Noname manuscript No.
(will be inserted by the editor)

Quantum Abstract Detecting Systems

Elías F. Combarro · José Ranilla ·
Ignacio Fernández Rúa

Received: date / Accepted: date

Abstract In this paper, we study Quantum Abstract Detecting Systems (QADS), that generalize some key characteristics of the operators used in Grover's algorithm, a wide variety of quantum walks and the quantum abstract search algorithm. A QADS is an algorithm that constructs a quantum state and a quantum operator that help testing whether a circuit-implemented boolean function f is identically zero. We also identify some relatively weak properties of QADS that lead to the construction of algorithms for the detection problem (i.e. determining whether there is a marked element in a given set). Our results provide not only a common framework to all the aforementioned search methods, and their transformation into algorithms for the detection problem, but also allow the development of new similar methods. As an example, we construct a modification of Grover's algorithm (from the tensor product of controlled QADS) that shows improved detection probability

Keywords Quantum Detection · Quantum Search · Quantum Walks · Grover Search

1 Introduction

It is well-known that quantum computation outperforms classical computation when *searching* in an unsorted database, i.e., finding a *marked* element in a

E.F. Combarro
Computer Science Department, University of Oviedo
E-mail: efernandezca@uniovi.es

J. Ranilla
Computer Science Department, University of Oviedo
E-mail: ranilla@uniovi.es

I.F. Rúa
Mathematics Department, University of Oviedo
E-mail: rua@uniovi.es

list of unordered ones. The first quant quantum algorithm solving this problem was Grover's algorithm [9], where the elements of the list are marked by the evaluation of a boolean function f (i.e., x is marked iff $f(x) = 1$). A quantum oracle O evaluating such a function f is combined with an amplitude amplification operator G for marked elements, to achieve quadratic speed-up over the best classical algorithm on the oracle model. Namely, given the function f, Grover's algorithm constructs a uniform superposition *initial state* $|\psi_0\rangle$, 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 yields a marked element with high probability.

A related problem is that of *detecting* the existence of marked elements. It is clear that if an element is found by a searching algorithm, the detection problem is implicitly solved. However, there are some situations where finding a particular marked element is not strictly necessary. For instance, when studying the commutativity of an algebra described by a multiplication table it is enough to detect the existence of a nonmatching pair of constants to guarantee that the algebra is noncommutative [4]. In this context, Grover's quantum operator can be used as a *detecting operator* of the existence of marked elements, i.e., to determine whether f is identically zero or not. The key observation is that, when f is zero, the initial state is one of the fixed eigenvectors of the operator U. Repeated hits of U leave invariant the initial state, and so measurement yields such a state with certainty. On the other hand, when f is not zero, the operator U does not fix the initial state, and so measurement after a certain number of hits gives $|\psi_0\rangle$ with small probability. These two facts can be used to distinguish the case when f is zero or not, solving the detection problem (the details can be found in Appendix A).

Quantum walks are also a family of algorithms that solve the search problem. In these algorithms, a connected, non-directed, non-bipartite graph (V, E) is taken, with some of its vertices marked by a boolean function f. The edges of the graph are walked by reflection operators. In the case of Szegedy's quantum walk [15], reflection operators are taken around vertices involving marked vertices. In the case of Santos' quantum walk ("with queries"), the reflection operators (around all the edges in the graph), are combined with the quantum oracle O. When the graph is a $2D$ grid it can be walked by a "lackadaisical" quantum walk [16]. This means that the reflection operators not only reflect around edges in the graph, but also around self-loops over every vertex. In any case, the following pattern is common to all the previous quantum walks: the *initial state* $|\psi_0\rangle$ (of an uniform superposition of edges in the graph), is repeatedly hit by a quantum operator U (product of the reflection operators and the quantum oracle O). Measurement of the resulting state yields an edge involving a marked vertex, with high probability. Just like with Grover's search, this algorithm can be adapted to *detect* marked elements (see [15, Section 9]). The relevant fact is again that, when no marked vertices exist, the initial state $|\psi_0\rangle$ is one of its fixed eigenvectors. So, repeated hits of the *detecting operator* U leave such a state invariant, a property that can be checked upon measurement. Again, the details of these constructions can be found in Appendix A.

Some of the previous quantum search algorithms fit into the general machinery of the quantum abstract search [2]. In this setting, an initial *initial state* $|\psi_{start}\rangle$ is hit by a unitary operator U, which is the product of a reflection operator around an aimed state $|\psi_{good}\rangle$ (which is usually a uniform superposition of marked elements of the computational basis), and a second map which only fixes the initial state. This property, together with the fact that the reflection operator is the identity when no marked elements exist, allows to use the operator U as a *detecing operator*, as above. On the other hand, as noticed in [16], the laickadaisical quantum walk based on the Grover oracle can not be explained in terms of the quantum abstract search. However, we will see that it fits into the theory developed in the present paper.

So, we can see that these searching methods can be specifically adapted for the detection problem. In all cases, the key feature is the invariance of the initial state when no marked elements exist. This was repeatedly noticed in our works on quantum algorithms for the commutativity of an algebra (based on Grover's algorithm [4], adiabatic computation [5] and quantum walks [6]). Actually, quantum abstract detecting systems (QADS) were first introduced in the later reference. In this paper, we study such systems, identifying relatively weak properties that lead to the construction of algorithms for the detection problem. Our results provide not only a common framework to all the aforementioned search methods, and their transformation into algorithms for the detection problem, but also allow the development of new similar methods. As an example, we construct a modification of Grover's algorithm (from the tensor product of controlled QADS) with improved detection probability. This shows that our abstraction goes beyond a simple theoretical development, and that it may have an impact on developing actual combinations of detecting methodologies in practice.

The outline of the paper is as follows. In Section 2 we introduce the definition of a quantum abstract detecting system, and relate it to well-known procedures that solve the detection (or searching) problem. Section 3 is devoted to transformations that allow the construction of new QADS from others. The properties required for a QADS to be of practical use are collected in Section 4, whereas a detecting scheme based on them, and some computational experiments are given in Section 5. Conclusions and future work are given in Section 6. The appendices contain detailed examples of QADS, and detailed proofs of the results stated in the main text.

2 Quantum Abstract Detecting Systems

Motivated by our study of commutativity of algebras using quantum walks, quantum abstract detecting systems were introduced in [6, Section 4].

Definition 1 A *quantum abstract detecting system (QADS)* is any (classical deterministic) algorithm that takes, from a set of inputs $\mathcal{M}$, a boolean function (given by a circuit) $f : \{0,1\}^k \to \{0,1\}$ and outputs a unitary transformation $U = U(f)$ on a Hilbert space $\mathcal{H}$ whose dimension only depends on k, together with a state $|\psi_0\rangle \in \mathcal{H}$ (that only depends on k too) such that

$$\{x \in \{0,1\}^k \mid f(x) = 1\} = \emptyset \Longrightarrow U|\psi_0\rangle = |\psi_0\rangle$$

The transformation U will be called *detecting operator* and $|\psi_0\rangle$ is known as the *initial state.*

The rationale behind this definition is as follows. The QADS provides the necessary tools to solve a detection problem in a quantum setting, namely the detecting operator and the initial state. Such a detection problem is instantiated by the boolean function $f \in \mathcal{M}$, which should be understood as an indicator function of the subset $W := \{x \in \{0,1\}^k \mid f(x) = 1\}$ of *marked* vertices. The output of the algorithm, i.e., the detecting operator U is to be used repeatedly in a detecting scheme (see Section 5 below) to iteratively generate a final state $U^t|\psi_0\rangle = |\psi_t\rangle$. The nonemptiness of W is detected by testing the departure of such a final state from $|\psi_0\rangle$.

As seen in the Introduction, Grover's search algorithm, quantum walks (both Szegedy's, Santos' or Wong's), and the quantum abstract search, can be seen as QADS. A thorough description of this fact can be found in Appendix A. In all these QADS, the input set $\mathcal{M}$ contains all boolean functions. This is the usual case. However, there are some situations in which restrictions on $\mathcal{M}$ may apply. This is the case of algorithms solving promise problems, like Deutsch-Jozsa, that can be covered with our definition, too (the details of this fact are given in Appendix A). The only conditions required of the set $\mathcal{M}$ are that it is infinite (i.e., there is no $K \in \mathbb{N}$ such that every boolean function f belonging to $\mathcal{M}$ has domain $\{0,1\}^k$ with $k \leq K$), and that if $f : \{0,1\}^k \to \{0,1\} \in \mathcal{M}$, then the zero constant function with domain $\{0,1\}^k$ also belongs to $\mathcal{M}$. These conditions guarantee that the addressed detecting problem is not trivial. Observe, also, that the quantum abstract detecting systems, as introduced in [6, Section 4], have to be understood as the ouput of a QADS, for a particular instantiation of the input set $\mathcal{M}$.

As a final example of QADS, we have any algorithm generating just the oracle of Grover's or the abstract quantum search, or of Santos' or Wong's quantum walks, together with the corresponding initial state. However, it seems reasonable to assume that in order for these systems to effectively detect the existence of marked elements, some kind of amplification is required (the operators that have been dropped in this new setting). This is the reason why we want to consider properties of a QADS in terms of constructibility, efficiency and detection rate. This will be accomplished in Section 4.

3 Algorithmic closure of QADS

In this section, we consider different procedures that allow to derive new QADS from others. These algorithmic transformations preserve the class of QADS, and so we can talk of an algorithmic closure of QADS. In particular, fixed an initial state $|\psi_0\rangle$, the corresponding detecting operators (for any possible QADS) form a group under the product. Moreover, such a group is a subgroup of the stabiliser of the initial state. 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 formal description of these transformations, and the proof of their preservation of QADS, can be found in Appendix B. Their description as quantum circuits and operators is given in Table 1.

There are some other "natural" transformations which do not preserve the closure of QADS. This is the case of the scalar multiplication. For instance, if O is a Grover oracle, then iO can never be the unitary operator output of a QADS since it has no eigenvalue equal to 1.

Observe than some of the previous transformations overlap, like the extension of a QADS, which can be also regarded as a tensor product of the QADS with the trivial QADS (Figure 1).

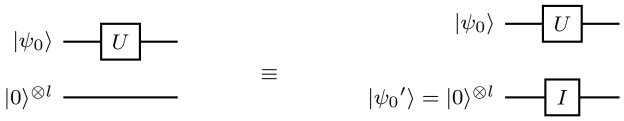


Fig. 1 Equivalent transformations in the algorithmic closure of a QADS

On the other hand, combination of several of such algorithmic closure procedures yield new constructions of QADS, like the *phase doubly controlled* QADS. This QADS combines a rotation around the $Y-$axis, $R_y(\theta)$, and a doubly controlled QADS, in the following way: $(R_y(\theta) \otimes I)^\dagger (U \otimes U')_{dc}(R_y(\theta) \otimes I)$ (the initial state is $|0\rangle|\psi_0\rangle|\psi_0{}'\rangle$) (Figure 2).

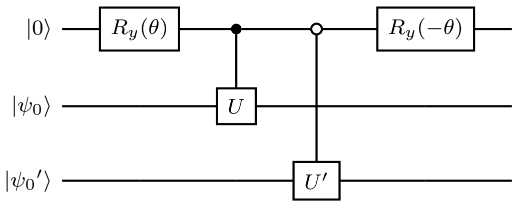


Fig. 2 Phase doubly controlled QADS

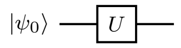
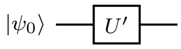
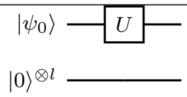
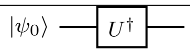
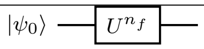
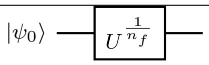
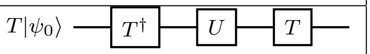
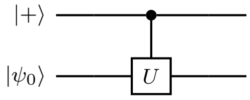
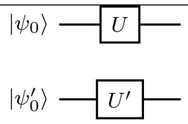
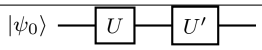
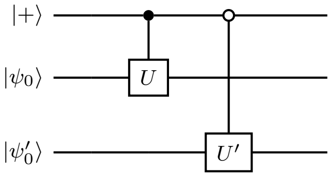
Name	Initial state	Detecting operator	Circuit
QADS#1 QADS#2	$\vert\psi_0\rangle$ $\vert{\psi_0}'\rangle$	U U'	 
Extension	$\vert\psi_0\rangle\vert 0\rangle^{\otimes l}$	$U \otimes I$	
Inversion	$\vert\psi_0\rangle$	$U^\dagger$	
Powers	$\vert\psi_0\rangle$	U^{n_f}	
Roots	$\vert\psi_0\rangle$	U^{1/n_f}	
Conjugation	$T\vert\psi_0\rangle$	$TUT^\dagger$	
Controlled	$\vert+\rangle\vert\psi_0\rangle$	$U_c\vert i\rangle\vert x\rangle = \vert i\rangle U^i\vert x\rangle$	
Tensor product	$\vert\psi_0\rangle\vert{\psi_0}'\rangle$	$U \otimes U'$	 $\vert\psi_0\rangle$ U $\vert\psi_0'\rangle$ U'
Product	$\vert\psi_0\rangle(= \vert{\psi_0}'\rangle)$	$U'U$	
Doubly controlled	$\vert+\rangle\vert\psi_0\rangle\vert{\psi_0}'\rangle$	$U_{dc}\vert i\rangle\vert x\rangle\vert x'\rangle = \vert i\rangle U^i\vert x\rangle U'^{1-i}\vert x'\rangle$	 $\vert+\rangle$ $\vert\psi_0\rangle$ U $\vert\psi_0'\rangle$ U'

Table 1 Transformations in the algorithmic closure of a QADS

Finally, let us notice that the fact that the tensor product of QADS is a QADS is possible because the condition $U|\psi_0\rangle = |\psi_0\rangle$ is necessary for (but not equivalent to) $W = \emptyset$, i.e., to the non-existence of marked elements. Relaxing the condition from the original definition of QADS given in [6, Section 4], allows for the construction of new QADS from other ones, such as the tensor product just mentioned.

4 Properties of QADS

In this section we introduce desirable properties for a QADS to be of practical interest. Namely, the QADS should be realized in a reasonable amount of time (*efficient constructibility*), and it should have a detection rate asymptotically independent of the input size (*constant detection rate*). The way these properties fit into the machinery of a detecting scheme will be addressed in the next section.

4.1 Efficient constructibility

The first property required of QADS is efficient constructibility of its output. The description of both the input and the output functions is given in terms of circuits. Namely, the input boolean function f can be described by a classical circuit, involving a set of classical universal gates, such as NAND. Such a description is usually provided as a directed acyclic graph, and so the input size n of f upper bounds k, the number of variables of f. The finiteness of the set of classical gates of a given size guarantees that any two descriptions of f are linear one in another.

On the other hand, the unitary transformation U can be described in terms of a quantum circuit that is to be constructed by the QADS from the classical circuit f. Moreover, the QADS must provide an actual construction of the initial state $|\psi_0\rangle$ from the $|\mathbf{0}\rangle$ state of $\mathcal{H}$ in terms of a quantum circuit. The quantum gates of both circuits are to be taken from a universal gate set, such as for instance single qubit and CNOT gates [12, Section 4.5.2]. Because of the Solovay-Kitaev theorem [12, Appendix 3], the actual choice $\mathcal{F}$ of such a universal set is irrelevant, since any unitary transformation of another universal gate set can be approximated to a desired precision ϵ using $\Theta(\log^c(1/\epsilon))$ gates from $\mathcal{F}$ (where $c \approx 2$).

For any QADS to be of practical use, it seems reasonable that both the unitary operator and the initial state $|\psi_0\rangle$ should be computed in polynomial time in the input size n. This is measured by the width and depth of the circuit implementing the detecting operator, together with the number of gates involved.

Definition 2 We shall say that a QADS is *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.

Observe that, if a QADS is efficiently contructible then, in particular, the Hilbert state $\mathcal{H}$ containing the initial state $|\psi_0\rangle$ must be isomorphic to a tensor product of $O(\text{poly}(n))$ copies of $\mathbb{C}^2$.

Examples of efficient constructible QADS include that of Grover's algorithm, Szegedy's quantum walk, and Deutsch-Jozsa's algorithm. Also, algorithmic closure procedures such as extension, inversion, powers, conjugation, tensor product, and (double) controlling, are efficiently constructible as long as the original QADS are. A concrete example of a non-efficiently constructible QADS (unless $P = NP$) is given in Appendix C, together with details on the previous examples.

4.2 Constant detection rate and efficient detection

The second property of interest for a QADS is having a constant detection rate, which is related to the usefulness of a QADS in terms of the detection capability that will be addressed in the next section. The definition of a constant detection rate was introduced in [6, Section 4], and it is the natural extension of Szegedy's quantum hitting time [15, Section 8]. Next, we explore such notion, and introduce the concept of efficient detection.

Definition 3 Let $(|\psi_0\rangle, U = U(f))$ be the output of a QADS on input $f \in \mathcal{M}$. Given $0 < \delta \leq 1$, we shall say that $T : \mathbb{N} \to \mathbb{N}$ is a *δ-quantum detecting time for the QADS* (or, simply, T is δ-detecting for the QADS) if for all nonzero $f \in \mathcal{M}$ of input size k

$$\frac{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T(k)+1} \leq 1 - \delta.$$

Notice that the function of detecting time T depends on the input size of the function f and not, like in the case of efficient constructibility, of n (the size of f itself). This is due to the fact that the QADS provide an output that encapsulates in quantum terms the function f. In this sense, the overall complexity of the detecting scheme that will be given in Section 5 is given by the cost of preparing the initial state and the detecting operator (i.e., the running time of the QADS) plus the depth of the circuit for $U^{T(k)}$ (i.e, $T(k)$ times the depth of the circuit implementing U).

Clearly, a first example of QADS for which no function $T : \mathbb{N} \to \mathbb{N}$ can be $\delta-$detecting is the identity QADS. A nontrivial QADS with the same property, and a QADS with a constant $\delta-$detecting function are given in Appendix D. Another QADS which has a constant $\delta-$detecting function (in this case $T(k) = 1$) is the QADS of Deutsch-Jozsa's algorithm. The QADS of Grover's algorithm can be shown to have a $\frac{\sqrt{2}-1}{4\sqrt{2}}-$detecting function of order $O(\sqrt{2^k})$, when only one marked element exists. QADS from quantum walks have also $\delta-$detecting functions. For instance, that of Szegedy's quantum walk has a $\frac{1}{4}-$detecting function of order $O\left(\frac{1}{\sqrt{\theta(P)}}\right)$, where $\theta(P)$ is the eigenvalue gap of the matrix P associated with the graph. The non-controlled QADS of the same quantum walk has a $\frac{1}{4}-$detecting function for the complete graph. Finally, the controlled QADS of Santos' quantum walk has a $\frac{1}{24}-$detecting function.

With respect to the procedures in the algorithmic closure of QADS, the detecting time is generally well-behaved. For instance, the extension, inversion and conjugation QADS preserve the $\delta-$detecting time. Other QADS, such as the root, (doubly) controlled or tensor product of QADS, have the same quantum detection time, but for different δ. However, observe that the product of QADS does not preserve the detecting time, since T is simultaneously $\delta-$detecting time for a QADS and its inversion, but their product is the identity QADS, that has no detecting time. Appendix D contains the proofs of all the facts stated above. There, a relation between the $\delta-$detecting time and the quantum hitting time of quantum walks, can be found too.

5 Detection with a QADS

In this section, the usefulness of QADS is made apparent, and an actual algorithm for detection is introduced. The main idea is to use the QADS to provide the initial state and an operator to repeatedly evolve it, in a decision procedure to detect the existence of marked elements (i.e., existence of x such such that $f(x) = 1$). The properties of QADS presented in the previous section translate into properties of efficiency of the corresponding detecting procedure. The algorithm, whose circuit version is given in Figure 3, is as follows (Algorithm 1).

```
Algorithm 1 (Detection scheme)
INPUT: A QADS Q, a boolean function $f : \{0,1\}^k \to \{0,1\}$ from the set of inputs $\mathcal{M}$ of the QADS, and a natural number $T$.
PROCEDURE:
- PRECOMPUTATION of the initial state $|\psi_0\rangle$ and the detecting operator $U$ with $Q$ on input $f$.
- COMPUTATION:
        - Choose $t$ uniformly in the set $\{0, 1, \ldots, T\}$
        - Compute $|\psi_t\rangle = U^t|\psi_0\rangle$.
-MEASUREMENT of $|\psi_t\rangle$ on an orthonormal basis containing $|\psi_0\rangle$.
OUTPUT:
- NO: If the measurement is the initial state $|\psi_0\rangle$.
- YES: Otherwise.
```

The correctness and properties of this algorithm are given in the main theorem of this paper (Theorem 1).

Theorem 1 (Main) *The detection scheme 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*

$$\frac{\sum_{t=0}^{T} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T+1}$$

Therefore, if a QADS is both efficiently constructible and has $\delta-$detecting time, then the detection scheme can be run in $O(poly(n))$ precomputation time, and the detection problem can be solved by a one-side error quantum algorithm with error at most δ. The probability of success of the algorithm is $1 - \frac{\sum_{t=0}^{T} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T+1}$.

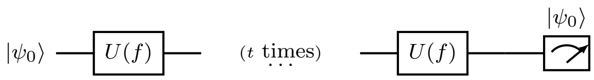


Fig. 3 Circuit of the detection scheme of a QADS

Because of the theorem (whose proof can be found in Appendix E), the actual usefulness of a particular QADS has to be analized in terms of a trade-off between the precomputation cost and the number of iterations. Recall from the previous section that the overall complexity of the detecting scheme is the cost of preparing the initial state and the detecting operator (i.e., the running time of the QADS) plus the depth of the circuit for $U^{T(k)}$ (i.e, $T(k)$ times the depth of the circuit implementing U). For instance, the QADS of Grover search provides efficient constructibility and a detection time of order $O(\sqrt{2^k})$, which is optimal among the class of quantum algorithms that do not look into the oracle. On the other hand, the QADS of Example 8 (Appendix C) provides constant detecting time, but the precomputation of the detecting operator encapsulates the cost of finding a solution to the detection problem.

We comment in Appendix E on the relation between the detecting scheme for QADS and the one given in [15] for quantum walks. Here, we make a further observation on the detecting scheme average error probability when the detecting operator matrix and the amplitudes of the initial state are real. Assuming that $\langle\psi_0|U^t|\psi_0\rangle$ is uniformly distributed in the interval $[-1, 1]$, the expected value of the error probability is $\int_{-1}^{1} \frac{1}{2}x^2dx = \frac{1}{3}$. If the detecting operator is controlled (see Table 1), because of the proof of Proposition 2 (Appendix D), we know that the expected value of the detecting scheme based on the controlled QADS is $\int_{-1}^{1} \frac{1}{2}\left(\frac{1+x}{2}\right)^2 dx = \frac{1}{3}$, and so both QADS provide the same expected success probability.

However, there is a difference between the uncontrolled and the controlled QADS. While the probability mass of error of the former is symmetrically distributed among positive and negative values, the probability mass of the later is skewed towards the positive ones. Thus, if U is the detecting operator

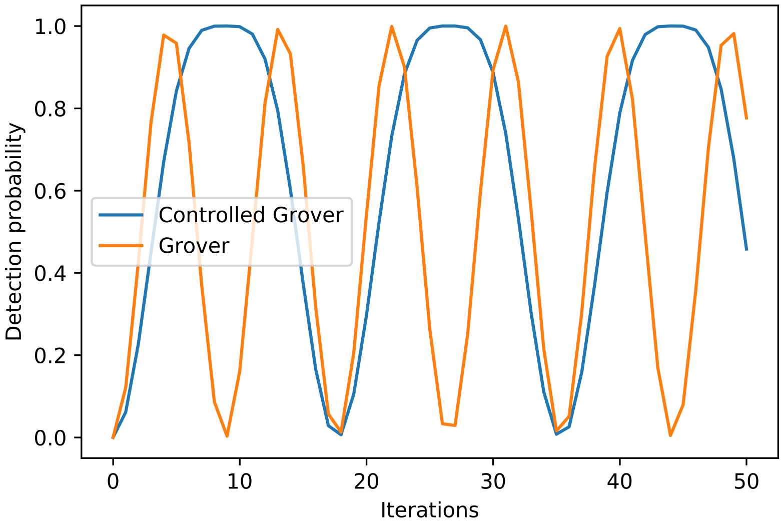


Fig. 4 Probability of detection for a fixed number of iterations with Grover and controlled Grover QADS. Just one out of 32 elements is marked

of an uncontrolled QADS, when $\langle\psi_0|U^t|\psi_0\rangle$ is close to -1 we will have a low probability of detecting with t iterations, while the controlled version of the QADS will correctly detect with high probability.

Figure 4 illustrates such a fact by showing the probability of detecting after exactly $t \in \{0, \ldots, 50\}$ iterations with operator U of Grover's search QADS and with the corresponding controlled version in a situation in which exactly 1 out of $32 = 2^5$ elements is marked. Notice that there are several regions in which the success probabilities are complementary. In fact, the zones in which the controlled version of Grover outperforms the uncontrolled Grover are those in which $\langle\psi_0|U^t|\psi_0\rangle$ is negative.

One might wonder if controlling a controlled operator might provide some advantages for other QADS. The expected value of the error probability for this double-controlled operator is $\int_{-1}^{1} \frac{1}{2}\left(\frac{1+\frac{1+x}{2}}{2}\right)^2 dx = \frac{7}{12}$, which provides a higher error probability than the previous ones. Further controlling provides increasing error rates, namely $\frac{37}{48}, \frac{169}{192}, \frac{721}{768}, \frac{2977}{3072}, \frac{12097}{12288}$, and so this approach must be dropped.

However, the complementarity shown in Figure 4 can be exploited in order to obtain higher detection probabilities in Algorithm 1 by using tensor products of QADS. In Figure 5, we show the success probability of the detection scheme (that is, $1 - \frac{\sum_{t=0}^{T} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T+1}$) when used with QADS whose detecting operators are constructed from Grover's search QADS. Namely, we consider the original Grover operator, the controlled Grover operator and their three

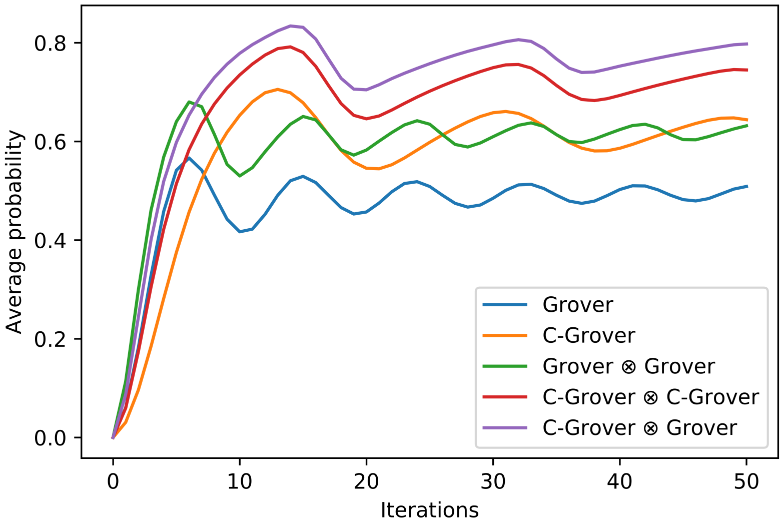


Fig. 5 Probability of success with the detection scheme (Algorithm 1) with Grover, controlled Grover QADS and their tensor products. We consider 32 elements, one of which is marked

possible tensor products (Grover ⊗ Grover, Controlled-Grover ⊗ Controlled-Grover and Controlled-Grover ⊗ Grover). Again, we study the situation in which we have 32 elements, exactly one of which is marked (but the results are similar with other sizes). As it can be seen, the tensor products involving controlled Grover achieve higher success probabilities than the other methods, with the product of Grover and its controlled version (which, as we have pointed out, are complementary in some regions) getting the best overall results. This shows that the methods that we have introduced in this paper can be applied to construct new algorithms that improve the detection probability of existing algorithms (possibly at the cost of increasing the dimension of the Hilbert space).

6 Conclusions and future work

In this paper, we have introduced a general framework for dealing with detection problems in a quantum computation setting. The notion of a QADS (Quantum Abstract Detecting System) generalises many techniques proposed in the literature, including Grover and quantum walks searches, by focusing on the fundamental and common aspects of such procedures. Using this abstract approach, we detach from the particular characteristic of the different methods, and so we can uniformly focus on their computational values: efficient constructibility and detecting time. Based on this general approach, we have been able to introduce a series of operations that preserve the class of QADS. These operations carry out new detecting schemes based on known ones. Some of them might yield better computational performance, as exemplified by the tensoring of Grover and Grover-controlled QADS. As future projects, we consider providing a unifying setting for other quantum computing techniques (such as for instance quantum error-correcting codes), giving an abstract explanation of the algorithmic closures of QADS in categorical terms, and studying specific families of QADS (such as combinatorial QADS [10]).

Acknowledgments

The authors thank the referees for carefully reading our manuscript, and for giving such constructive comments which substantially helped improving the quality of the paper. 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.

A Detailed examples of QADS

In this appendix, we provide detailed examples of algorithms and procedures that can be seen as QADS.

Example 1 (Grover search [9]) Given an arbitrary boolean function $f : \{0,1\}^k \to \{0,1\}$, Grover's algorithm requires a state space $\mathcal{H} = (\mathbb{C}^2)^{\otimes k}$ to look for marked elements (i.e., those in $W = \{x \in \{0,1\}^k \mid f(x) = 1\}$), and the initial state $|\psi_0\rangle$, which is the superposition of all the elements of the computational basis $\frac{1}{\sqrt{2^k}} \sum_{x=0}^{2^k-1} |x\rangle$. The search iterates two operators that can be effectively constructed, namely:

- Oracle: $O(|x\rangle) = (-1)^{f(x)}|x\rangle$, i.e., $O = I - 2\sum_{x\in W} |x\rangle\langle x|$.
- Diffusion operator: $G = 2|\psi_0\rangle\langle\psi_0| - I$

The algorithm which constructs $U := GO$ from f is a QADS because $U|\psi_0\rangle = |\psi_0\rangle$ if and only if

$$\frac{1}{\sqrt{2^k}}\left(\sum_{x\notin W} |x\rangle - \sum_{x\in W} |x\rangle\right) = O|\psi_0\rangle = G^{-1}|\psi_0\rangle = G|\psi_0\rangle = |\psi_0\rangle$$

which is equivalent to $W = \emptyset$.

Example 2 (Szegedy's quantum walk [15]) Let $(V \subseteq \{0,1\}^k, E)$ be a connected, non-directed, non-bipartite graph. Szegedy's quantum search requires a state space $\mathcal{H} \subseteq (\mathbb{C}^2)^{\otimes 2k}$ with basis $\{|x\rangle|y\rangle \mid x, y \in V\}$ representing potential edges of the graph. If for any $x \in V$, the set of adjacent vertices $y \in Y$ is denoted by $A_x = \{y \in Y \mid \{x,y\} \in E\}$, then the (doubly stochastic) matrix associated with the graph is $P \in \mathcal{M}_{|V|\times|V|}(\mathbb{R})$ given by

$$P_{xy} = \begin{cases} \frac{1}{|A_x|} & \text{if } y \in A_x \\ 0 & \text{otherwise} \end{cases}$$

Searching for vertices marked according to a boolean function $f : \{0,1\}^k \to \{0,1\}$ (i.e., those in $W = \{x \in V \mid f(x) = 1\}$), requires the matrix associated with the leaking graph (i.e, the directed graph obtained from V converting all outer arcs from a marked vertex in a loop):

$$P^W_{xy} = \begin{cases} P_{xy} & \text{if } x \notin W \\ \delta_{x,y} & \text{otherwise} \end{cases}$$

The initial state $|\psi_0\rangle$ is the weighted superposition of the potential graph edges

$$\frac{1}{\sqrt{|V|}} \sum_{x \in V} \frac{1}{\sqrt{|A_x|}} \sum_{y \in A_x} |x\rangle|y\rangle$$

and the quantum walk iterates the following two reflection operators:

- $R^W_A = 2\sum_{x\in V} |\Phi^W_x\rangle\langle\Phi^W_x| - I$, where $|\Phi^W_x\rangle = |x\rangle \otimes \left(\sum_{y\in V} \sqrt{P^W_{xy}}|y\rangle\right)$
- $R^W_B = 2\sum_{y\in V} |\Psi^W_y\rangle\langle\Psi^W_y| - I$, where $|\Psi^W_y\rangle = \left(\sum_{x\in V} \sqrt{P^W_{xy}}|x\rangle\right) \otimes |y\rangle$

If $|\Phi_x\rangle = |x\rangle \otimes \left(\sum_{y\in V} \sqrt{P_{xy}}|y\rangle\right)$, $|\Psi_y\rangle = \left(\sum_{x\in V} \sqrt{P_{xy}}|x\rangle\right) \otimes |y\rangle$, then observe that $|\psi_0\rangle = \frac{1}{\sqrt{|V|}}\sum_{x\in V}|\Phi_x\rangle = \frac{1}{\sqrt{|V|}}\sum_{y\in V}|\Psi_y\rangle$, and that $|\Phi^W_x\rangle = \begin{cases} |x\rangle|x\rangle & \text{if } x \in W \\ |\Phi_x\rangle & \text{if } x \notin W \end{cases}$. Moreover, since the graph has no loops, $\{|\Phi_x\rangle\}_{x\in V} \cup \{|x\rangle|x\rangle\}_{x\in W}$ is an orthonormal family, and so

$$R^W_A(|\psi_0\rangle) = \frac{1}{\sqrt{|V|}} \left(\sum_{x\in V\setminus W} |\Phi_x\rangle - \sum_{x\in W} |\Phi_x\rangle \right) = \frac{1}{\sqrt{|V|}} \sum_{x\in V} (-1)^{f(x)} |\Phi_x\rangle$$

(an analogous property holds for R^W_B). Both R^W_A and R^W_B can be algorithmically constructed from f, and so the algorithm which computes $U := R^W_B R^W_A$ is a QADS (with respect to the graph (V, E)), since

$$\begin{aligned} U|\psi_0\rangle = |\psi_0\rangle &\iff R^W_B|\psi_0\rangle = R^W_A|\psi_0\rangle \\ \iff \frac{1}{\sqrt{|V|}} \sum_{y\in V} (-1)^{f(y)}|\Psi_y\rangle &= \frac{1}{\sqrt{|V|}} \sum_{x\in V} (-1)^{f(x)}|\Phi_x\rangle \\ \iff \frac{1}{\sqrt{|V|}} \sum_{x,y\in V} (-1)^{f(y)}\sqrt{P_{xy}}|x\rangle|y\rangle &= \frac{1}{\sqrt{|V|}} \sum_{x,y\in V} (-1)^{f(x)}\sqrt{P_{xy}}|x\rangle|y\rangle \end{aligned}$$

which is true when $f \neq 0$.

Example 3 (Santos' quantum walk [13]) Since this procedure is Sgezedy's quantum walk with queries, the set up for both methods is the same. The difference consists in that in Santos' quantum walk the leaking graph is no longer used, and Grover's oracle is used instead. Namely, the following operators are iterated:

- Oracle: $O \otimes I$
- Reflection $R_A = 2\sum_{x\in V} |\Phi_x\rangle\langle\Phi_x| - I$
- Reflection $R_B = 2\sum_{y\in V} |\Psi_y\rangle\langle\Psi_y| - I$

Any algorithm computing $U := R_B R_A O$ is a QADS because $R_A|\psi_0\rangle = |\psi_0\rangle = R_B|\psi_0\rangle$ and so

$$U|\psi_0\rangle = |\psi_0\rangle \iff (O \otimes I)|\psi_0\rangle = |\psi_0\rangle \iff$$

$$\frac{1}{\sqrt{|V|}} \left(\sum_{x\in V\setminus W} |x\rangle - \sum_{x\in W} |x\rangle \right) \otimes \left(\sum_{y\in V} \sqrt{P_{xy}}|y\rangle \right) = \frac{1}{\sqrt{|V|}} \sum_{x\in V} |x\rangle \otimes \left(\sum_{y\in V} \sqrt{P_{xy}}|y\rangle \right)$$

which is equivalent to $W = \emptyset$.

Example 4 (Quantum abstract search [2]) Let $\mathcal{H} = (\mathbb{C}^2)^{\otimes k}$ be a state space containing two states $|\psi_0\rangle$ (with real amplitudes) and $|\psi_{good}\rangle$. In the quantum abstract search the later is the aim state to be found from the former. Two unitary transformations are used:

- $U_1 = I - 2|\psi_{good}\rangle\langle\psi_{good}|$
- U_2: described by a real unitary matrix such that $|\psi_0\rangle$ is the only eigenvector (up to phase change) with eigenvalue 1.

Because of the characteristics of such operators, non-orthogonality of the initial and the "good" states is implicitly assumed. For instance, $|\psi_0\rangle$ is usually taken as the uniform superposition of all basic states, and $|\psi_{good}\rangle$ is in the computational basis. In our detection setting, we allow $|\psi_{good}\rangle$ to be the zero state, corresponding to the non-existence of marked elements. Also, from the point of view of a detecting problem, the "good" states $\sqrt{\frac{5}{6}}|0\rangle + \sqrt{\frac{1}{6}}|1\rangle$ and $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ behave similarly, as the key feature is that both are nonzero and they have the same supporting computational basis elements. Therefore, we shall assume that $|\psi_{good}\rangle$ is a uniform superposition of computational states.

With this setting in mind, let $f : \{0,1\}^k \to \{0,1\}$ be an arbitrary boolean function. Any algorithm taking f as an input that outputs a constructible initial state $|\psi_0\rangle$ and the constructible operator $U := U_2U_1$ where $|\psi_{good}\rangle = \begin{cases} \frac{1}{\sqrt{|W|}}\sum_{x\in W}|x\rangle & \text{if } W \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$, is a QADS since

$$W = \emptyset \Longrightarrow |\psi_0\rangle \in |\psi_{good}\rangle^{\perp} \Longrightarrow U_1|\psi_0\rangle = |\psi_0\rangle \Longrightarrow U|\psi_0\rangle = |\psi_0\rangle$$

Example 5 (Wong's quantum walk [16]) This type of search is applied to $2D$ grids of 2^k vertices $\{|0\rangle, \ldots, |2^k - 1\rangle\}$ when they are walked by a "lackadaisical" quantum walk (i.e., where each vertex has a self-loop of weight $0 < l$). Detection of marked vertices by a boolean function $f : \{0,1\}^k \to \{0,1\}$ requires the construction of the initial state $|\psi_0\rangle = \frac{1}{\sqrt{2^k}}\sum_{x=0}^{k-1}|x\rangle|s_c\rangle \in \mathcal{H} = (\mathbb{C}^2)^{\otimes k} \otimes \mathbb{C}^5$ of this weighted quantum walk, where

$$|s_c\rangle = \frac{1}{\sqrt{4+l}}(|\rightarrow\rangle + |\leftarrow\rangle + |\uparrow\rangle + |\downarrow\rangle + \sqrt{l}|\circlearrowleft\rangle)$$

The grid is walked by iteration of the following two operators:

- Grover diffusion coin for a weighted graph: $I \otimes C$, where $C = 2|s_c\rangle\langle s_c| - I$.
- Flip-flop shift: S such that $S(|x\rangle|\rightarrow\rangle) = |x+e_1\rangle|\leftarrow\rangle, S(|x\rangle|\leftarrow\rangle) = |x-e_1\rangle|\rightarrow\rangle, S(|x\rangle|\uparrow\rangle) = |x+e_2\rangle|\downarrow\rangle, S(|x\rangle|\downarrow\rangle) = |x-e_2\rangle|\uparrow\rangle$, and $S(|x\rangle|\circlearrowleft\rangle) = |x\rangle|\circlearrowleft\rangle$, where e_1, e_2 denote the basic vector directions of the 2D grid.

Notice that $|\psi_0\rangle$ is an 1−eigenvector of both operators, i.e., $(I \otimes (2|s_c\rangle\langle s_c| - I))|\psi_0\rangle = |\psi_0\rangle = S|\psi_0\rangle$. On the other hand, the detection for marked elements in $W = \{x \in \{0,1\}^k \mid f(x) = 1\}$ is carried out by one of the following two oracles:

- Grover's oracle: $O \otimes I$
- SKW oracle: $O_{SKW} = I - 2\sum_{x\in W}|x, s_c\rangle\langle x, s_c|$

Observe that $(O \otimes I)|\psi_0\rangle = |\psi_0\rangle \Longleftrightarrow W = \emptyset$ (just like in Santos's quantum walk), and notice that

$$|\psi_0\rangle = (I - 2\sum_{x\in W}|x, s_c\rangle\langle x, s_c|)|\psi_0\rangle = \frac{1}{\sqrt{2^k}}\left(\sum_{x\notin W}|x\rangle|s_c\rangle - \sum_{x\in W}|x\rangle|s_c\rangle\right) \Longleftrightarrow W = \emptyset$$

Therefore, any algorithm computing $|\psi_0\rangle$ and $U := (O\otimes I)S(I\otimes C)$ or $U := (O\otimes I)SO_{SKW}$ is a QADS.

As noticed in [16], the laickadaisical quantum walk based on the Grover oracle does not fit into the general machinery of the quantum abstract search. However, we have seen that it fits into our definition. Also, the laickadaisical quantum walk for 2D grids can be naturally considered for regular graphs of torus type. This generalization can be also described in terms of our QADS.

Example 6 (Deutsch-Jozsa's algorithm [7]) Given a boolean function $f : \{0,1\}^k \to \{0,1\}$ which is promised to be either constant or balanced (i.e., $f(x) = 1$ for exactly half of all possible x), Deutsch-Jozsa's algorithm prepares an initial state $|\psi_0\rangle = |0\rangle^{\otimes k}|1\rangle$ in the Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes(k+1)}$, and uses the following two constructible operators:

- Hadamard transform: $H^{\otimes(k+1)}$, where H is the Hadamard gate.
- Unitary version of f: $U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$.

The algorithm which constructs $U := H^{\otimes(k+1)}U_f H^{\otimes(k+1)}$ from f is a QADS since

$$|\psi_0\rangle = H^{\otimes(k+1)}U_f H^{\otimes(k+1)}|\psi_0\rangle$$

if and only if

$$\sum_{x=0}^{2^k-1} \frac{|x\rangle|-\rangle}{\sqrt{2^k}} = U_f \sum_{x=0}^{2^k-1} \frac{|x\rangle|-\rangle}{\sqrt{2^k}} = \sum_{x=0}^{2^k-1} \frac{(-1)^{f(x)}|x\rangle|-\rangle}{\sqrt{2^k}}$$

where $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. This is equivalent to $\forall x \in \{0,1\}^k : \ f(x) = 0$, i.e., $W = \emptyset$.

Example 7 (Oracle) In examples 1, 3, 4 or 5, any algorithm that simply generates the oracle O generating (alt. $O \otimes I$, U_1, $O \otimes I$ or O_{SKW}), together with the initial state $|\psi_0\rangle$, is also a QADS.

B Formal description of procedures in the algorithmic closure of QADS

In this appendix, we provide a formal description of the procedures contained in Table 1, all of them in the algorithmic closure of QADS.

Proposition 1 *Consider a QADS that generates a pair* $(|\psi_0\rangle)\ ,\ U) \in \mathcal{H} \times \mathcal{U}(\mathcal{H})$ *for any given boolean input* f *from a set of inputs* $\mathcal{M}$, *where* $\mathcal{U}(\mathcal{H})$ *is the group of unitary operators on the Hilbert space* $\mathcal{H}$.

1. *Algorithms generating the following pairs of initial state/unitary transformation, are also QADS.*
   (a) *Extension:* $(|\psi_0\rangle|0\rangle^{\otimes l}\ ,\ U \otimes I) \in \mathcal{H}' \times \mathcal{U}(\mathcal{H}')$, *where* $\mathcal{H}' = \mathcal{H} \otimes (\mathbb{C}^2)^l$.
   (b) *Inversion:* $(|\psi_0\rangle\ ,\ U^\dagger) \in \mathcal{H} \times \mathcal{U}(\mathcal{H})$.
   (c) *Powers:* $(|\psi_0\rangle\ ,\ U^{n_f}) \in \mathcal{H} \times \mathcal{U}(\mathcal{H})$, *for all* $n_f \in \mathbb{N}$.
   (d) *Roots:* $(|\psi_0\rangle\ ,\ U^{1/n_f}) \in \mathcal{H} \times \mathcal{U}(\mathcal{H})$, *for all* $n_f \in \mathbb{N}$.
   (e) *Conjugation:* $(T|\psi_0\rangle\ ,\ TUT^\dagger) \in \mathcal{H}\times\mathcal{U}(\mathcal{H})$, *for all* $T \in \mathcal{U}(\mathcal{H})$. *Moreover, conjugation induces an equivalence relation on the set of possible outputs of a QADS for a given input* $f \in \mathcal{M}$.
   (f) *Controlled detecting operator:* $(|+\rangle|\psi_0\rangle\ ,\ U_c) \in \mathbb{C}^2 \otimes \mathcal{H} \times \mathcal{U}(\mathbb{C}^2 \otimes \mathcal{H})$, *where* $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ *and* $U_c|i\rangle|x\rangle = |i\rangle U^i|x\rangle$.
2. *If a second QADS generates pairs* $(|\psi_0{}'\rangle\ ,\ U') \in \mathcal{H}' \times \mathcal{U}(\mathcal{H}')$ *for boolean functions from the same set of inputs* $\mathcal{M}$, *then:*
   (a) *A QADS tensor product of QADS can be realized:* $(|\psi_0\rangle|\psi_0{}'\rangle\ ,\ U \otimes U') \in \mathcal{H} \otimes \mathcal{H}' \times \mathcal{U}(\mathcal{H} \otimes \mathcal{H}')$.
   (b) *If* $\mathcal{H}' = \mathcal{H}$ *and* $|\psi_0{}'\rangle = |\psi_0\rangle$, *then a product of detecting operators can be considered as a QADS:* $(|\psi_0\rangle\ ,\ U'U) \in \mathcal{H} \times \mathcal{U}(\mathcal{H})$.
   (c) *The pair of QADS can be doubly controlled according to the following scheme:* $(|+\rangle|\psi_0\rangle|\psi_0{}'\rangle\ ,\ (U \otimes U')_{dc}) \in \mathbb{C}^2 \otimes \mathcal{H} \otimes \mathcal{H}' \times \mathcal{U}(\mathbb{C}^2 \otimes \mathcal{H} \otimes \mathcal{H}')$, *where* $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ *and* $(U \otimes U')_{dc}|i\rangle|x\rangle|x'\rangle = |i\rangle U^i|x\rangle U'^{1-i}|x'\rangle$. *It is also a QADS.*

Proof 1. Assume $W = \{x \in \{0,1\}^k \mid f(x) = 1\} = \emptyset$, so that $U|\psi_0\rangle = |\psi_0\rangle$. Then:
   (a) $(U \otimes I)(|\psi_0\rangle|0^{\otimes l}\rangle) = |\psi_0\rangle|0^{\otimes l}\rangle$.
   (b) $|\psi_0\rangle = U^\dagger|\psi_0\rangle$.

   (c) $U^{n_f}|\psi_0\rangle = U^{n_f-1}|\psi_0\rangle = \cdots = |\psi_0\rangle$.
   (d) If $U = \sum_{j=1}^t e^{\lambda_j i}|x_j\rangle\langle x_j|$, with $\lambda_1 = 0$ and $|x_1\rangle = |\psi_0\rangle$, then $U^{1/n_f} = \sum_{j=1}^t e^{\lambda_j i/n_f}|x_j\rangle\langle x_j|$ and so $U^{1/n_f}|\psi_0\rangle = |\psi_0\rangle$.
   (e) $(TUT^\dagger)(T|\psi_0\rangle) = T|\psi_0\rangle$.
   (f) $U_c(|+\rangle|\psi_0\rangle) = \frac{|0\rangle|\psi_0\rangle+|1\rangle U|\psi_0\rangle}{\sqrt{2}} = |+\rangle|\psi_0\rangle$.
2. (a) We have $(U \otimes U')(|\psi_0\rangle|\psi_0{}'\rangle) = |\psi_0\rangle|\psi_0{}'\rangle$ whenever $U|\psi_0\rangle = |\psi_0\rangle$ and $U'|\psi_0{}'\rangle = |\psi_0{}'\rangle$, which is always the case when $W = \emptyset$.
   (b) If $f = 0$, then $U'U|\psi_0\rangle = U'|\psi_0\rangle = |\psi_0\rangle$.
   (c) Finally, $(U \otimes U')_{dc}(|+\rangle|\psi_0\rangle|\psi_0{}'\rangle) = \frac{|0\rangle|\psi_0\rangle U'|\psi_0{}'\rangle+|1\rangle U|\psi_0\rangle|\psi_0{}'\rangle}{\sqrt{2}} = |+\rangle|\psi_0\rangle|\psi_0{}'\rangle$ if $U|\psi_0\rangle = |\psi_0\rangle$ and $U'|\psi_0{}'\rangle = |\psi_0{}'\rangle$, which is true when $f = 0$.

Corollary 1 *If $|\psi_0\rangle$ is the initial space of a QADS, then the set G of detecting operators (for any possible QADSwith the same initial state) is a group under the product, which is a subgroup of the stabiliser of $|\psi_0\rangle$, under the action of the unitary group.*

Proof Since $|\psi_0\rangle$ is the initial state of a QADS, the set G is nonempty. Moreover, since "Inversion", and "Product" are in the algorithmic closure of QADS, G is a subgroup of the unitary group, and any of its elements stabilise $|\psi_0\rangle$.

C On the efficient constructibility of QADS

In this appendix, we give examples of efficient and non-efficient constructible QADS.

Example 8 Let us provide an example of a non-efficiently constructible QADS (unless $P = NP$). Consider the algorithm that, on any input $f : \{0,1\}^k \to \{0,1\}$, outputs the zero state of $\mathcal{H} = \mathbb{C}^2$, together with the unitary operator realized by a gateless circuit, when $W = \emptyset$, and by a circuit consisting on a single X gate, when $W \neq \emptyset$. The output construction of the QADS encapsulates the detection problem of an element $x \in \{0,1\}^k$ such that $f(x) = 1$, and so it could be used in a polynomial-time reduction of SAT.

Example 9 For the examples of the previous section we have the following results on efficient constructibility:

1. The QADS for Grover search is efficiently constructible, as its output can be computed in $O(n)$ time [12, Section 6.1.2]. Observe that the oracle can be straightforwardly implemented from an actual implementation of the input function f, which can be assumed to be given in a reversible form [12, Section 3.2.5].
2. The initial state and the unitary operator of Deutsch-Jozsa's algorithm require also $O(n)$ to be computed, and so the corresponding QADS is also efficiently constructible.
3. Szegedy's quantum walk initial state and operator for Ambaini's Element Distinctness problem [1] can be realised in $O(n \log n)$ depth, according to [11,8], and so the QADS of Example 2 are efficient constructible.
4. The QADS of the quantum abstract search is efficiently constructible whenever the initial and good states, together with the operator U_2 can be computed in $O(\text{poly}(n))$.
5. The oracles of the previous examples are, in particular, also efficiently constructible QADS.

Example 10 Consider a QADS that is efficiently constructible. Then, the following QADS from Proposition 1 are also constructible:

1. Extension, provided that the number t is $O(\text{poly}(n))$.
2. Inversion (just by inversion of the quantum circuit describing U).
3. Powers, as long as n_f is $O(\text{poly}(f))$.
4. Conjugation, provided that the circuit for the unitary operator T has size $O(\text{poly}(n))$.
5. Controlled detecting operator, because of [12, Section 4.3].

The tensor product of two QADS is also efficiently constructible assuming both QADS are. The same property holds for the product and the doubly controlled QADS.

D On the detection rate and efficient detection of QADS

In this appendix, we explore in detail aspects on the detection rate of QADS. In particular, we provide $\delta-$detecting functions for some QADS appearing in the main text, we prove the existence of $\delta-$detecting functions for some procedures in the algorithmic closure of QADS, and finally we show a relation between the $\delta-$detecting function and the quantum hitting time for quantum walks.

Example 11 (A QADS with no $\delta-$detecting function) Consider the QADS associated to Grover's oracle, and let $\mathcal{M} = \{f : \{0,1\}^k \to \{0,1\} \mid f(x_0) = 1 \text{ for exactly none or one value } x_0\}$. It is straigtforward to see that $O^t|\psi_0\rangle = \begin{cases} |\psi_0\rangle & \text{if } t \text{ even} \\ \frac{1}{\sqrt{2^k}}\left(\sum_{x\neq x_0}|x\rangle - |x_0\rangle\right) & \text{if } t \text{ odd} \end{cases}$, and so $\langle\psi_0|O^t|\psi_0\rangle = 1 - \frac{t \bmod 2}{2^{k-1}} \geq 1 - \frac{1}{2^{k-1}}$. Hence, for all $t \in \mathbb{N}$, $\frac{\sum_{t=0}^{T}|\langle\psi_0|O^t|\psi_0\rangle|^2}{T+1} \geq \left(1 - \frac{1}{2^{k-1}}\right)^2 \geq 1 - \frac{1}{2^{k-2}}$. Therefore, for any $\delta > 0$, no function $T : \mathbb{N} \to \mathbb{N}$ can be δ-detecting for such a QADS.

Example 12 (A QADS with constant $\delta-$detecting function) The QADS in Example 8, has a constant $\delta-$detecting function (namely, $T(k) = 1$ is $\frac{1}{2}-$detecting). Observe that, however, such a QADS encapsulates the detecting problem in the construction of the operator U, and so it can not be efficiently constructible (unless $P = NP$). This shows the importance for a QADSto be simultaneously efficiently constructible, and to have a $\delta-$detecting fucntion.

Example 13 For the examples mentioned in the paper, we have the following results on $\delta - detection$:

1. Let us consider the QADS of Grover search for

$$\mathcal{M} = \{f : \{0,1\}^k \to \{0,1\} \mid f(x_0) = 1 \text{ for exactly none or one value } x_0\ ,\ k \geq 2\}$$

For all $k \geq 2$, let $\theta_k = 2\arccos\left(\sqrt{\frac{2^k-1}{2^k}}\right)$, and let R_k be the closest integer to $\frac{\arccos\left(\sqrt{\frac{1}{2^k}}\right)}{\theta_k}$ so that $\cos(\theta_k + R_k\theta_k) \leq \frac{\sqrt{2}}{2}$ [12]. Define, for all $k \in \mathbb{N}$, $T(k)$ the smallest natural number greater than $\frac{8}{\sin(\theta_k)} - 1$ such that $T(k) \equiv 2R_k \pmod{2\pi}$. The function T is $\frac{\sqrt{2}-1}{4\sqrt{2}}-$detecting for the QADS since

$$\frac{\sum_{t=0}^{T(k)}|\langle\psi_0|U^t|\psi_0\rangle|^2}{T(k)+1} = \frac{\sum_{t=0}^{T(k)}\left(\sqrt{\frac{2^k-1}{2^k}}\cos\left(\frac{2t+1}{2}\theta_k\right) + \sqrt{\frac{1}{2^k}}\sin\left(\frac{2t+1}{2}\theta_k\right)\right)^2}{T(k)+1}$$

$$= \frac{\sum_{t=0}^{T(k)}\left(\frac{2^k-1}{2^k}\cos^2\left(\frac{2t+1}{2}\theta_k\right) + \frac{1}{2^k}\sin^2\left(\frac{2t+1}{2}\theta_k\right) + 2\frac{\sqrt{2^k-1}}{2^k}\cos\left(\frac{2t+1}{2}\theta_k\right)\sin\left(\frac{2t+1}{2}\theta_k\right)\right)}{T(k)+1}$$

$$\leq \frac{\sum_{t=0}^{T(k)}\left(\frac{2^k-1}{2^k}\cos^2\left(\frac{2t+1}{2}\theta_k\right) + \frac{1}{2^k}\left(1-\cos^2\left(\frac{2t+1}{2}\theta_k\right)\right) + \frac{1}{\sqrt{2^{k-2}}}\cos\left(\frac{2t+1}{2}\theta_k\right)\sin\left(\frac{2t+1}{2}\theta_k\right)\right)}{T(k)+1}$$

$$= \frac{1}{2^k} + \frac{\sum_{t=0}^{T(k)}\left(\frac{2^k-2}{2^k}\left(\frac{1+\cos((2t+1)\theta_k)}{2}\right) + \frac{1}{\sqrt{2^{k-2}}}\frac{\sin((2t+1)\theta_k)}{2}\right)}{T(k)+1}$$

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

$$= \frac{1}{2^k} + \frac{2^{k-1}-1}{2^k} + \frac{\sum_{t=0}^{T(k)}\left(\frac{2^k-2}{2^{k+1}}\cos((2t+1)\theta_k) + \frac{1}{\sqrt{2^k}}\sin((2t+1)\theta_k)\right)}{T(k)+1}$$

$$\leq \frac{1}{4} + \frac{1}{2} + \frac{\sin\left((T(k)+1)\theta_k\right)\left(\frac{2^k-2}{2^{k+1}}\cos\left((T(k)+1)\theta_k\right) + \frac{1}{\sqrt{2^k}}\sin\left((T(k)+1)\theta_k\right)\right)}{\sin\left(\theta_k\right)\left(T(k)+1\right)}$$

$$\leq \frac{3}{4} + \frac{1\cdot\left(1\cdot\frac{\sqrt{2}}{2} + \sqrt{\frac{1}{2}}\cdot 1\right)}{\sin\left(\theta_k\right)\left(T(k)+1\right)} \leq \frac{3}{4} + \frac{1}{4\sqrt{2}} = 1 - \frac{\sqrt{2}-1}{4\sqrt{2}}$$

Moreover, $T(k) \in O(\sqrt{2^k})$ [3, Proof of Theorem 3].

2. From Proposition 1, we can construct a QADS from the QADS of Grover search by simply taking as output the same initial state and an $\sqrt{2^k}-$th root of the operator U. For any input function $f : \{0,1\}^k \to \{0,1\}$ this new QADS requires $\sqrt{2^k}$ iterations of the detecting operator to replicate a single iteration in Grover's QADS. Therefore, the same bounding technique of the previous example shows that a $\frac{\sqrt{2}-1}{4\sqrt{2}}-$detecting function $T \in O(2^k)$ for the QADS can be considered.
3. Consider the QADS of Deutsch-Jozsa's algorithm, and let $T(k) = 1$. We shall show that T is $\frac{1}{2}-$detecting for such a QADS. Namely, if f is balanced, then

$$\frac{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T(k)+1} = \frac{|\langle\psi_0|\psi_0\rangle|^2 + |\langle\psi_0|H^{\otimes(k+1)}U_f H^{\otimes(k+1)}|\psi_0\rangle|^2}{2} = \frac{1}{2}$$

because $H^{\otimes(k+1)}|\psi_0\rangle = \sum_{x=0}^{2^k-1}\frac{|x\rangle|-\rangle}{\sqrt{2^k}}$ and $U_f H^{\otimes(k+1)}|\psi_0\rangle = \frac{\left(\sum_{f(x)=0}|x\rangle - \sum_{f(x)=1}|x\rangle\right)|-\rangle}{\sqrt{2^k}}$.
4. The controlled QADS of Szegedy's quantum walk for

$$\mathcal{M} = \{f : \{0,1\}^k \to \{0,1\} \mid f(x_0) = 1 \text{ for less than half values}\}$$

has, because of Proposition 3, a $\frac{1}{4}-$detecting time $T \in O\left(\frac{1}{\sqrt{\theta(P)}}\right)$, where $\theta(P)$ is the eigenvalue gap of the matrix P associated with the graph, by application of the quantum hitting time [15].
5. For some specific graphs, the non-controlled QADS of Szegedy's quantum walk can also be shown to have a $\delta-$detecting time. For instance, let us consider

$$\mathcal{M}=\{f:\{0,1\}^k\to\{0,1\} \mid f(x_0)=1 \text{ for exactly none or one value } x_0 \text{ , } k\geq 3\}$$

for the complete graph of 2^k vertices. Explicit expressions for $U^t|\psi_0\rangle$ and the quantum hitting time $Q(T)$ of this graph, can be found in [14]. We can use them to get

$$\langle\psi_0|U^t|\psi_0\rangle = \frac{2(2^k-1)^2 T_{2t}\left(\frac{2^k-2}{2^k-1}\right) + 2^k - 2}{2^k(2^{k+1}-3)}$$

$$Q(T) = \frac{2(2^k-1)^2\left(2T+1-U_{2t}\left(\frac{2^k-2}{2^k-1}\right)\right)}{2^k(2^{k+1}-3)(T+1)} \geq \frac{7}{10}\cdot\left(2 - \frac{1+U_{2t}\left(\frac{2^k-2}{2^k-1}\right)}{T+1}\right)$$

where T_{2t} and U_{2t} are the Chebyshev polynomial of the first and second kinds. Taking $T(k) = \left\lceil \frac{\frac{1}{\sin\arccos\left(\frac{2^k-2}{2^k-1}\right)} - 1}{2} \right\rceil$ we have that the real scalar product $\langle\psi_0|U^t|\psi_0\rangle$ is non-negative for all $0 \leq t \leq T(k)$, and $Q(T(k)) \geq \frac{1}{5}$. Therefore, by Proposition 3, $T(k)$ is $\frac{1}{10}-$detecting for the QADS.

6. For the same set $\mathcal{M}$, the controlled QADS of Santos' quantum walk with respect to the complete graph with 2^k vertices, has also a $\delta-$detecting time. According to [13, Section 3.1], the Hilbert space $\mathcal{H}$ can be decomposed in an $U-$invariant $3-$dimensional subspace and its orthogonal complement (over which U is the identity). Therefore, $U = -|v_{-1}\rangle\langle v_{-1}| + e^{i\theta}|v_+\rangle\langle v_+| + e^{-i\theta}|v_-\rangle\langle v_-|$ where $|v_+\rangle$ and $|v_-\rangle$ are complex conjugates, and $\cos\theta = \frac{1+\cos^2\phi}{2}$ with $\cos\phi = \frac{2^k-3}{2^k-1}$. Since $|\psi_0\rangle = \lambda_{-1}|v_{-1}\rangle + \lambda_+|v_+\rangle + \overline{\lambda_-}|v_-\rangle$, with $\lambda_+ = \frac{-i}{\sqrt{2}}, \lambda_- = \overline{\lambda_+}$, we have

$$\frac{\sum_{t=0}^{T(k)} \|U^t|\psi_0\rangle - |\psi_0\rangle\|^2}{T(k)+1}$$

$$= \frac{\sum_{t=0}^{T(k)} \left(|\lambda_{-1}|^2|(-1)^t - 1|^2 + |\lambda_+|^2|e^{it\theta} - 1|^2 + |\lambda_-|^2|e^{-it\theta} - 1|^2\right)}{T(k)+1}$$

$$\geq \frac{\sum_{t=0}^{T(k)} 2\left(\frac{1}{2}|e^{it\theta} - 1|^2\right)}{T(k)+1} = \frac{\sum_{t=0}^{T(k)} 2(1 - \cos(t\theta))}{T(k)+1}$$

$$= 2\left(1 - \frac{\sin\left(\frac{(T(k)+1)\theta}{2}\right)\cos\left(\frac{T(k)\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)(T(k)+1)}\right) \geq 2\left(1 - \frac{\cos\left(\frac{T(k)\theta}{2}\right)}{\sin\left(\frac{\theta}{2}\right)T(k)}\right)$$

Take now $T(k) = \lceil\frac{\pi}{2\theta}\rceil$, so that $\cos\left(\frac{T(k)\theta}{2}\right) \leq \frac{\sqrt{2}}{2}$ and $\sin\left(\frac{\theta}{2}\right)\cdot T(k) \geq \frac{\sqrt{2}}{2}\varepsilon$ for some $1 < \varepsilon < \frac{6}{5}$. Hence, $\frac{\sum_{t=0}^{T(k)} \|U^t|\psi_0\rangle - |\psi_0\rangle\|^2}{T(k)+1} \geq 4\cdot\frac{1}{48}$, and so $T \in O(\sqrt{2^k})$ is $\frac{1}{24}-$detecting for the controlled QADS, because of Proposition 3.

Proposition 2 (Detecting times for procedures in the algorithmic closure) *Consider a $\delta-$detecting time $T \geq 1$ for a given QADS. Then,*

1. *T is $\delta-$detecting time for the extension, inversion and conjugation QADS.*
2. *$S(k) = T(k)\cdot n_f$ is $\frac{\delta}{2L}-$detecting time for the root QADS, provided that n_f depends only on the input size k of f, and that $n_f \leq L$ for all $f \in \mathcal{M}$. As a consequence, if T' is $\delta'-$detecting for the power QADS with $L' \geq n_f$ depending only on the input size k of f, then $\frac{T'}{n_f}$ is $\frac{\delta'}{2L'}-$detecting time for the original QADS.*
3. *T is $\left(\frac{1+\frac{\delta}{2}-\sqrt{1-\delta}}{2}\right)-$detecting time for the QADS based on the controlled detecting operator.*
4. *If T is also $\delta'-$detecting for a second QADS, then: T is $\max\{\delta,\delta'\}-$detecting for the tensor product of both QADS, and $\left(\frac{1+\frac{\delta+\delta'}{2}-\sqrt{1-\delta}\sqrt{1-\delta'}}{2}\right)-$detecting for the doubly controlled QADS.*

Proof 1. This easily follows from the following equalities:

$$\langle\psi_0|U^t|\psi_0\rangle = \langle|\psi_0\rangle|0\rangle^{\otimes l}|(U\otimes I)^t||\psi_0\rangle|0\rangle^{\otimes l}\rangle$$
$$= \langle\psi_0|(U^\dagger)^t|\psi_0\rangle = \langle T|\psi_0\rangle|(TUT^\dagger)^t|T|\psi_0\rangle\rangle.$$

2. For all $\frac{T(k)+1}{S(k)+1} \geq \frac{1}{2n_f} \geq \frac{1}{2L}$. Now, if $A = \{0, n_f, 2\cdot n_f \ldots, T(k)\cdot n_f\}$, then

$$\frac{\sum_{t=0}^{S(k)} |\langle\psi_0|U^{\frac{t}{n_f}}|\psi_0\rangle|^2}{S(k)+1}$$

$$= \frac{\sum_{t\in A} |\langle\psi_0|U^{\frac{t}{n_f}}|\psi_0\rangle|^2 + \sum_{t\in\{0,\ldots,S(k)\}\setminus A} |\langle\psi_0|U^{\frac{t}{n_f}}|\psi_0\rangle|^2}{S(k)+1}$$

$$\le \frac{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T(k)+1} \cdot \frac{T(k)+1}{S(k)+1} + \frac{(S(k)-T(k))}{S(k)+1}$$

$$\le (1-\delta)\cdot\frac{T(k)+1}{S(k)+1} + \frac{(S(k)-T(k))}{S(k)+1} \le 1-\frac{\delta}{2L}$$

3. Let $|{\psi_0}_c\rangle = |+\rangle|\psi_0\rangle$. For all $t = 0,\dots,T$, we have $U_c^t|{\psi_0}_c\rangle = \frac{|0\rangle|\psi_0\rangle+|1\rangle U^t|\psi_0\rangle}{\sqrt{2}}$, and so $\langle{\psi_0}_c|U_c^t|{\psi_0}_c\rangle = \frac{1+\langle\psi_0|U^t|\psi_0\rangle}{2}$, and $|\langle{\psi_0}_c|U_c^t|{\psi_0}_c\rangle| \le \frac{1+|\langle\psi_0|U^t|\psi_0\rangle|}{2}$. Therefore:

$$\frac{\sum_{t=0}^{T(k)} |\langle{\psi_0}_c|U_c^t|{\psi_0}_c\rangle|^2}{T(k)+1} = \frac{\left(\sqrt{\sum_{t=0}^{T(k)}\left(\frac{1+|\langle\psi_0|U^t|\psi_0\rangle|}{2}\right)^2}\right)^2}{T(k)+1}$$

$$\le \left(\frac{\sqrt{\sum_{t=0}^{T(k)} 1^2} + \sqrt{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}}{2\sqrt{T(k)+1}}\right)^2 \le \left(\frac{1+\sqrt{1-\delta}}{2}\right)^2 = 1-\left(\frac{1+\frac{\delta}{2}-\sqrt{1-\delta}}{2}\right)$$

and so T is $\left(\frac{1+\frac{\delta}{2}-\sqrt{1-\delta}}{2}\right)$−detecting time for the QADS based on the controlled detecting operator.

4. For all $t = 0,\dots,T$, we have

$$\langle|\psi_0\rangle|\psi_0'\rangle|(U\otimes U')^t||\psi_0\rangle|\psi_0'\rangle\rangle = \langle\psi_0|U^t|\psi_0\rangle\langle\psi_0'|U'^t|\psi_0'\rangle$$

Therefore:

$$\frac{\sum_{t=0}^{T(k)} |\langle|\psi_0\rangle|\psi_0'\rangle|(U\otimes U')^t||\psi_0\rangle|\psi_0'\rangle\rangle|^2}{T(k)+1} \le$$

$$\min\left\{\frac{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T(k)+1}, \frac{\sum_{t=0}^{T(k)} |\langle\psi_0'|U'^t|\psi_0'\rangle|^2}{T(k)+1}\right\}$$

$$\le \min\left\{1-\delta, 1-\delta'\right\} = 1-\max\{\delta,\delta'\}$$

because $|\langle\psi_0|U^t|\psi_0\rangle|, |\langle\psi_0'|U'^t|\psi_0'\rangle| \le 1$.

Finally, for the doubly controlled QADS, let $|{\psi_0}_{dc}\rangle = |+\rangle|\psi_0\rangle|\psi_0'\rangle$. For all $t = 0,\dots,T$, we have

$$(U\otimes U')_{dc}^t(|+\rangle|\psi_0\rangle|\psi_0'\rangle) = \frac{|0\rangle|\psi_0\rangle U'^t|\psi_0'\rangle + |1\rangle U^t|\psi_0\rangle|\psi_0'\rangle}{\sqrt{2}}$$

and so $\langle{\psi_0}_{dc}|(U\otimes U')_{dc}^t|{\psi_0}_{dc}\rangle = \frac{\langle\psi_0'|U'^t|\psi_0'\rangle+\langle\psi_0|U^t|\psi_0\rangle}{2}$. Therefore:

$$\frac{\sum_{t=0}^{T(k)} |\langle{\psi_0}_{dc}|(U\otimes U')_{dc}^t|{\psi_0}_{dc}\rangle|^2}{T(k)+1}$$

$$= \frac{\left(\sqrt{\sum_{t=0}^{T(k)}\left(\frac{|\langle\psi_0'|U'^t|\psi_0'\rangle|+|\langle\psi_0|U^t|\psi_0\rangle|}{2}\right)^2}\right)^2}{T(k)+1}$$

$$\le \left(\frac{\sqrt{\sum_{t=0}^{T(k)} |\langle\psi_0'|U'^t|\psi_0'\rangle|^2} + \sqrt{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}}{2\sqrt{T(k)+1}}\right)^2$$

$$\le \left(\frac{\sqrt{1-\delta'}+\sqrt{1-\delta}}{2}\right)^2 = 1-\left(\frac{1+\frac{\delta+\delta'}{2}-\sqrt{1-\delta}\sqrt{1-\delta'}}{2}\right)$$

Motivated by the quantum hitting time of quantum walks, an alternative definition of $\delta-$detecting time for the detecting operator U of a QADS was introduced in [6, Section 4], namely a $R \in \mathbb{N}$ such that

$$\frac{1}{R+1}\sum_{t=0}^{R} \| U^t|\psi_0\rangle - |\psi_0\rangle\|^2 \geq 4\delta \tag{1}$$

Next, we shall show a relation between both definitions.

Proposition 3 *1. Let Q be a QADS, and let $T : \mathbb{N} \to \mathbb{N}$ be such that for all nonzero $f \in \mathcal{M}$ of input size k, the detecting operator U provided by Q on input f satisfies equation (1) for $R = T(k)$. If $\langle\psi_0|U^t|\psi_0\rangle$ is real and nonnegative for all $t \leq T(k)$, then T is 2δ-detecting for the QADS. In particular, this is true when Q outputs controlled operators such that $\langle\psi_0|U^t|\psi_0\rangle$ is real for all $t \in \mathbb{N}$.*

2. Reciprocally, if $T : \mathbb{N} \to \mathbb{N}$ is $\delta'-$detecting for a QADS Q, then for all nonzero $f \in \mathcal{M}$ of input size k, the detecting operator U provided by Q on input f satisfies equation (1) for $R = T(k)$ and $\delta = \frac{1-\sqrt{1-\delta'}}{2}$.

Proof 1. Because $\|U^t|\psi_0\rangle - |\psi_0\rangle\|^2 = 2(1 - \Re\langle\psi_0|U^t|\psi_0\rangle)$ we have

$$4\delta \leq \frac{\sum_{t=0}^{T(k)} \|U^t|\psi_0\rangle - |\psi(0)\rangle\|^2}{T(k)+1}$$
$$= 2\left(1 - \frac{\sum_{t=0}^{T(k)} \Re\langle\psi_0|U^t|\psi_0\rangle}{T(k)+1}\right) = 2\left(1 - \frac{\sum_{t=0}^{T(k)} \langle\psi_0|U^t|\psi_0\rangle}{T(k)+1}\right)$$

since $\langle\psi_0|U^t|\psi_0\rangle$ is a real number. Now, because such a number is nonnegative, we have

$$\frac{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T(k)+1} \leq \frac{\sum_{t=0}^{T(k)} \langle\psi_0|U^t|\psi_0\rangle}{T(k)+1} \leq 1 - 2\delta$$

In particular, if Q outputs controlled operators such that $\langle\psi_0|U^t|\psi_0\rangle$ is real, for all $t \in \mathbb{N}$, because of the proof of Proposition 2 we know that $\langle\psi_{0c}|U_c^t|\psi_{0c}\rangle = \frac{1+\langle\psi_0|U^t|\psi_0\rangle}{2}$ is always real and nonnegative.

2. Cauchy-Schwarz inequality gives us

$$\sum_{t=0}^{T(k)} \frac{1}{T(k)+1}|\langle\psi_0|U^t|\psi_0\rangle| \leq \frac{1}{\sqrt{T(k)+1}}\sqrt{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}$$

Since $\Re\langle\psi_0|U^t|\psi_0\rangle \leq |\langle\psi_0|U^t|\psi_0\rangle|$ we have

$$\frac{\sum_{t=0}^{T(k)} \|U^t|\psi_0\rangle - |\psi(0)\rangle\|^2}{T(k)+1}$$
$$= 2\left(1 - \frac{\sum_{t=0}^{T(k)} \Re\langle\psi_0|U^t|\psi_0\rangle}{T(k)+1}\right) \geq 2\left(1 - \frac{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|}{T(k)+1}\right)$$
$$\geq 2\left(1 - \sqrt{\frac{\sum_{t=0}^{T(k)} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T(k)+1}}\right) \geq 4\left(\frac{1-\sqrt{1-\delta'}}{2}\right)$$

The condition *real and nonnegative* in the previous proposition is necessary. Just observe that a QADS that provides, for nonzero inputs, a detecting operator U satisfying $U|\psi_0\rangle = \lambda|\psi_0\rangle$ with $\lambda \neq 1$, satisfies equation (1) with $R = 1$ for $\delta = \frac{|\lambda-1|^2}{8}$. However, $T = 1$ is not $\delta'-$detecting time for any $\delta' > 0$.

E On the detection with a QADS

In this final appendix, we prove the main theorem of the paper, and we comment on the definition of QADS introduced in [6].

Proof (Of the main theorem) If $f = 0$, then $U|\psi_0\rangle = |\psi_0\rangle$, and so for all $t \in \{0, \ldots, T\}$ the measurement of $U^t|\psi_0\rangle$ is $|\psi_0\rangle$. Hence, the algorithm's output NO is always correct. When $f \neq 0$, NO is an output on integer t with a probability $|\langle\psi_0|U^t|\psi_0\rangle|^2$. So, the error probability of the algorithm is the average $\frac{\sum_{t=0}^{T} |\langle\psi_0|U^t|\psi_0\rangle|^2}{T+1}$. When the QADS in efficiently constructible and has $\delta-$detecting time, the number of iterations of the algorithm to be taken is $T(k)$. This yields the promised one-sided error quantum algorithm requiring $O(\text{poly}(n))$ precomputation time.

Remark 1 The relation between the detecting scheme for QADS and the one given in [15] for quantum walks, is implicitly contained in Proposition 3 (Appendix D). The error probability in the later case is bounded by δ of equation (1) [6], while in the former case it is bounded by 2δ. An explanation for this gap is that the inner product $\langle\psi_0|U^t|\psi_0\rangle$ tests the state $U_c^t|\psi_0\rangle$ for both $|0\rangle$ and $|1\rangle$ in the auxiliary register, while the norm $\||U^t|\psi_0\rangle - |\psi_0\rangle\|$ only accounts for the control qubit $|1\rangle$. In order to boost up the success probability for quantum walks, a second measurement is carried out in the final state. If the measured vertex is marked, then the error probability is improved. This was the rationale for the map m in the (preliminary) definition of a QADS in [6], since a quantum-walk-like detecting scheme was assumed. Such map was thought to provide a boosting up of the detection probability, but this can be achieved by the detecting scheme given in Section 5 when the QADS provides a controlled detecting operator (Section 4). The broader approach adopte in this paper includes the boosting up probability directly in the detection scheme.

References

1. Ambainis, A.: Quantum walk algorithm for element distinctness. SIAM J. Comput. **37**(1), 210–239 (2007)
2. 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)
3. Boyer, M., Brassard, G., Høyer, P., Tapp, A.: Tight bounds on quantum searching. Fortschr. Phys **46 (4-5)**, 493–505 (1998)
4. Combarro, E.F., Ranilla, J., Rúa, I.: A quantum algorithm for the commutativity of finite dimensional algebras. IEEE Access **7**, 45554–45562 (2019)
5. Combarro, E.F., Ranilla, J., Rúa, I.F.: Experiments testing the commutativity of finite-dimensional algebras with a quantum adiabatic algorithm. Computational and Mathematical Methods **1**(1), e1009 (2019)
6. Combarro, E.F., Ranilla, J., Rúa, I.F.: Quantum walks for the determination of commutativity of finite dimensional algebras. J. Comput. Appl. Math. **354**, 496–506 (2019)
7. Deutsch, D., Jozsa, R.: Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **439**(1907), 553–558 (1992)
8. Gilyén, A.P.: Quantum walk based search methods and algorithmic applications. Master's thesis, Eötvös Loránd University (2014)
9. 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)
10. Hernández-Cáceres, J., Combarro, E., Ranilla, J., Rúa, I.: Some properties of combinatorial quantum abstract detecting systems. In: Poster presented at the 15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020) (2020)

11. Loke, T., Wang, J.B.: Efficient quantum circuits for Szegedy quantum walks. Ann. Physics **382**, 64–84 (2017)
12. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press (2011)
13. Santos, R.A.M.: Szegedy's quantum walk with queries. Quantum Information Processing **15**(11), 4461–4475 (2016)
14. Santos, R.A.M., Portugal, R.: Quantum hitting time on the complete graph. International Journal of Quantum Information **8**(5), 881–894 (2010)
15. 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)
16. Wong, T.: Faster search by lackadaisical quantum walk. Quantum Inf Process **17 (68)** (2018)