since $|\langle\psi|m_i\rangle|^2$ is the probability of measuring $|m_i\rangle$ from the state $|\psi\rangle$, observe that the coefficients add up to 1 and no normalization is needed. For the sake of brevity, we will write sums as an inner product of vectors.

$$\begin{aligned}\sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i| &= \vec{\psi} \cdot \vec{p}^{\,t}, \text{ where } \vec{\psi} = (|\psi_0\rangle\langle\psi_0|, \ldots, |\psi_N\rangle\langle\psi_N|) \text{ and } \vec{p} \\ &= (p_1, \ldots, p_N).\end{aligned}$$

Theorem 13 *Given a QMDA$_n$ $(U_0, U, U_1, k, |\psi_0\rangle)$, and assuming that every O represents a measurement in an orthonormal basis $M = \{|m_i\rangle\}_{i=1}^{N}$, the probability of measuring the state $|\psi_0\rangle$ at the end of the algorithm is given by $\hat{M}_1 \hat{M}^k \hat{M}_0$.*

Proof We begin proving that the mixed state after the pth measurement, being $p \leq k+1$, is

$$\vec{m} \cdot \hat{M}^{p-1} \hat{M}_0,$$

where $\vec{m} = (|m_1\rangle\langle m_1|, \ldots, |m_N\rangle\langle m_N|)$.

We will prove this by induction over p. Let us denote some useful states: $|\varphi_0\rangle := U_0|\psi_0\rangle$ and $|\varphi_i\rangle := U|m_i\rangle$. For $p = 1$, we have to follow the circuit until the first O measurement. It starts in the state $|\psi_0\rangle\langle\psi_0|$ and evolves to $|\varphi_0\rangle\langle\varphi_0|$ after applying U_0. Here, the first measurement is taken, which leaves us with the mixed state

$$\sum_{i=1}^{N} |\langle m_i|\varphi_0\rangle|^2 |m_i\rangle\langle m_i| = \vec{m} \cdot \hat{M}_0 = \vec{m} \cdot \hat{M}^{p-1} \hat{M}_0$$

The next step is to prove that, if the result is correct for p, then it will be for $p+1$. So, our induction hypothesis is that, after the pth measurement, the state of the circuit is

$$\vec{m} \cdot \hat{M}^{p-1} \hat{M}_0.$$

Then we apply a U gate that evolves the state to

$$\vec{\varphi} \cdot \hat{M}^{p-1}\hat{M}_0 = \sum_{i=1}^{N} \left(\hat{M}^{p-1}\hat{M}_0\right)_i |\varphi_i\rangle\langle\varphi_i|,$$

where $\left(\hat{M}^{p-1}\hat{M}_0\right)_i$ represents the ith element of the column vector $\hat{M}^{p-1}\hat{M}_0$. Moreover, $\hat{M}_{i\cdot}$ will stand for the ith row of $\hat{M}$. The next measurement occurs, so the new state is

$$\begin{aligned}\sum_{j=1}^{N}\left(\sum_{i=1}^{N}|\langle m_j|\varphi_i\rangle|^2\left(\hat{M}^{p-1}\hat{M}_0\right)_i\right)|m_j\rangle\langle m_j| &= \sum_{j=1}^{N}\hat{M}_{j\cdot}\hat{M}^{p-1}\hat{M}_0|m_j\rangle\langle m_j| \\ &= \vec{m}\cdot\hat{M}^{p}\hat{M}_0.\end{aligned}$$

With this result, we know that the final state of the circuit will be

$$\sum_{i=1}^{N}\hat{M}_{i\cdot}\hat{M}^{k-1}\hat{M}_0|\phi_i\rangle\langle\phi_i| = \vec{\phi}\cdot\hat{M}^{k}\hat{M}_0,$$

for $|\phi_i\rangle := U_1|m_i\rangle$. This is due to the fact that, according to what has been proved, the state after the $(k+1)$th measurement (the last application of an O), will be $\vec{m}\cdot\hat{M}^k\hat{M}_0$. The next step is to apply U_1, obtaining the final state $\vec{\phi}\cdot\hat{M}^k\hat{M}_0$.

We are now ready to calculate the probability of error of the algorithm when every O represents a measurement, which is given by the probability of measuring $|\psi_0\rangle$ after the final measurement. The final state of the circuit is $\vec{\phi}\cdot\hat{M}^k\hat{M}_0$; therefore, the probability of measuring $|\psi_0\rangle$ in this situation is

$$\langle\psi_0|\left(\sum_{i=1}^{N}\left(\hat{M}^k\hat{M}_0\right)_i|\phi_i\rangle\langle\phi_i|\right)|\psi_0\rangle = \sum_{i=1}^{N}|\langle\psi_0|U_1|m_i\rangle|^2\left(\hat{M}^k\hat{M}_0\right)_i = \hat{M}_1\hat{M}^k\hat{M}_0.$$

□

When we add noise to our measurements, if the current pure state is $|\psi\rangle\langle\psi|$ and we apply a measurement in the orthonormal basis $\{|m_i\rangle\}_{i=1}^{N}$, the state evolves to

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{n}\langle m_i|E|m_j\rangle|\langle\psi|m_j\rangle|^2\right)|m_i\rangle\langle m_i| = \sum_{j=1}^{n}|\langle\psi|m_j\rangle|^2\sum_{i=1}^{n}\langle m_i|E|m_j\rangle|m_i\rangle\langle m_i|.$$

Basically, this means that the probability of measuring $|m_i\rangle$ is the sum of the probabilities of every situation in which we should have measured $|m_j\rangle$ ($|\langle\psi|m_j\rangle|^2$)

but noise made us measure $|m_i\rangle$ ($\langle m_i|E|m_j\rangle$). Again, since

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\langle m_i|E|m_j\rangle|\langle\psi|m_j\rangle|^2=\sum_{j=1}^{n}|\langle\psi|m_j\rangle|^2\sum_{i=1}^{n}\langle m_i|E|m_j\rangle=\sum_{j=1}^{n}|\langle\psi|m_j\rangle|^2=1,$$

no normalization is needed.

Theorem 14 *Given a QMDA$_n$ $(U_0, U, U_1, k, |\psi_0\rangle)$, and assuming that every O represents a noisy measurement in an orthonormal basis $M = \{|m_i\rangle\}_{i=1}^{N}$, being E the associated readout error stochastic matrix, the probability of measuring the state $|\psi_0\rangle$ at the end of the algorithm is given by $\hat{M}_1(\hat{E}\hat{M})^k\hat{E}\hat{M}_0$, where $\hat{E} := (\langle m_i|E|m_j\rangle)_{1\leq i,j\leq N}$.*

Proof The proof is analogous to the previous one. We begin proving that the mixed state after the pth measurement, being $p \leq k+1$, is

$$\vec{m}\cdot(\hat{E}\hat{M})^{p-1}\hat{E}\hat{M}_0.$$

We will prove this by induction over p. For $p = 1$, we follow the circuit until the first O measurement. After evolving from $|\psi_0\rangle\langle\psi_0|$ to $|\varphi_0\rangle\langle\varphi_0|$, the first measurement is taken:

$$\sum_{j=1}^{n}|\langle\varphi_0|m_j\rangle|^2\sum_{i=1}^{n}\langle m_i|E|m_j\rangle|m_i\rangle\langle m_i|=\vec{m}\cdot\hat{E}\hat{M}_0=\vec{m}\cdot(\hat{E}\hat{M})^{p-1}\hat{E}\hat{M}_0$$

Now we assume that the result is correct for p, and we will prove it for $p+1$. So, our induction hypothesis is that, after the pth measurement, the state of the circuit is

$$\vec{m}\cdot(\hat{E}\hat{M})^{p-1}\hat{E}\hat{M}_0.$$

Then we apply a U gate that evolves the state to

$$\vec{\varphi}\cdot(\hat{E}\hat{M})^{p-1}\hat{E}\hat{M}_0=\sum_{i=1}^{N}\left((\hat{E}\hat{M})^{p-1}\hat{E}\hat{M}_0\right)_i|\varphi_i\rangle\langle\varphi_i|.$$

The next measurement occurs, so the new state is

$$\begin{aligned}&\sum_{i=1}^{N}\left((\hat{E}\hat{M})^{p-1}\hat{E}\hat{M}_0\right)_i\sum_{j=1}^{N}|\langle m_j|\varphi_i\rangle|^2\sum_{k=1}^{N}\langle m_k|E|m_j\rangle|m_k\rangle\langle m_k|\\&=\sum_{k=1}^{N}\left(\sum_{j=1}^{N}\langle m_k|E|m_j\rangle\sum_{i=1}^{N}|\langle m_j|\varphi_i\rangle|^2\left((\hat{E}\hat{M})^{p-1}\hat{E}\hat{M}_0\right)_i\right)|m_k\rangle\langle m_k|\end{aligned}$$

$$= \sum_{k=1}^{N} \hat{E}_k . \hat{M} (\hat{E}\hat{M})^{p-1} \hat{E}\hat{M}_0 |m_k\rangle\langle m_k| = \vec{m} \cdot (\hat{E}\hat{M})^p \hat{E}\hat{M}_0.$$

With this result, we know that the final state of the circuit, after the k applications of O and the gate U_1, will be $\vec{\phi} \cdot (\hat{E}\hat{M})^k \hat{E}\hat{M}_0$. The probability of error of the algorithm, then, is given by the probability of measuring $|\psi_0\rangle$ at the end:

$$\langle\psi_0| \left(\sum_{i=1}^{N} \left((\hat{E}\hat{M})^k \hat{E}\hat{M}_0 \right)_i |\phi_i\rangle\langle\phi_i| \right) |\psi_0\rangle = \sum_{i=1}^{N} |\langle\psi_0|U_1|m_i\rangle|^2 \left((\hat{E}\hat{M})^k \hat{E}\hat{M}_0 \right)_i$$
$$= \hat{M}_1 (\hat{E}\hat{M})^k \hat{E}\hat{M}_0.$$

□

Proposition 4 *Let $(U_0, U, U_1, k, |\psi_0\rangle)$ be a QMDA$_n$ and M an orthonormal basis of a Hilbert space of dimension N. Then*

$$\hat{M}_1 \hat{M}^k \hat{M}_0 \geq \frac{1}{N^{2(k+1)}} > 0.$$

Proof We expand $\hat{M}_1 \hat{M}^k \hat{M}_0$ as follows

$$\sum_{i_0=1}^{N} |\langle\psi_0|U_1|m_{i_0}\rangle|^2 \sum_{i_1=1}^{N} |\langle m_{i_0}|U|m_{i_1}\rangle|^2 \ldots \sum_{i_k=1}^{N} |\langle m_{i_{k-1}}|U|m_{i_k}\rangle|^2 |\langle m_{i_k}|U_0|\psi_0\rangle|^2$$
$$= \sum_{i_0=1}^{N} \sum_{i_1=1}^{N} \cdots \sum_{i_k=1}^{N} |\langle\psi_0|U_1|m_{i_0}\rangle|^2 |\langle m_{i_0}|U|m_{i_1}\rangle|^2 \ldots |\langle m_{i_{k-1}}|U|m_{i_k}\rangle|^2$$
$$|\langle m_{i_k}|U_0|\psi_0\rangle|^2. \tag{A.1}$$

Since we have a summation of positive terms, we only need to prove that one of them is $\geq \frac{1}{N^{2(k+1)}}$. Firstly, the components of $\hat{M}_1$ add up to 1, so there exists a $1 \leq j_0 \leq N$ such that $|\langle\psi_0|U_1|m_{j_0}\rangle|^2 \geq \frac{1}{N} \Rightarrow |\langle m_{j_0}|U_1^\dagger|\psi_0\rangle| \geq \frac{1}{\sqrt{N}}$. Here we can apply the basic property $U_1 U^k U_0|\psi_0\rangle = |\psi_0\rangle \Rightarrow U^k U_0|\psi_0\rangle = U_1^\dagger|\psi_0\rangle$, which implies:

$$\frac{1}{\sqrt{N}} \leq |\langle m_{j_0}|U^k U_0|\psi_0\rangle| = \left| \langle m_{j_0}|U^k \left(\sum_{i_k=1}^{N} |m_{i_k}\rangle\langle m_{i_k}| \right) U_0|\psi_0\rangle \right|$$
$$= \left| \sum_{i_k=1}^{N} \langle m_{i_k}|U_0|\psi_0\rangle \langle m_{j_0}|U^k|m_{i_k}\rangle \right|$$
$$\leq \sum_{i_k=1}^{N} |\langle m_{i_k}|U_0|\psi_0\rangle| |\langle m_{j_0}|U^k|m_{i_k}\rangle|.$$

Since the summation is $\geq \frac{1}{\sqrt{N}}$ and every term is nonnegative, then some of them must be $\geq \frac{1}{N\sqrt{N}}$, so there exists a $1 \leq j_k \leq N$ such that $|\langle m_{j_k}|U_0|\psi_0\rangle||\langle m_{j_0}|U^k|m_{j_k}\rangle| \geq \frac{1}{N\sqrt{N}}$. Applying the same argument again we get

$$\begin{aligned}\frac{1}{N\sqrt{N}} &\leq |\langle m_{j_k}|U_0|\psi_0\rangle||\langle m_{j_0}|U^k|m_{j_k}\rangle| \\ &\leq |\langle m_{i_k}|U_0|\psi_0\rangle| \sum_{i_{k-1}}^{N} |\langle m_{j_0}|U^{k-1}|m_{i_{k-1}}\rangle||\langle m_{i_{k-1}}|U|m_{j_k}\rangle|.\end{aligned}$$

From this inequality we deduce that there exists a $1 \leq j_{k-1} \leq N$ such that

$$|\langle m_{j_0}|U^{k-1}|m_{j_{k-1}}\rangle||\langle m_{j_{k-1}}|U|m_{j_k}\rangle||\langle m_{i_k}|U_0|\psi_0\rangle| \geq \frac{1}{N^2\sqrt{N}}.$$

Reiterating the procedure we will find $j_1, j_2, \ldots j_{k-2}$ such that

$$\begin{aligned}&|\langle m_{j_0}|U|m_{i_1}\rangle| \ldots |\langle m_{j_{k-1}}|U|m_{j_k}\rangle||\langle m_{j_k}|U_0|\psi_0\rangle| \geq \frac{1}{N^k\sqrt{N}} \\ &\Rightarrow |\langle\psi_0|U_1|m_{j_0}\rangle|^2|\langle m_{j_0}|U|m_{j_1}\rangle|^2 \ldots |\langle m_{j_{k-1}}|U|m_{j_k}\rangle|^2|\langle m_{j_k}|U_0|\psi_0\rangle|^2 \geq \frac{1}{N^{2(k+1)}}\end{aligned}$$

Since this last expression represents one of the terms of (A.1), we conclude that

$$\hat{M}_1\hat{M}^k\hat{M}_0 \geq \frac{1}{N^{2(k+1)}} > 0. \qquad \square$$

Theorem 15 *Let $(U_0, U, U_1, k, |\psi_0\rangle)$ be a QMDA$_n$ and let $A = \{|a_i\rangle\}_{i=1}^N$ be an orthonormal basis of eigenvectors of U. Then $\hat{A} = I_N$, $\hat{A}_1^t = \hat{A}_0$ and*

$$\hat{A}_1\hat{A}^k\hat{A}_0 = \hat{A}_1\hat{A}_1^t = \hat{A}_0^t\hat{A}_0 \geq \frac{1}{N}.$$

Moreover,

$$\hat{A}_1\hat{A}^k\hat{A}_0 = \frac{1}{N} \Leftrightarrow |\langle a_i|U_0|\psi_0\rangle|^2 = \frac{1}{N}, \quad \forall i = 1, \ldots, N.$$

Proof It is immediate to see that, because $|a_i\rangle$ is an eigenvector of U, then

$$\hat{A} = (|\langle a_i|U|a_j\rangle|^2)_{1\leq i,j\leq N} = (|\langle a_i|e^{i\phi_j}|a_j\rangle|^2)_{1\leq i,j\leq N} = (|\langle a_i|a_j\rangle|^2)_{1\leq i,j\leq N} = I_N.$$

Therefore, $\hat{A}_1\hat{A}^k\hat{A}_0 = \hat{A}_1\hat{A}_0$. In addition, let us show that under these conditions $\hat{A}_1^t = \hat{A}_0$. We can notice that the ith component of $\hat{A}_1$ is

$$|\langle a_i|U_1^\dagger|\psi_0\rangle|^2 = |\langle a_i|U^kU_0|\psi_0\rangle|^2 = |\langle a_i|U_0|\psi_0\rangle|^2,$$

which corresponds to the ith component of $\hat{A}_0$. Here, we used the fact that $U|a_i\rangle = \lambda_i|a_i\rangle \Rightarrow \langle a_i|U^\dagger = \overline{\lambda_i}\langle a_i| \Rightarrow (\overline{\lambda_i})^{-1}\langle a_i| = \langle a_i|U$.

To prove the inequality, we expand the product $\hat{A}_0^t\hat{A}_0$:

$$\sum_{i=1}^{N} |\langle a_i|U_0|\psi_0\rangle|^2|\langle a_i|U_0|\psi_0\rangle|^2 = \sum_{i=1}^{N}(|\langle a_i|U_0|\psi_0\rangle|^2)^2.$$

This is a summation of squared real numbers, (each $|\langle\psi_0|U_1|a_i\rangle|^2$). In other words, we have a real function $\sum_{i=1}^{N} x_i^2$ where $\sum_{i=1}^{N} x_i = 1$, and this function reaches its minimum $\frac{1}{N}$ when $x_i = \frac{1}{N}, \forall i = 1, \ldots, N$. Hence, $\hat{A}_1\hat{A}^k\hat{A}_0 = \sum_{i=1}^{N}(|\langle\psi_0|U_1|a_i\rangle|^2)^2 \geq \frac{1}{N}$, and $\hat{A}_1\hat{A}^k\hat{A}_0 = \frac{1}{N} \Leftrightarrow |\langle a_i|U_0|\psi_0\rangle|^2 = \frac{1}{N}, \ \forall i = 1, \ldots, N$. □

Proposition 5 *If M is a P-combination of the basis A, the following properties are a consequence of the properties 1 and 2a.*

$$2b. \quad \sum_{i=1}^{P} \sigma_i(j_1)\sigma_i(j_2) = 0, \ \ \forall j_1 \neq j_2$$

$$2c. \quad \sum_{j=1}^{P} \sigma_i(j) = 0, \ \ \forall i \neq 1$$

$$2d. \quad \sum_{i=1}^{P} \sigma_i(j) = 0, \ \ \forall j \neq 1$$

Proof Property 2c is a direct consequence of 1 and 2a, and property 2d is a direct consequence of 1 and 2b, so we only need to prove that 2b is a consequence of 2a. As M is an orthonormal basis (due to 2a), then, for any k (and assuming without loss of generality that $k \leq P$),

$$|a_k\rangle = \sum_{i=1}^{N}\langle m_i|a_k\rangle|m_i\rangle = \sum_{i=1}^{P}\frac{1}{\sqrt{P}}\sigma_i(k)|m_i\rangle = \sum_{i=1}^{P}\sum_{j=1}^{P}\frac{1}{P}\sigma_i(k)\sigma_i(j)|a_j\rangle$$
$$= \sum_{j=1}^{P}\frac{1}{P}\left(\sum_{i=1}^{P}\sigma_i(k)\sigma_i(j)\right)|a_j\rangle.$$

This immediately implies that $\sum_{i=1}^{P}\sigma_i(k)\sigma_i(j) = 0$ whenever $j \neq k$. This proves 2b for a fixed k, but as k could have been chosen as desired, the proof is general. □

Proposition 6 *If $S(k)$ is a Sylvester matrix and $\sigma_i(j) := S(k)_{ij}$, then, for all k and any given a basis A,*

$$|m_{Pd+i}\rangle = \frac{1}{\sqrt{P}}\sum_{j=1}^{P}\sigma_i(j)|a_{Pd+j}\rangle$$

is a P-combination of the basis A for $P = 2^k$.

Proof We will prove every property for the rows and columns of every $S(k)$ by induction. For $k = 1$, $S(1) = \begin{pmatrix} + & + \\ + & - \end{pmatrix}$ and the properties can be easily verified. Now let us assume that $S(k)$ verifies the properties. We shall prove that $S(k+1)$ does.

$$S(k+1) = \begin{pmatrix} + & + \\ + & - \end{pmatrix} \otimes S(k) = \begin{pmatrix} S(k) & S(k) \\ S(k) & -S(k) \end{pmatrix}.$$

Properties 1a and 1b are satisfied trivially. In properties 2a and 3a rows are multiplied, and we have three ways of doing it: multiplying two rows from the upper half of $S(k+1)$, two from the lower half or one from each half. A row from the upper half is of the form $S(k)_{i\cdot}||S(k)_{i\cdot}$, where '||' stands for the concatenation symbol; a row from the lower half would be $S(k)_{i\cdot}||(-S(k)_{i\cdot})$. For the first case, the product of rows i, j, using the symbol '*' to denote the term-by-term product, will result in

$$S(k)_{i\cdot} * S(k)_{j\cdot}||S(k)_{i\cdot} * S(k)_{j\cdot} = S(k)_{(i,j)_r\cdot}||S(k)_{(i,j)_r\cdot} = S(k+1)_{(i,j)_r\cdot},$$

which proves property 3a. Moreover,

$$\sum_{l=1}^{2^{k+1}} S(k+1)_{il} * S(k+1)_{jl} = \sum_{l=1}^{2^{k+1}} S(k+1)_{(i,j)_r l} = \sum_{l=1}^{2^k} S(k)_{(i,j)_r l} + \sum_{l=1}^{2^k} S(k)_{(i,j)_r l} = 0$$

proves property 2a. The other two cases are solved similarly, as well as the procedure for property 3b. □

Theorem 16 *Given a QMDA$_n$, A an orthonormal basis of eigenvectors of U and M a P-combination basis of A, then, if the eigenvalue associated with $|a_i\rangle$ is $\lambda_i = e^{i\varphi_i}$,*

$$\begin{aligned}\hat{M}_1\hat{M}^k\hat{M}_0 = &\sum_{d=0}^{N/P-1} \frac{1}{P}\left(\sum_{j=1}^{P}|\beta_{Pd+j}|^2\right)^2 + \sum_{i=2}^{P}\left(\frac{1}{P}\sum_{j=1}^{P}\cos\varphi_{Pd+j,Pd+(i,j)_c}\right)^k \\ &\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_{Pd+j}||\beta_{Pd+(i,j)_c}|\cos\beta_{Pd+j,Pd+(i,j)_c}\right) \\ &\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_{Pd+j}||\beta_{Pd+(i,j)_c}|\cos(\beta_{Pd+j,Pd+(i,j)_c} + k\varphi_{Pd+j,Pd+(i,j)_c})\right),\end{aligned}$$

where $\varphi_{ij} = \varphi_i - \varphi_j$, and β_{ij} is the angle between $\beta_i := \langle a_i|U_0|\psi_0\rangle$ and $\beta_j := \langle a_j|U_0|\psi_0\rangle$.

Proof We will begin calculating $\hat{M}_0$. We should remember that $\beta_j = \langle a_j|U_0|\psi_0\rangle \in \mathbb{C}$, $\hat{\beta}_i$ is the argument of β_i and $\beta_{ij} = \widehat{\beta_i, \beta_j} = \hat{\beta}_i - \hat{\beta}_j$. A generic element of this matrix would be

$$\left|\frac{1}{\sqrt{P}}\left(\sum_{j=1}^{P}\sigma_i(j)\langle a_{Pd+j}|\right)U_0|\psi_0\rangle\right|^2 = \frac{1}{P}\left|\sum_{j=1}^{P}\sigma_i(j)\langle a_{Pd+j}|U_0|\psi_0\rangle\right|^2 = \frac{1}{P}\left|\sum_{j=1}^{P}\sigma_i(j)\beta_{Pd+j}\right|^2.$$

For $\hat{M}_1$, we have

$$\left|\frac{1}{\sqrt{P}}\left(\sum_{j=1}^{P}\sigma_i(j)\langle a_{Pd+j}|\right)U_1^{\dagger}|\psi_0\rangle\right|^2 = \frac{1}{P}\left|\sum_{j=1}^{P}\sigma_i(j)\langle a_{Pd+j}|U^k U_0|\psi_0\rangle\right|^2 = \frac{1}{P}\left|\sum_{j=1}^{P}\sigma_i(j)\lambda_{Pd+j}^k\beta_{Pd+j}\right|^2.$$

We conclude then,

$$\hat{M}_0 = \frac{1}{P}\begin{pmatrix} \left|\sum_{j=1}^{P}\sigma_1(j)\beta_j\right|^2 \\ \vdots \\ \left|\sum_{j=1}^{P}\sigma_P(j)\beta_j\right|^2 \\ \vdots \\ \left|\sum_{j=1}^{P}\sigma_1(j)\beta_{N-P+j}\right|^2 \\ \vdots \\ \left|\sum_{j=1}^{P}\sigma_P(j)\beta_{N-P+j}\right|^2 \end{pmatrix}, \quad \hat{M}_1 = \frac{1}{P}\begin{pmatrix} \left|\sum_{j=1}^{P}\sigma_1(j)\lambda_j^k\beta_j\right|^2 \\ \vdots \\ \left|\sum_{j=1}^{P}\sigma_P(j)\lambda_j^k\beta_j\right|^2 \\ \vdots \\ \left|\sum_{j=1}^{P}\sigma_1(j)\lambda_{N-P+j}^k\beta_{N-P+j}\right|^2 \\ \vdots \\ \left|\sum_{j=1}^{P}\sigma_P(j)\lambda_{N-P+j}^k\beta_{N-P+j}\right|^2 \end{pmatrix}^t.$$

For $\hat{M}$, if we consider, for example, $d_1 = d_2 = 0$, we have

$$\left|\frac{1}{P}\left(\sum_{j=1}^{P}\sigma_{i_1}(j)\langle a_j|\right)U\left(\sum_{j=1}^{P}\sigma_{i_2}(j)|a_j\rangle\right)\right|^2 = \frac{1}{P^2}\left|\sum_{j=1}^{P}\sigma_{i_1}(j)\sigma_{i_2}(j)\langle a_j|U|a_j\rangle\right|^2 = \frac{1}{P^2}\left|\sum_{j=1}^{P}\sigma_{i_1}(j)\sigma_{i_2}(j)\lambda_j\right|^2.$$

On the other hand, it is easy to see that, when $d_1 \neq d_2$, the term will be 0. Combining these two properties together, we obtain that $\hat{M} =$

$$\frac{1}{P^2}\begin{pmatrix} \left|\sum_{j=1}^{P}\lambda_j\right|^2 & \dots & \left|\sum_{j=1}^{P}\sigma_P(j)\lambda_j\right|^2 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ \left|\sum_{j=1}^{P}\sigma_P(j)\lambda_j\right|^2 & \dots & \left|\sum_{j=1}^{P}\lambda_j\right|^2 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & \left|\sum_{j=1}^{P}\lambda_{N-P+j}\right|^2 & \dots & \left|\sum_{j=1}^{P}\sigma_P(j)\lambda_{N-P+j}\right|^2 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & \left|\sum_{j=1}^{P}\sigma_P(j)\lambda_{N-P+j}\right|^2 & \dots & \left|\sum_{j=1}^{P}\lambda_{N-P+j}\right|^2 \end{pmatrix}$$

The next step is calculating $\hat{M}^k$, for which we will need the properties of P-combination bases. We should notice that $\hat{M}$ includes several sub-matrices of size $P \times P$ that we can treat separately, so we will focus on the first one:

$$S_1 = \begin{pmatrix} \left|\sum_{j=1}^{P}\lambda_j\right|^2 & \dots & \left|\sum_{j=1}^{P}\sigma_P(j)\lambda_j\right|^2 \\ \vdots & \ddots & \vdots \\ \left|\sum_{j=1}^{P}\sigma_P(j)\lambda_j\right|^2 & \dots & \left|\sum_{j=1}^{P}\lambda_j\right|^2 \end{pmatrix}.$$

A generic element $i_1 i_2$ of this matrix would be $\left|\sum_{j=1}^{P}\sigma_{i_1}(j)\sigma_{i_2}(j)\lambda_j\right|^2 = \left|\sum_{j=1}^{P}\sigma_{(i_1,i_2)_r}(j)\lambda_j\right|^2$. Property 3a ensures us that each $\left|\sum_{j=1}^{P}\sigma_i(j)\lambda_j\right|^2$ will appear only once in every row and column of S_1. This motivates the definition:

$$A_i := \left|\sum_{j=1}^{P}\sigma_i(j)\lambda_j\right|^2,$$

$$A_{i_1 i_2} := \left|\sum_{j=1}^{P}\sigma_{i_1}(j)\sigma_{i_2}(j)\lambda_j\right|^2 = \left|\sum_{j=1}^{P}\sigma_{(i_1,i_2)_r}(j)\lambda_j\right|^2 = A_{(i_1,i_2)_r}.$$

Rewriting the matrix:

$$S_1 = (A_{i_1 i_2})_{1\leq i_1,i_2\leq P} = \begin{pmatrix} A_{11} & A_{12} & A_{13} & \dots & A_{1P} \\ A_{21} & A_{22} & A_{23} & \dots & A_{2P} \\ A_{31} & A_{32} & A_{33} & \dots & A_{3P} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{P1} & A_{P2} & A_{P3} & \dots & A_{PP} \end{pmatrix}$$

$$= \begin{pmatrix} A_1 & A_2 & A_3 & \dots & A_P \\ A_2 & A_1 & A_{(2,3)_r} & \dots & A_{(2,P)_r} \\ A_3 & A_{(3,2)_r} & A_1 & \dots & A_{(3,P)_r} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_P & A_{(P,2)_r} & A_{(P,3)_r} & \dots & A_1 \end{pmatrix}$$

Now we define the numbers

$$B^k_{i_1 i_2} := \frac{1}{P} \sum_{j_1=1}^{P} \sigma_{i_1}(j_1)\sigma_{i_2}(j_1) \left(\sum_{j_2=1}^{P} \sigma_{j_2}(j_1) A_{j_2} \right)^k .$$

We will prove that $S_1^k = (A_{i_1 i_2})^k_{1 \le i_1, i_2 \le P} = (B^k_{i_1 i_2})_{1 \le i_1, i_2 \le P}$ by induction. We first show that $B^1_{i_1 i_2} = A_{i_1 i_2}$:

$$\begin{aligned} B^1_{i_1 i_2} &= \frac{1}{P} \sum_{j_1=1}^{P} \sigma_{i_1}(j_1)\sigma_{i_2}(j_1) \left(\sum_{j_2=1}^{P} \sigma_{j_2}(j_1) A_{j_2} \right) \\ &= \frac{1}{P} \sum_{j_2=1}^{P} A_{j_2} \sum_{j_1=1}^{P} \sigma_{(i_1,i_2)_r}(j_1)\sigma_{j_2}(j_1). \end{aligned}$$

However, due to 3a and 2a, $\sum_{j_1=1}^{P} \sigma_{(i_1,i_2)_r}(j_1)\sigma_{j_2}(j_1) = 0$ for all j_2 except when $j_2 = (i_1, i_2)_r$, which means

$$\frac{1}{P} \sum_{j_2=1}^{P} A_{j_2} \sum_{j_1=1}^{P} \sigma_{(i_1,i_2)_r}(j_1)\sigma_{j_2}(j_1) = \frac{1}{P} A_{(i_1,i_2)_r} \sum_{j_1=1}^{P} 1 = A_{(i_1,i_2)_r} = A_{i_1 i_2}.$$

We suppose now that $S_1^k = (B^k_{i_1 i_2})_{1 \le i_1, i_2 \le P}$ and we have to prove that $(S_1^{k+1})_{i_1 i_2} = \sum_{l=1}^{P} B^k_{i_1 l} A_{l i_2} = B^{k+1}_{i_1 i_2}$:

$$\begin{aligned} \sum_{l=1}^{P} B^k_{i_1 l} A_{l i_2} &= \frac{1}{P} \sum_{l=1}^{P} \sum_{j_1=1}^{P} \sigma_{i_1}(j_1)\sigma_l(j_1) \left(\sum_{j_2=1}^{P} \sigma_{j_2}(j_1) A_{j_2} \right)^k A_{l i_2} \\ &= \frac{1}{P} \sum_{j_1=1}^{P} \sigma_{i_1}(j_1) \left(\sum_{j_2=1}^{P} \sigma_{j_2}(j_1) A_{j_2} \right)^k \sum_{l=1}^{P} \sigma_l(j_1) B^1_{l i_2}. \end{aligned} \tag{A.2}$$

Focusing on the last sum of this expression:

$$\sum_{l=1}^{P} \sigma_l(j_1) B^1_{l i_2} = \frac{1}{P} \sum_{l=1}^{P} \sigma_l(j_1) \sum_{j_3=1}^{P} \sigma_l(j_3)\sigma_{i_2}(j_3) \left(\sum_{j_4=1}^{P} \sigma_{j_4}(j_3) A_{j_4} \right)$$

$$= \frac{1}{P}\sum_{j_4=1}^{P} A_{j_4} \sum_{l=1}^{P} \sigma_l(j_1) \sum_{j_3=1}^{P} \sigma_l(j_3)\sigma_{(i_2,j_4)_r}(j_3)$$
$$= \frac{1}{P}\sum_{j_4=1}^{P} A_{j_4}\sigma_{(i_2,j_4)_r}(j_1) \sum_{j_3=1}^{P} 1 = \sigma_{i_2}(j_1) \sum_{j_4=1}^{P} \sigma_{j_4}(j_1)A_{j_4}.$$

Substituting in A.2, we obtain

$$\sum_{l=1}^{P} B^k_{i_1 l} A_{l i_2} = \frac{1}{P}\sum_{j_1=1}^{P} \sigma_{i_1}(j_1) \left(\sum_{j_2=1}^{P} \sigma_{j_2}(j_1)A_{j_2}\right)^k \sigma_{i_2}(j_1) \sum_{j_4=1}^{P} \sigma_{j_4}(j_1)A_{j_4}$$
$$= \frac{1}{P}\sum_{j_1=1}^{P} \sigma_{i_1}(j_1)\sigma_{i_2}(j_1) \left(\sum_{j_2=1}^{P} \sigma_{j_2}(j_1)A_{j_2}\right)^{k+1} = B^{k+1}_{i_1 i_2}.$$

Once this result is proved, it can be applied to every S_{d+1}:

$$\hat{M}^k = \frac{1}{P^{2k}} \begin{pmatrix} S_1^k & 0 & \dots & 0 & 0 \\ 0 & S_2^k & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & S^k_{N/P-1} & 0 \\ 0 & 0 & \dots & 0 & S^k_{N/P} \end{pmatrix}.$$

Now we can calculate S^k_{d+1}/P^{2k}, that is, $B^k_{i_1 i_2}/P^{2k}$ for each component. We will use the property of complex numbers: for $x, y \in \mathbb{C}$, $|x \pm y|^2 = |x|^2 + |y|^2 \pm 2 < x, y >= |x|^2 + |y|^2 \pm 2|x||y| \cos\widehat{x, y}$. Its generalization is

$$\left|\sum_{j=1}^{P} \sigma_i(j)x_j\right|^2 = \sum_{j_1=1}^{P}\sum_{j_2=1}^{P} \sigma_i(j_1)\sigma_i(j_2)|x_{j_1}||x_{j_2}| \cos\widehat{x_{j_1}, x_{j_2}}.$$

We focus again on S_1:

$$\frac{B^k_{i_1 i_2}}{P^{2k}} = \frac{1}{P}\sum_{j_1=1}^{P} \sigma_{i_1}(j_1)\sigma_{i_2}(j_1) \left(\frac{\sum_{j_2=1}^{P} \sigma_{j_2}(j_1)A_{j_2}}{P^2}\right)^k. \tag{A.3}$$

Now, we deduce

$$\frac{\sum_{j_2=1}^{P} \sigma_{j_2}(j_1)A_{j_2}}{P^2} = \frac{1}{P^2}\sum_{j_2=1}^{P} \sigma_{j_2}(j_1) \left|\sum_{j_3=1}^{P} \sigma_{j_2}(j_3)\lambda_{j_3}\right|^2$$

$$
\begin{aligned}
&= \frac{1}{P^2} \sum_{j_2=1}^{P} \sigma_{j_2}(j_1) \sum_{j_3=1}^{P} \sum_{j_4=1}^{P} \sigma_{j_2}(j_3)\sigma_{j_2}(j_4) \cos \varphi_{j_3 j_4} \\
&= \frac{1}{P^2} \sum_{j_3=1}^{P} \sum_{j_4=1}^{P} \cos \varphi_{j_3 j_4} \sum_{j_2=1}^{P} \sigma_{j_2}((j_1, j_3)_c)\sigma_{j_2}(j_4) \\
&= \frac{1}{P^2} \sum_{j_3=1}^{P} \cos \varphi_{j_3(j_1,j_3)_c} \sum_{j_2=1}^{P} 1 = \frac{1}{P} \sum_{j_3=1}^{P} \cos \varphi_{j_3(j_1,j_3)_c}.
\end{aligned}
$$

Coming back to A.3, we have

$$
\frac{B^k_{i_1 i_2}}{P^{2k}} = \frac{1}{P} \sum_{j_1=1}^{P} \sigma_{i_1}(j_1)\sigma_{i_2}(j_1) \left(\frac{1}{P} \sum_{j_2=1}^{P} \cos \varphi_{j_2(j_1,j_2)_c} \right)^k.
$$

For S_{d+1}, we have

$$
\frac{B^k_{Pd+i_1, Pd+i_2}}{P^{2k}} = \frac{1}{P} \sum_{j_1=1}^{P} \sigma_{i_1}(j_1)\sigma_{i_2}(j_1) \left(\frac{1}{P} \sum_{j_2=1}^{P} \cos \varphi_{Pd+j_2, Pd+(j_1,j_2)_c} \right)^k.
$$

We are ready to multiply $\hat{M}^k \hat{M}_0$. The first P components will correspond with $d = 0$, the next P with $d = 1$, etc. For $d = 0$, the ith component of the column vector would be

$$
\begin{aligned}
\sum_{l=1}^{P} \frac{B^k_{il}}{P^{2k}} \cdot (\hat{M}_0)_l &= \frac{1}{P^2} \sum_{l=1}^{P} \sum_{j_1=1}^{P} \sigma_i(j_1)\sigma_l(j_1) \left(\frac{1}{P} \sum_{j_2=1}^{P} \cos \varphi_{j_2(j_1,j_2)_c} \right)^k \left| \sum_{j=1}^{P} \sigma_l(j)\beta_j \right|^2 \\
&= \frac{1}{P^2} \sum_{j_1=1}^{P} \sigma_i(j_1) \left(\frac{1}{P} \sum_{j_2=1}^{P} \cos \varphi_{j_2(j_1,j_2)_c} \right)^k \\
&\quad \cdot \sum_{j_3=1}^{P} \sum_{j_4=1}^{P} |\beta_{j_3}||\beta_{j_4}| \cos \beta_{j_3 j_4} \sum_{l=1}^{P} \sigma_l((j_1, j_3)_c)\sigma_l(j_4) \\
&= \sum_{j_1=1}^{P} \sigma_i(j_1) \left(\frac{1}{P} \sum_{j_2=1}^{P} \cos \varphi_{j_2(j_1,j_2)_c} \right)^k \\
&\quad \cdot \frac{1}{P} \sum_{j_3=1}^{P} |\beta_{j_3}||\beta_{(j_1,j_3)_c}| \cos \beta_{j_3(j_1,j_3)_c}.
\end{aligned}
$$

Before continuing, we should notice that $\arg(e^{ik\varphi_i}\beta_i) = k\varphi_i + \arg(\beta_i)$, which means that $\widehat{(e^{ik\varphi_i}\beta_i, e^{ik\varphi_j}\beta_j)} = k\varphi_i + \arg(\beta_i) - (k\varphi_j + \arg(\beta_j)) = k\varphi_{ij} + \beta_{ij}$. With

this, it is time to add $\hat{M}_1$. Finally,

$$\hat{M}_1\hat{M}^k\hat{M}_0 = \frac{1}{P}\sum_{i=1}^{P}\sum_{j_1=1}^{P}\sigma_i(j_1)\left(\frac{1}{P}\sum_{j_2=1}^{P}\cos\varphi_{j_2(j_1,j_2)_c}\right)^k \left(\frac{1}{P}\sum_{j_3=1}^{P}|\beta_{j_3}||\beta_{(j_1,j_3)_c}|\cos\beta_{j_3(j_1,j_3)_c}\right)\left|\sum_{j_4=1}^{P}\sigma_i(j)\lambda_{j_4}^k\beta_{j_4}\right|^2.$$

Applying the same procedure as before, we deduce

$$\frac{1}{P}\sum_{i=1}^{P}\sigma_i(j_1)\left|\sum_{j_4=1}^{P}\sigma_i(j)\lambda_{j_4}\beta_{j_4}\right|^2 = \sum_{j_4=1}^{P}|\beta_{j_4}||\beta_{(j_1,j_4)_c}|\cos(\beta_{j_4(j_1,j_4)_c}+k\varphi_{j_4(j_1,j_4)_c}).$$

Substituting in the previous expression, we obtain

$$\hat{M}_1\hat{M}^k\hat{M}_0 = P\sum_{i=1}^{P}\left(\frac{1}{P}\sum_{j=1}^{P}\cos\varphi_{j(i,j)_c}\right)^k\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_j||\beta_{(i,j)_c}|\cos\beta_{j(i,j)_c}\right)\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_j||\beta_{(i,j)_c}|\cos(\beta_{j(i,j)_c}+k\varphi_{j(i,j)_c})\right)$$

Moreover, when $i=1$, then $(1,\,j)_c = j$, so that $\cos\varphi_{j(i,j)_c} = \cos\varphi_{jj} = \cos 0 = 1$. Separating this case, we have

$$\begin{aligned}\hat{M}_1\hat{M}^k\hat{M}_0 &= P\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_j|^2\right)^2 + P\sum_{i=2}^{P}\left(\frac{1}{P}\sum_{j=1}^{P}\cos\varphi_{j(i,j)_c}\right)^k\\ &\quad\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_j||\beta_{(i,j)_c}|\cos\beta_{j(i,j)_c}\right)\\ &\quad\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_j||\beta_{(i,j)_c}|\cos(\beta_{j(i,j)_c}+k\varphi_{j(i,j)_c})\right)\\ &= \frac{1}{P}\left(\sum_{j=1}^{P}|\beta_j|^2\right)^2 + P\sum_{i=2}^{P}\left(\frac{1}{P}\sum_{j=1}^{P}\cos\varphi_{j(i,j)_c}\right)^k\\ &\quad\cdot\left(\frac{1}{P}\sum_{j=1}^{P}|\beta_j||\beta_{(i,j)_c}|\cos\beta_{j(i,j)_c}\right)\end{aligned}$$

$$\cdot \left(\frac{1}{P} \sum_{j=1}^{P} |\beta_j||\beta_{(i,j)_c}| \cos(\beta_{j(i,j)_c} + k\varphi_{j(i,j)_c}) \right)$$

This completes the case $d = 0$. The overall formula of the algorithm is

$$\begin{aligned}
\hat{M}_1 \hat{M}^k \hat{M}_0 = & \sum_{d=0}^{N/P-1} \frac{1}{P} \left(\sum_{j=1}^{P} |\beta_{Pd+j}|^2 \right)^2 \\
& + P \sum_{i=2}^{P} \left(\frac{1}{P} \sum_{j=1}^{P} \cos \varphi_{Pd+j,Pd+(i,j)_c} \right)^k \\
& \cdot \left(\frac{1}{P} \sum_{j=1}^{P} |\beta_{Pd+j}||\beta_{Pd+(i,j)_c}| \cos \beta_{Pd+j,Pd+(i,j)_c} \right) \\
& \cdot \left(\frac{1}{P} \sum_{j=1}^{P} |\beta_{Pd+j}||\beta_{Pd+(i,j)_c}| \cos(\beta_{Pd+j,Pd+(i,j)_c} + k\varphi_{Pd+j,Pd+(i,j)_c}) \right)
\end{aligned}$$

□

Theorem 17 *Given a QMDA$_n$, A an orthonormal basis of eigenvectors of U, and M a 2-combination basis, then*

$$\begin{aligned}
\hat{M}_1 \hat{M}^k \hat{M}_0 = \frac{1}{2} \Bigg[& \sum_{i=1}^{N/2} \left(|\beta_{2i-1}|^2 + |\beta_{2i}|^2 \right)^2 + \\
& + 4 \sum_{i=1}^{N/2} |\beta_{2i-1}|^2 |\beta_{2i}|^2 \cos^k \varphi_{2i-1,2i} \cos \beta_{2i-1,2i} \cos(\beta_{2i-1,2i} + k\varphi_{2i-1,2i}) \Bigg].
\end{aligned}$$

Moreover, defining $C_i := \cos^k \varphi_{2i-1,2i} \cos \beta_{2i-1,2i} \cos(\beta_{2i-1,2i} + k\varphi_{2i-1,2i})$*, the following bound is verified:*

$$\hat{M}_1 \hat{M}^k \hat{M}_0 \geq \frac{1}{2 \sum_{i=1}^{N/2} \frac{1}{C_i + 1}}.$$

The equality is satisfied if and only if

$$\begin{aligned}
\forall j = 1, \ldots, N/2, \ |\beta_{2j-1}|^2 + |\beta_{2j}|^2 = & \frac{1}{\sum_{i=1}^{N/2} \frac{C_j + 1}{C_i + 1}}, \ \textit{and, if } C_j \neq 0 \\
& \Rightarrow \ |\beta_{2j-1}|^2 = |\beta_{2j}|^2.
\end{aligned}$$

Proof $\hat{M}_1\hat{M}^k\hat{M}_0$ for $P = 2$ is obtained directly from formula of Theorem 4: $\hat{M}_1\hat{M}^k\hat{M}_0 =$

$$\sum_{d=0}^{N/2-1}\frac{1}{2}\left(\sum_{j=1}^{2}|\beta_{2d+j}|^2\right)^2+2\sum_{i=2}^{2}\left(\frac{1}{2}\sum_{j=1}^{2}\cos\varphi_{2d+j,2d+(i,j)_c}\right)^k$$
$$\cdot\left(\frac{1}{2}\sum_{j=1}^{2}|\beta_{2d+j}||\beta_{2d+(i,j)_c}|\cos\beta_{2d+j,2d+(i,j)_c}\right)$$
$$\cdot\left(\frac{1}{2}\sum_{j=1}^{2}|\beta_{2d+j}||\beta_{2d+(i,j)_c}|\cos(\beta_{2d+j,2d+(i,j)_c}+k\varphi_{2d+j,2d+(i,j)_c})\right)$$
$$=\frac{1}{2}\left(\sum_{d=1}^{N/2}\left(|\beta_{2d-1}|^2+|\beta_{2d}|^2\right)^2+4\sum_{d=1}^{N/2}|\beta_{2d-1}|^2|\beta_{2d}|^2\cos^k\varphi_{2d-1,2d}\cos\beta_{2d-1,2d}\cos(\beta_{2d-1,2d}+k\varphi_{2d-1,2d})\right)$$

It is important to notice that the cosines are independent from each $|\beta_i|^2$, because they only depend on the argument of β_i, and not on the module. Both values can be chosen as desired and independently when building the algorithm. This allows us to rewrite the expression as $\sum_{i=1}^{N/2}\left(|\beta_{2i-1}|^2+|\beta_{2i}|^2\right)^2+4\sum_{i=1}^{N/2}C_i|\beta_{2i-1}|^2|\beta_{2i}|^2$, where each $C_i=\cos^k\varphi_{2i-1,2i}\cos\beta_{2i-1,2i}\cos(\beta_{2i-1,2i}+k\varphi_{2i-1,2i})$ can be considered a constant. The reason why this is not possible for $P>2$ is that, in those cases, the angles of the cosines are combined (for example, pairing 1-2, 3-4 some times and 1-3, 2-4 other times), which prevents writing them as constants independent from each other.

Writing $x_j=|\beta_j|^2$, we must minimize the function with the restriction $\sum_{j=1}^{N}x_j=1$. If $M:=N/2$, we obtain

$$f(x_1,\ldots,x_{N-1})=\sum_{i=1}^{M-1}(x_{2i-1}+x_{2i})^2+\left(1-\sum_{i=1}^{N-2}x_i\right)^2$$
$$+4\sum_{i=1}^{M-1}C_ix_{2i-1}x_{2i}+4C_Mx_{N-1}\left(1-\sum_{i=1}^{N-1}x_i\right).$$

Its derivative with respect to a variable x_{2j} is

$$\frac{\partial f}{\partial x_{2j}}=2(x_{2j-1}+x_{2j})-2\left(1-\sum_{i=1}^{N-2}x_i\right)+4C_jx_{2j-1}-4C_Mx_{N-1}=0$$
$$(2C_j+1)x_{2j-1}+x_{2j}+\sum_{i=1}^{N-2}x_i-2C_Mx_{N-1}=1$$

When deriving with respect to x_{2j-1},

$$x_{2j-1}+(2C_j+1)x_{2j}+\sum_{i=1}^{N-2}x_i-2C_Mx_{N-1}=1,$$

so we can subtract the equations and get

$$2C_j x_{2j-1} - 2C_j x_{2j} = 0 \Rightarrow x_{2j-1} = x_{2j}.$$

When we derive with respect to x_{N-1}, we arrive to an analogous result:

$$\frac{\partial f}{\partial x_{N-1}} = 4C_M \left(1 - \sum_{i=1}^{N-1} x_i\right) - 4C_M x_{N-1} = 0$$
$$x_{N-1} = \left(1 - \sum_{i=1}^{N-1} x_i\right) = x_N.$$

It might be the case that $C_j = 0$, so that the equation cannot be cancelled. In that case, then for j, k such that $C_j = C_k = 0$, we deduce from the previous equations that $x_{2j-1} + x_{2j} = x_{2k-1} + x_{2k} := p$. We will suppose, without loss of generality, that those $C_j = 0$ are exactly the last r, so that $C_i \neq 0$, $\forall i = 1, \ldots, M - r$, for which $x_{2i-1} = x_{2i}$. Let us rewrite f accordingly and take into account that p is also a variable to be computed.

$$\begin{aligned} f(x_1, \ldots, x_N) &= \sum_{i=1}^{M} (x_{2i-1} + x_{2i})^2 + 4 \sum_{i=1}^{M} C_i x_{2i-1} x_{2i} \\ &= rp^2 + 4 \sum_{i=1}^{M-r} x_{2i}^2 + 4 \sum_{i=1}^{M-r} C_i x_{2i}^2 \\ &= rp^2 + 4 \sum_{i=1}^{M-r} (C_i + 1) x_{2i}^2 = rp^2 + 4 \sum_{i=1}^{M-r-1} (C_i + 1) x_{2i}^2 \\ &\quad + 4(C_{M-r} + 1) \left(\frac{1}{2} - \frac{rp}{2} - \sum_{i=1}^{M-r-1} x_{2i}\right)^2. \end{aligned}$$

We derive with respect to any variable x_{2j}.

$$\frac{\partial f}{\partial x_{2j}} = 8(C_j + 1) x_{2j} - 8(C_{M-r} + 1) \left(\frac{1}{2} - \frac{rp}{2} - \sum_{i=1}^{M-r-1} x_{2i}\right) = 0$$
$$(C_j + 1) x_{2j} = (C_{M-r} + 1) \left(\frac{1}{2} - \frac{rp}{2} - \sum_{i=1}^{M-r-1} x_{2i}\right)$$
$$(C_j + 1) x_{2j} = (C_{M-r} + 1) x_{M-r}.$$

Now we derive with respect to p.

$$\frac{\partial f}{\partial p} = 2rp - 4r(C_{M-r}+1)\left(\frac{1}{2} - \frac{rp}{2} - \sum_{i=1}^{M-r-1} x_{2i}\right) = 0$$
$$p = 2(C_{M-r}+1)x_{M-r}.$$

This is equivalent to $(C_j+1)x_{2j} = (C_{M-r}+1)x_{M-r}$, due to the fact that, for each $k = M-r+1,\ldots,M$, $(C_k+1)(x_{2k-1}+x_{2k}) = 2(C_{M-r}+1)x_{M-r}$, which is the same as the previous one but without $x_{2k-1} = x_{2k}$ being necessary. Moreover, we have $(C_k+1)(x_{2k-1}+x_{2k}) = (C_j+1)(x_{2j-1}+x_{2j})$ for every pair (j,k). This allows us to deduce

$$\sum_{i=1}^{N} x_i = \sum_{i=1}^{M} x_{2i-1}+x_{2i} = \sum_{i=1}^{M} \frac{C_j+1}{C_i+1}(x_{2j-1}+x_{2j}) = 1 \;\Rightarrow\; x_{2j-1}+x_{2j} = \frac{1}{\sum_{i=1}^{M}\frac{C_j+1}{C_i+1}}.$$

For those j such that $C_j \neq 0$ we have, additionally, the promised $x_{2j} = x_{2j-1}$. The previous procedure is only possible if $C_i \neq -1$, $\forall i$, but this is satisfied in our particular case. If, for example, $\cos^k\varphi_{12}\cos\beta_{12}\cos(\beta_{12}+k\varphi_{12}) = -1$, there are only four possibilities: $(-1)\cdot 1\cdot 1$, $1\cdot(-1)\cdot 1$, $1\cdot 1\cdot(-1)$ or $(-1)\cdot(-1)\cdot(-1)$. It is easy to discard them one by one. Finally, the value of the function in the critical point is

$$\begin{aligned}
&\sum_{j=1}^{M}(x_{2j-1}+x_{2j})^2 + 4\sum_{j=1}^{M} C_j x_{2j-1}x_{2j} \\
&= \sum_{j=1}^{M}\frac{1}{\left(\sum_{i=1}^{M}\frac{C_j+1}{C_i+1}\right)^2} + \sum_{j=1}^{M-r} C_j\frac{1}{\left(\sum_{i=1}^{M}\frac{C_j+1}{C_i+1}\right)^2} \\
&= \sum_{j=1}^{M}\frac{1}{\left(\sum_{i=1}^{M}\frac{C_j+1}{C_i+1}\right)^2} + \sum_{j=1}^{M} C_j\frac{1}{\left(\sum_{i=1}^{M}\frac{C_j+1}{C_i+1}\right)^2} \\
&= \frac{1}{\left(\sum_{i=1}^{M}\frac{1}{C_i+1}\right)^2}\sum_{j=1}^{M}\frac{1}{(C_j+1)} = \frac{1}{\sum_{i=1}^{M}\frac{1}{C_i+1}}.
\end{aligned}$$

In the worst case ($C_i = 1, \forall i$), f would take the value $\frac{1}{2^{n-2}}$. On the other hand, if $x_1 = 1$ and the rest of the variables are 0, then $f = 1$. This confirms that the critical point is the minimum of the function. □

Theorem 18 *Let $(U_0, U, U_1, k, |\psi_0\rangle)$ be a QMDA$_n$, $(V_0, V_1, V, k, |\varphi_0\rangle)$ a QMDA$_m$ and X, Y two orthonormal bases of dimension 2^n and 2^m, respectively. Then, given the QMDA$_{n+m}$ $(U_1 \otimes V_1, U \otimes V, U_0 \otimes V_0, k, |\psi_0\rangle \otimes |\varphi_0\rangle)$, the basis $Z = \{|x_i\rangle \otimes |y_j\rangle, \forall i = 1, \ldots, 2^n, \forall j = 1, \ldots, 2^m\}$ verifies $\hat{Z}_0 = \hat{X}_0 \otimes \hat{Y}_0$, $\hat{Z}_1 = \hat{X}_1 \otimes \hat{Y}_1$ and $\hat{Z} = \hat{X} \otimes \hat{Y}$. As a consequence, $\hat{Z}_1 \hat{Z}^k \hat{Z}_0 = \hat{X}_1 \hat{X}^k \hat{X}_0 \cdot \hat{Y}_1 \hat{Y}^k \hat{Y}_0$.*

Proof First, we will sort the basis Z as follows:

$$Z = \{|x_1\rangle \otimes |y_1\rangle, \ldots, |x_1\rangle \otimes |y_m\rangle, \ldots, |x_n\rangle \otimes |y_1\rangle, \ldots, |x_n\rangle \otimes |y_m\rangle\}.$$

Proving this result for $\hat{Z}_0$ and $\hat{Z}_1$ is almost immediate, as they are column and row vectors. Hence, we will detail the proof for $\hat{Z}$. If we look at an ij component of $\hat{Z}$ where $i = (c_1 - 1)m + r_1$ and $j = (c_2 - 1)m + r_2$, being $1 \leq c_1, c_2 \leq n$ and $1 \leq r_1, r_2 \leq m$, then

$$\begin{aligned}\hat{Z}_{ij} &= |\langle z_i|(U \otimes V)|z_j\rangle|^2 = |(\langle x_{c_1}| \otimes \langle y_{r_1}|)(U \otimes V)(|x_{c_2}\rangle \otimes |y_{r_2}\rangle)|^2 \\ &= |(\langle x_{c_1}|U|x_{c_2}\rangle) \otimes (\langle y_{r_1}|V|y_{r_2}\rangle)|^2 \\ &= |\langle x_{c_1}|U|x_{c_2}\rangle|^2 |\langle y_{r_1}|V|y_{r_2}\rangle|^2 = \hat{X}_{c_1 c_2} \hat{Y}_{r_1 r_2}.\end{aligned}$$

This immediately implies that $\hat{Z} = \hat{X} \otimes \hat{Y}$. Having proved this, the last equality is straightforward.

$$\hat{Z}_1 \hat{Z}^k \hat{Z}_0 = (\hat{X}_1 \otimes \hat{Y}_1) \cdot (\hat{X} \otimes \hat{Y})^k \cdot (\hat{X}_0 \otimes \hat{Y}_0) = \hat{X}_1 \hat{X}^k \hat{X}_0 \cdot \hat{Y}_1 \hat{Y}^k \hat{Y}_0.$$

□

Appendix B: Proofs of the results in Sect. 4

Theorem 19 *Given k, we consider the QMDA$_1$ $EV_{1,k}$ and we define $c := \cos\theta_k$, $s := \sin\theta_k$. If every O is equivalent to a measurement in the basis M where $|m_1\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ and $|m_2\rangle = \sin\frac{\theta}{2}|0\rangle - e^{i\varphi}\cos\frac{\theta}{2}|1\rangle$, then*

$$\hat{M}_1 \hat{M}^k \hat{M}_0 = \frac{1}{2} + \frac{(c^2 - s^2 + 2s^2\sin^2\theta\sin^2\varphi)^k (4c^2 s^2 \sin^2\theta\cos^2\varphi - (c^2 - s^2)^2\cos^2\theta)}{2}.$$

Proof We begin with $\hat{M}_0$ taking into account that $U_0|\psi_0\rangle = (c \;\; s)^t$.

$$\begin{aligned}\langle m_1|U_0|\psi_0\rangle &= \left(\cos\tfrac{\theta}{2}\; e^{-i\varphi}\sin\tfrac{\theta}{2}\right)\begin{pmatrix}c\\ s\end{pmatrix} = c\cos\frac{\theta}{2} + e^{-i\varphi}s\sin\frac{\theta}{2} \\ &= c\cos\frac{\theta}{2} + s\sin\frac{\theta}{2}\cos\varphi - i\left(s\sin\frac{\theta}{2}\sin\varphi\right) \\ &\Rightarrow |\langle m_1|U_0|\psi_0\rangle|^2 = \left(c\cos\frac{\theta}{2} + s\sin\frac{\theta}{2}\cos\varphi\right)^2 + s^2\sin^2\frac{\theta}{2}\sin^2\varphi\end{aligned}$$

$$= c^2 \cos^2 \frac{\theta}{2} + 2cs \cos \frac{\theta}{2} \sin \frac{\theta}{2} \cos\varphi + s^2 \sin^2 \frac{\theta}{2}$$
$$= c^2 \cos^2 \frac{\theta}{2} + cs \sin\theta \cos\varphi + s^2 \sin^2 \frac{\theta}{2}.$$

As $\hat{M}_0$ only has two components that sum to one, we deduce:

$$\hat{M}_0 = \begin{pmatrix} c^2 \cos^2 \frac{\theta}{2} + cs \sin\theta \cos\varphi + s^2 \sin^2 \frac{\theta}{2} \\ c^2 \sin^2 \frac{\theta}{2} - cs \sin\theta \cos\varphi + s^2 \cos^2 \frac{\theta}{2} \end{pmatrix}.$$

Besides, $U_1^\dagger |\psi_0\rangle = (s \;\; c)^t$, so $\hat{M}_1$ is built in the same way as $\hat{M}_0$ but exchanging the c and s:

$$\hat{M}_1 = \begin{pmatrix} s^2 \cos^2 \frac{\theta}{2} + cs \sin\theta \cos\varphi + c^2 \sin^2 \frac{\theta}{2} \\ s^2 \sin^2 \frac{\theta}{2} - cs \sin\theta \cos\varphi + c^2 \cos^2 \frac{\theta}{2} \end{pmatrix}^t.$$

For $\hat{M}$, we calculate the first component $\hat{M}_{11}$.

$$\begin{aligned} \langle m_1|U|m_1\rangle &= \left(\cos\tfrac{\theta}{2} \;\; e^{-i\varphi} \sin\tfrac{\theta}{2}\right) \begin{pmatrix} c & -s \\ s & c \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi} \sin\frac{\theta}{2} \end{pmatrix} \\ &= \left(\cos\tfrac{\theta}{2} \;\; e^{-i\varphi} \sin\tfrac{\theta}{2}\right) \begin{pmatrix} c\cos\frac{\theta}{2} - se^{i\varphi} \sin\frac{\theta}{2} \\ s\cos\frac{\theta}{2} + ce^{i\varphi} \sin\frac{\theta}{2} \end{pmatrix} \\ &= c + (e^{-i\varphi} - e^{i\varphi}) s \cos\frac{\theta}{2} \sin\frac{\theta}{2} = c - i\left(2s \cos\frac{\theta}{2} \sin\frac{\theta}{2} \sin\varphi\right) \\ &= c - i(s \sin\theta \sin\varphi) \Rightarrow \\ &\quad \Rightarrow |\langle m_1|U|m_1\rangle|^2 = c^2 + s^2 \sin^2\theta \sin^2\varphi. \end{aligned}$$

We know that its rows and columns add up to 1, so we conclude that

$$\hat{M} = \begin{pmatrix} c^2 + s^2 \sin^2\theta \sin^2\varphi & s^2 - s^2 \sin^2\theta \sin^2\varphi \\ s^2 - s^2 \sin^2\theta \sin^2\varphi & c^2 + s^2 \sin^2\theta \sin^2\varphi \end{pmatrix}.$$

For calculating $\hat{M}^k$, we use a lemma that is easily proved by induction:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}^k = \frac{1}{2} \begin{pmatrix} (a+b)^k + (a-b)^k & (a+b)^k - (a-b)^k \\ (a+b)^k - (a-b)^k & (a+b)^k + (a-b)^k \end{pmatrix} \Rightarrow$$
$$\hat{M}^k = \frac{1}{2} \begin{pmatrix} 1 + (c^2 - s^2 + 2s^2 \sin^2\theta \sin^2\varphi)^k & 1 - (c^2 - s^2 + 2s^2 \sin^2\theta \sin^2\varphi)^k \\ 1 - (c^2 - s^2 + 2s^2 \sin^2\theta \sin^2\varphi)^k & 1 + (c^2 - s^2 + 2s^2 \sin^2\theta \sin^2\varphi)^k \end{pmatrix}$$
$$= \frac{1}{2} \begin{pmatrix} 1 + A^k & 1 - A^k \\ 1 - A^k & 1 + A^k \end{pmatrix}.$$

We are ready to calculate the final probability.

$$\hat{M}^k\hat{M}_0 = \frac{1}{2}\begin{pmatrix}1+A^k & 1-A^k\\ 1-A^k & 1+A^k\end{pmatrix}\begin{pmatrix}c^2\cos^2\frac{\theta}{2}+cs\sin\theta\cos\varphi+s^2\sin^2\frac{\theta}{2}\\ c^2\sin^2\frac{\theta}{2}-cs\sin\theta\cos\varphi+s^2\cos^2\frac{\theta}{2}\end{pmatrix} =$$

$$= \frac{1}{2}\begin{pmatrix}1+A^k[(c^2-s^2)(\cos^2\frac{\theta}{2}-\sin^2\frac{\theta}{2})+2cs\sin\theta\cos\varphi]\\ 1-A^k[(c^2-s^2)(\cos^2\frac{\theta}{2}-\sin^2\frac{\theta}{2})+2cs\sin\theta\cos\varphi]\end{pmatrix}.$$

$$\hat{M}_1\hat{M}^k\hat{M}_0 = \frac{1}{2}\begin{pmatrix}s^2\cos^2\frac{\theta}{2}+cs\sin\theta\cos\varphi+c^2\sin^2\frac{\theta}{2}\\ s^2\sin^2\frac{\theta}{2}-cs\sin\theta\cos\varphi+c^2\cos^2\frac{\theta}{2}\end{pmatrix}^t\begin{pmatrix}1+A^k[(c^2-s^2)\cos\theta+2cs\sin\theta\cos\varphi]\\ 1-A^k[(c^2-s^2)\cos\theta+2cs\sin\theta\cos\varphi]\end{pmatrix} =$$

$$= \frac{1}{2}+\frac{A^k[(c^2-s^2)\cos\theta+2cs\sin\theta\cos\varphi][-(c^2-s^2)\cos\theta+2cs\sin\theta\cos\varphi]}{2} =$$

$$= \frac{1}{2}+\frac{(c^2-s^2+2s^2\sin^2\theta\sin^2\varphi)^k(4c^2s^2\sin^2\theta\cos^2\varphi-(c^2-s^2)^2\cos^2\theta)}{2}.$$

□

Theorem 20 *Given k and $EV_{1,n}$, the critical points of the formula in Theorem 8 are reached for the bases $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ y $\{|+i\rangle, |-i\rangle\}$.*

Proof We have to derive the formula of Theorem 8 with respect to both variables. We should remember to take $0 \leq \varphi \leq 2\pi$ and $0 \leq \theta \leq \pi$.

$$\frac{\partial f}{\partial\varphi} = \frac{k(c^2-s^2+2s^2\sin^2\theta\sin^2\varphi)^{k-1}4s^2\sin^2\theta\sin\varphi\cos\varphi(4c^2s^2\sin^2\theta\cos^2\varphi-(c^2-s^2)^2\cos^2\theta)}{2}$$
$$-\frac{(c^2-s^2+2s^2\sin^2\theta\sin^2\varphi)^k 8c^2s^2\sin^2\theta\cos\varphi\sin\varphi}{2}$$
$$\frac{\partial f}{\partial\theta} = \frac{k(c^2-s^2+2s^2\sin^2\theta\sin^2\varphi)^{k-1}4s^2\sin^2\varphi\sin\theta\cos\theta(4c^2s^2\sin^2\theta\cos^2\varphi-(c^2-s^2)^2\cos^2\theta)}{2}$$
$$+\frac{(c^2-s^2+2s^2\sin^2\theta\sin^2\varphi)^k(8c^2s^2\cos^2\varphi\sin\theta\cos\theta+2(c^2-s^2)^2\cos\theta\sin\theta)}{2}$$

We notice that $s = \sin\frac{\pi}{2(k+2)}$, $c = \cos\frac{\pi}{2(k+2)}$, but $0 < \frac{\pi}{2(k+2)} < \frac{\pi}{4}$, which necessarily implies that $0 < s < \frac{1}{\sqrt{2}}$, $\frac{1}{\sqrt{2}} < c < 1$, and as a consequence, $c > s$. This also means that $c^2 - s^2 + 2s^2\sin^2\theta\sin^2\varphi > 0$, so:

$$\frac{\partial f}{\partial\varphi} = 0 \Leftrightarrow \sin^2\theta\sin\varphi\cos\varphi[k(4c^2s^2\sin^2\theta\cos^2\varphi-(c^2-s^2)^2\cos^2\theta)$$
$$-2c^2(c^2-s^2+2s^2\sin^2\theta\sin^2\varphi)] = 0; \tag{A.4}$$
$$\frac{\partial f}{\partial\theta} = 0 \Leftrightarrow \sin\theta\cos\theta[2ks^2\sin^2\varphi(4c^2s^2\sin^2\theta\cos^2\varphi-(c^2-s^2)^2\cos^2\theta)+$$
$$+(c^2-s^2+2s^2\sin^2\theta\sin^2\varphi)(4c^2s^2\cos^2\varphi+(c^2-s^2)^2)] = 0. \tag{A.5}$$

It is immediate that, if $\sin\theta = 0 \Rightarrow \theta = 0, \pi$, then both partial derivatives are 0 regardless of the value for φ. This critical point corresponds with $\{|0\rangle, |1\rangle\}$. Another

possibility for $\frac{\partial f}{\partial \theta} = 0$ is $\cos\theta = 0 \Rightarrow \theta = \frac{\pi}{2}$. Then

$$\frac{\partial f}{\partial \varphi} = \sin\varphi\cos\varphi[2ks^2\cos^2\varphi - (c^2 - s^2 + 2s^2\sin^2\varphi)] = 0.$$

If $\sin\varphi = 0 \Rightarrow \varphi = 0, \pi$ we have the critical point for the basis $\{|+\rangle, |-\rangle\}$; and if $\cos\varphi = 0 \Rightarrow \varphi = \frac{\pi}{2}, \frac{3\pi}{2}$ and the critical point would be $\{|+i\rangle, |-i\rangle\}$. If none of both is 0, then

$$\begin{aligned}
&2ks^2\cos^2\varphi - (c^2 - s^2 + 2s^2\sin^2\varphi) = 0\\
&2ks^2\cos^2\varphi - (1 - 2s^2 + 2s^2\sin^2\varphi) = 0\\
&2s^2(k\cos^2\varphi + 1 - \sin^2\varphi) = 1\\
&k\cos^2\varphi + \cos^2\varphi = \frac{1}{2s^2}\\
&\cos^2\varphi = \frac{1}{2s^2(k+1)}.
\end{aligned}$$

However, $2s^2(k+1) \leq 1, \forall k > 0$, which is a contradiction.
The last case for A.5 to be 0 occurs when

$$2ks^2\sin^2\varphi(4c^2s^2\sin^2\theta\cos^2\varphi - (c^2 - s^2)^2\cos^2\theta) + (c^2 - s^2 + 2s^2\sin^2\theta\sin^2\varphi)$$
$$(4c^2s^2\cos^2\varphi + (c^2 - s^2)^2) = 0.$$

If $\frac{\partial f}{\partial \varphi}$ in A.4 is also 0, there are three possibilities which lead us to contradictions. If $\sin\varphi = 0$, then

$$(c^2 - s^2)(4c^2s^2 + (c^2 - s^2)^2) = 0 \;\Rightarrow\; 4c^2s^2 = -(c^2 - s^2)^2 < 0 \quad \#$$

If $\cos\varphi = 0$, then

$$\begin{aligned}
&-2ks^2(c^2 - s^2)^2\cos^2\theta + (c^2 - s^2 + 2s^2\sin^2\theta)(c^2 - s^2)^2 = 0\\
&2s^2(-k\cos^2\theta - 1 + \sin^2\theta) = -1 \;\Rightarrow\; \cos^2\theta = \frac{1}{2s^2(k+1)} \quad \#
\end{aligned}$$

Finally, we can have

$$k(4c^2s^2\sin^2\theta\cos^2\varphi - (c^2 - s^2)^2\cos^2\theta) - 2c^2(c^2 - s^2 + 2s^2\sin^2\theta\sin^2\varphi) = 0;$$
$$2ks^2\sin^2\varphi(4c^2s^2\sin^2\theta\cos^2\varphi - (c^2 - s^2)^2\cos^2\theta) + (c^2 - s^2 + 2s^2\sin^2\theta\sin^2\varphi)$$
$$(4c^2s^2\cos^2\varphi + (c^2 - s^2)^2) = 0.$$

We isolate $4c^2s^2\sin^2\theta\cos^2\varphi - (c^2 - s^2)^2\cos^2\theta$ in the first equation and substitute it in the second, obtaining

$$4c^2s^2\sin^2\varphi(c^2 - s^2 + 2s^2\sin^2\theta\sin^2\varphi) + (c^2 - s^2 + 2s^2\sin^2\theta\sin^2\varphi)$$

$$(4c^2s^2\cos^2\varphi + (c^2 - s^2)^2) = 0$$
$$c^4 + 2c^2s^2 + s^4 = 0 \;\Rightarrow\; (c^2 + s^2)^2 = 0 \;\Rightarrow\; 1 = 0 \quad \#$$

□

References

1. Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of FOCS, pp. 124–134 (1994)
2. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC'96), ACM, NY, USA, pp. 212–219 (1996)
3. Elitzur, A.C., Vaidman, L.: Quantum mechanical interaction-free measurements. Found. Phys. **23**(7), 987–997 (1993)
4. Itano, W.M., Heinzen, D.J., Bollinger, J., Wineland, D.: Quantum Zeno effect. Phys. Rev. A **41**(5), 2295 (1990)
5. Salih, H., Li, Z.-H., Al-Amri, M., Zubairy, M.S.: Protocol for direct counterfactual quantum communication. Phys. Rev. Lett. **110**(17), 170502 (2013)
6. Hance, J.R., Rarity, J.: Counterfactual ghost imaging. npj Quantum Inf. **7**(1), 1–7 (2021)
7. Lin, C.Y.-Y., Lin, H.-H.: Upper bounds on quantum query complexity inspired by the Elitzur–Vaidman bomb tester, arXiv preprint arXiv:1410.0932
8. Noh, T.-G., et al.: Counterfactual quantum cryptography. Phys. Rev. Lett. **103**(23), 230–501 (2009)
9. Zilberberg, O., Romito, A., Gefen, Y.: Many-body manifestation of interaction-free measurement: the Elitzur–Vaidman bomb. Phys. Rev. B **93**(11), 115411 (2016)
10. Combarro, E.F., Ranilla, J., Rúa, I.F.: Quantum abstract detecting systems. Quantum Inf. Process. **19**(8), 258 (2020)
11. Cáceres, J.H., Combarro, E.F., Rúa, I.F.: Combinatorial and rotational quantum abstract detecting systems. Quantum Inf. Process. **21**(2), 1–27 (2022)
12. Bravyi, S., Sheldon, S., Kandala, A., Mckay, D.C., Gambetta, J.M.: Mitigating measurement errors in multiqubit experiments. Phys. Rev. A **103**(4), 042605 (2021)
13. Sylvester, J.J., LX.: Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. Lond. Edinb. Dublin Philos. Mag. J. Sci. **34**(232), 461–475 (1867)