Quantum Walks for the Determination of Commutativity of Finite Dimensional Algebras

Elías F. Combarro[a], José Ranilla[a], I.F. Rúa[b]

[a] *Computer Science Department, University of Oviedo (Spain)*
[b] *Mathematics Department, University of Oviedo (Spain)*

Abstract

Quantum walks provide a framework for the construction of quantum algorithms. Based on this approach, we consider different walks for testing the commutativity of a finite dimensional algebra. In particular, we consider Szegedy's and Santo's quantum walks constructed from complete and torus graphs. Results of numerical experiments are presented, showing that for some choices of the quantum walks we can obtain better detections probabilities than with previous quantum algorithms addressing this problem that were based on Grover's quantum search. Additionally, we introduce a general notion of quantum detection system that encompasses all the methods consider in this work, among others, and develop the idea of quantum hitting time for this kind of systems as an extension of Szegedy's seminal ideas.

Keywords: Quantum Walks, Commutativity, Finite Dimensional Algebras

1. Introduction

The proposal of using atomic-scaled states of matter to perform computations can be traced back to the works of Feynman, Manin or Benioff [1, 2, 3]. This paradigm of computation, known as quantum computing, outperforms (at least theoretically) classic computations in some situations. For example, the well-known quantum algorithms of Deutsch-Josza [4], Grover [5] or Shor [6] have been proved to be *better* than any alternative classical algorithm. These procedures are usually described in terms of quantum gates, which can be thought as the quantum analogues of the classical logical gates [7].

While other algorithms addressing particular problems exist [8], general frameworks for the construction of quantum algorithms can be found in the literature too. One of them is that of adiabatic algorithms, based on the evolution of a quantum system under a certain sequence of Hamiltonian transformations [9, 10]. Another one is based on the quantum analogue of random walks on graphs, and it is naturally called *quantum walks*. Because, apparently, there are not so many quantum alternatives outperforming classical algorithms [11], a proposal for broading the scope of problems in which the known frameworks can be applied has been issued [12]. Based on this direction of research, we have recently considered quantum algorithms for testing the commutativity of a finite dimensional algebra. One of them is based on Grover's quantum search algorithm; the second one on quantum adiabatic techniques [13, 14]. This problem is of interest in the context of the computational classification of finite division algebras (known as finite semifields) [15], because testing whether a given semifield A coordinatizes a symplectic plane, requires testing the commutativity of $O(|A|^2)$ algebras.

In this paper we approach the mentioned commutativity problem from the framework of quantum walks. Based on this approach, we consider different walks for testing the commutativity of a finite dimensional algebra (definitions and facts on these algebraic structures can be found in Section 2). In particular, we consider Szegedy's and Santo's quantum walks constructed from complete or torus graphs (Section 3 is devoted to these quantum walks). In Section 4 we address the detection problem for these quantum walks and we introduce a general framework to study this kind of problem, and the corresponding results of numerical experiments

Email addresses: efernandezca@uniovi.es (Elías F. Combarro), ranilla@uniovi.es (José Ranilla), rua@uniovi.es (I.F. Rúa)

carried out on a quantum computer simulator are presented in Section 5. Conclusions on the most suitable quantum walks solving this problem and future lines of research are given in the final section.

2. Finite Dimensional Algebras

From now on, K will denote a field, i.e., an algebraic ring in which division is uniquely possible. Examples of fields include infinite fields such as the real or complex numbers, or the Galois finite fields $\mathbb{F}_q$ [16]. An algebra over the field K (simply called $K-$algebra) will be a $K-$vector space together with a bilinear product $\cdot$ [17]. The algebra is associative (resp. commutative) if the multiplication satisfies the associativity (resp. commutativity) property:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),\ \forall a, b, c \in A \qquad (\text{resp. } a \cdot b = b \cdot a,\ \forall a, b \in A)$$

When A has an identity it is called a unital algebra. Morevoer, it is called a division algebra if left and right multiplicative inverses exist for all nonzero elements. If the underlying $K-$vector space is finite-dimensional, then the $K-$algebra is also called finite dimensional. It is straightforward to see that matrix rings over the field K, Lie and Jordan algebras (i.e., $K-$algebras satisfying Lie or Jordan axioms [18]) or finite semifields (i.e., $\mathbb{F}_q-$finite dimensional division algebras [19]), are examples of $K-$algebras.

Given two elements $a, b \in A$, the commutator of a and b is defined as $[a, b] = ab - ba$. Let A be a $n-$dimensional $K-$algebra ($n \in \mathbb{N}$), and let $B = \{x_1, \ldots, x_n\}$ be a K-basis of a A. Then, there exists a unique set of constants $\{M_{ijk}\}_{i,j,k=1}^{n} \subseteq K$ such that

$$x_i \cdot x_j = \sum_{k=1}^{n} M_{ijk} x_k\ ,\ \forall i, j \in \{1, \ldots, n\}$$

These multiplication constants are also known as cubical array, 3-cube or multiplication table corresponding to A with respect to the basis B. They completely determine the product in A, because of the distributivity of the multiplication with respect to the sum. Notice that A is a commutative algebra if and only if the commutator $[x_i, x_j]$ is zero for all $i, j = 1, \ldots, n$, i.e., if and only if $M_{ijk} = M_{jik}$, for all $1 \leq i, j, k \leq n$. In case the algebra A is not commutative, it is evident that there must exist an even number of multiplication constants witnessing this fact. Namely, those M_{ijk} different from M_{jik}. As a consequence, from a computational point of view, when testing the commutativity of a finite dimensional algebra it is enough to *detect* the existence of such multiplication constants. This will be of importance in our work, since we need only to cope with the *detection* problem and not with the *finding* problem.

In the classical case, it can be proved (cf. [13]) that any probabilistic algorithm with bounded error requires $\Theta(n^3)$ consults to the multiplication table. In order to reduce this complexity, we have previously studied quantum approaches to this detection problem in two different ways: with the use of Grover's search algorithm ([13]) and with the application of quantum adiabatic techniques ([14]). In the latter case, we have obtained a method, using a local schedule, that runs in $O(\sqrt{n^3})$ time, while in the former we were able to prove the following theorem:

Theorem 1. *There is a quantum decision algorithm on the gate model requiring $\Theta(\sqrt{n^3})$ queries to the oracle O^A such that, on output NO certifies the noncommutativity of A with certainty, while on output YES the probability of A being noncommutative is a constant strictly greater than 0. Moreover, it is query-optimal among the quantum algorithms, in the sense that any other algorithm with bounded error probability for testing the commutativity of the finite dimensional $K-$algebra A uses $\Omega(\sqrt{n^3})$ queries.*

In this work, we use quantum walks ir order to improve the detection probabilities of this Grover's search-based method.

3. Quantum Walks

Classical random walks are probabilistic procedures which allow to move between the adjacent vertices of a graph. This random behavior, which is controlled by a time-reversible Markov chain, arises in many mathematical and physical models [20]. The quantum analogue of random walks, that is, a quantum procedure

mimicking the movement between the adjacent vertex of a graph are quantum walks [21]. Examples of quantum walks include the coined discrete-time [22], the continuous-time [23] or the coinless quantum walks [24]. These walks have been successfully used to solve different problems such as the element distinctness [25] or the triangle finding [26]. In general, these quantum walks allow to detect or find vertices with specific properties in the graph.

In this paper, we focus on Szegedy's quantum walk on a bipartite graph [27] and in its query version [28]. The discrete structures considered will be the complete and torus graphs. All of them are natural choices in the context of the commutativity problem addressed in this paper (see Section 5 below). Also, as Grover's quantum search algorithm has been proved to be equivalent to a coined quantum walk [29], we include our previous algorithm [13] in this setting.

Szegedy's quantum walk is inspired on the algorithm for testing element distinctness, and it can be seen as a quantum walk on the vertices of the graph to be walked. Its main characteristic is the use of the *leaking* graph, a modified directed graph where the marked vertices are absorbent sinks. On the other hand, Santo's quantum walk follows a Grover-like approach, using queries to an oracle to reflect around marked vertices. Our main reason for considering these two quantum walks is that the first one is foundational in the design of quantum algorithms, while the second one has been shown to boost up the probability of finding marked elements (at least, in the case of the complete graph [28]).

Let (V, E) be a connected, non-directed, non-bipartite graph with a finite set of N vertices. For any $x \in V$, consider the set of adjacent vertices $y \in Y$, i.e., $A_x = \{y \in Y \mid \{x, y\} \in E\}$. The matrix associated with the graph is $P \in \mathcal{M}_{|V|\times|V|}(\mathbb{R})$ defined by

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

This matrix is stochastic since the elements of any of its rows add up to one. Observe that, because the graph is non-directed, the matriz P is symmetric, and so doubly stochastic.

Assume that M out of the N vertices of the graph are "marked", i.e., there exists a fixed subset W of V of cardinality M containing those elements whose existence we want to *detect* in our graph (it might be perfectly possible that W is the empty set). The stochastic matrix of the corresponding *leaking* graph, i.e, the directed graph obtained from V converting all outer arcs from a marked vertex in a loop, is

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

From the graph (V, E), a N^2-dimensional Hilbert space $\mathbb{C}^N \otimes \mathbb{C}^N$ is constructed, with its computational basis given by $\{|x, y\rangle \mid x, y \in V\}$. The following linear operators on $\mathbb{C}^N \otimes \mathbb{C}^N$ will be used:

- $R_A = 2\sum_x |\Phi_x\rangle\langle\Phi_x| - I_{N^2}$
- $R_B = 2\sum_y |\Psi_y\rangle\langle\Psi_y| - I_{N^2}$
- $R'_A = 2\sum_x |\Phi'_x\rangle\langle\Phi'_x| - I_{N^2}$
- $R'_B = 2\sum_y |\Psi'_y\rangle\langle\Psi'_y| - I_{N^2}$
- $R_M = (I_N - 2\sum_{x\in W} |x\rangle\langle x|) \otimes I_N$

These operators reflect the Hilbert space around different subspaces, namely those generated by:

- $|\Phi_x\rangle = |x\rangle \otimes \left(\sum_y \sqrt{P_{xy}}|y\rangle\right)$
- $|\Psi_y\rangle = \left(\sum_x \sqrt{P_{xy}}|x\rangle\right) \otimes |y\rangle$
- $|\Phi'_x\rangle = |x\rangle \otimes \left(\sum_y \sqrt{P'_{xy}}|y\rangle\right)$
- $|\Psi'_y\rangle = \left(\sum_x \sqrt{P'_{xy}}|x\rangle\right) \otimes |y\rangle$

Suitable combination of the previous operators give the evolution operators of the two quantum walks that will be considered in the paper. Namely:

- For Szegedy's quantum walk, we consider $U_{P'} = R'_B R'_A$
- For Santos' quantum walk, we apply $U_P = R_B R_A R_M$

As mentioned above, the two quantum walks have a different behavior when dealing with a marked vertex: Szegedy's quantum walk *stays* in the vertex (because of the use of the leaking graph), while Santos' quantum walk *reflects* around the vertex (because of the use of the oracle).

The initial state $|\psi(0)\rangle$ depends only on the graph considered, and not in the nature of the quantum walk under study. It is simply a uniform superposition of the edges in the graph:

$$|\psi(0)\rangle = \frac{1}{\sqrt{2|E|}} \sum_{x,y} |x\rangle|y\rangle$$

The quantum walk per se simply iterates the operator U_P or $U_{P'}$ to create a sequence of states recursively defined by the rule $|\psi(t+1)\rangle = U_*|\psi(t)\rangle$, for all $t \in \mathbb{N}$, with $* \in \{P', P\}$.

However, we are not simply interested in walking our bipartite graph of adjacent vertices, but using the walk to *detect* the existence of elements in the set W. The details of such a detection procedure will be given in the following section.

4. Detection Problem with Quantum Walks

As mentioned in Section 2, our interest is in the testing of commutativity of finite dimensional algebras. To that extent, it is enough for our purposes to be able to determine if there are elements $1 \leq i, j, k \leq n$ such that $M_{ijk} \neq M_{jik}$, with n the dimension of the K-algebra and $\{M_{ijk}\}_{i,j,k=1}^n \subseteq K$ its multiplication constants. In the nomenclature of the previous section, this means that we are not interested in finding an element in $W = \{(i, j, k) : M_{ijk} \neq M_{jik}\}$ but only in determining whether W is empty or not.

Following [27], detecting the non-emptiness of the set W with the use of quantum walks requires adding an extra control qubit to our quantum walk Hilbert space. The evolution is finally described by the controlled operator cU_* (where $* \in \{P', P\}$):

$$cU_* : |a\rangle \otimes |x, y\rangle \to |a\rangle \otimes U_*^{1-a}|x, y\rangle$$

i.e., the second register is transformed by the quantum walk operator if the content of the first register is $|0\rangle$, and it is left untouched otherwise. In this situation, the initial state $|0\rangle \otimes |\psi(0)\rangle$ is prepared with a Hadamard transformation in the first register to get the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi(0)\rangle$, which is later processed by t walk steps, $\frac{1}{\sqrt{2}}(|0\rangle \otimes U_*^t|\psi(0)\rangle + |1\rangle \otimes |\psi(0)\rangle)$, before applying a Hadamard transformation to obtain the final state

$$\frac{1}{2}|0\rangle \otimes (U_*^t|\psi(0)\rangle + |\psi(0)\rangle) + \frac{1}{2}|1\rangle \otimes (U_*^t|\psi(0)\rangle - |\psi(0)\rangle)$$

The final measurement is carried out on the control bit and the left walk register. If the control register is 1 or the element measured in the left walk register is marked, then W is not empty.

The number of iterations which have to be applied in order to get a bounded side error algorithm is related, in the case of the Szegedy's quantum walk, to the *quantum hitting time* [27]. It is defined as the smallest natural number T such that

$$\frac{1}{T+1} \sum_{t=0}^{T} \|U_{P'}^t|\psi(0)\rangle - |\psi(0)\rangle\|^2 \geq 1 - \frac{M}{N}$$

(observe the dependence of T from the set of marked elements W). According to [27, Section 9], if $\mathcal{T}$ is an upper bound for all possible hitting time T, then choosing a random number of iterations $1 \leq t \leq \mathcal{T}$, guarantees that the detection method success with probability at least $\frac{1}{8}$ (cf. Remark 2 below).

In the case of Santos' quantum walk, no stopping condition is given in [28]. This is because Santos' analysis is focused on showing that the quantum walk boosts up the probability of *finding* a marked vertex, with respect to Szegedy's quantum walk. So, the focus of attention is on the maximum probability attained by each of the walks.

In our particular situation, being the main interest providing an efficient algorithm for testing the commutativity of a finite dimensional algebra, we need to provide for an analogue of Szegedy's quantum hitting time. Some extensions of this concept can be found in the literature in the context of abstract search algorithms [30, 31]. These approaches are based on the application of two operators (a reflection and an operator with a unique $1-$eigenvector). However, since we do not need to find but to detect, we propose a generalization of Szegedy's quantum hitting time in an alternative, less restrictive way.

Definition 1. Let V be a set of N elements, and let $\mathcal{M}$ be a subset of the power set $P(V)$, containing the empty set (if $W \in \mathcal{M}$, W is a set of M "marked" elements). Let $|\psi(0)\rangle$ be a state in a Hilbert space $\mathcal{H}$, and let m be a map from the computational basis of $\mathcal{H}$ into V. Consider also a set $\mathcal{U} = \{U_W \ | W \in \mathcal{M}\}$ of unitary transformations on $\mathcal{H}$. The triple $(\mathcal{U}, |\psi(0)\rangle, m)$ will be called a *quantum detecting system* for $\mathcal{M}$, if for all $W \in \mathcal{M}$ it holds that

$$W = \emptyset \Longleftrightarrow U_W|\psi(0)\rangle = |\psi(0)\rangle$$

The transformations U_W will be called *detecting operators*.

Notice that our proposal encompasses the abstract search algorithm but not the other way around. What is more, all the quantum methods that we consider in this work are special cases of quantum detection systems, as the following examples show.

Example 1.
1. The set of Grover operators on $\mathcal{H} = \mathbb{C}^N$ is a detecting system together with the uniform state $|\psi(0)\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$. The map m can be taken to be the natural correspondence between the elements in the computational basis of $\mathcal{H}$, and the 2^N elements in which the Grover search is performed.
2. The set of Santos' and Sezgedy's evolution operators on the quantum walk space $\mathcal{H} = \mathbb{C}^{N^2}$ is a detecting family with respect to the initial state $|\psi(0)\rangle = \frac{1}{\sqrt{2|E|}} \sum_{x,y} |x\rangle|y\rangle$. The map m can be taken to be $|x\rangle|y\rangle \to x$, i.e., the content of the left register of $\mathcal{H}$.

The following definition is the natural extension of Szegedy's quantum hitting time in this setting:

Definition 2. If U_W is a detecting operator, then we say that T is a *δ-quantum detecting time for U_W* (or, simply, T is δ-detecting for U_W) if

$$\frac{1}{T+1} \sum_{t=0}^{T} \|U_W^t|\psi(0)\rangle - |\psi(0)\rangle\|^2 \geq 4\delta$$

The rationale of this definition is given by the following result, which extends Sgezedy's [27, Section 9].

Theorem 2. *Let U_W be a detecting operator on a Hilbert space $\mathcal{H}$ and let cU_W be the corresponding controlled operator on the Hilbert space $\mathbb{C}^2 \otimes \mathcal{H}$:*

$$cU_W : |a\rangle \otimes |x, y\rangle \to |a\rangle \otimes U_W^{1-a}|x, y\rangle$$

The following algorithm detects the nonemptiness of W with bounded one side error and success probability at least δ provided that T is δ-detecting for U_W.

Algorithm: *Detecting the nonemptiness of W*

Pick uniformly an integer $t \in \{0, \ldots, T\}$
Initialize the state to $|0\rangle \otimes |\psi(0)\rangle$
Apply a Hadamard transformation in the first (control) qubit, $H \otimes I$, to get $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi(0)\rangle$
Apply t iterations of the controlled operator cU_W to get $\frac{1}{\sqrt{2}}(|0\rangle \otimes U_W^t|\psi(0)\rangle + |1\rangle \otimes |\psi(0)\rangle)$

Apply a Hadamard transformation in the first (control) qubit, $H \otimes I$,
to get $\frac{1}{2}|0\rangle \otimes (U_W^t|\psi(0)\rangle + |\psi(0)\rangle) + \frac{1}{2}|1\rangle \otimes (U_W^t|\psi(0)\rangle - |\psi(0)\rangle)$
Measure the control bit $|a\rangle$ and the state $|\xi\rangle \in \mathcal{H}$.
If $|a\rangle = |1\rangle$ or $m|\xi\rangle$ is a marked element, return "W NOT EMPTY"
Else, return "W EMPTY"

Proof. If W is empty, then from the definition of detecting operator, we get that $U_W^t|\psi(0)\rangle = |\psi(0)\rangle$, so the algorithm never outputs "W NOT EMPTY".

If W is not empty, because of the definition of quantum detecting time, we have that the average over $0 \leq t \leq T$ of $\|U_W^t|\psi(0)\rangle - |\psi(0)\rangle\|^2$ is at least 4δ. Therefore, in average, we have the following bound:

$$\left\| \frac{1}{2}|1\rangle \otimes (U_W^t|\psi(0)\rangle - |\psi(0)\rangle) \right\|^2 = \frac{1}{4} \left\| |1\rangle \otimes (U_W^t|\psi(0)\rangle - |\psi(0)\rangle) \right\|^2 \geq \frac{1}{4} 4\delta = \delta$$

Thus, the probability of measuring the control bit equal to $|1\rangle$ and returning "W NOT EMPTY" is at least δ. □

Remark 1. Observe that testing if $m|\xi\rangle$ is a marked element is not needed to prove the algorithm correctness. Its effect is to boost up the probability of success in accordance with the analysis of the original Szegedy's quantum walk [27, Section 9].

Remark 2. The connection with Sezgedy's quantum hitting time is clear: if T is the quantum hitting time of $U_{P'}$ and provided that $\frac{|W|}{|V|} \leq \frac{1}{2}$, we have that

$$\frac{1}{T+1} \sum_{t=0}^{T} \|U_{P'}^t|\psi(0)\rangle - |\psi(0)\rangle\|^2 \geq 1 - \frac{M}{N} \geq \frac{1}{2}$$

Thus, T is $\frac{1}{8}$-detecting for $U_{P'}$ and we can apply the algorithm above to detect the presence of marked elements with one-sided bounded error. If, on the other hand, $\frac{|W|}{|V|} > \frac{1}{2}$, we can simply choose an element from V uniformly at random and test whether it is marked or not. We will succeed with probability greater than $\frac{1}{2}$ and, consequently, this (classical) algorithm is, again, one-sided bounded error for the problem of detection.

Because of this last remark, we will pay special attention to the quantum hitting times of the detecting operators that we are going to use in our numerical experiments in the next section.

5. Numerical experiments

Next, we apply the detecting algorithm of the previous section to our problem of interest: testing the commutativity of an algebra A of finite dimension n. We will consider Szegedy's and Santos' quantum walks in combination with two different types of graphs in the set of multiplication constants: the complete graph, and the torus graph. The first graph is perhaps the most studied and best understood in the context of quantum walks. The second one is a natural choice in the context of our problem, because of the "3−dimensional" description of the multiplication constants of the algebra.

So, let (V, E) be one of the following two graphs on the cartesian product $V = \{0, 1, \ldots, n-1\}^3$:

- Complete graph:

$$EC = \{\{(i,j,k)\ ,\ (i',j',k')\} \mid (i,j,k),(i',j',k') \in V \text{ s.t. } (i,j,k) \neq (i',j',k')\}$$

  that is, there is a unique edge linking any two different vertices.

- Torus graph:

$$ET = \{(i,j,k)\ ,\ (i',j',k') \mid (i,j,k),(i',j',k') \in V \text{ s.t. } (i,j,k) - (i',j',k') \equiv (\pm 1,0,0),(0,\pm 1,0) \text{ or } (0,0,\pm 1) \bmod n\}$$

  so two vertices are linked if and only if the difference is, up to sign and mod n, one of the vectors of the standard basis $\{e_1, e_2, e_3\}$ of $\mathbb{R}^3$.

For these graphs, the associated stochastic matrices are

$$PC_{(i,j,k),(i',j',k')} = \frac{\delta_{(i,j,k),(i',j',k')}}{n^3-1}$$

and

$$PT_{(i,j,k),(i',j',k')} = \begin{cases} \frac{1+\delta_{n,2}}{6} & \text{if } (i,j,k)-(i',j',k') \equiv \pm e_1, \pm e_2, \pm e_3 \bmod n \\ 0 & \text{otherwise} \end{cases}$$

The evolution operators of the four different types of quantum walks that will be considered in the paper are:

- Szegedy's quantum walk on the complete graph: $U_{PC'} = R'_B R'_A$, with $P = PC$.
- Szegedy's quantum walk on the torus graph: $U_{PT'} = R'_B R'_A$, with $P = PT$.
- Santos' quantum walk on the complete graph: $U_{PC} = R_B R_A R_M$, with $P = PC$.
- Santos' quantum walk on the torus graph: $U_{PT} = R_B R_A R_M$, with $P = PT$.

Finally, the initial state $|\psi(0)\rangle$ will be, for the complete graph,

$$|\psi(0)\rangle = \frac{1}{\sqrt{n^3(n^3-1)}} \sum_{(i,j,k)\neq(i',j',k')} |(i,j,k)\rangle|(i',j',k')\rangle$$

and in the case of the torus graph,

$$|\psi(0)\rangle = \frac{1}{\sqrt{\frac{6n^3}{1+\delta_{n,2}}}} \sum_{(i,j,k)-(i',j',k') \equiv \pm e_1, \pm e_2, \pm e_3 \bmod n} |(i,j,k)\rangle|(i',j',k')\rangle$$

For each of the four quantum walks considered in the paper (i.e., $* \in \{PC, PC', PT, PT'\}$) the algorithm of the previous section reads in our situation:

Main Algorithm: Testing the commutativity of the algebra A

Pick uniformly an integer $t \in \{0, \ldots, T\}$
Initialize the state to $|0\rangle \otimes |\psi(0)\rangle$
Apply a Hadamard transformation in the first (control) qubit, $H \otimes I$, to get $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\psi(0)\rangle$
Apply t iterations of the controlled operator cU_* to get $\frac{1}{\sqrt{2}}(|0\rangle \otimes U_*^t|\psi(0)\rangle + |1\rangle \otimes |\psi(0)\rangle)$
Apply a Hadamard transformation in the first (control) qubit, $H \otimes I$,
to get $\frac{1}{2}|0\rangle \otimes (U_*^t|\psi(0)\rangle + |\psi(0)\rangle) + \frac{1}{2}|1\rangle \otimes (U_*^t|\psi(0)\rangle - |\psi(0)\rangle)$
Measure the control bit $|a\rangle$ and the left register of $U_*^t|\psi(0)\rangle + |\psi(0)\rangle$.
If $|a\rangle = |1\rangle$ or the left register $|ijk\rangle$ is such that $M_{ijk} \neq M_{jik}$, return "A NOT CONMMUTATIVE"
Else, return "A COMMUTATIVE"

The previous algorithm has been programmed in MATLAB and executed in a server with 12 cores and 1TB of RAM. This has allowed us to scale up our experiments and test finite dimensional algebras of dimensions from $n = 2$ up to $n = 7$ over an arbitrary field K. We have specifically focused our study on the extremal case of an algebra with only one pair of multiplication constants witnessing its noncommutativity. Then, we hace that the proportion of marked elements is exactly $\frac{2}{n^3}$. Since $n \geq 2$, this proportion is always strictly less than $\frac{1}{2}$ and the reasoning for the quantum hitting time that we stated in Remark 2 applies in our case. Consequently, we can apply Theorem 2 to prove the adequacy of our algorithm. Notice also that the analyses in [32] and in [27, Section 11] together with Remark 2 and Theorem 2 allow us to conclude that for both complete and torus graphs, Szegedy's quantum walk succeeds in time $O(\sqrt{n^3})$, exactly as the algorithm we proposed in [13].

Figures 1 through 6 summarize the behavior of the different quantum walks considered for different number of iterations T. Namely, we present the probability of the algorithm returning "A NOT CONMMUTATIVE", that is given by (cf. Remark 1)

$$\frac{4}{T+1}\sum_{t=0}^{T}\sum_{\{x,y\}\in E, x\in W}(|\langle U_*^t|\psi(0)\rangle + |\psi(0)\rangle, |x\rangle|y\rangle\rangle|^2 + \|U_*^t|\psi(0)\rangle - |\psi(0)\rangle\|^2)$$

Also, it has been included the detecting probability of our algorithm for the same problem [13], based on Grover's search, to compare.

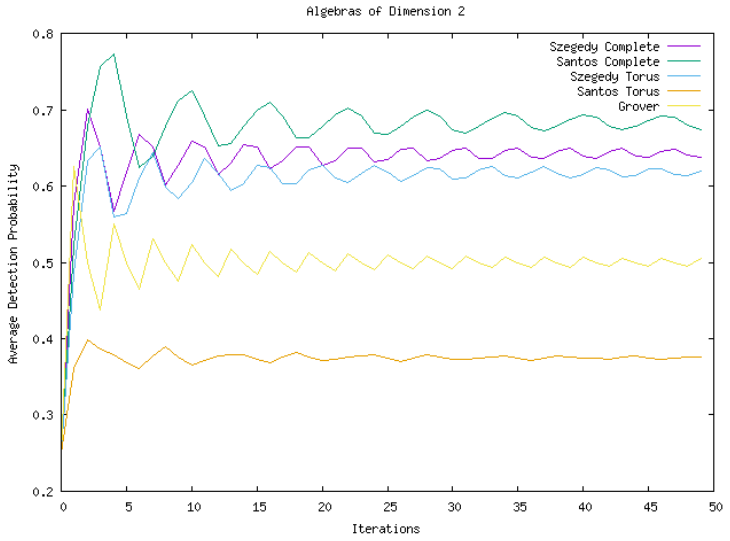

Figure 1: Probability of detecting the unique pair of non-commutative witnesses for $K-$algebras of dimension $n = 2$

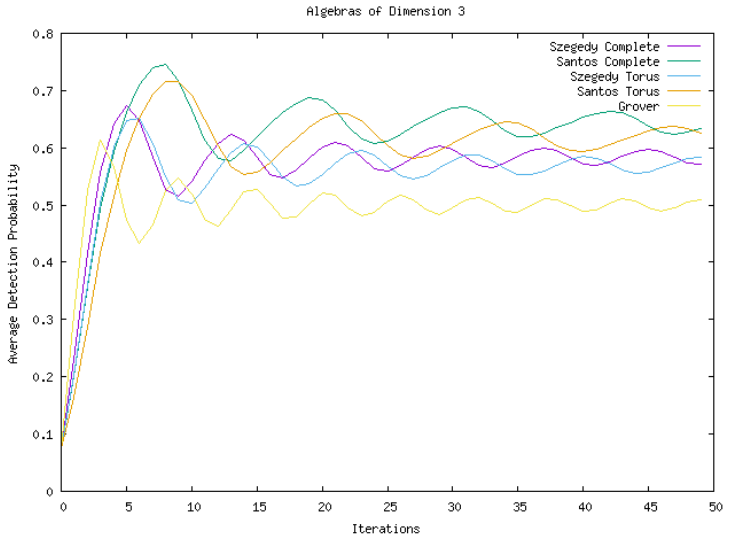

Figure 2: Probability of detecting the unique pair of non-commutative witnesses for $K-$algebras of dimension $n = 3$

As we can see, for a fixed type of quantum walk (Szegedy's or Santos') the detecting probabilities are greater in the case of the complete graph than in the case of the torus graph. Moreover, in accordance with the results

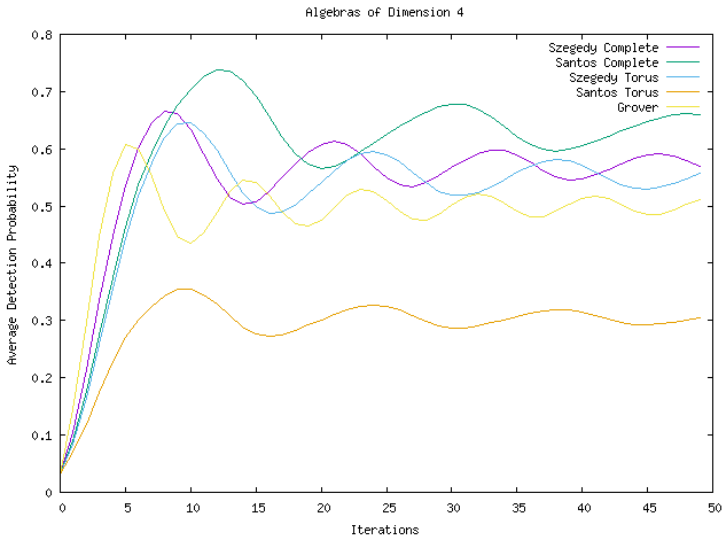

Figure 3: Probability of detecting the unique pair of non-commutative witnesses for $K-$algebras of dimension $n = 4$

presented in [28] in relation with the finding problem, the best detecting probability is attained with Santos' quantum walk on the complete graph, beating Szegedy's marks. The performance of Santos' quantum walk with the torus is sometimes (for odd values of n) even better than Sgezdy's algorithm with the complete graph (this partially confirms, in the detection context, Santos' conjecture in [28] that this kind of quantum walk can boost up probabilities not only for the complete graph.

An exception occurs with even n, where the Santos' quantum walk with the torus have a specially low sequence of detecting probabilities. Such a probability is even worse than the detecting probability using Grover's algorithm which, except for this particular instance, is always outperformed by any of the quantum walks considered. An explanation for this anomaly is that in the even case the operator U_{PT} has an eigenvalue -1 which affects the walking in the graph. A possible solution for this might be the use of Lackadaisical quantum walks as presented in [33], where every vertex has a self-loop adding an absorbing probability to the stochastic matrix of the quantum walk.

The particular quantum hitting times for our experiments can be found in figure 7. It is clear that Szegedy's quantum walks (both with the complete and torus graphs) have a smaller hitting time than Santos', and that the complete walk always hits sooner than the corresponding torus walk. So, in combination with the results on probability above, Santos' quantum walk provides better results from the point of view of probability, but more iterations are required to be obtained. The detection probability obtained in each of the quantum hitting times is presented is figure 8, which confirms this last observation. Also, notice that these probabilities are greater than what Theorem 2 would let us to expect (cf. Remark 2). This is because of the effect of the particular choice of m in this setting (see Definition 1 and Remark 1).

A final observation is the apparently independence of the maximum and minimum detecting probabilities of n (except in the case of Santos' quantum walk with the torus and n even). Namely, the probability function for greater values of n appears to be an "amplification" in the X axis of the probability function for smaller values of n, without significantly altering the upper and lower bounds.

6. Conclusions and future work

In this work we have presented a practical approach to the determination of the commutativity of a finite dimensional algebra with the use of quantum walks. Previous proposals of quantum algorithms solving this problem were the use of Grover's search algorithm and the use of Adiabatic techniques. Specifically, we have considered two types of quantum walks (Szegedy's and Santos') with two different underlying discrete structures (the complete and torus graphs).

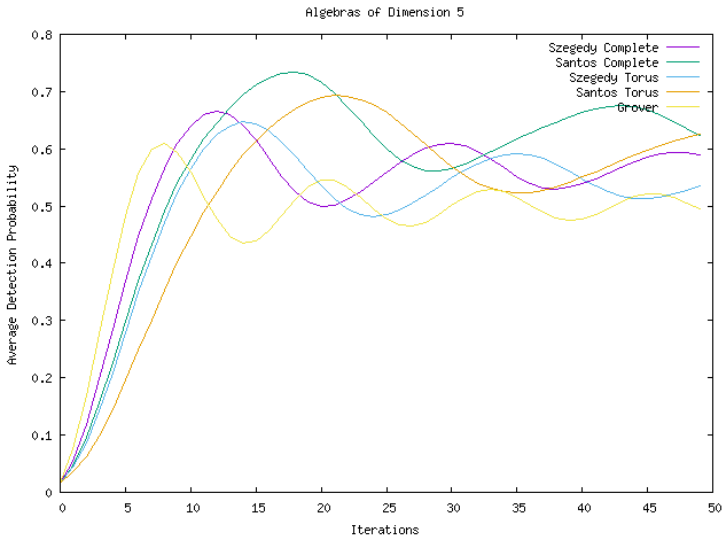

Figure 4: Probability of detecting the unique pair of non-commutative witnesses for $K-$algebras of dimension $n = 5$

Since a quantum hitting time for Santos' quantum walk was not given in her proposal, we have introduced such a concept in accordance with Szegedy's definition. This quantum hitting time is introduced in a more general setting so it can not only be applied to Santos' quantum walk, but also for other types of *detecting operators*. We have also use it to prove that, when the hitting time is used as the stop criteria of a detecting procedure, it yields a a bounded one side error algorithm.

Finally, we have run experiments testing the four quantum walks under study for algebras of dimensions $n = 2, \ldots, 7$ over any field K. An analysis of their performance, and also of our Grover's algorithm solving the same problem, shows that the best results are obtained with Santos' quantum walk and the complete graph. However, to get this results it is necessary a bigger number of iterations, as the quantum hitting time is greater.

As future open problems which are left by this study is the analysis of the possible "solution" using Laickadaisical quantum walks for the odd behavior of Santos' quantum walk in the torus when n is even, a analytic study of the behavior of the walks on the torus graph, or a deeper study of the extended notion of quantum hitting time introduced.

Acknowledgments

This work has been partially supported by MINECO-16-TEC2015-67387-C4-3-R and MTM - 2017 - 83506 - C2 - 2 - P.

References

[1] R. Feynman, Simulating physics with computers, International Journal of Theoretical Physics 21 (6) (1982) 467–488.

[2] Y. Manin, Vychislimoe i nevychislimoe, Sov. Radio (1980) 13–15.

[3] P. Benioff, The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines, Journal of statistical physics 22 (5) (1980) 563–591.

[4] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 439 (1907) (1992) 553–558.

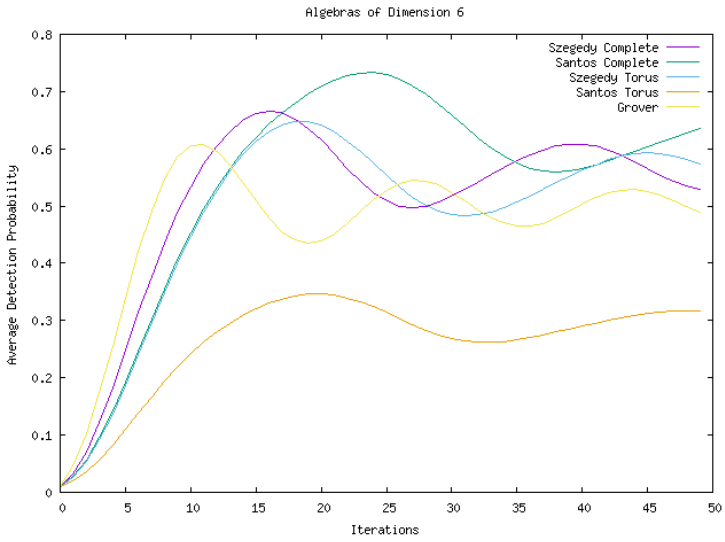

Figure 5: Probability of detecting the unique pair of non-commutative witnesses for $K-$algebras of dimension $n = 6$

[5] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC '96, ACM, New York, NY, USA, 1996, pp. 212–219.

[6] P. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings of FOCS (1994) 124–134.

[7] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition, Cambridge University Press, 2011.

[8] S. Jordan, Quantum Algorithm Zoo, 2011-18.
URL `http://math.nist.gov/quantum/zoo/`

[9] E. Farhi, J. Goldstone, S. Gutmann, M. Sipser, Quantum computation by adiabatic evolution, arXiv:quant-ph/0001106v1, 2000.

[10] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, D. Preda, A quantum adiabatic evolution algorithm applied to random instances of an NP-Complete problem, Science 292 (5516) (2001) 472–475.

[11] P. Shor, Why haven't more quantum algorithms been found?, Journal of the ACM 50 (1) (2003) 87–90.

[12] A. Montanaro, Quantum algorithms: an overview, Npj Quantum Information 2 (2016) 15023.

[13] E. F. Combarro, J. Ranilla, I. Rúa, A quantum algorithm for the commutativity of finite dimensional algebras, Submitted.

[14] E. F. Combarro, I. F. Rúa, J. Ranilla, Experiments testing the commutativity of finite-dimensional algebras with a quantum adiabatic algorithm, in: Proceedings 18th Computational and Mathematical Methods in Science and Engineering (CMMSE 2018), 2018.

[15] E. F. Combarro, I. F. Rúa, J. Ranilla, New advances in the computational exploration of semifields, International Journal of Computer Mathematics 88 (9) (2011) 1990–2000.

[16] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of mathematics and its applications 20.

[17] S. Lang, Algebra, Addison-Wesley, 1965.

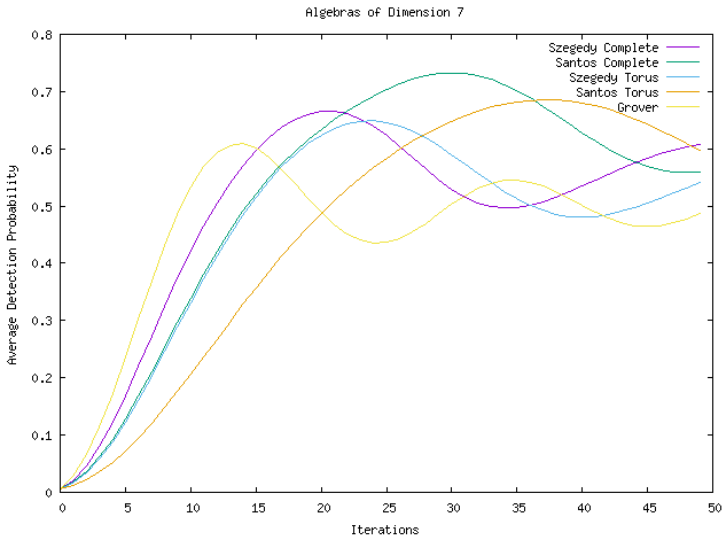

Figure 6: Probability of detecting the unique pair of non-commutative witnesses for $K-$algebras of dimension $n = 2$

[18] R. D. Schafer, An introduction to nonassociative algebras, Pure and Applied Mathematics 22.

[19] I. F. Rúa, E. F. Combarro, J. Ranilla, Classification of semifields of order 64, J. of Algebra 322 (11) (2009) 941–961.

[20] L. Lovász, Random walks on graphs: A survey, in: D. Miklós, V. T. Sós, T. Szőnyi (Eds.), Combinatorics, Paul Erdős is Eighty, Vol. 2, János Bolyai Mathematical Society, Budapest, 1996, pp. 353–398.

[21] S. E. Venegas-Andraca, Quantum Walks for Computer Scientists, Synthesis Lectures on Quantum Computing, Morgan & Claypool Publishers, 2008.

[22] Y. Aharonov, L. Davidovich, N. Zagury, Quantum random walks, Phys. Rev. A 48 (1993) 1687–1690.

[23] E. Farhi, S. Gutmann, Quantum computation and decision trees, Physical Review A 58 (2) (1998) 915–928.

[24] R. Portugal, Quantum Walks and Search Algorithms, Springer New York, 2013.

[25] A. Ambainis, Quantum walks and their algorithmic applications, International Journal of Quantum Information 1 (2003) 507–518.

[26] F. Magniez, M. Santha, M. Szegedy, Quantum algorithms for the triangle problem, SIAM Journal on Computing 37 (2) (2007) 413–424.

[27] M. Szegedy, Quantum speed-up of markov chain based algorithms, in: Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, FOCS '04, IEEE Computer Society, Washington, DC, USA, 2004, pp. 32–41.

[28] R. A. M. Santos, Szegedy's quantum walk with queries, Quantum Information Processing 15 (11) (2016) 4461–4475.

[29] T. Wong, Equivalence of szegedys and coined quantum walks, Quantum Inf Process 16 (215).

[30] A. Ambainis, J. Kempe, A. Rivosh, Coins make quantum walks faster, in: Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA '05, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2005, pp. 1099–1108.

[31] A. Tulsi, Faster quantum-walk algorithm for the two-dimensional spatial search, Phys. Rev. A 78 (2008) 012310.

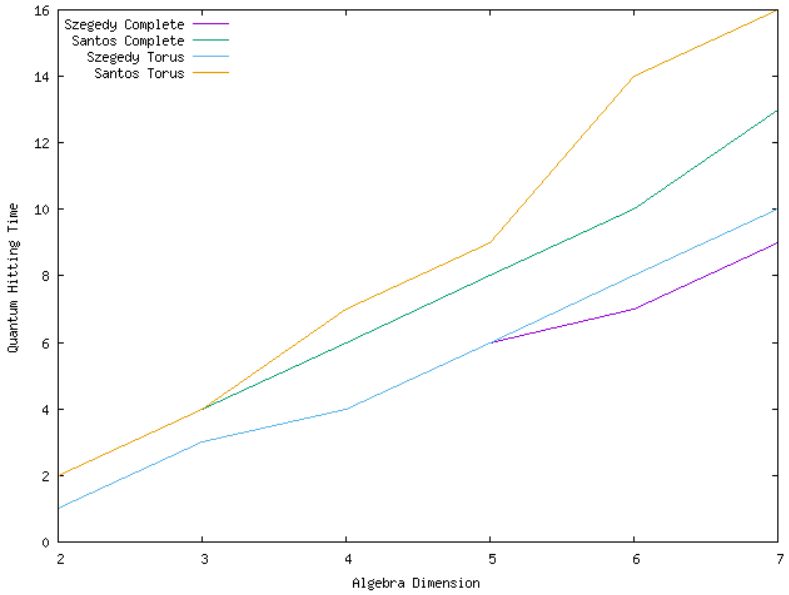

Figure 7: Quantum hitting times for detecting a unique pair of non-commutative witness for $K-$algebras of dimensions $n = 2, \ldots, 7$

[32] R. A. M. Santos, R. Portugal, Quantum hitting time on the complete graph, International Journal of Quantum Information 8 (5) (2010) 881–894.

[33] T. Wong, Faster search by lackadaisical quantum walk, Quantum Inf Process 17 (68).

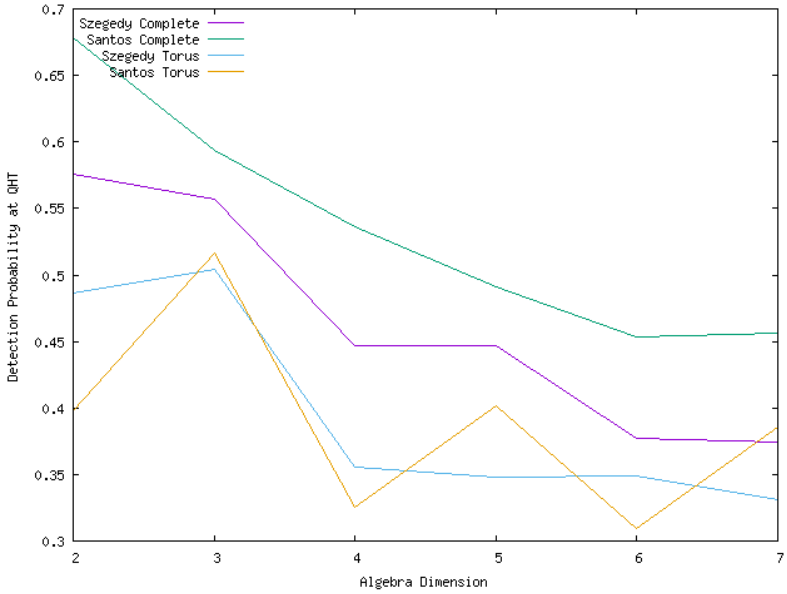

Figure 8: Detecting probability, at the quantum hitting times, of unique pair of non-commutative witness for $K-$algebras of dimensions $n = 2, \ldots, 7$