




# Combinatorial and rotational quantum abstract detecting systems

J. M. Hernández Cáceres<sup>1</sup> · E. F. Combarro<sup>2</sup> · I. F. Rúa<sup>1</sup> 

Received: 2 February 2021 / Accepted: 10 November 2021  
© The Author(s) 2022

## Abstract

Quantum abstract detecting systems (QADS) were introduced as a common framework for the study and design of detecting algorithms in a quantum computing setting. In this paper, we introduce new families of such QADS, known as combinatorial and rotational, which, respectively, generalize detecting systems based on single qubit controlled gates and on Grover's algorithm. We study the algorithmic closure of each family and prove that some of these QADS are equivalent (in the sense of having the same detection rate) to others constructed from tensor product of controlled operators and their square roots. We also apply the combinatorial QADS construction to a problem of eigenvalue decision, and to a problem of phase estimation.

**Keywords** Quantum abstract detecting systems · Grover's algorithm · Quantum walks · Quantum abstract search · Combinatorial QADS · Rotational QADS

## 1 Introduction

Quantum abstract detecting systems were introduced in [4] as a common framework for the study and design of detection algorithms in a quantum computing setting. Namely, given a black-box oracle for a Boolean function  $f$ , the QADS construct an initial state and an operator that can be used to detect if the function is identically zero or not. For instance, if  $O$  denotes a quantum oracle evaluating  $f$ , then the QADS related to Grover's algorithm [7] constructs a uniform superposition *initial state*  $|\varphi_0\rangle$

---

✉ I. F. Rúa  
rua@uniovi.es

J. M. Hernández Cáceres  
UO279369@uniovi.es

E. F. Combarro  
efernandezca@uniovi.es

<sup>1</sup> Mathematics Department, University of Oviedo, Oviedo, Spain

<sup>2</sup> Computer Science Department, University of Oviedo, Oviedo, Spain

and a quantum operator  $U = GO$ , product of the quantum oracle and the diffusion operator  $G$ . Such an operator can be used to evolve the quantum system from the initial state, so that measurement of the resulting state  $U^t|\varphi_0\rangle$  gives always  $|\varphi_0\rangle$  when  $f$  is zero, whereas when  $f$  is not zero, it gives the initial state with small probability. These facts can be used to determine whether  $f$  is zero or not, i.e., to *detect* the existence of an element  $x$  such that  $f(x) = 1$ .

In general, a QADS is any (classical deterministic) algorithm that takes, from a set of inputs  $\mathcal{M}$ , a Boolean function (given by a circuit)  $f : \{0, 1\}^k \rightarrow \{0, 1\}$  and outputs a unitary transformation  $U = U_f$  on a Hilbert space  $\mathcal{H}$  whose dimension only depends on  $k$ , together with a state  $|\varphi_0\rangle \in \mathcal{H}$  (that only depends on  $k$  too) such that

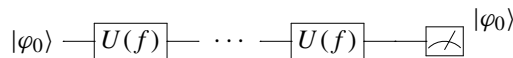
$$\{x \in \{0, 1\}^k \mid f(x) = 1\} = \emptyset \implies U|\varphi_0\rangle = |\varphi_0\rangle$$

The transformation  $U$  is called *detecting operator*, and  $|\varphi_0\rangle$  is known as the *initial state*.

QADS related to other well-known quantum computing search methodologies, such as quantum walks [12,14,16,18] or the quantum abstract search [3] and even other non-search techniques (like Deutsch–Jozsa algorithm [5]) have been considered [4]. In all these cases, the detection scheme is similar to the one for Grover’s QADS:

**Algorithm 1 (Detection scheme)**  
*INPUT:* A QADS  $Q$ , a boolean function  $f : \{0, 1\}^k \rightarrow \{0, 1\}$  from the set of inputs  $\mathcal{M}$  of the QADS, and a natural number  $T$ .  
*PROCEDURE:*  
 - *PRECOMPUTATION* of the initial state  $|\varphi_0\rangle$  and the detecting operator  $U$  with  $Q$  on input  $f$ .  
 - *COMPUTATION:*  
     - Choose  $t$  uniformly in the set  $\{0, 1, \dots, T\}$   
     - Compute  $|\varphi_t\rangle = U^t|\varphi_0\rangle$ .  
 - *MEASUREMENT* of  $|\varphi_t\rangle$  on an orthonormal basis containing  $|\varphi_0\rangle$ .  
*OUTPUT:*  
 - *NO:* If the measurement is the initial state  $|\varphi_0\rangle$ .  
 - *YES:* Otherwise.

The detection scheme is readily described by the following circuit:



There are two main advantages for the introduction of the QADS methodology. The first one is that it helps to systematically analyze the effectiveness of the detection procedures under study. Namely, the actual usefulness of a particular QADS can be analyzed in terms of a trade-off between the precomputation cost of the QADS (efficient constructibility), and the number of iterations required to achieve a bounded success probability in Algorithm 1. A QADS is called *efficiently constructible* if for any input circuit  $f \in \mathcal{M}$  of size  $n$ , the output pair initial state/unitary transformation can be computed in  $O(\text{poly}(n))$  time and, as a consequence, their circuits are of  $O(\text{poly}(n))$

width, depth and number of gates. On the other hand, if  $(|\varphi_0\rangle, U = U(f))$  is the output of a QADS on input  $f \in \mathcal{M}$ , then for a given  $0 < \delta \leq 1$ , a function  $T : \mathbb{N} \rightarrow \mathbb{N}$  is a  $\delta$ -quantum detecting time for the QADS, if for all nonzero  $f \in \mathcal{M}$  of input size  $k$

$$\frac{\sum_{t=0}^{T(k)} |\langle \varphi_0 | U^t | \varphi_0 \rangle|^2}{T(k) + 1} \leq 1 - \delta.$$

So, for instance, the QADS of Grover search provides efficient constructibility and a  $\frac{\sqrt{2}-1}{4\sqrt{2}}$ -detection time of order  $O(\sqrt{2^k})$ , which is optimal among the class of quantum algorithms that do not look into the oracle. In general, the following result can be proved:

**Theorem 1** [4, Main Theorem] *The detection scheme of Algorithm 1 always provides a correct output on input zero (i.e., when no marked elements do exist), and so the probability of error is fully attributed to nonzero inputs. Namely, such a probability is equal to*

$$\frac{\sum_{t=0}^T |\langle \varphi_0 | U^t | \varphi_0 \rangle|^2}{T + 1}$$

*Therefore, if a QADS is both efficiently constructible and has  $\delta$ -detecting time, then the detection scheme can be run in  $O(\text{poly}(n))$  precomputation time, and the detection problem can be solved by a one-side error quantum algorithm with error at most  $1 - \delta$ .*

The second advantage is that the methodology allows to construct new QADS from given ones, which might yield better detecting probabilities. These transformations are members of the *algorithmic closure* of QADS. Most of these closure procedures are quite natural, such as extending the number of qubits used, inverting the detecting operator, multiplication of detecting operators with the same initial state, conjugation by a unitary operator, or controlling of a detecting operator with a qubit. The description of some of them as quantum circuits and operators is given in Table 1.

In this paper, we introduce new families of QADS, known as combinatorial and rotational, which, respectively, generalize detecting systems based on single qubit controlled gates and on Grover's algorithm. We study the algorithmic closure of each family and prove that some of these QADS are equivalent (in the sense of having the same detection rate) to others constructed from tensor product of controlled operators and their square roots.

The structure of the paper is as follows. In Sect. 2, we introduce combinatorial QADS and study their algorithmic closure. Rotational QADS are introduced and studied in Sect. 3, including their algorithmic closure. Applications of the combinatorial QADS construction to an eigenvalue decision problem and to a phase estimation problem are given in Sect. 4. Finally, some conclusions and intended future work are collected in Sect. 5. Detailed proofs of the results presented in the paper can be found in Appendix.

**Table 1** Transformations in the algorithmic closure of a QADS

Name	Initial state	Detecting operator	Circuit
QADS#1	$ \varphi_0\rangle$	$U$	
Extension	$ \varphi_0\rangle 0\rangle^{\otimes l}$	$U \otimes I$	
Inversion	$ \varphi_0\rangle$	$U^\dagger$	
Powers	$ \varphi_0\rangle$	$U^{n_f}$	
Roots	$ \varphi_0\rangle$	$U^{1/n_f}$	
Conjugation	$T \varphi_0\rangle$	$TUT^\dagger$	
Controlled	$ +\rangle \varphi_0\rangle$	$U_c( i\rangle x\rangle =  i\rangle U^i  x\rangle$	
Tensor product	$ \varphi_0\rangle \varphi_0'\rangle$	$U \otimes U'$	
Product	$ \varphi_0\rangle (=  \varphi_0'\rangle)$	$U'U$	
Doubly controlled	$ +\rangle \varphi_0\rangle \varphi_0'\rangle$	$U_{dc}( i\rangle x\rangle x'\rangle =  i\rangle U^i  x\rangle U'^{i-1}  x'\rangle$	

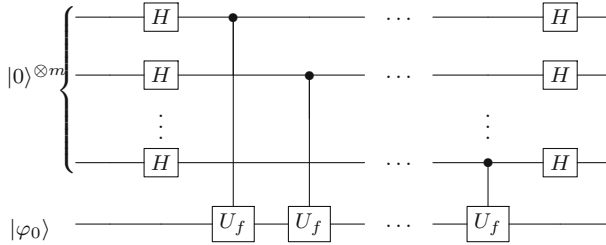


Fig. 1 Quantum circuit of a combinatorial QADS

### 2 m-Combinatorial QADS

In this section, we introduce *m*-combinatorial QADSs as a generalization of QADS based on single qubit controlled gates. We also study their properties, in particular their efficient constructibility, detecting times, and algorithmic closure. First, let us introduce the definition of combinatorial QADS.

**Definition 1** If  $U_f$  is the detecting operator of a QADS  $Q$ ,  $|\varphi_0\rangle$  is its initial state, and  $m$  is a nonnegative integer, we define the  $m$ -combinatorial QADS obtained from  $Q$  as the QADS whose initial state is  $|0\rangle^{\otimes m}|\varphi_0\rangle$ , and whose detecting operator is given by

$$C(m, U_f) := (H^{\otimes m} \otimes I) c_1 U_f \cdots c_m U_f (H^{\otimes m} \otimes I)$$

where  $c_i U_f$  is the unitary operator that applies  $U_f$  to the second register if the  $i$ th qubit of the first register is  $|1\rangle$  and applies the identity if that qubit is  $|0\rangle$  (i.e., it is the operator  $U_f$  controlled by the  $i$ th qubit of the first register).

Observe that when  $m = 1$ , we recover the *controlled QADS* of [4] (7th entry in Table 1 above). The following result, whose proof can be found in appendix, guarantees that the  $m$ -combinatorial QADS is indeed a QADS, and that it is efficiently constructible provided the original QADS is.

**Proposition 1** *If we have a QADS  $Q$  providing an output  $(U_f, |\varphi_0\rangle)$  on input  $f$ , then for all  $m \geq 1$  the algorithm that returns the operator depicted in circuit Fig. 1 and the state  $|0\rangle^{\otimes m}|\varphi_0\rangle$  is also a QADS. What is more, if the original QADS is efficiently constructible, so is the new QADS, for fixed  $m$ .*

The reason that justifies the name “combinatorial” for this type of QADS is given in the following result, where the amplitude of the state  $C(m, U_f)|0\rangle^{\otimes m}|\varphi_0\rangle$  related to the state  $|0\rangle^{\otimes m}|\varphi_0\rangle$  is given.

**Proposition 2** *The amplitude of the state  $C(m, U_f)|0\rangle^{\otimes m}|\varphi_0\rangle$  related to the basis state  $|0\rangle^{\otimes m}|\varphi_0\rangle$  is*

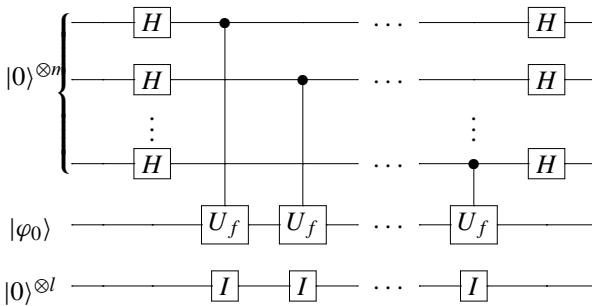
$$\frac{1}{2^m} \sum_{k=0}^m \binom{m}{k} \langle \varphi_0 | U_f^k | \varphi_0 \rangle \tag{2}$$

In appendix, a concrete and complete description of the state  $C(m, U_f)|0\rangle^{\otimes m}|\varphi_0\rangle$  is given (Proposition 7). Such an expression can be useful, for instance, for providing algebraic proofs of some of the results related to the algorithmic closure of combinatorial QADS that we introduce next. The proofs below are based on circuit depiction of the QADS operators, which are less cumbersome. (More details are given in appendix.) In these results, we determine some procedures which leave the subclass of combinatorial QADS algorithmically closed.

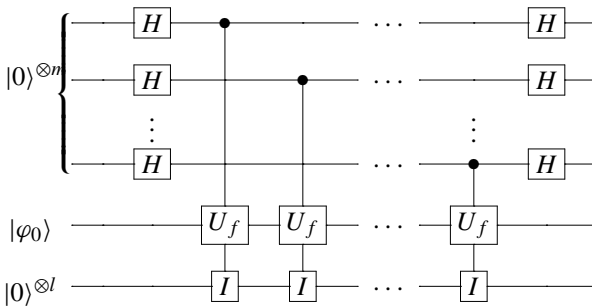
**Proposition 3** *The extension, powers, and roots of an  $m$ -combinatorial QADS are also  $m$ -combinatorial QADS.*

**Graphical sketch of proof**

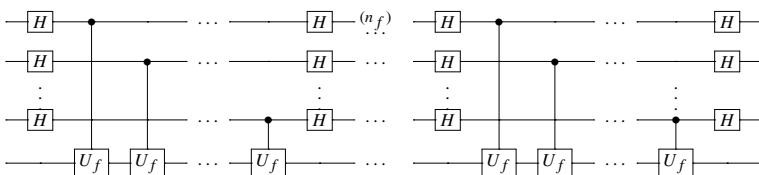
1. Extension: It is straightforward to see that the following circuit



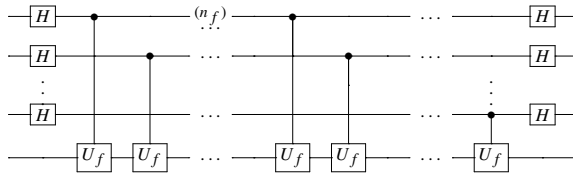
is equivalent to



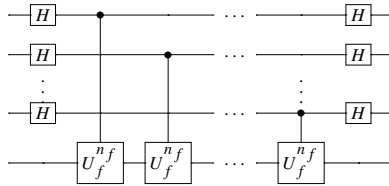
2. Powers and roots: Since  $H^2 = I$ , and  $U_f$  commutes with itself, we have the following equivalency for  $n_f$  copies of the  $m$ -combinatorial detecting operator:



≡



≡



□

Some other operations in the algorithmic closure of QADS might not leave the subclass of combinatorial QADS closed. This is, for instance, the case of the product of two combinatorial QADS when the corresponding detecting operators do not commute. Next, we provide a result relating the detecting times of the combinatorial and the original QADS. Its proof can be found in appendix.

**Proposition 4** *Let  $Q$  be a QADS, and let  $\tilde{Q}$  be the corresponding  $m$ -combinatorial QADS. Suppose  $S : \mathbb{N} \rightarrow \mathbb{N}$  is a  $\delta$ -detecting time for  $\tilde{Q}$ , and let  $z_l := \langle \varphi_0 | U_f^l | \varphi_0 \rangle$  for any  $l \in \mathbb{N}$ . Assume that, for all  $w \in \mathbb{N}$ , there exist  $a_w \in \mathbb{R}$ ,  $\alpha_w \in (0, \frac{\pi}{2})$  such that  $\frac{(1-\delta)2^{2m}}{\cos^2 \alpha_w \binom{2m}{m}} \leq 1 - \delta$ , with  $\delta > 0$ , and such that for all  $l = 0, \dots, m \cdot S(k)$ ,  $\arg(z_l) \in [a_w - \alpha_w, a_w + \alpha_w]$ . Then,  $T : \mathbb{N} \rightarrow \mathbb{N}$  given by  $T(w) = m \cdot S(w)$  for all  $w \in \mathbb{N}$  is  $\frac{\delta}{2m}$ -detecting time for  $Q$ .*

The conditions on the previous result are satisfied, for instance, for a family of QADS known as rotational, that we introduce in the next section.

### 3 Rotational QADS

In some well-studied searching procedures, the iterating operator acts only on a small-dimensional invariant subspace, leaving the remaining directions unchanged. This is the case, for instance, of the operator of Szegedy’s quantum walk with queries on the complete graph [14], which acts on an invariant three-dimensional space when only one vertex is marked, and on an invariant four-dimensional space when multiple marked vertices are considered. Of course, this is also the case of the operator of Grover’s search, which acts as a rotation in a two-dimensional invariant subspace and leaves the orthogonal directions unaltered [7]. In this section, we consider QADS in

which the detecting operator  $U_f$  behaves in this way, acting as a rotation in a two-dimensional invariant subspace. Such an operator can be described by a matrix in  $SO(2)$ . As in the case of the combinatorial QADS, we study their properties, such as an explicit expression of the final amplitude, and their algorithmic closure. We also consider combinatorial QADS derived from rotational QADS, concluding some interesting equivalences.

The definition of a rotational QADS is as follows.

**Definition 2** If  $U_f$  is the detecting operator of a QADS  $Q$  with initial state  $|\varphi_0\rangle$ , we shall say that it is a rotational QADS if there exist  $\alpha \in [0, 2\pi)$ , orthonormal states  $|\varphi_1\rangle, |\varphi_2\rangle$ , and  $\beta_1, \beta_2 \in \mathbb{R}$ , such that

1.  $|\varphi_0\rangle = \beta_1|\varphi_1\rangle + \beta_2|\varphi_2\rangle$
2.  $U_f|\varphi_1\rangle = \cos \alpha |\varphi_1\rangle + \sin \alpha |\varphi_2\rangle$
3.  $U_f|\varphi_2\rangle = -\sin \alpha |\varphi_1\rangle + \cos \alpha |\varphi_2\rangle$

As said before, the QADS associated with Grover's search is a rotational QADS. The detecting operator  $U_f$  of a rotational QADS can be straightforwardly described by a matrix  $\begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \in SO(2)$ , since the coordinate matrix of  $U_f$  with respect to an orthonormal basis whose first two elements are  $|\varphi_1\rangle, |\varphi_2\rangle$  is

$$\left( \begin{array}{cc|c} \cos \alpha & -\sin \alpha & 0 \\ \sin \alpha & \cos \alpha & 0 \\ \hline 0 & 0 & I_{n-2} \end{array} \right)$$

In the following result, we obtain the amplitude of the state  $U_f|\varphi_0\rangle$ . Its proof can be found in Appendix, together with a generalized version for QADS that can be described by an arbitrary matrix in the orthogonal group  $O(n)$  (Proposition 8).

**Proposition 5** Given a rotational QADS with output  $(|\varphi_0\rangle, U_f)$ , the state after  $k$  hits of the detecting operator on the initial state is

$$U_f^k|\varphi_0\rangle = (\beta_1 \cos k\alpha - \beta_2 \sin k\alpha)|\varphi_1\rangle + (\beta_1 \sin k\alpha + \beta_2 \cos k\alpha)|\varphi_2\rangle$$

In particular, the amplitude of such a final state, related to the initial state  $|\varphi_0\rangle$ , is  $\cos k\alpha$ .

Analogously as in the case of combinatorial QADS, we consider different procedures that allow to derive new rotational QADS from others. The proof, again, can be found in Appendix.

**Proposition 6** The powers, roots, and inversion of a rotational QADS are also rotational QADS. Also, if two rotational QADS share the same initial state, then their product is also a rotational QADS.

Like in the case of combinatorial QADS, some other operations in the algorithmic closure of QADS might not leave the subclass of rotational QADS closed. This is,



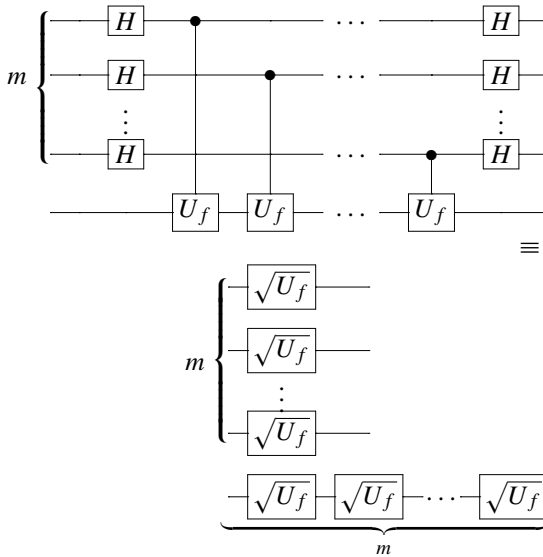
for instance, the case of the extension of a rotational QADS, or the product of two rotational QADS when they do not share the same initial state.

Next, we want to study the  $m$ -combinatorial QADS of a rotational QADS. In particular, we study the amplitude of the final state, related to the initial state, which is connected to the detection rate when a single hit of the detecting operator is used. As a consequence of Proposition 9 of Appendix, we conclude some interesting equivalences of detecting operators from different QADS in the algorithmic closure related to the square root QADS.

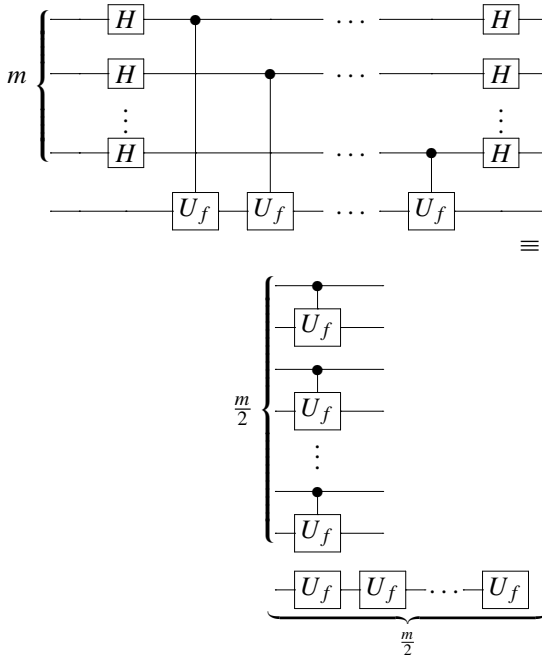
**Theorem 2** *If  $Q$  is a rotation QADS,  $m \in \mathbb{Z}^+$ , and we consider the corresponding  $m$ -combinatorial QADS, then the amplitude of the initial state after one hit of the detecting operator, i.e., of  $C(m, U_f)|0\rangle^m|\varphi_0\rangle$ , related to the initial state  $|0\rangle^m|\varphi_0\rangle$ , is*

$$\frac{1}{2^m} \sum_{k=0}^m \binom{m}{k} \cos k\alpha = \left(\cos\left(\frac{\alpha}{2}\right)\right)^m \cos\left(\frac{\alpha}{2}m\right) \tag{3}$$

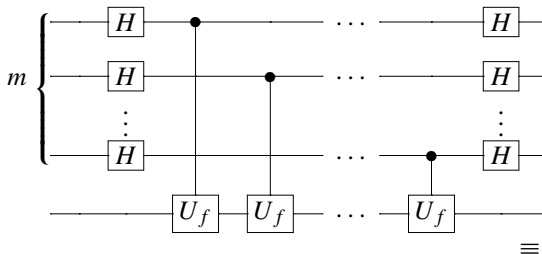
As a consequence, the  $m$ -combinatorial QADS of a rotational QADS is equivalent, in terms of detection rate when one single hit of the detecting operator is taken, to the tensor product of  $m$  copies of its square root QADS, tensored with the  $m$ th power of its square root QADS.

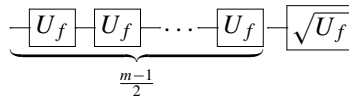
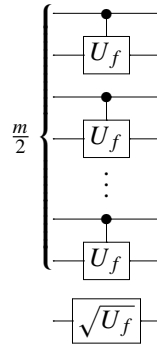


In particular, when  $m$  is even, it is equivalent to the tensor product of  $\frac{m}{2}$  copies of its controlled QADS, tensored with its  $\frac{m}{2}$ th power.



On the other hand, when  $m$  is odd, it is equivalent to the tensor product of  $\frac{m-1}{2}$  copies of its controlled QADS plus one copy of its square roots, tensored with a product of exactly the same operators.





Let us finish this section with the previously mentioned result on the detecting time of a family of QADS. Its proof can be also found in Appendix.

**Corollary 1** *Let  $Q$  be a rotational QADS with a rotation angle smaller than  $\theta_w$ , on entries  $f$  of size  $w$ , and let  $\tilde{Q}$  be the corresponding  $m$ -combinatorial QADS. Suppose  $S : \mathbb{N} \rightarrow \mathbb{N}$  is a  $\tilde{\delta}$ -detecting time for  $\tilde{Q}$  such that  $m < \min \left\{ \frac{1}{4(1-\tilde{\delta})^2}, \frac{\pi}{2\Delta} \right\}$ , where  $\Delta \geq \theta_w S(w)$ , for all  $w \in \mathbb{N}$ . Then,  $T : \mathbb{N} \rightarrow \mathbb{N}$  given by  $T(w) = m \cdot S(w)$  for all  $w \in \mathbb{N}$ , is  $\frac{\delta}{2m}$ -detecting time for  $Q$ , where  $\delta = \frac{1-2\sqrt{m(1-\tilde{\delta})}}{2} > 0$ .*

## 4 Applications

### 4.1 Decision on eigenvalues

Although the QADS methodology was initially introduced as a common framework to deal with the detection problem, it can also be adapted to other problems. Consider, for instance, the situation in which we are given a quantum state  $|\varphi_0\rangle$  and an unitary operator  $U$ , under the promise that  $|\varphi_0\rangle$  is one of its eigenvectors, and we want to check whether the associated eigenvalue is  $e^{i\alpha}$  or not. Namely,

**Problem 1**  
 INPUT: A real value  $\alpha$ , a quantum state  $|\varphi_0\rangle$ ,  $U_\beta \in \{U_\gamma\}_{\gamma \in [0, 2\pi)}$ , such that  $U_\beta|\varphi_0\rangle = e^{i\beta}|\varphi_0\rangle$ .  
 PROBLEM: Decide whether  $\beta = \alpha$  or not.

If  $\alpha$  and  $|\varphi_0\rangle$  are efficiently computable, then this problem can be approached with an efficiently constructible  $m$ -combinatorial QADS. In fact, let us consider the unitary

transformation  $V = e^{-i\alpha}U$ . Then,

$$V|\varphi_0\rangle = e^{-i\alpha}U_\beta|\varphi_0\rangle = e^{i(\beta-\alpha)}|\varphi_0\rangle = |\varphi_0\rangle$$

where the last equality holds if and only if  $\alpha = \beta$ .

Now, from the results of Sect. 2, we know that the projection of the final state  $C(m, V)|0\rangle^m|\varphi_0\rangle$  on the  $m$ -combinatorial QADS initial state  $|0\rangle^m|\varphi_0\rangle$  is

$$\frac{1}{2^m} \sum_{k=0}^m \binom{m}{k} \langle \varphi_0 | V^k | \varphi_0 \rangle = \frac{1}{2^m} \sum_{k=0}^m \binom{m}{k} (e^{i(\beta-\alpha)})^k = \left( \frac{1 + e^{i(\beta-\alpha)}}{2} \right)^m.$$

Thus, the probability of measuring  $|0\rangle^m|\varphi_0\rangle$  is

$$\begin{aligned} \left| \left( \frac{1 + e^{i(\beta-\alpha)}}{2} \right)^m \right|^2 &= \left| \left( \frac{1 + e^{i(\beta-\alpha)}}{2} \right)^2 \right|^m \\ &= \left( \frac{|1 + \cos(\beta - \alpha) + i \sin(\beta - \alpha)|^2}{4} \right)^m \\ &= \left( \frac{1 + 2 \cos(\beta - \alpha) + \cos^2(\beta - \alpha) + \sin^2(\beta - \alpha)}{4} \right)^m \\ &= \left( \frac{2 + 2 \cos(\beta - \alpha)}{4} \right)^m \\ &= \left( \frac{1 + \cos(\beta - \alpha)}{2} \right)^m \\ &= \left( \cos\left(\frac{\beta - \alpha}{2}\right) \right)^{2m}. \end{aligned}$$

Therefore, we can think of the following procedure to decide whether  $\alpha = \beta$ .

**Algorithm 2 (For the eigenvalue decision problem)**

*INPUT:* A real value  $\alpha$ , a quantum state  $|\varphi_0\rangle$ ,  $U_\beta \in \{U_\gamma\}_{\gamma \in [0, 2\pi]}$ , such that  $U_\beta|\varphi_0\rangle = e^{i\beta}|\varphi_0\rangle$ .

*PROCEDURE:*

- *PRECOMPUTATION* of the initial state  $|\varphi_0\rangle$ , the unitary operator  $V = e^{-i\alpha}U$ , and the output of the corresponding  $m$ -combinatorial QADS  $(C(m, V), |0\rangle^m|\varphi_0\rangle)$ , for a chosen  $m$ .

- *COMPUTATION:*

- Compute  $|\varphi\rangle = C(m, V)|0\rangle^m|\varphi_0\rangle$ .

- *MEASUREMENT* of  $|\varphi\rangle$  on an orthonormal basis containing  $|\varphi_0\rangle$ .

*OUTPUT:*

- *YES:* If the measurement is the initial state  $|\varphi_0\rangle$ .

- *NO:* Otherwise.

The observations above prove the following result.

**Theorem 3** *Algorithm 2 is always correct when it outputs NO. So, the probability of error is fully attributed to a YES answer. Namely, such a probability is equal to*

$$\theta = \left( \cos \left( \frac{\beta - \alpha}{2} \right) \right)^{2m}$$

*Therefore, if the QADS is efficiently constructible, then the eigenvalue decision problem can be solved in  $O(\text{poly}(n))$  precomputation time of a one-side error quantum algorithm with error at most  $\theta$ , which decreases exponentially with  $m$ . The probability of success of the algorithm is  $1 - \theta$ .*

## 4.2 Phase estimation

### 4.2.1 Generalized Hadamard test

Another application of the QADS methodology is on phase estimation. Consider again that we are given a quantum state  $|\varphi_0\rangle$  and an unitary operator  $U$ , under the promise that  $|\varphi_0\rangle$  is one of its eigenvectors with associated eigenvalue is  $e^{i\alpha}$ . The aim is to estimate  $\alpha$ .

#### Problem 2

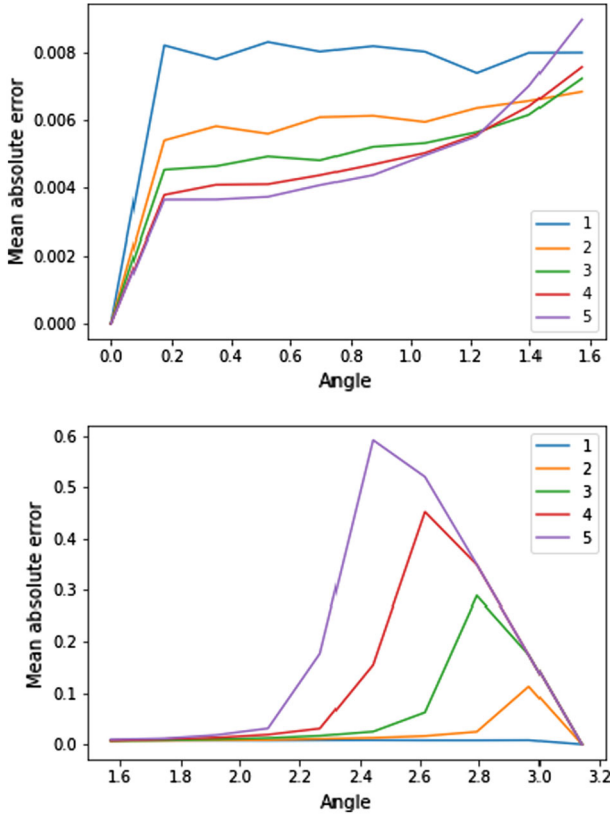
INPUT: A quantum state  $|\varphi_0\rangle$ ,  $U_\beta \in \{U_\gamma\}_{\gamma \in [0, \pi]}$ , such that  $U_\beta |\varphi_0\rangle = e^{i\beta} |\varphi_0\rangle$ , and a natural number *SHOTS*.

PROBLEM: An approximation  $\alpha$  of  $\beta$ , using at most *SHOTS* executions of prefixed quantum circuit.

Of course, this problem can be solved with the well-known quantum phase estimation (QPE) algorithm [10, Section 5.2]. However, as pointed out in [11] “the size and shallowness of the QPE circuit is important since, in the absence of error correction or error mitigation, one expects entropy build-up during computation.” In fact, it has been shown in [8] that, when implemented on current quantum hardware, the accuracy of the QPE algorithm is “severely constrained by NISQ’s physical characteristics such as coherence time and error rates.” For these reasons, some authors have proposed replacing the QPE algorithm with less demanding methods that make implementing quantum algorithms that rely on it easier in practice (see, for instance, [1,6,9,13,15,17]).

A simpler algorithm that sometimes is used for the phase estimation problem instead of QPE is the Hadamard test. It consists in the quantum circuit of Fig. 1 with  $m = 1$ , with a final measurement of the controlling qubit [2]. The probability of measuring the quantum state  $|\varphi_0\rangle$  is  $\cos^2\left(\frac{\beta}{2}\right)$ . Running the test *SHOTS* times provides an approximation  $P$  of such a probability, from which  $\beta$  can be estimated. Namely,  $\alpha = \arccos(2P - 1)$ .

If we follow a similar procedure with  $m > 1$  (i.e., with another combinatorial QADS), we obtain a generalization of the Hadamard test. In this case, the probability

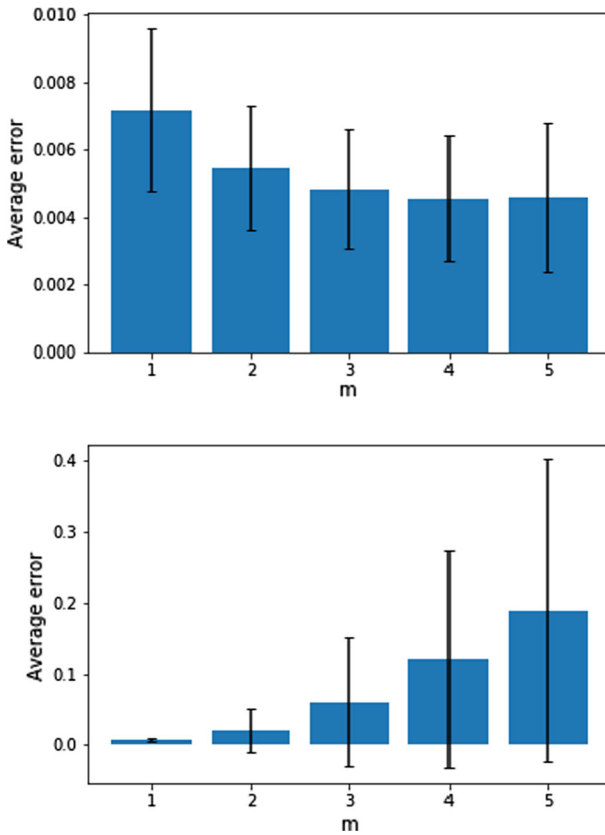


**Fig. 2** Mean absolute error of the estimated phase with  $10^3$  experiments of the  $m$ -Hadamard test (with  $m = 1, \dots, 5$ ), with  $10^4$  SHOTS, for 10 different equispaced phase values

of measuring the quantum state  $|\varphi_0\rangle$  is  $\cos\left(\frac{\beta}{2}\right)^{2m}$ , and running the test SHOTS times provides an approximation  $P$  of such a probability, from which  $\beta$  can be estimated as  $\alpha = \arccos\left(2^{\frac{1}{m}}\sqrt{P} - 1\right)$ .

We have tested this “ $m$ -Hadamard test” with different values of  $m$ , and 10 equispaced angles in  $[0, \pi)$ , with a number of SHOTS equal to  $10^4$ . We run the experiment  $10^3$  times to get an estimation of the phase, measuring the mean absolute error of such an estimation. The results are collected in Fig. 2. For convenience, the interval  $[0, \pi)$  has been split in two subintervals  $[0, \frac{\pi}{2})$  and  $[\frac{\pi}{2}, \pi)$ . Observe the different scale of the two figures. When the phase is “small” (namely in the first subinterval),  $m$  bigger yields a smaller mean absolute error, and the opposite occurs for bigger phases. This can be easily explained by the effect of the  $m$ th root, since in the first case the cosines are closer to one, whereas in the second one, cosines are closer to zero.

Another way of visualizing this fact is with the average error for the five phases in the first interval, and for the five phases in the second interval (in both cases for  $m = 1, \dots, 5$ ), as depicted in Fig. 3. We can see that increasing  $m$  is better for the

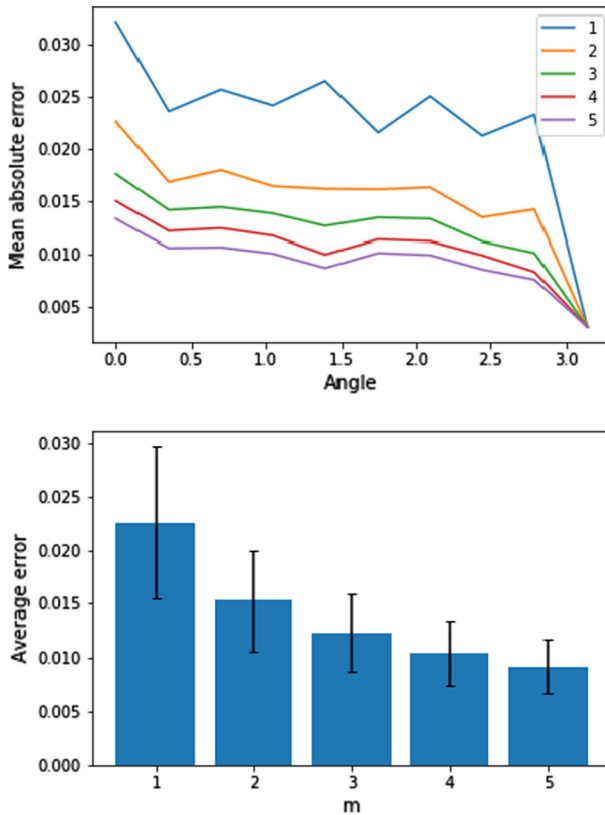


**Fig. 3** Average error of the estimated phase with  $10^3$  experiments of the  $m$ -Hadamard test (with  $m = 1, \dots, 5$ ), with  $10^4$  SHOTS, for the equispaced phase values in the first and second halves of the interval  $[0, \pi)$

estimation of angles in the first subinterval, but it is worse for those in the second subinterval. Therefore, we can conclude that unless the phase is promised to be in the first half of the interval  $[0, \pi)$ , the  $m$ -Hadamard test with  $m > 1$  cannot be directly used.

#### 4.2.2 Dichotomy search

An alternative for phase estimation is a dichotomy search based on the decision of eigenvalues procedure of the previous subsection. The idea is, as in the original dichotomy search, to iteratively split the interval  $[0, \pi)$  in halves, deciding in each iteration to which half the phase belongs to. The decision is based on comparing the phase against the angles that define each subinterval. So, in the first iteration, the phase is compared against 0 and  $\pi$ , in the second one, against 0 and  $\frac{\pi}{2}$  or against  $\frac{\pi}{2}$  and  $\pi$ , and so on. For this decision, we also use Theorem 3, choosing the “left” or “right”



**Fig. 4** Mean absolute and average errors of the estimated phase with  $10^3$  experiments of the dichotomy search with 10 steps, and  $10^3$  *SHOTS* in each step, for 10 different equispaced phase values

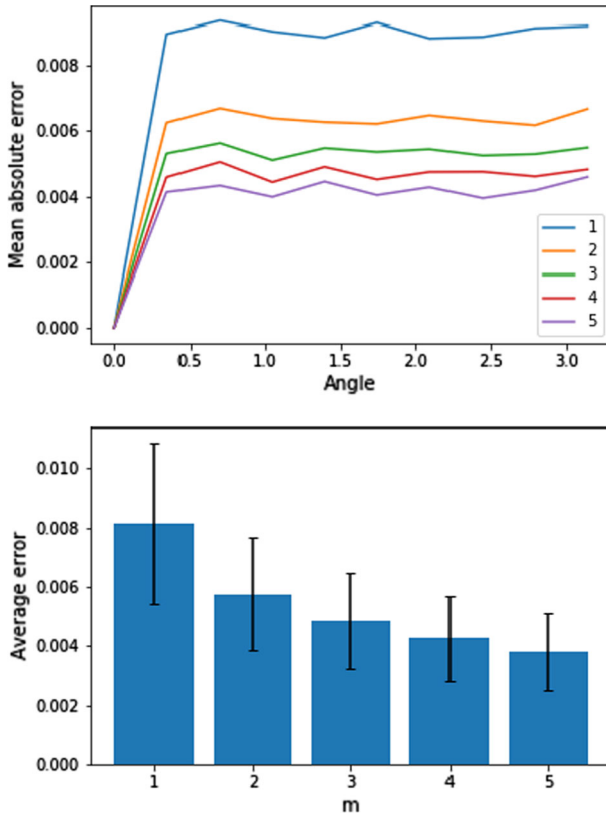
subinterval, depending on which extreme angle provides a bigger probability  $\theta$ . ( $\alpha$  takes the value of one or another extreme angle.)

We have tested this dichotomy test with different values of  $m$ , and 10 equispaced angles in  $[0, \pi)$ , with 10 iterations, and a number of *SHOTS* equal to  $10^3$  in each iteration. We run the experiment  $10^3$  times to get an estimation of the phase, measuring the mean absolute error of such an estimation, and the overall average error for different values of  $m$ . The results are collected in Fig. 4. It can be noticed that this method provides uniformly better results when  $m$  increases. However, the error is still bigger than the error provided by the standard Hadamard test.

#### 4.2.3 Hybrid methodology

As a consequence, we propose a hybrid approach which takes the advantages of each of the methods presented above. First, we use the dichotomy search to “locate” the phase, and then, we get an actual estimation by using the Hadamard test. We have experimented with this hybrid methodology with different values of  $m$ , and 10 equispaced angles in  $[0, \pi)$ , with 2 iterations of the dichotomy search, with a number of





**Fig. 5** Mean absolute and average errors of the estimated phase with  $10^3$  experiments of the hybrid methodology with 2 steps of the dichotomy search, and  $10^3$  SHOTS in each step, plus 8000 SHOTS off the  $m$ -Hadamard test, for 10 different equispaced phase values

$10^3$  SHOTS in each iteration. Another 8000 SHOTS are used in the  $m$ -Hadamard test. In order to apply the  $m$ -Hadamard test, we hit the operator with a rotation of angle  $e^{i \cdot L}$ , where  $L$  is the lower extreme of the interval in which the phase is located. In the end, we add the Hadamard estimation to  $L$ .

The results are collected in Fig. 5. As in the case of the dichotomy search, this methodology provides uniformly better results when  $m$  increases. Moreover, the overall error when  $m > 1$  beat those of the standard Hadamard test.

### 5 Conclusions and future work

In this paper, we explore the QADS framework introduced in [4] for dealing with detection problems in a quantum computation setting. Namely, we study two specific classes of QADS. The first one is that of combinatorial QADS that generalize the well-known controlled operators. We have determined their efficient constructibility, the expression of the state after application of the detecting operator, and their algorithm

closure as a subclass of QADS. As an application, we have considered the problem of deciding whether, for a given pair operator–eigenvector, the corresponding eigenvalue is one given or not. The second family is that of rotational QADS, which include as a particular case the QADS from Grover’s search. We have studied the expression of the state after application of the detecting operator on the initial state, the algorithmic closure of this subclass of QADS, and also we have considered their combinatorial QADS. Interestingly, we have derived some nice equivalences for these QADS, in terms of tensor products and products of square roots of the original QADS. As future projects, we want to study other families of QADS that include measurements, or QADS that resemble the combinatorial ones with different controlled operators (functional QADS).

**Acknowledgements** This work was supported in part by the MINECO under Grant MTM-2017-83506-C2-2-P and Grant MINECO-16-TEC2015-67387-C4-3-R and in part by the MICINN under Grant RTI2018-098085-B-C44, Grant FC-GRUPIN-IDI/2018/000193, and under Grant FC-GRUPIN-IDI/2018/000226, MCI-21-PID2020-119082RBC22 - Ministerio de Economía e Industria.

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

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

## A Appendix

In this appendix, we include proofs of the results presented in the main part of the paper. We also collect some auxiliary results hinted in the main text.

**Proof of Proposition 1** The new algorithm is a QADS because if  $f = 0$ , then  $U_f|\varphi_0\rangle = |\varphi_0\rangle$ . Therefore,  $c_i U_f |\psi\rangle |\varphi_0\rangle = |\psi\rangle |\varphi_0\rangle$ , for all  $|\psi\rangle$ , and for all  $i$ . Consequently,

$$C(m, U_f)|0\rangle^{\otimes m} |\varphi_0\rangle = [(H^{\otimes m} \otimes I) c_1 U_f \cdots c_m U_f (H^{\otimes m} \otimes I)] |0\rangle^{\otimes m} |\varphi_0\rangle = |0\rangle^{\otimes m} |\varphi_0\rangle$$

which shows that the  $m$ –combinatorial QADS is actually a QADS.

When the QADS is efficiently constructible,  $|\varphi_0\rangle$  can be constructed in polynomial time (on  $n$ , the size of  $f$ ), and the same holds for the initial state  $|0\rangle^{\otimes m} |\varphi_0\rangle$ , for fixed  $m$ . On the other hand, because of [10][Section 4.3], any controlled operator  $c_i U_f$  can also be constructed in polynomial time because of the constructibility of the QADS. Therefore, the  $m$ –combinatorial QADS is constructible, with a cost of order  $O(m \cdot \text{poly}(n))$ .  $\square$

**Proof of Proposition 2** Applying  $H^{\otimes m} \otimes I$  to the state  $|0\rangle^{\otimes m}|\varphi_0\rangle$ , we get

$$|\psi\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle|\varphi_0\rangle.$$

Using the controlled versions of the  $U_f$  operator, we get

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle U_f^{|x|}|\varphi_0\rangle$$

where  $|x|$  is the Hamming weight of  $x$ , i.e., if  $x$  is described by exactly  $|x|$  ones and  $m - |x|$  zeroes, then the controlled operators  $c_i U_f$  will contribute with exactly  $|x|$  hits of  $U_f$ . Therefore,

$$\begin{aligned} \langle |0\rangle^{\otimes m}|\varphi_0\rangle, (H^{\otimes m} \otimes I)|\psi\rangle &= \langle (H^{\otimes m} \otimes I)|0\rangle^{\otimes m}|\varphi_0\rangle, |\psi\rangle \\ &= \left\langle \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} |y\rangle|\varphi_0\rangle, \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle U_f^{|x|}|\varphi_0\rangle \right\rangle \\ &= \frac{1}{2^m} \sum_{x=0}^{2^m-1} \langle \varphi_0| U_f^{|x|}|\varphi_0\rangle \\ &= \frac{1}{2^m} \sum_{k=0}^m \binom{m}{k} \langle \varphi_0| U_f^k|\varphi_0\rangle \end{aligned}$$

as desired. □

**Proposition 7** Given a QADS with output  $(|\varphi_0\rangle, U_f)$ , and a natural number  $m$ , the state of the corresponding  $m$ -combinatorial QADS, after one hit of the detecting operator on the initial state, is:

$$\frac{1}{2^m} \sum_{y=0}^{2^m-1} |y\rangle \left( \sum_{k=0}^m \left( \sum_{s=0}^{\lfloor \frac{k}{2} \rfloor} \binom{|y|}{2s} \binom{m - |y|}{k - 2s} - \sum_{s=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{|y|}{2s+1} \binom{m - |y|}{k - 2s - 1} \right) U_f^k \right) |\varphi_0\rangle$$

**Proof** From the proof of Proposition 2, we get the state

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle U_f^{|x|}|\varphi_0\rangle$$

after applying  $H^{\otimes m} \otimes I$  to the initial state  $|0\rangle^{\otimes m}|\varphi_0\rangle$ , and then the controlled gates on the operators  $U_f$ . Now, we apply  $H^{\otimes m} \otimes I$  to get

$$\frac{1}{\sqrt{2^m}} \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^m-1} (-1)^{x \cdot y} |y\rangle U_f^{|x|} |\varphi_0\rangle = \frac{1}{2^m} \sum_{y=0}^{2^m-1} |y\rangle \left( \sum_{x=0}^{2^m-1} (-1)^{x \cdot y} U_f^{|x|} \right) |\varphi_0\rangle.$$

Now, we fix a binary array  $y$  with  $|y|$  ones and  $m - |y|$  zeroes. Assume that another array  $x$  of the same length  $m$  contains  $t$  ones colliding in positions of the array  $y$  with a one, and  $|x| - t$  ones colliding in zero entries of the array  $y$ . (Its remaining entries are all zero.) W.l.o.g. this can be depicted as:

$$\begin{aligned} y &= (1 \dots 1^{|y|} \dots 1 \mid 0 \dots 0^{m-|y|} \dots 0) \\ x &= (1 \dots 1^t \mid 0^{|y|-t} \mid 0 \dots 0^{|x|-t} \mid 1 \dots 1^{m-|y|-|x|+t} \mid 0) \end{aligned}$$

The number of arrays  $x$  in this situation is

$$\binom{|y|}{t} \binom{m - |y|}{|x| - t}$$

Now,  $x \cdot y = 0$  if and only if  $t$  is even. In this case, the possible values of  $t$  are of the form  $t = 2s$ , where  $s = 0, 1, \dots, \lfloor \frac{|x|}{2} \rfloor$ . On the other hand,  $x \cdot y = 1$  if and only if  $t$  is odd, and the possible values of  $t$  are of the form  $t = 2s + 1$ , where  $s = 0, 1, \dots, \lfloor \frac{|x|-1}{2} \rfloor$ . Summarizing, the number of possible  $x$  such that  $x \cdot y = 0$  is

$$\sum_{s=0}^{\lfloor \frac{k}{2} \rfloor} \binom{|y|}{2s} \binom{m - |y|}{k - 2s}$$

whereas the number of possible  $x$  such that  $x \cdot y = 1$  is

$$\sum_{s=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{|y|}{2s+1} \binom{m - |y|}{k - 2s - 1}$$

This gives us the desired expression for the final state of the  $m$ -combinatorial QADS. □

**Proof of Proposition 3** Consider a QADS that, on input  $f$ , provides an output  $(|\varphi_0\rangle, U_f)$ , and let  $(|0\rangle^{\otimes m}|\varphi_0\rangle, C(m, U_f))$  be the output of the corresponding  $m$ -combinatorial QADS.

1. Extension: Observe that

$$(c_i U_f \otimes I) |x\rangle |\psi\rangle |\xi\rangle = (\alpha |0\rangle |\psi\rangle + \beta |1\rangle U_f |\psi\rangle) |\xi\rangle$$

$$= (\alpha|0\rangle + \beta|1\rangle)(U_f \otimes I)|\psi\rangle|\xi\rangle = c_i(U_f \otimes I)|x\rangle|\psi\rangle|\xi\rangle$$

where  $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ . So,  $C(m, U_f) \otimes I = C(m, U_f \otimes I)$ .

2. Powers: For any unitary operators  $U$  and  $V$

$$cVcU|x\rangle|\varphi\rangle = \alpha|0\rangle|\varphi\rangle + \beta|1\rangle VU|\varphi\rangle = c(VU)|x\rangle|\varphi\rangle$$

where  $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ . Also, notice that when  $U$  and  $V$  commute,

$$\begin{aligned} c_2Vc_1U|x\rangle|y\rangle|\psi\rangle &= c_2V(\alpha|0\rangle|y\rangle|\psi\rangle + \beta|1\rangle|y\rangleU|\psi\rangle) \\ &= \alpha\gamma|0\rangle|0\rangle|\psi\rangle + \alpha\delta|0\rangle|1\rangleV|\psi\rangle + \beta\gamma|1\rangle|0\rangleU|\psi\rangle + \beta\delta|1\rangle|1\rangleVU|\psi\rangle \\ &= \gamma\alpha|0\rangle|0\rangle|\psi\rangle + \gamma\beta|1\rangle|0\rangleU|\psi\rangle + \delta\alpha|0\rangle|1\rangleV|\psi\rangle + \delta\beta|1\rangle|1\rangleUV|\psi\rangle \\ &= c_1U(\gamma|x\rangle|0\rangle|\psi\rangle + \delta|x\rangle|1\rangleV|\psi\rangle) = c_1Uc_2V|x\rangle|y\rangle|\varphi\rangle \end{aligned}$$

where  $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ ,  $|y\rangle = \gamma|0\rangle + \delta|1\rangle$ . Because  $H^2 = I$ , we have  $C(m, U_f)^{n_f} = C(m, U_f^{n_f})$ .

3. Roots: Taking in the previous equation  $V = U_f^{n_f}$ , we have that  $U_f = V^{1/n_f}$ , and that  $C(m, V^{1/n_f})^{n_f} = C(m, V)$ , i.e.,  $C(m, V^{1/n_f}) = C(m, V)^{1/n_f}$ . This shows that the  $n_f$ th root of an  $m$ -combinatorial QADS is also an  $m$ -combinatorial QADS.

□

**Proof of Proposition 4** Let  $w \in \mathbb{N}$  be fixed, and denote  $T = T(w)$ ,  $S = S(w) = m \cdot T(w)$ ,  $a = a_w$ , and  $\alpha = \alpha_w$ . By Proposition 3, we have that, for all  $s \in \mathbb{N}$ ,  $C(m, U_f)^s = C(m, U_f^s)$ , and by Proposition 2 we know the amplitude of the state  $C(m, U_f)|0\rangle^{\otimes m}|\varphi_0\rangle$ , so

$$\begin{aligned} \frac{\sum_{s=0}^S | \langle |0^{\otimes m}\rangle|\varphi_0\rangle C(m, U_f)^s |0^{\otimes m}\rangle|\varphi_0\rangle |^2}{S + 1} &= \frac{\sum_{s=0}^S \left| \sum_{k=0}^m \binom{m}{k} \langle \varphi_0 | U_f^{ks} | \varphi_0 \rangle \right|^2}{2^{2m}(S + 1)} \\ &= \frac{\sum_{s=0}^S \left| \sum_{k=0}^m \binom{m}{k} z_{ks} \right|^2}{2^{2m}(S + 1)} \\ &\leq 1 - \tilde{\delta}. \end{aligned}$$

Let us define the following sets,

$$\begin{aligned} A_0 &:= \{0\} \\ \overline{A_0} &:= \{1, \dots, T\} = \{0, \dots, T\} \setminus \{A_0\} \\ A_k &:= \{k, 2k, \dots, Sk\}, \text{ for all } 1 \leq k \leq m \\ \overline{A_k} &:= \{0, \dots, T\} \setminus \{A_k\}. \end{aligned}$$

Now, using the fact that  $\sum_{k=0}^m \binom{m}{k}^2 = \binom{2m}{m}$  hence

$$\frac{\sum_{t=0}^T |\langle \varphi_0 | U_f^t | \varphi_0 \rangle|^2}{T+1} = \frac{\sum_{t=0}^T |z_t|^2}{T+1} = \frac{\sum_{k=0}^m \binom{m}{k}^2}{\binom{2m}{m}} \cdot \frac{\sum_{t=0}^T |z_t|^2}{T+1} = \frac{\sum_{k=0}^m \binom{m}{k}^2 \left( \sum_{t \in A_k} |z_t|^2 + \sum_{t \in \bar{A}_k} |z_t|^2 \right)}{\binom{2m}{m}(T+1)}.$$

But, since  $|z_t| \leq 1$ ,  $|A_k| = T - S$  for  $k > 0$ , and  $|z_0|^2 = 1$ , we find

$$\begin{aligned} \frac{\sum_{k=0}^m \binom{m}{k}^2 \left( \sum_{t \in A_k} |z_t|^2 + \sum_{t \in \bar{A}_k} |z_t|^2 \right)}{\binom{2m}{m}(T+1)} &\leq \frac{(|z_0|^2 + T) + \sum_{k=1}^m \binom{m}{k}^2 \left( \sum_{s=0}^S |z_{ks}|^2 + (T - S) \right)}{\binom{2m}{m}(T+1)} \\ &= \frac{\sum_{k=0}^m \binom{m}{k}^2 \left( \sum_{s=0}^S |z_{ks}|^2 + (T - S) \right)}{\binom{2m}{m}(T+1)} \\ &= \frac{\sum_{s=0}^S \sum_{k=0}^m \binom{m}{k}^2 |z_{ks}|^2}{\binom{2m}{m}(T+1)} + \frac{\sum_{k=0}^m \binom{m}{k}^2}{\binom{2m}{m}} \cdot \frac{T - S}{T + 1} \\ &\leq \frac{\sum_{s=0}^S \left( \sum_{k=0}^m \binom{m}{k} |z_{ks}| \right)^2}{\binom{2m}{m}(T+1)} + \frac{T - S}{T + 1} \end{aligned}$$

because  $\binom{m}{k} |z_{ks}| = \binom{m}{k} z_{ks} \geq 0$ . Therefore, by the *generalized reverse triangle inequality*, we have

$$\begin{aligned} \frac{\sum_{s=0}^S \left( \sum_{k=0}^m \binom{m}{k} |z_{ks}| \right)^2}{\binom{2m}{m}(T+1)} + \frac{T - S}{T + 1} &\leq \frac{\sum_{s=0}^S \left| \sum_{k=0}^m \binom{m}{k} z_{ks} \right|^2}{\cos^2 \alpha \binom{2m}{m}(T+1)} \cdot \frac{2^{2m}(S+1)}{2^{2m}(S+1)} + \frac{T - S}{T + 1} \\ &\leq (1 - \delta) \cdot \frac{2^{2m}(S+1)}{\cos^2 \alpha \binom{2m}{m}(T+1)} + \frac{T - S}{T + 1} \\ &\leq (1 - \delta) \cdot \frac{S + 1}{T + 1} + \frac{T - S}{T + 1} \leq 1 - \frac{\delta}{2m} \end{aligned}$$

since  $\frac{S+1}{T+1} \geq \frac{1}{2m}$ . □

**Proof of Proposition 5** In terms of  $|\varphi_1\rangle, |\varphi_2\rangle$ , for all  $k \geq 0$ , the action of  $U_f^k$  on  $|\varphi_0\rangle$  is given by the matrix

$$\begin{pmatrix} \cos \alpha - \sin \alpha \\ \sin \alpha \quad \cos \alpha \end{pmatrix}^k = \begin{pmatrix} \cos k\alpha - \sin k\alpha \\ \sin k\alpha \quad \cos k\alpha \end{pmatrix}$$

. (The  $n - 2$  invariant directions have been omitted.) The final state has coordinates related to  $|\varphi_1\rangle, |\varphi_2\rangle$  given by the array

$$\begin{pmatrix} \cos k\alpha & -\sin k\alpha \\ \sin k\alpha & \cos k\alpha \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \beta_1 \cos k\alpha - \beta_2 \sin k\alpha \\ \beta_1 \sin k\alpha + \beta_2 \cos k\alpha \end{pmatrix}$$

as desired.

On the other hand,

$$\begin{aligned} \langle \varphi_0 | U_f^k | \varphi_0 \rangle &= (\overline{\beta_1}, \overline{\beta_2}) \begin{pmatrix} \beta_1 \cos k\alpha - \beta_2 \sin k\alpha \\ \beta_1 \sin k\alpha + \beta_2 \cos k\alpha \end{pmatrix} \\ &= |\beta_1|^2 \cos k\alpha + (\overline{\beta_2} \beta_1 - \overline{\beta_1} \beta_2) \sin k\alpha + |\beta_2|^2 \cos k\alpha \\ &= \cos k\alpha. \end{aligned}$$

□

**Proposition 8** Let  $Q$  be a QADS such that for any input function  $U_f$  can be described by an orthogonal matrix with respect to a suitable orthonormal basis. Then, there exist an orthonormal basis  $\{|\varphi_1^1\rangle, |\varphi_2^1\rangle, \dots, |\varphi_1^l\rangle, |\varphi_2^l\rangle, |\varphi_{2l+1}\rangle, \dots, |\varphi_n\rangle\}$ , angles  $\theta_1, \dots, \theta_k \in [0, 2\pi)$ , complex scalars  $\beta_1^2, \beta_1^2, \dots, \beta_1^l, \beta_2^l, \beta_{2l+1}, \dots, \beta_n$ , such that the final state  $U_f|\varphi_0\rangle$  is

$$\begin{aligned} U_f^k|\varphi_0\rangle &= \sum_{i=1}^l ((\beta_1^i \cos k\theta_i - \beta_2^i \sin k\theta_i)|\varphi_1^i\rangle \\ &+ (\beta_1^i \sin k\theta_i + \beta_2^i \cos k\theta_i)|\varphi_2^i\rangle) + \sum_{i=2l+1}^{n-1} \beta_i |\varphi_i\rangle + (\pm 1)^k \beta_n |\varphi_n\rangle \end{aligned}$$

As a consequence, when the  $\beta_j^i$  are real, the amplitude of such a final state, related to the initial state  $|\varphi_0\rangle$ , is

$$\sum_{i=1}^l ((|\beta_1^i|^2 + |\beta_2^i|^2) \cos k\theta_i) + \sum_{i=2l+1}^{n-1} |\beta_i|^2 + (\pm 1)^k |\beta_n|$$

**Proof** Since  $U_f$  admits a coordinate matrix in the orthogonal group  $O(n)$ , there must exist an orthonormal basis  $\{|\varphi_1^1\rangle, |\varphi_2^1\rangle, \dots, |\varphi_1^l\rangle, |\varphi_2^l\rangle, |\varphi_{2l+1}\rangle, \dots, |\varphi_n\rangle\}$  such that the coordinate matrix of  $U_f$  with respect to such a basis is the block diagonal matrix

$$\begin{pmatrix} R_{\theta_1} & & & & & & & \\ & R_{\theta_2} & & & & & & \\ & & \dots & & & & & \\ & & & R_{\theta_k} & & & & \\ & & & & I_{n-2k-1} & & & \\ & & & & & & \pm 1 & \end{pmatrix}$$

for some angles  $\theta_1, \dots, \theta_k \in [0, 2\pi)$ , where  $R_{\theta_i} = \begin{pmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{pmatrix}$ ,  $I_{n-2k-1}$  is the identity matrix, and the sign of the last diagonal entry depends on whether  $U_f$  is a rotation or a reflection. The initial state can be written as a linear combination of the basis in the following way:

$$|\varphi_0\rangle = \sum_{i=1}^l (\beta_1^i |\varphi_1^i\rangle + \beta_2^i |\varphi_2^i\rangle) + \sum_{i=2l+1}^n \beta_i |\varphi_i\rangle$$

for some complex coordinates  $\beta_1^2, \beta_1^2, \dots, \beta_1^l, \beta_2^l, \beta_{2l+1}, \dots, \beta_n$ . Straightforward application of the same ideas of the previous proof yields the desired expression for  $U_f^k |\varphi_0\rangle$ , and  $\langle \varphi_0 | U_f^k | \varphi_0 \rangle$ . □

**Proof of Proposition 6**

1. Powers: The action of  $U_f^{n_f}$  on  $|\varphi_0\rangle$  is given by the matrix

$$\begin{pmatrix} \cos n_f \alpha & -\sin n_f \alpha \\ \sin n_f \alpha & \cos n_f \alpha \end{pmatrix}$$

. (Again, the  $n - 2$  invariant directions have been omitted.)

2. Roots: The action of  $U_f^{\frac{1}{n_f}}$  on  $|\varphi_0\rangle$  is given by the matrix

$$\begin{pmatrix} \cos \left(\frac{\alpha}{n_f}\right) & -\sin \left(\frac{\alpha}{n_f}\right) \\ \sin \left(\frac{\alpha}{n_f}\right) & \cos \left(\frac{\alpha}{n_f}\right) \end{pmatrix}$$

3. Inversion: The action of  $U_f^\dagger$  on  $|\varphi_0\rangle$  is given by the matrix

$$\begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix} = \begin{pmatrix} \cos -\alpha & -\sin -\alpha \\ \sin -\alpha & \cos -\alpha \end{pmatrix}$$

Note that in this case  $U^\dagger = U^{-1}$

4. Product: The action of  $U_f U_f'$  on  $|\varphi_0\rangle$  is given by the matrix

$$\begin{pmatrix} \cos (\alpha + \alpha') & -\sin (\alpha + \alpha') \\ \sin (\alpha + \alpha') & \cos (\alpha + \alpha') \end{pmatrix}$$

Note that in general, rotation matrices do not commute under multiplication. However, if both rotations are taken with respect to the same initial state, then they do commute. □



**Proposition 9** *Let  $m$  be a natural number, then*

$$\sum_{k=0}^m \binom{m}{k} \cos k\alpha = 2^m \left(\cos\left(\frac{\alpha}{2}\right)\right)^m \cos\left(\frac{\alpha}{2}m\right). \tag{4}$$

**Proof** We know that  $\cos(x) = \frac{e^{ix}+e^{-ix}}{2}$ . So

$$\begin{aligned} \sum_{k=0}^m \binom{m}{k} \cos k\alpha &= \sum_{k=0}^m \binom{m}{k} \frac{e^{ik\alpha} + e^{-ik\alpha}}{2} \\ &= \frac{1}{2} \left[ \sum_{k=0}^m \binom{m}{k} (e^{i\alpha})^k + \sum_{k=0}^m \binom{m}{k} (e^{-i\alpha})^k \right]. \end{aligned}$$

Now, by the binomial theorem we have that

$$\sum_{k=0}^m \binom{m}{k} (e^{i\alpha})^k + \sum_{k=0}^m \binom{m}{k} (e^{-i\alpha})^k = \left[ (1 + e^{i\alpha})^m + (1 + e^{-i\alpha})^m \right].$$

Therefore,

$$\begin{aligned} \sum_{k=0}^m \binom{m}{k} \cos k\alpha &= \frac{1}{2} \left[ (1 + e^{i\alpha})^m + (1 + e^{-i\alpha})^m \right] \\ &= \frac{1}{2} \left[ e^{i\alpha m} (1 + e^{-i\alpha})^m + (1 + e^{-i\alpha})^m \right] \\ &= \frac{1}{2} \left[ e^{i\frac{\alpha}{2}m} (1 + e^{-i\alpha})^m (1 + e^{i\alpha m}) e^{-i\frac{\alpha}{2}m} \right] \\ &= \frac{1}{2} \left[ \left( e^{-\frac{i\alpha}{2}} + e^{\frac{i\alpha}{2}} \right)^m \left( e^{\frac{i\alpha}{2}m} + e^{-\frac{i\alpha}{2}m} \right) \right] \\ &= 2^m \left(\cos\left(\frac{\alpha}{2}\right)\right)^m \cos\left(\frac{\alpha}{2}m\right). \end{aligned}$$

□

**Corollary 2** *Under the hypothesis of Proposition 8, the amplitude of the final state of the corresponding  $m$ -combinatorial QADS, related to the initial state  $|0\rangle^m |\varphi_0\rangle$ , is*

$$\sum_{i=1}^l \left( (|\beta_1^i|^2 + |\beta_2^i|^2) \cos\left(\frac{\theta_i}{2}\right)^m \cos\left(\frac{\theta_i m}{2}\right) \right) + \sum_{i=2l+1}^{n-1} |\beta_i|^2 + \delta_{+*} |\beta_n|$$

where  $* \in \{+, -\}$ , depending on whether  $U_f$  is a rotation or a reflection.

**Proof of Theorem 2** Equation (3) is a direct consequence of Propositions 2, 5, and 9. On the other hand, for the equivalences the following facts are used:

- Since the QADS is rotational, we have that  $\langle \varphi_0 | \sqrt{U_f} | \varphi_0 \rangle = \cos\left(\frac{\alpha}{2}\right)$  (applying the same proof that in Proposition 5, with  $k = \frac{1}{2}$ ).
- For a tensor QADS, we directly have  $\langle \varphi_0 | \langle \psi_0 | U_f \otimes V_f | \varphi_0 \rangle | \psi_0 \rangle = \langle \varphi_0 | U_f | \varphi_0 \rangle \langle \psi_0 | V_f | \psi_0 \rangle$ .
- For a product QADS, in terms of equality of the detecting operators, we have

$$\begin{array}{c} \boxed{\sqrt{U}} \text{---} \boxed{\sqrt{U}} \text{---} \equiv \\ \text{---} \boxed{U} \text{---} \end{array}$$

- Since the QADS is rotational, in terms of one hit detection rate, we have

$$\begin{array}{c} \boxed{\sqrt{U_f}} \text{---} \equiv \\ \boxed{\sqrt{U_f}} \text{---} \\ \text{---} \bullet \text{---} \\ \text{---} \boxed{U_f} \text{---} \end{array}$$

This is because

$$\begin{aligned} \langle \psi_0 | \langle \psi_0 | \sqrt{U_f} \otimes \sqrt{U_f} | \psi_0 \rangle | \psi_0 \rangle &= \left( \langle \psi_0 | \sqrt{U_f} | \psi_0 \rangle \right)^2 \\ &= \cos\left(\frac{\alpha}{2}\right)^2 = \frac{1 + \cos \alpha}{2} = \langle \varphi_{0c} | U_f | \varphi_{0c} \rangle \end{aligned}$$

(proof of [4][Proposition 2, item 3]).

□

**Remark 1** Note that the last equivalence of the proof holds because the QADS is rotational. In general, such an equivalence is not true. For instance, take  $U_f$  as the gate  $NOT$ .

**Proof of Corollary 1** For all  $w \in \mathbb{N}$ , let us consider any possible input  $f$  of size  $w$ . For all  $0 \leq l \leq T(w) = m \cdot S(w)$ , we have that  $z_l = \cos(l\theta_w) > 0$ , because  $0 \leq l\theta_w \leq m \cdot S(w)\theta_w \leq m\Delta < \frac{\pi}{2}$ . Consequently, for all  $0 \leq l \leq T(w)$ ,  $\arg(z_l) \in [0 - \alpha_w, 0 + \alpha_w]$ , with  $\alpha_w$  as close to zero as desired. In particular, we can take  $\alpha_w$  such that  $\frac{(1-\tilde{\delta})2^{2m}}{\cos^2 \alpha_w \binom{2m}{m}} \leq 1 - \delta$ , because

$$1 - \delta > 1 - 2\delta = 2\sqrt{m}(1 - \tilde{\delta}) \geq \frac{2^{2m}}{\binom{2m}{m}} \cdot (1 - \tilde{\delta})$$

and  $\cos^2 \alpha_w$  can be made as close as needed to 1. The result now follows from Proposition 4. □

## References

1. Aaronson, S., Rall, P.: Quantum approximate counting, simplified. In: Symposium on Simplicity in Algorithms, pp. 24–32. SIAM (2020)
2. Aharonov, D., Jones, V.: A polynomial quantum algorithm for approximating the jones polynomial. *Algorithmica* **5**(3), 395–421 (2009)
3. Ambainis, A., Kempe, J., Rivosh, A.: Coins make quantum walks faster. In: Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA '05, pp. 1099–1108. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA (2005)
4. Combarro, E.F., Ranilla, J., Rúa, I.F.: Quantum abstract detecting systems. *Q. Inf. Process.* **19**(8), 258 (2020). <https://doi.org/10.1007/s11128-020-02763-w>
5. Deutsch, D., Jozsa, R.: Rapid solution of problems by quantum computation. *Proc. Royal Soc. London A: Math. Phys. Eng. Sci.* **439**(1907), 553–558 (1992)
6. Grinko, D., Gacon, J., Zoufal, C., Woerner, S.: Iterative quantum amplitude estimation. *npj Q. Inf.* **7**(1), 1–6 (2021)
7. 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, pp. 212–219. ACM, New York, NY, USA (1996)
8. Mohammadbagherpoor, H., Oh, Y.H., Singh, A., Yu, X., Rindos, A.J.: Experimental challenges of implementing quantum phase estimation algorithms on ibm quantum computer. arXiv preprint [arXiv:1903.07605](https://arxiv.org/abs/1903.07605) (2019)
9. Nakaji, K.: Faster amplitude estimation. arXiv preprint [arXiv:2003.02417](https://arxiv.org/abs/2003.02417) (2020)
10. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information, 10th edn. Cambridge University Press, Cambridge (2011)
11. O'Brien, T.E., Tarasinski, B., Terhal, B.M.: Quantum phase estimation of multiple eigenvalues for small-scale (noisy) experiments. *New J. Phys.* **21**(2), 023022 (2019)
12. Portugal, R.: Quantum Walks and Search Algorithms. Springer, New York (2013)
13. Rall, P.: Faster coherent quantum algorithms for phase, energy, and amplitude estimation. arXiv preprint [arXiv:2103.09717](https://arxiv.org/abs/2103.09717) (2021)
14. Santos, R.A.M.: Szegedy's quantum walk with queries. *Q. Inf. Process.* **15**(11), 4461–4475 (2016)
15. Suzuki, Y., Uno, S., Raymond, R., Tanaka, T., Onodera, T., Yamamoto, N.: Amplitude estimation without phase estimation. *Q. Inf. Process.* **19**(2), 1–17 (2020)
16. Szegedy, M.: Quantum speed-up of markov chain based algorithms. In: Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, FOCS '04, pp. 32–41. IEEE Computer Society, Washington, DC, USA (2004)
17. Wie, C.R.: Simpler quantum counting. arXiv preprint [arXiv:1907.08119](https://arxiv.org/abs/1907.08119) (2019)
18. Wong, T.: Equivalence of Szegedy's and coined quantum walks. *Quantum Inf Process* **16**(215), 1–15 (2017)

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