On the hitting times of quantum versus random walks *

Frédéric Magniez† Ashwin Nayak‡ Peter C. Richter§ Miklos Santha¶

Abstract

The *hitting time* of a classical random walk (Markov chain) is the time required to *detect* the presence of – or equivalently, to *find* – a marked state. The hitting time of a quantum walk is subtler to define; in particular, it is unknown whether the detection and finding problems have the same time complexity. In this paper we define new Monte Carlo type classical and quantum hitting times, and we prove several relationships among these and the already existing Las Vegas type definitions. In particular, we show that for some marked state the two types of hitting time are of the same order in both the classical and the quantum case.

Then, we present new quantum algorithms for the detection and finding problems. The complexities of both algorithms are related to the new, potentially smaller, quantum hitting times. The detection algorithm is based on phase estimation and is particularly simple. The finding algorithm combines a similar phase estimation based procedure with ideas of Tulsi from his recent theorem [Tul08] for the 2D grid. Extending his result, we show that we can find a unique marked element with constant probability and with the same complexity as detection for a large class of quantum walks—the quantum analogue of state-transitive reversible ergodic Markov chains.

Further, we prove that for any reversible ergodic Markov chain P, the quantum hitting time of the quantum analogue of P has the same order as the square root of the classical hitting time of P. We also investigate the (im)possibility of achieving a gap greater than quadratic using an alternative quantum walk. In doing so, we define a notion of reversibility for a broad class of quantum walks and show how to derive from any such quantum walk a classical analogue. For the special case of quantum walks built on reflections, we show that the hitting time of the classical analogue is exactly the square of the quantum walk.

1 Introduction

1.1 Background

Many classical randomized algorithms are based on *random walks*, or *Markov chains*. Some use random walks to generate random samples from the Markov chain's stationary distribution, in which case the *mixing time* of the Markov chain is the complexity measure of interest. Others use random walks to search for a "marked" state in the Markov chain, in which case the *hitting time* is of interest. In recent years, researchers studying *quantum walks* have attempted to define natural notions of "quantum mixing time" [NV00, ABN$^+$01, AAKV01] and "quantum hitting time" [AKR05, Sze04, MNRS07] and to develop quantum algorithmic applications to sampling and search problems.

*A preliminary version of this article appeared in *Proceedings of the Twentieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 86–95, 2009.

†LIAFA, Univ. Paris 7, CNRS; F-75205 Paris cedex 13, France; magniez@liafa.jussieu.fr.

‡Department of Combinatorics and Optimization and Institute for Quantum Computing, University of Waterloo; and Perimeter Institute for Theoretical Physics. 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada; ashwin.nayak@uwaterloo.ca.

§LRI, Univ. Paris-Sud, CNRS; peter.c.richter@gmail.com

¶LIAFA, Univ. Paris 7, CNRS; F-75205 Paris cedex 13, France; and Centre for Quantum Technologies, National University of Singapore, Singapore 117543; santha@lri.fr.

A few years ago, Ambainis [Amb07] designed a discrete quantum walk algorithm for a basic and well-studied problem—the "element distinctness problem". Following this, quantum walk algorithms were discovered for triangle finding [MSS07], matrix product verification [BŠ06], and group commutativity testing [MN07]. All of these are "hitting time" applications involving quantum walk search on Johnson graphs—highly-connected graphs whose vertices are subsets of a fixed set and whose edges connect subsets differing by at most two elements. Quantum walk algorithms for the generic *spatial search* problem [AA05] were given by Shenvi, Kempe, and Whaley [SKW03] on the hypercube, and by Childs and Goldstone [CG04] and Ambainis, Kempe, and Rivosh [AKR05] on the torus. Szegedy [Sze04] showed that for any symmetric Markov chain and any subset M of marked elements, we can detect whether or not M is nonempty in at most (of the order of) the square-root of the classical hitting time. To achieve this goal, Szegedy defined a quantum analogue of any symmetric Markov chain. Later Magniez, Nayak, Roland, and Santha [MNRS07] extended this to define a quantum analogue of the larger class of irreducible Markov chains.

Largely unresolved by Szegedy's work is the question: with what probability does the algorithm output a marked state, as opposed to merely detecting that M is nonempty? (Szegedy gave a partial solution, for *state-transitive* Markov chains, in the same piece of work.) This issue was addressed in its full generality by Magniez *et al.* [MNRS07], who gave an algorithm which finds a marked state with constant probability but whose complexity may be more than the square root of the classical hitting time. Indeed, for the $\sqrt{N} \times \sqrt{N}$ grid their bound is $\Theta(N)$ whereas the classical hitting time is $\Theta(N \log N)$. The algorithms due to Ambainis *et al.* [AKR05], Szegedy [Sze04], and Childs and Goldstone [CG04] perform better on the grid if there is a *unique* marked state: they find the marked state in time $\mathrm{O}(\sqrt{N} \cdot \log N)$. (The case of multiple marked elements may be reduced to this case at the cost of a polylog factor increase in run-time.)

For some time it remained unclear if one could do better, until Tulsi [Tul08] showed how to find a unique marked element in time $\mathrm{O}(\sqrt{N \log N})$. His algorithm seems to be something of a departure from previous quantum walk algorithms, most of which have been analyzable as the product of two reflections *à la* the Grover algorithm [Gro96]. The 2D grid was the canonical example of a graph on which it was unknown how to find a marked state quantumly with the same complexity as detection. Tulsi's result thus raises the question: is finding ever any harder than detection?

A commonly proposed reduction from finding to detection is a divide and conquer strategy. Assuming the detection algorithm claims a marked element exists (outputs "yes"), we conduct the following search:

> We start with the entire state space as the set S that potentially contains a marked element. Then, we choose a subset $S_0 \subset S$ of half the size of S. We then invoke the detection algorithm, in which we consider a state to be "marked" if in addition to being originally marked, it is also contained in S_0. If the detection algorithm outputs "yes", we update $S \leftarrow S_0$. If the output is "no", we update $S \leftarrow S - S_0$. We repeat the procedure until the set S contains only one element, at which point we expect to have a marked state.

While this strategy is correct, it bounds the search time in the presence of a set of marked elements by the detection time for the *worst case* marked state, times a factor that is polylogarithmic in the size of the state space. This is unsatisfactory for a number of reasons. We expect to be able to find marked states more easily when they are larger in number. Moreover, some marked states may be easier to detect than others, so that even when there is only one marked state, the complexity of the above algorithm may be far from optimal. Finally, the state space may be large enough to significantly affect the complexity. Indeed, we expect that there be algorithms that do not suffer from these drawbacks.

1.2 Contribution, relation with prior work, and organization

In this paper we address several questions related to classical and quantum hitting times, essentially for the special case of a unique marked element. In the literature on Markov chains, hitting time is usually defined as the complexity of the natural Las Vegas algorithm for finding a marked element by running the chain. We first give an alternative definition based on the Monte Carlo version of the same algorithm. To our knowledge, this variant of the hitting time has not been considered previously. We show that for some marked state, the two hitting times are of the same order (Theorem 2.3).

Within the setting of the so called "abstract search algorithms" presented by Ambainis *et al.* [AKR05], we introduce quantum analogues of the two classical hitting times (Definition 3.2). A rigorous analysis of the complexity of algorithms that incorporate quantum walks requires that we take into account all the costs associated with their use. We refer the reader to Refs. [MNRS07, San08] for an explanation of these costs, and how they motivate the notions of quantum hitting time we study. The analogue of the Las Vegas hitting time was already present in Szegedy's work [Sze04], whereas the other is new. Unlike in the classical case, detection and finding are substantially different problems in quantum computing. We address both problems here.

For the detection problem, we introduce a new algorithm **Detect** based on phase estimation which is similar to the approach of Magniez *et al.* [MNRS07]. Our algorithm can detect the presence of a marked element in the starting state, even in the presence of multiple marked elements. The advantages of this algorithm are its simplicity and the fact that its complexity is related to the new Monte Carlo type quantum hitting time (Theorem 3.5 and Corollary 3.6). This is an improvement over the Szegedy detection algorithm [Sze04] whose analysis was related to the potentially larger Las Vegas quantum hitting time, and also over the algorithm due to Ambainis *et al.* [AKR05], whose complexity was characterized by a potentially larger quantity, the inverse of the smallest eigenphase of the abstract search algorithm.

We then present a variant of the above algorithm, called **Rotate**, which can sometimes be used for the more difficult problem of finding, and whose complexity is also related to the Monte Carlo type quantum hitting time (Theorem 3.9). Combining **Rotate** with the ideas in the Tulsi algorithm [Tul08] for the 2D grid, we can find a unique marked element with constant probability and with the same complexity as detection for a large class of quantum walks—the quantum analogue of state-transitive reversible ergodic Markov chains (Theorem 4.9 and Corollary 4.10).

As in the classical case, for some marked elements the two types of the quantum hitting time are of the same order (Fact 3.10 and Theorem 3.14). For any reversible ergodic Markov chain P, we prove that the quantum hitting time of the quantum analogue of P is of same order as the square root of the classical hitting time of P (Theorem 3.15). Moreover, for the Las Vegas hitting times they are exactly the same.

Finally, we investigate the (im)possibility of achieving a greater than quadratic gap using some other quantum walk. For this we consider general quantum walks on the edges of an undirected graph G; these were defined, for example, in the survey article of Ambainis [Amb03], see also [San08]. We define a quite natural notion of reversibility for general quantum walks. We conjecture that for any reversible quantum walk U_2 on an undirected graph G, there exists a reversible ergodic Markov chain P on G such that for every marked state, the quantum hitting time of U_2 is at least the square root of the classical hitting time of P. We are able to prove this in the special case of quantum walks built on reflections (Theorem 3.18), thus elucidating the necessity of going beyond the reflections framework for super-quadratic speed-up. Our proof introduces a classical analogue of such quantum walks which might be of independent interest (Definition 3.6). Curiously, the classical analogue is reversible if the quantum walk is reversible (Lemma 3.17).

1.3 Subsequent work

Some of our results for the detection problem extend easily to handle multiple marked elements. For instance, the same quadratic speed-up for detection due to quantum algorithms holds when there are multiple marked elements in the state space X. The detection algorithm and its analysis are similar and are omitted from this article. But the generalization for the finding problem with multiple marked elements was open until recent work of Krovi, Magniez, Ozols, and Roland [KMOR10]. They made a significant leap by presenting a quantum algorithm for the finding problem in the presence of multiple marked elements in any reversible Markov chain. Taking a new, simpler, and more general approach, they introduce a notion of interpolation between any reversible chain and a perturbed version of this chain, in which the marked states are absorbing. The quantum analogue of the interpolated walk not only detects but also finds marked states with a quadratic speed-up over classical hitting time.

2 Classical hitting times

Let P be an ergodic Markov chain over state space $X = \{1, \ldots, n\}$, which we identify with its transition probability matrix. Let the stationary distribution of P be π. Throughout this article, we assume that P is *reversible*, namely $\pi_y p_{yx} = \pi_x p_{xy}$, for all $x, y \in X$. The *symmetrized form* of P is $S = \Pi^{1/2} P \Pi^{-1/2}$ with $\Pi = \mathrm{diag}(\pi_x)_x$. The matrices P and S have the same spectrum since they are similar. Moreover S is symmetric since P is reversible. We further suppose that the eigenvalues of P are nonnegative, by replacing P with $(P + I)/2$ if necessary. In fact, since P is ergodic, this transformation ensures that its smallest eigenvalue is positive. Let P_{-z} be the $(n-1) \times (n-1)$ matrix we get by deleting from P the row and column indexed by $z \in X$. Similarly, for a vector v, we let v_{-z} stand for the vector obtained by omitting the z-coordinate of v. Observe that S_{-z} is symmetric, and is similar to P_{-z} since it satisfies $S_{-z} = \Pi_{-z}^{1/2} P_{-z} \Pi_{-z}^{-1/2}$.

Claim 2.1. *The eigenvalues of P_{-z} are all in the interval $[\kappa_n, 1)$, where κ_n is the smallest eigenvalue of P. Moreover, $\|P_{-z}\| \in (\kappa_2, 1)$, where κ_2 is the second largest eigenvalue of P.*

Proof. The proof globally proceeds along the lines of the proof of Lemma 8 in [Sze04]. Since S_{-z} is similar to P_{-z}, we prove the claim for S_{-z} instead. For $x \in X$, let e_x denote the characteristic vector of x. Let $w_1, w_2, \ldots, w_n$ be the orthonormal eigenvectors of S with associated eigenvalues $1 = \kappa_1 \geq \ldots \geq \kappa_n > 0$. Let v be an arbitrary eigenvector of S_{-z} with eigenvalue λ. That $\|S_{-z}\| \leq 1$ follows as in Lemma 1, Section 5 of Ref. [MNRS07]. Since P is ergodic, $\|S_{-z}\| < 1$, therefore $\lambda < 1$. We show that $\lambda \geq \kappa_n$. This is obviously true if $\lambda = \kappa_k$ for some k; let us suppose that this is not the case.

Let w be the vector obtained from v by augmenting it with a 0 in the z-coordinate. We express both w and e_z in the eigenbasis of S: let $w = \sum_{k=1}^n \gamma_k w_k$ and $e_z = \sum_{k=1}^n \delta_k w_k$. Then $w^\dagger S = \lambda w^\dagger + \nu e_z^\dagger$ for some real number ν. Moreover, $\nu \neq 0$; otherwise w would be an eigenvector of S, meaning that $\lambda = \kappa_k$ for some k, which contradicts our supposition. For $k = 1, \ldots, n$, we have $\kappa_k \gamma_k = \lambda \gamma_k + \nu \delta_k$. Since w and e_z are orthogonal, we also have $\sum_{k=1}^n \gamma_k \bar{\delta_k} = 0$. Therefore $\sum_{k=1}^n \frac{|\delta_k|^2}{\kappa_k - \lambda} = 0$. The first statement in our claim then follows since the left hand side of the above equation would be positive if λ were less than κ_n.

Next we show that S_{-z} has an eigenvalue greater than κ_2, which proves the second statement. The function $f(\alpha) = \sum_{k=1}^n \frac{|\delta_k|^2}{\kappa_k - \alpha}$ has a root in $(\kappa_2, 1)$, as $f(\alpha) \to +\infty$ as $\alpha \to 1-$, it tends to $-\infty$ as $\alpha \to \kappa_2+$, and $f(\alpha)$ is a continuous function of α in the interval $(\kappa_2, 1)$. For any root β of f, we may construct an eigenvector w_β of S_{-z} as follows. We let $w_\beta = \sum_{k=1}^n \gamma_{\beta,k} w_k$, where $\gamma_{\beta,k} = \eta \, \tilde{\gamma}_{\beta,k}$, $\tilde{\gamma}_{\beta,k} = \frac{\delta_k}{(\kappa_k - \beta)}$, and $\eta = \left[\sum_{k=1}^n |\tilde{\gamma}_{\beta,k}|^2 \right]^{-1/2}$. We may verify that w_β is orthogonal to e_z:

$$w_\beta^\dagger e_z \quad = \quad \eta \sum_{k=1}^n \frac{|\delta_k|^2}{\kappa_k - \beta} \quad = \quad \eta \, f(\beta) \quad = \quad 0,$$

and that $v_\beta = (w_\beta)_{-z}$ is an eigenvector of S_{-z} with eigenvalue β: $v_\beta^\dagger S_{-z} = (w_\beta^\dagger S)_{-z}$, and

$$w_\beta^\dagger S - \eta e_z^\dagger \quad = \quad \eta \sum_{k=1}^n \frac{\kappa_k \delta_k}{\kappa_k - \beta} w_k^\dagger - \eta \sum_{k=1}^n \delta_k w_k^\dagger \quad = \quad \beta w_\beta^\dagger.$$

□

Definition 2.1 (Las Vegas hitting time)**.** *For $z \in X$, the* Las Vegas z-hitting time *of P, denoted by $\mathsf{HT}(P, z)$, is the expected number of steps the chain P takes to reach the state z when started in the initial distribution π, which is the stationary distribution of P.*

It is well known that the z-hitting time of P is given by the formula $\mathsf{HT}(P, z) = \pi_{-z}^\dagger (I - P_{-z})^{-1} u_{-z}$, where u is the all-ones vector. Simple algebra shows that

$$\pi_{-z}^\dagger (I - P_{-z})^{-1} u_{-z} \quad = \quad \sqrt{\pi_{-z}}^\dagger (I - S_{-z})^{-1} \sqrt{\pi_{-z}},$$

where $\sqrt{\pi_{-z}}$ is the entry-wise square root of π_{-z}. Let $\{v_j : j \leq n-1\}$ be the set of orthonormal eigenvectors of S_{-z} where the eigenvalue of v_j is $\lambda_j = \cos\theta_j$ with $0 < \theta_j \leq \pi/2$. By reordering the eigenvalues we can suppose that $1 > \lambda_1 \geq \ldots \geq \lambda_{n-1} \geq 0$. If $\sqrt{\pi_{-z}} = \sum_j \nu_j v_j$ is the decomposition of $\sqrt{\pi_{-z}}$ in the eigenbasis of S_{-z} then the z-hitting time satisfies:

$$\mathsf{HT}(P,z) \quad = \quad \sum_j \frac{\nu_j^2}{1-\lambda_j}.$$

This may be viewed as the expectation of a random variable that takes value $1/(1-\lambda_j)$ with probability ν_j^2. When $0 < \theta \leq \pi/2$, we have $1 - \theta^2/2 \leq \cos\theta \leq 1 - \theta^2/4$. Therefore we can approximate the hitting time with another expectation that is very closely related to the analogous quantum notion. More precisely, let H_z be the random variable which takes the value $1/\theta_j^2$ with probability ν_j^2, and 0 with probability $1 - \sum_j \nu_j^2$. We denote the expectation of H_z by $\mathbb{E}[H_z]$. Then we have $2\,\mathbb{E}[H_z] \leq \mathsf{HT}(P,z) \leq 4\,\mathbb{E}[H_z]$.

In the definition of the hitting time the Markov chain is used in a Las Vegas algorithm: we count the (expected) number of steps to reach the marked element without error. We may also use the chain as an algorithm that reaches the marked element with some probability smaller than 1, leading to a Monte Carlo type definition. Technically, to be able to underline the analogies between the classical and quantum notions, we define the hitting time with error via the random variable H_z.

Definition 2.2 (Monte Carlo hitting time)**.** *For $z \in X$ and for $0 < \varepsilon < 1$, the* ε-error Monte Carlo z-hitting time *of P, denoted by $\mathsf{HT}_\varepsilon(P,z)$ is defined as*

$$\mathsf{HT}_\varepsilon(P,z) \quad = \quad \min\ \{y\ :\ \Pr[H_z > y] \leq \varepsilon\}.$$

Observe that for all z, if $\varepsilon \leq \varepsilon'$ then $\mathsf{HT}_{\varepsilon'}(P,z) \leq \mathsf{HT}_\varepsilon(P,z)$. We first show that the use of H_z for the definition of the Monte Carlo hitting time is well founded. For this, let us denote by $h_\varepsilon(P,z)$ the smallest integer k such that the probability that the chain does not reach z in the first k steps is at most ε.

Theorem 2.2. *For all z and ε, we have*

$$\begin{aligned} h_\varepsilon(P,z) &\leq \left(4\ln\frac{2}{\varepsilon}\right)\mathsf{HT}_{\varepsilon/2}(P,z), \quad \textit{and} \\ \mathsf{HT}_\varepsilon(P,z) &\leq \frac{1}{2}\,h_{\varepsilon/3}(P,z). \end{aligned}$$

The proof of this theorem is presented in Appendix A.

How much smaller than the Las Vegas hitting time can the Monte Carlo hitting time be? The following results state that for some z they are of the same order of magnitude.

Theorem 2.3. *We have the following inequalities between the two notions of hitting time:*

- *For all z and ε,* $\mathsf{HT}_\varepsilon(P,z) \leq \frac{1}{2\varepsilon}\,\mathsf{HT}(P,z)$.
- *There exists z such that for all $\varepsilon < 1/2$,* $\mathsf{HT}(P,z) \leq 4\,\mathsf{HT}_\varepsilon(P,z)$.

Proof. The first statement simply follows from the Markov inequality and from the relation $\mathbb{E}[H_z] \leq \mathsf{HT}(P,z)/2$. For the second statement, we find an element z such that $\nu_1^2 \geq 1/2$. The existence of such an element is assured by Lemma 8 in Ref. [Sze04]. Then $\mathsf{HT}(P,z) \leq \sum_j 4\nu_j^2/\theta_j^2 \leq 4/\theta_1^2 \leq 4\,\mathsf{HT}_\varepsilon(P,z)$, for $\varepsilon < 1/2$.

We now justify the existence of such a z, following the argument of Lemma 8 in [Sze04]. Let $w_1, w_2, \ldots, w_n$ be the orthonormal eigenvectors of S with associated eigenvalues $1 = \kappa_1 \geq \ldots \geq \kappa_n > 0$. Observe that $\sum_z |(w_1)_z|^2 = 1 = \sum_z |(w_2)_z|^2$. Therefore, there is z such that $|(w_1)_z| \leq |(w_2)_z|$. Fix for now such a z.

Let w be the vector obtained from v_1, the normalized principal eigenvector of S_{-z} with eigenvalue λ_1, by augmenting it with a 0 in the z-coordinate. We express both w and e_z in the eigenbasis of S: let $w = \sum_{k=1}^n \gamma_k w_k$ and $e_z = \sum_{k=1}^n \delta_k w_k$, with $|\delta_1| \leq |\delta_2|$.

From Claim 2.1 and its proof, we get that $\lambda_1 \in (\kappa_2, 1)$, and that $\sum_{k=2}^{n} \frac{|\delta_k|^2}{\lambda_1 - \kappa_k} = \frac{|\delta_1|^2}{1-\lambda_1}$. Since $|\delta_1| \leq |\delta_2|$, this equation implies that $1 - \lambda_1 \leq \lambda_1 - \kappa_2$, and therefore $1 - \lambda_1 \leq \lambda_1 - \kappa_k$, for $2 \leq k \leq n$. Injecting these inequalities in the same equation leads to $\sum_{k=2}^{n} \frac{|\delta_k|^2}{(\kappa_k - \lambda_1)^2} \leq \frac{|\delta_1|^2}{(1-\lambda_1)^2}$.

Again, as in the proof of Claim 2.1, there exists $\nu \neq 0$, such that $\gamma_k = \frac{\nu \delta_k}{\kappa_k - \lambda_1}$ for all $k = 1, \ldots, n$. Combining this with the last inequality, we get $\sum_{k=2}^{n} \gamma_k^2 \leq \gamma_1^2$. But $\sum_{k=1}^{n} \gamma_k^2 = 1$, therefore $\gamma_1^2 \geq \frac{1}{2}$.

The proof concludes by observing that $\gamma_1 = \nu_1$. Indeed, γ_1 is the w_1-component of w, where w is v_1 augmented with a 0 in the z-coordinate. Since the normalized principal eigenvector w_1 is simply $\sqrt{\pi}$, we can express γ_1 as the inner product between $\sqrt{\pi_{-z}}$ and v_1. The latter quantity is nothing other than ν_1. □

Observe that for state transitive Markov chains P, both notions of hitting time are independent of z, and therefore they are within a constant factor of each other when ε is a constant.

3 Quantum hitting times

3.1 Two notions of quantum walk

For a state $|\psi\rangle$ in the Hilbert space $\mathcal{H}$, let $\Pi_\psi = |\psi\rangle\langle\psi|$ denote the orthogonal projector onto $\mathsf{Span}(|\psi\rangle)$, and let $\mathrm{ref}(\psi) = 2\Pi_\psi - \mathrm{Id}$ denote the reflection through the line generated by $|\psi\rangle$, where Id is the identity operator on $\mathcal{H}$. Let $U = U_2 U_1$ be an *abstract search algorithm* as in [AKR05], where $U_1 = -\mathrm{ref}(\mu)$ for a "target vector" $|\mu\rangle \in \mathcal{H}$ with real coefficients in a canonical orthonormal basis for the Hilbert space $\mathcal{H}$, U_2 is a unitary operator on $\mathcal{H}$ whose matrix representation in the canonial basis has only real entries, and U_2 has a unique 1-eigenvector $|\phi_0\rangle$. It follows that $|\phi_0\rangle$ has real coefficients in the canonical orthonormal basis for the Hilbert space $\mathcal{H}$. The state $|\mu\rangle$ is the quantum analogue of the state z which we seek in the classical walk P, U_2 the analogue of P, and $|\phi_0\rangle$ the analogue of the stationary distribution π.

We refer to the notion of "abstract search algorithm" for both the finding and the detection problems. Moreover, we only describe the abstract search algorithm for a unique target vector. It could be extended to a subspace of target vectors, by letting U_1 be the reflection through the subspace orthogonal to target vectors. Nonetheless, in this paper we focus on the special case of a unique target vector.

The abstract search algorithm usually starts with state $|\phi_0\rangle$, and iterates U several times in order to get a large deviation from $|\phi_0\rangle$. In this paper, we prefer to start with a slightly different initial state. The general behavior of the abstract search algorithm remains unchanged by this. We replace the starting state $|\phi_0\rangle$ by $|\widetilde{\phi}_0\rangle = |\phi_0\rangle - \langle\phi_0|\mu\rangle|\mu\rangle$, the (unnormalized) projection of the 1-eigenvector $|\phi_0\rangle$ of U_2 on the space orthogonal to $|\mu\rangle$. This substitution was first considered in [Sze04], and corresponds to first making a measurement according to $(\Pi_\mu, \mathrm{Id} - \Pi_\mu)$. If the measurement outputs $|\mu\rangle$ we are done. Otherwise we run the abstract search algorithm on the residual state.

This choice of the initial state is motivated by the results in Section 3.4 which relate quantum hitting time to classical hitting time. All other results in this article remain valid if we start with $|\phi_0\rangle$.

Ambainis *et al.* characterized the spectrum of U in terms of the decomposition of $|\mu\rangle$ in the eigenvector basis of U_2. One of their results is:

Theorem 3.1 ([AKR05])**.** *Let U_2 be a unitary matrix with real entries and a unique 1-eigenvector $|\phi_0\rangle$. Let $|\mu\rangle$ be a unit vector with real entries, and let $U_1 = \mathrm{Id} - 2|\mu\rangle\langle\mu|$. Let $U = U_2 U_1$.*

- *If $\langle\phi_0|\mu\rangle = 0$, then $|\widetilde{\phi}_0\rangle = |\phi_0\rangle$ and $U|\widetilde{\phi}_0\rangle = |\widetilde{\phi}_0\rangle$.*
- *If $\langle\phi_0|\mu\rangle \neq 0$, then U has no 1-eigenspace.*

Thus one can use U in order to detect if $\langle\phi_0|\mu\rangle \neq 0$. Indeed, in that case, after a certain number T of iterations of U on $|\widetilde{\phi}_0\rangle$, the state moves "far" from the initial state $|\widetilde{\phi}_0\rangle$. Such a deviation caused by some operator V (in our case $V = U^T$, i.e., U iterated T times) is usually detected by phase estimation with a single bit of precision. The latter operation requires the use of the controlled operator c-V and is better known as the *control test* or the *Hadamard test*. Namely observe that $(H \otimes \mathrm{Id})(\text{c-}V)(H \otimes \mathrm{Id})|0\rangle|\psi\rangle =$

$\frac{1}{2}|0\rangle(|\psi\rangle + V|\psi\rangle) + \frac{1}{2}|1\rangle(|\psi\rangle - V|\psi\rangle)$. Therefore a measurement of the first register gives outcome 1 with probability $\||\psi\rangle - V|\psi\rangle\|^2/4$.

Szegedy [Sze04] designed a generic method for constructing an abstract search algorithm given a (classical) Markov chain. Let $P = (p_{xy})$ be an ergodic Markov chain over state space $X = \{1, \ldots, n\}$ with stationary distribution π. The time-reversal P^* of this chain is defined by the equations $\pi_y p^*_{yx} = \pi_x p_{xy}$. The chain P is reversible if $P = P^*$.

The quantum analogue of P may be thought of as a walk on the *edges* of the original Markov chain, rather than on its vertices. Thus, its state space is a vector subspace of $\mathcal{H} = \mathbb{C}^{X \times X}$. If $\mathcal{K}$ is a subspace of $\mathcal{H}$ spanned by a set of orthonormal states $\{|\psi_i\rangle : i \in I\}$, then let $\Pi_{\mathcal{K}} = \sum_{i \in I} \Pi_{\psi_i}$ be the orthogonal projector onto $\mathcal{K}$, and let $\mathrm{ref}(\mathcal{K}) = 2\Pi_{\mathcal{K}} - \mathrm{Id}$ be the reflection through $\mathcal{K}$. Let $\mathcal{A} = \mathsf{Span}(|x\rangle|p_x\rangle : x \in X)$ and $\mathcal{B} = \mathsf{Span}(|p^*_y\rangle|y\rangle : y \in X)$ be vector subspaces of $\mathcal{H}$, where

$$|p_x\rangle \quad = \quad \sum_{y \in X} \sqrt{p_{xy}}\,|y\rangle \quad \text{and} \quad |p^*_y\rangle \quad = \quad \sum_{x \in X} \sqrt{p^*_{yx}}\,|x\rangle.$$

Define similarly for any $z \in X$ the subspaces $\mathcal{A}_{-z} = \mathsf{Span}(|x\rangle|p_x\rangle : x \in X \setminus \{z\})$ and $\mathcal{B}_{-z} = \mathsf{Span}(|p^*_y\rangle|y\rangle : y \in X \setminus \{z\})$.

Definition 3.1 ([Sze04, MNRS07])**.** *Let P be an ergodic Markov chain. The unitary operation $W(P) = \mathrm{ref}(\mathcal{B}) \cdot \mathrm{ref}(\mathcal{A})$ defined on $\mathcal{H}$ is called the* quantum analogue *of P; and the unitary operation $W(P, z) = \mathrm{ref}(\mathcal{B}_{-z}) \cdot \mathrm{ref}(\mathcal{A}_{-z})$ defined on $\mathcal{H}$ is called the* quantum analogue *of P_{-z}.*

The unitary operation SWAP is defined by $\mathsf{SWAP}|x\rangle|y\rangle = |y\rangle|x\rangle$. When P is reversible, the connection between the quantum walk of Szegedy and the quantum walk defined by Ambainis *et al.* is made explicit by the following fact.

Fact 3.2. *Let $z \in X$ and $|\mu\rangle = |z\rangle|p_z\rangle$. Let $U_2 = \mathsf{SWAP} \cdot \mathrm{ref}(\mathcal{A})$ and $U_1 = \mathrm{Id} - 2|\mu\rangle\langle\mu|$. If P is reversible then $(U_2U_1)^2 = W(P, z)$. In particular, the unitary operators $U = U_2U_1$ and $W(P, z)$ are diagonal in the same orthonormal basis.*

3.2 Phase estimation and quantum hitting time

Let U be a $d \times d$ unitary matrix with real entries. The potential eigenvalues of U are then 1, -1, and pairs of conjugate complex numbers $(\mathrm{e}^{\mathrm{i}\alpha_j}, \mathrm{e}^{-\mathrm{i}\alpha_j})$ with $0 < \alpha_j < \pi$, for $1 \leq j \leq J$, for some J.

Let $|\psi\rangle$ be a vector of dimension d with real entries and of norm at most one. Then $|\psi\rangle$ uniquely decomposes as

$$|\psi\rangle \quad = \quad \delta_0|w_0\rangle + \sum_{1 \leq j \leq J} \delta_j(|w^+_j\rangle + |w^-_j\rangle) + \delta_{-1}|w_{-1}\rangle, \tag{1}$$

where $\delta_0, \delta_{-1}, \delta_j$ are reals, $|w_0\rangle$ is a unit eigenvector of U with eigenvalue 1, $|w_{-1}\rangle$ is a unit eigenvector with eigenvalue -1, and $|w^+_j\rangle, |w^-_j\rangle$ are unit eigenvectors with respective eigenvalues $\mathrm{e}^{\mathrm{i}\alpha_j}$ and $\mathrm{e}^{-\mathrm{i}\alpha_j}$, and $|w^-_j\rangle = \overline{|w^+_j\rangle}$ (which is the vector whose coordinates are the complex conjugates of $|w^+_j\rangle$).

We now describe a procedure whose purpose is to detect if the state $|\psi\rangle$ has a component orthogonal to the 1-eigenspace of U. In the context of the abstract search algorithm, when in particular $|\phi_0\rangle$ plays the role of $|\psi\rangle$, this is equivalent to $\langle\phi_0|\mu\rangle \neq 0$. The idea, which is similar to the approach of Magniez *et al.* [MNRS07], is to apply the phase estimation algorithm due to Kitaev [Kit95, KSV02] and Cleve, Ekert, Macchiavello, and Mosca [CEMM98] to U.

Theorem 3.3 ([Kit95, KSV02, CEMM98])**.** *There is a quantum circuit* **Estimate** *that given an eigenvector $|v\rangle$ of a unitary operator U with eigenvalue $\mathrm{e}^{\mathrm{i}\alpha}$, determines the corresponding phase $\alpha \in (-\pi, \pi]$ with precision Δ and error probability at most $1/3$. If $|v\rangle$ is a 1-eigenvector of U, then* **Estimate** *determines $\alpha = 0$ with probability 1. Moreover,* **Estimate** *makes $\mathrm{O}(1/\Delta)$ calls to the controlled operator c-U and its inverse, and it contains $\mathrm{O}(\log^2(1/\Delta))$ additional gates.*

Based on the circuit **Estimate**, we can detect the presence of components orthogonal to the 1-eigenspace in an arbitrary state $|\psi\rangle$.

Detect(U, Δ, ε) — Input: $|\psi\rangle$

1. Apply $\Theta(\log(1/\varepsilon))$ times the phase estimation circuit **Estimate** for U with precision Δ to the same copy of state $|\psi\rangle$.
2. If at least one of the estimated phases is nonzero, `ACCEPT`. Otherwise `REJECT`.

Let QH be the random variable which takes the value $1/\alpha_j$ with probability $2\delta_j^2$, the value $1/\pi$ with probability δ_{-1}^2, and the value 0 otherwise. Observe that in the following lemma, and in the analysis of all our algorithms in this section, the probabilities in fact sum to $\|\psi\|^2$, where $|\psi\rangle$ is not necessarily normalized, and has norm at most 1.

Lemma 3.4. *Assume that* $\Pr[QH > 1/\Delta] \leq \varepsilon$. *Then the procedure* **Detect**(U, Δ, ε) *accepts* $|\psi\rangle$ *with probability* $\|\psi\|^2 - \delta_0^2 - \mathrm{O}(\varepsilon)$, *and moreover with probability* 0 *if* $|\delta_0| = \|\psi\|$. *In addition, the number of applications of c-U is* $\mathrm{O}(\log(1/\varepsilon)/\Delta)$.

Proof. Assume first that that $|\delta_0| = \|\psi\|$. Then, **Estimate** can compute the eigenphase of any w_0 with certainty. Then the procedure **Detect** rejects exactly with probability δ_0^2, and therefore accepts with probability $\|\psi\|^2 - \delta_0^2 = 0$.

Assume now that $\Pr[QH > 1/\Delta] \leq \varepsilon$, and $|\delta_0| < \|\psi\|$. First observe that **Estimate** with precision Δ uses $1/\Delta$ applications of c-U. Then the precision Δ in **Estimate** ensures a nonzero approximation of an eigenphase $\pm\alpha_j$ with probability at least 2/3 provided that $\alpha_j \geq \Delta$. By hypothesis, the contribution of these eigenphases has squared Euclidean norm $2\sum_j \delta_j^2 + \delta_{-1}^2 = \|\psi\|^2 - \delta_0^2$. The success probability is then amplified to $1 - \mathrm{O}(\varepsilon)$ by checking that all the $\mathrm{O}(\log(1/\varepsilon))$ outcomes of **Estimate** are nonzero. The contribution of the other eigenphases has squared Euclidean norm less than ε in the vector $|\psi\rangle$. Therefore the overall acceptance probability is at least $\|\psi\|^2 - \delta_0^2 - \mathrm{O}(\varepsilon)$. □

In the case of quantum walk, the above lemma justifies the following definitions of quantum hitting times. We later give an algorithmic interpretation for these notions, by providing a detection algorithm with complexity given by these hitting times (Corollary 3.6).

Let U be some abstract search U_2U_1, where $U_1 = \mathrm{Id} - 2|\mu\rangle\langle\mu|$, starting from state $|\widetilde{\phi}_0\rangle = |\phi_0\rangle - a_0|\mu\rangle$, where $a_0 = \langle\mu|\phi_0\rangle$. We now set $|\psi\rangle = |\widetilde{\phi}_0\rangle$. Again, QH is the random variable which takes the value $1/\alpha_j$ with probability $2\delta_j^2$, the value $1/\pi$ with probability δ_{-1}^2, and 0 otherwise.

Definition 3.2 (Quantum hitting time)**.** *The* (Las Vegas) quantum $|\mu\rangle$-hitting time *of* U_2 *is the expectation of* QH, *that is*

$$\mathsf{QHT}(U_2, |\mu\rangle) \quad = \quad 2\sum_j \frac{\delta_j^2}{\alpha_j} + \frac{\delta_{-1}^2}{\pi}.$$

For $0 < \varepsilon < 1$, *the* (Monte Carlo) quantum ε-error $|\mu\rangle$-hitting time *of* U_2 *is defined as*

$$\mathsf{QHT}_\varepsilon(U_2, |\mu\rangle) \quad = \quad \min\{y \,:\, \Pr[QH > y] \leq \varepsilon\}.$$

Using Theorem 3.1, Lemma 3.4 and our definition of quantum hitting time, we directly get bounds on the probability of acceptance of the procedure **Detect**:

Theorem 3.5. *For every* $T \geq \max\{1, \mathsf{QHT}_\varepsilon(U_2, |\mu\rangle)\}$, *the procedure* **Detect**$(U, 1/T, \varepsilon)$ *accepts* $|\widetilde{\phi}_0\rangle$ *with probability* $\|\widetilde{\phi}_0\|^2 - \mathrm{O}(\varepsilon)$ *if* $\langle\phi_0|\mu\rangle \neq 0$, *and accepts with probability* 0 *otherwise. Moreover the number of applications of c-U is* $\mathrm{O}(\log(1/\varepsilon) \times T)$.

We can encapsulate the projection of $|\phi_0\rangle$ to the space orthogonal to $|\mu\rangle$ into our algorithm such as in the following procedure, and deduce its behavior from the above theorem.

MainDetect$(U_2, |\mu\rangle, \Delta, \varepsilon)$ — Input: $|\psi\rangle$

1. Make a measurement according to $(\Pi_\mu, \mathrm{Id} - \Pi_\mu)$.
2. If the measurement outputs $|\mu\rangle$, `ACCEPT`.
   Otherwise apply **Detect**(U, Δ, ε) to the residual state.

Corollary 3.6. *For every $T \geq \max\{1, \mathsf{QHT}_\varepsilon(U_2, |\mu\rangle)\}$, the procedure* **MainDetect**$(U_2, |\mu\rangle, 1/T, \varepsilon)$ *accepts $|\phi_0\rangle$ with probability $1 - \mathrm{O}(\varepsilon)$ if $\langle\phi_0|\mu\rangle \neq 0$, and accepts with probability 0 otherwise.*

When the abstract search is built from the quantum analogue of a reversible Markov chain P and $|\mu\rangle = |z\rangle|p_z\rangle$ for some z, we use the following terminology:

- The *quantum z-hitting time of P* is $\mathsf{QHT}(P, z) = \mathsf{QHT}(\mathsf{SWAP} \cdot \mathrm{ref}(\mathcal{A}), |z\rangle|p_z\rangle)$;
- For $0 < \varepsilon < 1$, the *quantum ε-error z-hitting time of P* is $\mathsf{QHT}_\varepsilon(P, z) = \mathsf{QHT}_\varepsilon(\mathsf{SWAP} \cdot \mathrm{ref}(\mathcal{A}), |z\rangle|p_z\rangle)$.

With different, more technical arguments, Szegedy proved results similar to Theorem 3.5, but with an analysis based on the parameter $\mathsf{QHT}(P, z)$ and only for symmetric Markov chains:

Theorem 3.7 ([Sze04])**.** *When t is chosen uniformly at random in $\{1, 2, \ldots, \lceil \mathsf{QHT}(P, z) \rceil\}$, then the expectation of the deviation $\|(W(P, z))^t |\widetilde{\phi}_0\rangle - |\widetilde{\phi}_0\rangle\|$ is $\Omega(\|\widetilde{\phi}_0\|)$.*

Under certain assumptions, Ambainis *et al.* [AKR05] gave a similar result in terms of the smallest eigenphase of $U_2 U_1$.

Suppose we wish to not only detect if $\langle\mu|\phi_0\rangle \neq 0$, but also to map $|\phi_0\rangle$ to $|\mu\rangle$. Then we are led to a procedure different from **Detect**. One possibility is to try to use U in order to move some state $|\psi\rangle$ to an orthogonal state that is closer to $|\mu\rangle$. There *a priori* is no guarantee that this state will be "close enough" to $|\mu\rangle$. Nonetheless, in many cases it appears to have a better overlap with $|\mu\rangle$, that can even be as big as a constant, as in the case of Grover search. We will show how to ensure such a situation later in Section 4 for the quantum analogue of any reversible walk (Corollary 4.10).

Definition 3.3. *The* U-rotation *of $|\psi\rangle$ is the state obtained by flipping the phase of all the $|w_j^-\rangle$-components of $|\psi\rangle$, leading to the state $\delta_0|w_0\rangle + \sum_j \delta_j(|w_j^+\rangle - |w_j^-\rangle) + \delta_{-1}|w_{-1}\rangle$, using the notation of Eq. (1).*

Fact 3.8. *If $|\psi\rangle$ is orthogonal to both the 1-eigenspace and the (-1)-eigenspace of U, then the U-rotation of $|\psi\rangle$ is orthogonal to $|\psi\rangle$.*

An approximate version of the U-rotation of a state can be implemented efficiently by the following procedure with further assumptions on U. In the description below, we use **Estimate** *coherently* on a superposition of eigenvectors, without the final measurement that is implicit in the phase estimation procedure. We refer to this unitary operator as **Q-Estimate**.

Rotate(U, Δ, ε) — Input: $|\psi\rangle$

1. Apply $\Theta(\log(1/\varepsilon))$ times the phase estimation circuit $\mathbf{Q} - \mathbf{Estimate}$ for U with precision Δ to the same copy of state $|\psi\rangle$, but with fresh ancillary qubits each time.
2. If the majority of estimated phases are negative
   Perform a Phase Flip.
   Otherwise do nothing.
3. Undo the Phase Estimations of Step 1.

Indeed, **Rotate** effects a phase "correction" up to the error in the phase estimation procedure. The error in phase estimation is small as long as $|\widetilde{\phi}_0\rangle$ avoids the eigenspaces of U that have eigenvalues close to -1. This is naturally the case when we consider the quantum analogue of any reversible Markov chain with nonnegative eigenvalues.

Theorem 3.9. *Assume that all eigenvalues* $\mathrm{e}^{\mathrm{i}\alpha}$ *of* U *satisfy* $|\alpha| \leq \pi/2$. *Then for every* $T \geq \mathsf{QHT}_\varepsilon(U_2, |\mu\rangle)$, *the procedure* **Rotate**$(U, 1/T, \varepsilon)$ *maps* $|\widetilde{\phi}_0\rangle$ *to a state at Euclidean distance* $\mathrm{O}(\sqrt{\varepsilon}\,)$ *from the* U*-rotation of* $|\widetilde{\phi}_0\rangle$. *Moreover, the number of applications of c-*U *is* $\mathrm{O}(\log(1/\varepsilon) \times \mathsf{QHT}_\varepsilon(U_2, |\mu\rangle))$.

Proof. The proof follows the same argument as in Theorem 3.5. □

3.3 Comparison between QHT and QHT_ε

We assume henceforth that $\langle\phi_0|\mu\rangle \notin \{0, \pm 1\}$; otherwise, the problem is trivial—by our definition $\mathsf{QHT}_\varepsilon(U_2, |\mu\rangle) = \mathsf{QHT}(U_2, |\mu\rangle) = 0$. Recall that $|\widetilde{\phi}_0\rangle = |\phi_0\rangle - a_0|\mu\rangle$. We further assume that $|\widetilde{\phi}_0\rangle \neq 0$, for the same reason as above.

The Markov inequality immediately implies the following relationship between the Las Vegas and the Monte Carlo hitting times:

Fact 3.10. *For all* U_2, $|\mu\rangle$, *and* ε,

$$\mathsf{QHT}_\varepsilon(U_2, |\mu\rangle) \quad \leq \quad \frac{1}{\varepsilon}\,\mathsf{QHT}(U_2, |\mu\rangle).$$

The other direction requires a closer look at the spectral decomposition of U_2U_1. In this section, we again follow the framework of the abstract search algorithm $U = U_2U_1$. The eigenvalues of U_2 different from 1 are either -1 or they appear as complex conjugates $\mathrm{e}^{\pm\mathrm{i}\theta_j}$, where $\theta_j \in (0, \pi)$. For convenience, we assume that $\theta_{-1} = \pi$, $0 = \theta_0 \leq \theta_1 \leq \theta_2 \leq \ldots$, and we always use index j for positive integers. Recall that both $|\mu\rangle$ and the 1-eigenvector $|\phi_0\rangle$ of U_2 have real entries. Let $|\phi_{-1}\rangle$ be a unit eigenvector of U_2 with eigenvalue -1 and with real entries, and $|\phi_j^{\pm}\rangle$ be unit eigenvectors of U_2 with eigenvalues $\mathrm{e}^{\pm\mathrm{i}\theta_j}$ such that $|\phi_j^-\rangle = \overline{|\phi_j^+\rangle}$. Then writing $|\mu\rangle$ in the eigenspace decomposition of U_2 we get

$$|\mu\rangle \quad = \quad a_0|\phi_0\rangle + \sum_j a_j \left(|\phi_j^+\rangle + |\phi_j^-\rangle\right) + a_{-1}|\phi_{-1}\rangle, \tag{2}$$

where a_0, a_{-1}, a_j are real by the constraints we put on $|\mu\rangle, |\phi_0\rangle, |\phi_{-1}\rangle, |\phi_j\rangle$.

Ambainis *et al.* [AKR05] (see also Tulsi [Tul08]) show the following relation between the spectrum of U_2 and that of U.

Lemma 3.11 ([AKR05, Tul08])**.** *The eigenvalues* $\mathrm{e}^{\pm\mathrm{i}\alpha}$ *of the operator* U *are solutions of the equation:*

$$a_0^2 \cot\frac{\alpha}{2} + \sum_j a_j^2 \left(\cot\left(\frac{\alpha+\theta_j}{2}\right) + \cot\left(\frac{\alpha-\theta_j}{2}\right)\right) - a_{-1}^2 \tan\frac{\alpha}{2} \quad = \quad 0.$$

The corresponding unnormalized eigenvectors $|w_\alpha\rangle = |\mu\rangle + \mathrm{i}|w'_\alpha\rangle$ *satisfy* $\langle\mu|w'_\alpha\rangle = 0$ *and*

$$|w'_\alpha\rangle \quad = \quad a_0 \cot\frac{\alpha}{2}\,|\phi_0\rangle + \sum_j a_j \left(\cot\left(\frac{\alpha-\theta_j}{2}\right)|\phi_j^+\rangle + \cot\left(\frac{\alpha+\theta_j}{2}\right)|\phi_j^-\rangle\right) - a_{-1}\tan\frac{\alpha}{2}\,|\phi_{-1}\rangle.$$

As in the classical case, we are only able to upper bound QHT by QHT_ε for some particular target states $|\mu\rangle$. In the case of the quantum analogue of a Markov chain P as in Definition 3.1, a natural choice for target states $|\mu_z\rangle$ is $|z\rangle|p_z\rangle$ for a subset of the zs in the state space of the Markov chain. Motivated by the properties of the target states in this example, we consider in the following lemma a set of orthonormal vectors $M = \{|\mu_z\rangle\}$ whose (real) span contains $|\phi_0\rangle$, and also have the following property with respect to U_2, that we call U_2*-admissibility.*

Definition 3.4. *Let M be a set of orthonormal vectors with real entries. Then M is* U_2-admissible *if* $\mathsf{Span}(M) = \mathsf{Span}(|\phi_0\rangle, (|\phi_j^+\rangle + |\phi_j^-\rangle) : j \in J)$, *for some* $\emptyset \neq J \subseteq \{j \geq 1\}$.

Note that the choice of target states $M = \{|\mu_z\rangle\}$ leads directly to a $W(P)$-admissible M for any Markov chain P.

The following lemma shows that for some marked state $|\mu_z\rangle$ from a U_2-admissible set, the initial state $|\widetilde{\phi}_0\rangle$ has a large projection on the principal eigenspace of the abstract search algorithm $U = U_2(I - 2|\mu_z\rangle\langle\mu_z|)$.

Lemma 3.12. *Let $M = \{|\mu_z\rangle\}$ be a U_2-admissible set of orthonormal vectors with real coefficients in the standard basis. For every z, let α_z be the smallest positive real number α such that $\mathrm{e}^{\pm \mathrm{i}\alpha}$ are eigenvalues of the operator $U = U_2(I - 2|\mu_z\rangle\langle\mu_z|)$. Then there exists z such that the length of the projection of $|\widetilde{\phi}_0\rangle$ onto the subspace generated by $|w_{\alpha_z}\rangle$ and $|w_{-\alpha_z}\rangle$ is at least $1/\sqrt{2}$.*

The proof of this lemma is presented in Appendix B. This implies that the Monte Carlo hitting time of some state $|\mu_z\rangle$ is large, in fact, at least as large as its Las Vegas hitting time.

Corollary 3.13. *Let $M = \{|\mu_z\rangle\}$ be a U_2-admissible set of real orthonormal vectors. Then there exists z such that for all $\varepsilon < 1/2$,*

$$\mathsf{QHT}_\varepsilon(U_2, |\mu_z\rangle) \quad = \quad \frac{1}{\alpha_z}.$$

Theorem 3.14. *Let $M = \{|\mu_z\rangle\}$ be a U_2-admissible set of real orthonormal vectors. Then there exists z such that for all $\varepsilon < 1/2$,*

$$\mathsf{QHT}(U_2, |\mu_z\rangle) \quad \leq \quad \mathsf{QHT}_\varepsilon(U_2, |\mu_z\rangle).$$

Proof. This is a consequence of Corollary 3.13 since $\mathsf{QHT}(U_2, |\mu_z\rangle)$ is by definition at most $\frac{1}{\alpha_z}$. □

3.4 Quadratic detection speedup for reversible chains

Let P be an ergodic Markov chain over state space $X = \{1, \ldots, n\}$. We further suppose that P is a reversible Markov chain with *positive* eigenvalues, otherwise we simply replace P with $\gamma P + (1-\gamma)I$, for any $\gamma < 1/2$. The following theorem shows that the hitting times of the quantum analogue of P are quadratically smaller than those of P itself.

Theorem 3.15. *Assume that the eigenvalues of P are all positive. Then we have the following relations:*

- *For all $z \in X$,* $\mathsf{QHT}(P, z) \leq \sqrt{\mathsf{HT}(P, z)/2}$.
- *For all $z \in X$ and $\varepsilon \in [0, 1]$,* $\mathsf{QHT}_\varepsilon(P, z) = \sqrt{\mathsf{HT}_\varepsilon(P, z)}$.

Proof. We follow the notation introduced in Sections 2 and 3.1. Then $|\phi_0\rangle = \sum_x \sqrt{\pi_x}\,|x\rangle|p_x\rangle$, $|\mu\rangle = |z\rangle|p_z\rangle$, $|\widetilde{\phi}_0\rangle = \sum_{x \in X\setminus\{z\}} \sqrt{\pi_x}\,|x\rangle|p_x\rangle$. Let $\sqrt{\pi_{-z}} = \sum_j \nu_j v_j$ be the decomposition of $\sqrt{\pi_{-z}}$ in the normalized eigenbasis of S_{-z} where the eigenvalue of v_j is $\cos\theta_j$, with $0 < \theta_1 \leq \ldots \leq \theta_{n-1} < \pi/2$. Let $v_j[x]$ denote the x-coordinate of the vector v_j. We set $|\xi_j\rangle = \sum_{x \neq z} v_j[x]|x\rangle|p_x\rangle$ and $|\zeta_j\rangle = \sum_{y \neq z} v_j[y]|p_y^*\rangle|y\rangle$. Then $|\widetilde{\phi}_0\rangle = \sum_j \nu_j |\xi_j\rangle$. For every j, the vectors $|\xi_j\rangle$ and $|\zeta_j\rangle$ generate an eigenspace of $W(P, z)$ that is also generated by two normalized eigenvectors with eigenvalues respectively $\mathrm{e}^{2\mathrm{i}\theta_j}$ and $\mathrm{e}^{-2\mathrm{i}\theta_j}$. This argument is still true for $\mathsf{SWAP} \cdot \mathrm{ref}(\mathcal{A}_{-z})$ when we divide the phases by 2, leading to eigenvalues $\mathrm{e}^{\mathrm{i}\theta_j}$ and $\mathrm{e}^{-\mathrm{i}\theta_j}$ (cf. Fact 3.2). Since the length of the projection of $|\widetilde{\phi}_0\rangle$ to this eigenspace is ν_j^2, we have $\mathsf{QHT}(P, z) = \sum_{j=1}^{n-1} \frac{\nu_j^2}{\theta_j} = \mathbb{E}[\sqrt{H_z}]$.

By the Jensen inequality we get

$$\mathsf{QHT}(P, z) \quad \leq \quad \sqrt{\mathbb{E}[H_z]} \quad \leq \quad \sqrt{\mathsf{HT}(P, z)/2}.$$

The second relation above immediately follows from $QH^2 = H_z$. □

3.5 On the quadratic speedup threshold

In this section we consider a broad class of quantum walks defined on undirected graphs. We are able to show that for a special case of walks on graphs, the quadratic speedup is tight.

Let $X = \{1, 2, \ldots, n\}$. Our notion of quantum walk can be seen as a walk on the edges of a given undirected graph $G(X, E)$. Let $\mathcal{H}(G) = \mathsf{Span}(|xy\rangle : \{x, y\} \in E)$ be the Hilbert space that a quantum walk on G should preserve. In the rest of this section, we only consider operators and states in $\mathcal{H}(G)$ for some given G. Observe that SWAP preserves $\mathcal{H}(G)$ since G is undirected.

We introduce a notion of reversibility that is justified by Lemma 3.17 below.

Definition 3.5. *A* quantum walk *on an undirected graph $G = (X, E)$ is a unitary $U_2 = \mathsf{SWAP} \cdot F$ defined on a subspace of $\mathcal{H}(G)$, where F is a matrix with real entries of the form $F = \sum_{x \in X} |x\rangle\langle x| \otimes F^x$, and where U_2 has a single 1-eigenvector $|\phi_0\rangle$. The quantum walk is* reversible *when $\mathsf{SWAP}(|\phi_0\rangle) = |\phi_0\rangle$.*

Observe that the definition implies that $|\phi_0\rangle$ can be chosen with real entries. This definition of quantum walk appears, for example, in the survey paper of Ambainis [Amb03], see also [San08]. Szegedy considered for F^x a specific kind of reflection based on Markov chain transition probabilities (see Section 3.1).

Definition 3.6. *Let $U_2 = \mathsf{SWAP} \cdot F$ be a quantum walk with unit 1-eigenvector $|\phi_0\rangle = \sum_x \sqrt{\pi_x}|x\rangle|\phi^x\rangle$, where $\pi_x \geq 0$ and $|\phi^x\rangle$ is a unit vector with real entries. Then the* classical analogue *$P = (p_{xy})$ of U_2 is defined as $p_{xy} = \langle y|\phi^x\rangle^2$.*

Since $|\phi_0\rangle$ is a 1-eigenvector of $\mathsf{SWAP} \cdot F$ we directly get:

Fact 3.16. *Let $|\psi^x\rangle = F^x|\phi^x\rangle$. Then $|\phi_0\rangle = \sum_x \sqrt{\pi_x}|\psi^x\rangle|x\rangle$.*

Lemma 3.17. *The classical analogue P of a quantum walk U_2 on G is a Markov chain on G with stationary probability distribution π. Moreover, P is reversible if U_2 is a reversible quantum walk.*

Proof. First we show that P is a Markov chain on G. For every x, we have

$$\sum_y p_{xy} = \sum_y \langle y|\phi^x\rangle^2 = \|\phi^x\|^2 = 1.$$

Moreover $p_{xy} \neq 0$ implies $\langle y|\phi^x\rangle \neq 0$, which implies that $(x, y) \in E$ since $|\phi_0\rangle \in \mathcal{H}(G)$.

Now we verify that π is a stationary probability distribution. First, π is a probability distribution since $|\phi^x\rangle$ for all $x \in X$ and $|\phi_0\rangle$ are unit vectors. That π is a stationary probability distribution can be seen from the following sequence of equalities which hold for every $y \in X$:

$$\begin{aligned}
\sum_x \pi_x p_{xy} &= \sum_x \langle xy|\phi_0\rangle^2 && \text{by definition of } P \text{ and } |\phi_0\rangle \\
&= \sum_x \pi_y \langle x|\psi^y\rangle^2 && \text{by Fact 3.16} \\
&= \pi_y \|\psi^y\|^2 = \pi_y.
\end{aligned}$$

For reversibility, observe that we similarly have $\pi_x p_{xy} = \langle xy|\phi_0\rangle^2$ and $\pi_y p_{yx} = \langle yx|\phi_0\rangle^2 = (\langle xy|\mathsf{SWAP}|\phi_0\rangle)^2$. P is reversible when these two expressions are equal for every x, y, which happens when the quantum walk U_2 is reversible. □

Finally, we show that the quadratic speedup is tight in the special case of walks for which all of the unitaries F^x are reflections. We state the result using the notation above.

Theorem 3.18. *Let $U_2 = \mathsf{SWAP} \cdot F$ be a reversible quantum walk such that $F^x = 2|\phi^x\rangle\langle\phi^x| - I$, for all $x \in X$. Then for all z and ε,*

$$\mathsf{QHT}_\varepsilon(U_2, |z\rangle|\phi^z\rangle) = \mathsf{QHT}_\varepsilon(P, z) = \sqrt{\mathsf{HT}_\varepsilon(P, z)}.$$

Proof. Let $U_1 = I - 2|z\rangle\langle z| \otimes |\phi^z\rangle\langle\phi^z|$, for some fixed z. Under the hypothesis of the theorem, $(U_2U_1)^2$ is a product of two reflections $\mathrm{ref}(\mathcal{A}_{-z})$ and $\mathrm{ref}(\mathcal{B}_{-z})$, where $\mathcal{A}_{-z} = \mathsf{Span}(|x\rangle|\phi^x\rangle : x \in X \setminus \{z\})$ and $\mathcal{B}_{-z} = \mathsf{Span}(|\phi^y\rangle|y\rangle : y \in X \setminus \{z\}) = \mathsf{SWAP}(\mathcal{A}_{-z})$.

From [Sze04], we know that the spectrum of $(U_2U_1)^2$ is completely defined by the discriminant matrix $D = A^\dagger B$, where $A = \sum_{x\neq z}|x\rangle|\phi^x\rangle\langle x|$ and $B = \sum_{y\neq z}|\phi^y\rangle|y\rangle\langle y|$. We get that $D = (\langle x|\phi^y\rangle\langle\phi^x|y\rangle)_{x\neq z, y\neq z}$. The reversibility of U_2 guarantees that $\langle xy|\phi_0\rangle = \langle yx|\phi_0\rangle$, which implies that $\sqrt{\pi_x}\langle y|\phi^x\rangle = \sqrt{\pi_y}\langle x|\phi^y\rangle$. Since $|\phi^y\rangle$ has real entries, we have $D = \sqrt{\Pi}P_{-z}\sqrt{\Pi}^{-1}$, where $\Pi = \mathrm{diag}(\pi_x)_{x\neq z}$ and P_{-z} is the matrix obtained from P by deleting the row and column indexed by z.

Observe that this discriminant is exactly that of the quantum analogue $W(P, z)$. So $W(P, z)$ and $(U_2U_1)^2$ are equal up to a basis change which maps $|x\rangle|p_x\rangle$ to $|x\rangle|\phi^x\rangle$. □

4 Finding with constant probability

In this section, we extend a technique devised by Tulsi [Tul08] for finding a marked state on the 2D grid in time that is the square-root of the classical hitting time. We prove that it may be applied to a larger class of Markov chains and target states, including the quantum analogue of state-transitive reversible ergodic Markov chains. Combined with ideas developed in the earlier sections, the technique leads to an algorithm that can find (Corollary 4.10) a unique marked element with constant probability and with the same complexity as detection.

We use the notation of Section 3.1. In our application, there is no (-1)-eigenvector of U_2. Therefore the marked state $|\mu\rangle$ has the following decomposition in an eigenvector basis of U_2:

$$|\mu\rangle \quad = \quad a_0|\phi_0\rangle + \sum_{1\leq j\leq J} a_j(|\phi_j^+\rangle + |\phi_j^-\rangle), \tag{3}$$

where J is some positive integer. Last, we assume in the rest of this section that $\langle\phi_0|\mu\rangle \neq 0$.

Lemma 4.1. *The vectors $|\mu\rangle$ and $|\widetilde{\phi}_0\rangle$ have the following representation in the basis $\{|w_\alpha\rangle\}$ consisting of the eigenvectors of $U = U_2U_1$ as given by Lemma 3.11: $|\mu\rangle = \sum_\alpha \frac{1}{\||w_\alpha\rangle\|^2}|w_\alpha\rangle$, and $|\widetilde{\phi}_0\rangle = -\sum_\alpha \frac{a_0 \mathrm{i}\cot(\frac{\alpha}{2})}{\||w_\alpha\rangle\|^2}|w_\alpha\rangle$.*

Proof. Any vector $|\psi\rangle$ may be expressed in the orthogonal basis $\{|w_\alpha\rangle\}$ as $|\psi\rangle = \sum_\alpha \frac{\langle w_\alpha|\psi\rangle}{\||w_\alpha\rangle\|^2}|w_\alpha\rangle$. The first equation now follows from $\langle w_\alpha|\mu\rangle = (\langle\mu| - \mathrm{i}\langle w'_\alpha|)|\mu\rangle = 1$.

By Lemma 3.11, $\langle w_\alpha|\phi_0\rangle = (\langle\mu| - \mathrm{i}\langle w'_\alpha|)|\phi_0\rangle = a_0 - a_0\mathrm{i}\cot\frac{\alpha}{2}$. The second equation follows by combining the above with $|\widetilde{\phi}_0\rangle = |\phi_0\rangle - a_0|\mu\rangle$. □

Then the following is immediate.

Lemma 4.2. *The inner product of the target state $|\mu\rangle$ and the U-rotation of $|\widetilde{\phi}_0\rangle$ is $2a_0\sum_{\alpha>0}\frac{\cot(\frac{\alpha}{2})}{\||w_\alpha\rangle\|^2}$.*

Theorem 3.15 shows that the quantum hitting time is bounded by the square-root of the classical hitting time when U_2 is derived from a reversible Markov chain P, i.e., $U_2 = \mathsf{SWAP}\cdot\mathrm{ref}(\mathcal{A})$ in the notation of Section 3.2. This allows for the detection of marked elements (or more generally for checking if $\langle\mu|\phi_0\rangle \neq 0$) and also the creation of the U-rotation of $|\widetilde{\phi}_0\rangle$ in the stated time bound. However, the overlap of the U-rotation of $|\widetilde{\phi}_0\rangle$ with the target $|\mu\rangle$ may be o(1). Tulsi [Tul08] discovered a technique, described below, to boost this overlap to $\Omega(1)$ in the case of a quantum walk on the 2D grid.

Let $\theta \in [0, \pi/2)$. Let R_θ denote the rotation in $\mathbb{C}^2$ by angle θ:

$$R_\theta \quad = \quad \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$

and let $|\theta\rangle = R_\theta^\dagger|0\rangle$, and $|\theta^\perp\rangle = R_\theta^\dagger|1\rangle$. Define $U_1^\theta = |0\rangle\langle 0| \otimes \mathrm{Id} + |1\rangle\langle 1| \otimes U_1$, and $U_2^\theta = (|\theta\rangle\langle\theta| \otimes (-\mathrm{Id}) + |\theta^\perp\rangle\langle\theta^\perp| \otimes U_2)$. Then $U_1^\theta = \mathrm{Id} - 2|1\rangle\langle 1| \otimes |\mu\rangle\langle\mu|$, meaning that the modified marked state is $|1\rangle|\mu\rangle$. Then the

modified abstract search algorithm becomes:

$$\mathbf{T}(U_1, U_2, \theta) \quad = \quad U_2^\theta U_1^\theta \quad = \quad (|\theta\rangle\langle\theta| \otimes (-\mathrm{Id}) + |\theta^\perp\rangle\langle\theta^\perp| \otimes U_2)(|0\rangle\langle 0| \otimes \mathrm{Id} + |1\rangle\langle 1| \otimes U_1) \tag{4}$$

This is precisely the circuit used by Tulsi: his rotation $\hat{R}_\theta = R_\theta^\dagger$ in our notation. Tulsi [Tul08] proved that the principal eigenvalue of the operator above is closely related to that of the unitary operator U_2U_1. We extend his findings in terms that are more readily used in our context.

The eigenvalues of U_2^θ are the same as those of U_2, except for the addition of the new eigenvalue -1. The eigenvectors corresponding to eigenvalues $\mathrm{e}^{\pm \mathrm{i}\theta_j}$ are now $|\theta^\perp\rangle|\phi_j^\pm\rangle$. Any state of the form $|\theta\rangle|\psi\rangle$ is a -1 eigenvector of U_2^θ.

Fact 4.3. *The decomposition of $|1\rangle|\mu\rangle$ in the eigenvector basis of U_2^θ is:*

$$|1\rangle|\mu\rangle \quad = \quad \cos\theta\ |\theta^\perp\rangle \left(a_0|\phi_0\rangle + \sum_{1\le j\le J} a_j(|\phi_j^+\rangle + |\phi_j^-\rangle) \right) - \sin\theta\ |\theta\rangle|\mu\rangle,$$

where the coefficients a_0, a_j are precisely those in Eq. (3).

Lemma 4.4. *The eigenvalues $\mathrm{e}^{\pm \mathrm{i}\alpha^\theta}$, of the operator $\mathbf{T}(U_1, U_2, \theta)$ are solutions to the equation*

$$a_0^2 \cot\frac{x}{2} + \sum_j a_j^2 \left(\cot\left(\frac{x+\theta_j}{2}\right) + \cot\left(\frac{x-\theta_j}{2}\right)\right) - (\tan^2\theta)\tan\frac{x}{2} \quad = \quad 0.$$

The corresponding unnormalized eigenvectors $|w_{\alpha,\theta}\rangle = |1\rangle|\mu\rangle + \mathrm{i}|w'_{\alpha,\theta}\rangle$ satisfy $\langle 1,\mu|w'_{\alpha,\theta}\rangle = 0$ and

$$\begin{aligned} |w'_{\alpha,\theta}\rangle \quad = \quad & \cos\theta\ |\theta^\perp\rangle \left(a_0 \cot\left(\frac{\alpha^\theta}{2}\right)|\phi_0\rangle + \sum_j a_j \left(\cot\left(\frac{\alpha^\theta-\theta_j}{2}\right)|\phi_j^+\rangle + \cot\left(\frac{\alpha^\theta+\theta_j}{2}\right)|\phi_j^-\rangle\right)\right) \\ & - \sin\theta\ |\theta\rangle\left(\tan\left(\frac{\alpha^\theta}{2}\right)|\mu\rangle\right). \end{aligned}$$

Proof. We apply Lemma 3.11 from Section 3.3 with $a_0^\theta = a_0\cos\theta$, $a_j^\theta = a_j\cos\theta$, $a_{-1}^\theta = \sin\theta$. Note that U_2 does not have any (-1)-eigenvectors (by assumption), but U_2^θ does. □

The target vector in the modified algorithm is $|1\rangle|\mu\rangle$. The start state is chosen to be $|\widetilde{\phi}_{0,\theta}\rangle = |\theta^\perp\rangle|\phi_0\rangle - a_0\cos\theta|1\rangle|\mu\rangle$. The following are analogous to Lemmata 4.1 and 4.2:

Corollary 4.5. *The vectors $|1\rangle|\mu\rangle$ and $|\widetilde{\phi}_{0,\theta}\rangle$ have the following representation in the basis $\{|w_{\alpha,\theta}\rangle\}$ consisting of the eigenvectors of $\mathbf{T}(U_1, U_2, \theta)$ as given by Lemma 4.4:*

$$|1\rangle|\mu\rangle = \sum_{\alpha^\theta} \frac{1}{\|w_{\alpha,\theta}\|^2}|w_{\alpha,\theta}\rangle, \quad \textit{and} \quad |\widetilde{\phi}_{0,\theta}\rangle = -(a_0\mathrm{i}\cos\theta)\sum_{\alpha^\theta}\frac{\cot(\frac{\alpha^\theta}{2})}{\|w_{\alpha,\theta}\|^2}|w_{\alpha,\theta}\rangle.$$

Corollary 4.6. *The inner product of the target state $|1\rangle|\mu\rangle$ and the $\mathbf{T}(U_1, U_2, \theta)$-rotation of $|\widetilde{\phi}_{0,\theta}\rangle$ is given by the expression $(2a_0\cos\theta)\sum_{\alpha^\theta>0}\frac{\cot(\frac{\alpha^\theta}{2})}{\|w_{\alpha,\theta}\|^2}$.*

We choose for the rest of this section $\theta \in [0, \pi/2]$ such that $\tan\theta = a_0\cot(\alpha_1/2)/10$. Let α_1^θ be the smallest positive eigenphase of the modified search algorithm $\mathbf{T}(U_1, U_2, \theta)$.

Lemma 4.7 (proof in Appendix C) proves that α_1^θ is of the same order as the principal eigenphase α_1 of the original algorithm U_2U_1. Lemma 4.8 (proof in Appendix D) is the final piece in our argument. It relates the norm of the principal eigenvectors of the modified walk to the norm of the original ones. Both lemmata extend corresponding results by Tulsi in the case of the 2D grid.

Lemma 4.7. *There is a unique eigenvalue phase α_1^θ of the operator $\mathbf{T}(U_1, U_2, \theta)$ in $(0, \alpha_1]$. Moreover, $\cot(\alpha_1^\theta/2) \leq 1.01 \times \cot(\alpha_1/2)$. Therefore if $0 \leq \alpha_1 \leq \pi/4$, then $0.77 \times \alpha_1 \leq \alpha_1^\theta \leq \alpha_1$.*

Lemma 4.8. $\|w_{\pm\alpha_1,\theta}\| \leq (3\cos\theta) \times \|w_{\pm\alpha_1}\|$.

We have all the ingredients for the main result of this section.

Theorem 4.9. *Let $\varepsilon \in (0,1)$ be any constant. Suppose that the squared length of the projection of the state $|\mu\rangle$ onto the principal eigenspace of U_2U_1 is bounded below by $1-\varepsilon$. Then, for every $T \geq \mathsf{QHT}_\varepsilon(U_2, |\mu\rangle)/0.77$, the procedure* **Rotate**$(\mathbf{T}(U_1, U_2, \theta), 1/T, 1/4)$ *maps $|\widetilde{\phi}_{0,\theta}\rangle$ to a state with constant overlap with the target state $|1\rangle|\mu\rangle$.*

Proof. First we prove that $T' = \mathsf{QHT}_\varepsilon(U_2^\theta, |1\rangle|\mu\rangle)$ is of the order of $\mathsf{QHT}_\varepsilon(U_2, |\mu\rangle)$. Let $l = 2a_0^2(\cot^2\frac{\alpha_1}{2})/\|w_{\alpha_1}\|^2$. We know that $l \geq 1-\varepsilon$. Using Lemma 4.1 we get that $\mathsf{QHT}_\varepsilon(U_2, |\mu\rangle) = 1/\alpha_1$. Moreover, by definition, $T' \leq 1/\alpha_1^\theta$. By Lemma 4.7, $T' \leq 1/(0.77\alpha_1) = \mathsf{QHT}_\varepsilon(U_2, |\mu\rangle)/0.77$. We now get our conclusion by applying Corollary 4.6, Lemmata 4.7 and 4.8, and Theorem 3.9. □

We combine the above theorem with Lemma 3.12 to get our final result.

Corollary 4.10. *Let P be a state-transitive reversible ergodic Markov chain, and let z be any state. Set $|\mu\rangle = |z\rangle|p_z\rangle$, $U_1 = I - 2|\mu\rangle\langle\mu|$, and let U_2 be the quantum analogue of P. Then for every $\varepsilon \leq 1/2$ and $T \geq \mathsf{QHT}_\varepsilon(U_2, |\widetilde{\phi}_0\rangle)/0.77$, the procedure* **Rotate**$(\mathbf{T}(U_1, U_2, \theta), 1/T, 1/4)$ *maps $|\widetilde{\phi}_{0,\theta}\rangle$ to a state with constant overlap with the target state $|1\rangle|\mu\rangle$.*

Proof. The proof is direct once we realize that the conclusions of Lemma 3.12 for a particular element z remain valid for any element because of the state-transitivity of P. □

Acknowledgments

This research was supported in part by the European Commission IST Projects Qubit Applications (QAP) 015848 and Quantum Computer Science (QSC) 25596, the French ANR Defis program under contract ANR-08-EMER-012 (QRAC project), NSERC Canada, CIFAR, an Ontario ERA, QuantumWorks, MITACS, and ARO/NSA (USA). Some of this work was conducted while A.N. was visiting LRI, Univ Paris-Sud, Orsay, France.

Research at Perimeter Institute is supported in part by the Government of Canada through Industry Canada and by the Province of Ontario through MRI. Research at the Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation.

We thank the anonymous referees for their extensive comments on an earlier draft of this article, and especially for pointing out a technical error in the proof of the original Lemma 3.12.

References

[AA05] S. Aaronson and A. Ambainis. Quantum search of spatial regions. *Theory of Computing*, 1(4):47–79, 2005.

[AAKV01] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proceedings of the 33rd ACM Symposium on Theory of Computing*, pages 50–59, 2001.

[ABN+01] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous. One-dimensional quantum walks. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 37–49, 2001.

[AKR05] A. Ambainis, J. Kempe, and A. Rivosh. Coins make quantum walks faster. In *Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms*, pages 1099–1108, 2005.

[Amb03] A. Ambainis. Quantum walks and their algorithmic applications. *International Journal of Quantum Information*, 1:507–518, 2003.

[Amb07] Andris Ambainis. Quantum walk algorithm for Element Distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.

[BŠ06] H. Buhrman and R. Špalek. Quantum verification of matrix products. In *Proceedings of the 17th ACM-SIAM Symposium on Discrete Algorithms*, pages 880–889, 2006.

[CEMM98] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society of London, Series A*, 454:339–354, 1998.

[CG04] A. Childs and J. Goldstone. Spatial search and the Dirac equation. *Physical Review A*, 70:042312, 2004.

[Gro96] L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th ACM Symposium on the Theory of Computing*, pages 212–219, 1996.

[Kit95] A. Kitaev. Quantum measurements and the Abelian stabilizer problem. ECCC technical report 96-003 and arXiv.org e-print quant-ph/9511026, 1995.

[KMOR10] H. Krovi, F. Magniez, M. Ozols, and J. Roland. Finding is as easy as detecting for quantum walks. In *Proceedings of 37st International Colloquium on Automata, Languages and Programming*. LNCS, 2010.

[KSV02] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[MN07] F. Magniez and A. Nayak. Quantum complexity of testing group commutativity. *Algorithmica*, 48(3):221–232, 2007.

[MNRS07] F. Magniez, A. Nayak, J. Roland, and M. Santha. Search via quantum walk. In *Proceedings of the 39th ACM Symposium on Theory of Computing*, pages 575–584, 2007.

[MSS07] F. Magniez, M. Santha, and M. Szegedy. Quantum algorithms for the triangle problem. *SIAM Journal on Computing*, 37(2):611–629, 2007.

[NV00] A. Nayak and A. Vishwanath. Quantum walk on the line. Technical Report quant-ph/0010117, arXiv, 2000.

[San08] M. Santha. Quantum walk based search algorithms. In *Proceedings of the 5th Conference on Theory and Applications of Models of Computation*, volume 4978, pages 31–46. LNCS, 2008.

[SKW03] N. Shenvi, J. Kempe, and K. Whaley. A quantum random walk search algorithm. *Physical Review A*, 67:052307, 2003.

[Sze04] M. Szegedy. Quantum speed-up of Markov chain based algorithms. In *Proceedings of the 45th Symposium on Foundations of Computer Science*, pages 32–41, 2004.

[Tul08] A. Tulsi. Faster quantum walk algorithm for the two dimensional spatial search. *Physical Review A*, 78:012310, 2008.

A Proof of Theorem 2.2

Proof. For the first statement, we set $k = \left(4 \ln \frac{2}{\varepsilon}\right) \mathsf{HT}_{\varepsilon/2}(P, z)$, and we denote by s_k the probability that z is not reached in the first k steps. The claim follows if we show that $s_k \leq \varepsilon$. By a straightforward calculation, $s_k = \pi_{-z}^{\dagger} P_{-z}^k u_{-z} = \sum_j \nu_j^2 (\cos\theta_j)^k$. We bound s_k from above as follows:

$$\begin{aligned} s_k &\leq \sum_{j:1/\theta_j^2 > \mathsf{HT}_{\varepsilon/2}(P,z)} \nu_j^2 \; + \sum_{j:1/\theta_j^2 \leq \mathsf{HT}_{\varepsilon/2}(P,z)} \nu_j^2 (\cos\theta_j)^k \\ &\leq \varepsilon/2 \; + \; \left(1 - \frac{1}{4\,\mathsf{HT}_{\varepsilon/2}(P,z)}\right)^k. \end{aligned}$$

The first summation is at most $\varepsilon/2$ by the definition of $\mathsf{HT}_{\varepsilon/2}(P, z)$, and the bound for the second summation is justified since $1/\theta_j^2 \leq \mathsf{HT}_{\varepsilon/2}(P, z)$ implies $\cos\theta_j \leq 1 - 1/(4\mathsf{HT}_{\varepsilon/2}(P, z))$. Thus the second term is also at most $\varepsilon/2$ by the choice of k.

For the second statement, set $k = \frac{1}{2} h_{\varepsilon/3}(P, z)$. Then using the definition of $h_{\varepsilon/3}(P, z)$ and bounding $(1 - 1/2k)^{2k}$ from below by $1/3$, we get

$$\frac{\varepsilon}{3} \;\geq\; s_{2k} \;=\; \sum_j \nu_j^2 (\cos\theta_j)^{2k} \;>\; \sum_{j:\cos\theta_j > 1-\frac{1}{2k}} \nu_j^2 \left(1 - \frac{1}{2k}\right)^{2k} \;\geq\; \frac{1}{3} \sum_{j:\cos\theta_j > 1-\frac{1}{2k}} \nu_j^2.$$

Now observe that if $1/\theta_j^2 > k$, then $\cos\theta_j > 1 - \frac{1}{2k}$. Therefore $\Pr[H_z > k] \leq \varepsilon$, and the statement follows. □

B Proof of Lemma 3.12

Proof. Let $j \geq 1$ be the minimal integer $j \geq 1$ such that $a_j \neq 0$, for some $|\mu_z\rangle \in M$. Such an integer exists since $\mathsf{Span}(M) \neq \mathsf{Span}(|\phi_0\rangle)$. Assume for simplicity that $j = 1$, otherwise just restrict the Hilbert space to the subspace orthogonal to the $\mathrm{e}^{\pm \mathrm{i}\theta_k}$-eigenvectors, for $1 \leq k < j$.

Let $|\phi_1\rangle = (|\phi_1^+\rangle + |\phi_1^-\rangle)/\sqrt{2}$. We first claim that there exists z such that $a_{0,z}^2 = \langle \mu_z | \phi_0 \rangle^2 \leq \langle \mu_z | \phi_1 \rangle^2 = a_{1,z}^2$. The subscript z emphasizes the dependency of $a_{0,z}, a_{1,z}$ on z. The states $|\phi_0\rangle$ and $|\phi_1\rangle$ belong to $\mathsf{Span}(M)$ by the U_2-admissibility of M, so we get $\sum_z \langle \mu_z | \phi_0 \rangle^2 = 1 = \sum_z \langle \mu_z | \phi_1 \rangle^2$. Therefore there is some z such that, $\langle \mu_z | \phi_0 \rangle^2 \leq \langle \mu_z | \phi_1 \rangle^2$. Note that the right hand side is also $\langle \mu_z | \phi_1^{\pm} \rangle^2$.

Fix now arbitrarily such a z. To simplify the notation, we now refer to μ_z, α_z and coefficients $a_{j,z}$ without the subscript z.

We know from Lemma 3.11 that

$$a_0^2 \cot\frac{\alpha}{2} \;=\; -\sum_j a_j^2 \left(\cot\left(\frac{\alpha + \theta_j}{2}\right) + \cot\left(\frac{\alpha - \theta_j}{2}\right)\right) + a_{-1}^2 \tan\frac{\alpha}{2},$$

where $0 < \alpha < \theta_1 \leq \theta_2 \leq \ldots < \pi$. Since

$$-\left(\cot\left(\frac{\alpha + \theta_j}{2}\right) + \cot\left(\frac{\alpha - \theta_j}{2}\right)\right) \;=\; \frac{2\sin\alpha}{\cos\alpha - \cos\theta_j},$$

this is equivalent to

$$a_0^2 \cot\frac{\alpha}{2} \;=\; \sum_j a_j^2 \frac{2\sin\alpha}{\cos\alpha - \cos\theta_j} + a_{-1}^2 \tan\frac{\alpha}{2}. \tag{5}$$

Since all of the terms on the right hand side of Eq. (5) are positive, and $a_0^2 \leq a_1^2$, it follows that

$$\cot\frac{\alpha}{2} \;\geq\; \frac{2\sin\alpha}{\cos\alpha - \cos\theta_1}. \tag{6}$$

Since the right hand side decreases if θ_1 is replaced by some $\theta \in (\theta_1, \pi]$, we obtain for every $j > 1$,

$$\cot\frac{\alpha}{2} \quad \geq \quad \frac{2\sin\alpha}{\cos\alpha - \cos\theta_j}, \tag{7}$$

and

$$\cot\frac{\alpha}{2} \quad \geq \quad \frac{2\sin\alpha}{\cos\alpha - \cos\pi} \quad = \quad 2\tan\frac{\alpha}{2} \quad > \quad \tan\frac{\alpha}{2}. \tag{8}$$

We also know that the eigenvectors $|w_{\pm\alpha}\rangle = |\mu\rangle + \mathrm{i}|w'_{\pm\alpha}\rangle$ corresponding to the eigenvalues $\mathrm{e}^{\pm\mathrm{i}\alpha}$ satisfy

$$|w'_{\pm\alpha}\rangle = a_0 \cot\frac{\pm\alpha}{2}\,|\phi_0\rangle + \sum_j a_j \left(\cot\left(\frac{\pm\alpha - \theta_j}{2}\right)|\phi_j^+\rangle + \cot\left(\frac{\pm\alpha + \theta_j}{2}\right)|\phi_j^-\rangle\right) - a_{-1}\tan\frac{\pm\alpha}{2}\,|\phi\rangle.$$

Let us now define the vector $|s\rangle$ in the two dimensional space generated by $|w_{\pm\alpha}\rangle$ by

$$|s\rangle \quad = \quad \frac{|w_\alpha\rangle - |w_{-\alpha}\rangle}{\mathrm{i}}.$$

Observe that $|\mu\rangle$ is orthogonal to $|s\rangle$. Then the length of the projection of $|\widetilde{\phi}_0\rangle$ on $|s\rangle$ is the same as the one of $|\phi_0\rangle$. The length of the projection of $|\widetilde{\phi}_0\rangle$ on the subspace is therefore at least $|\langle s|\phi_0\rangle|/\|s\|$, which we now bound from below. Since the functions tan and cot are odd, we get

$$|s\rangle \quad = \quad 2a_0\cot\frac{\alpha}{2}\,|\phi_0\rangle + \sum_j a_j\left(\cot\left(\frac{\alpha - \theta_j}{2}\right) + \cot\left(\frac{\alpha + \theta_j}{2}\right)\right)\left(|\phi_j^+\rangle + |\phi_j^-\rangle\right) - 2a_{-1}\tan\frac{\alpha}{2}\,|\phi\rangle,$$

and therefore

$$\|s\|^2 \quad = \quad 4a_0^2\cot^2\frac{\alpha}{2} + 8\sum_j a_j^2\frac{\sin^2\alpha}{(\cos\alpha - \cos\theta_j)^2} + 4a_{-1}^2\tan^2\frac{\alpha}{2}.$$

From (5), (6), (7), and (8) it follows that

$$a_0^2\cot^2\frac{\alpha}{2} \quad \geq \quad 2\sum_j a_j^2\frac{\sin^2\alpha}{(\cos\alpha - \cos\theta_j)^2} + a_{-1}^2\tan^2\frac{\alpha}{2}$$

and therefore

$$\|s\|^2 \quad \leq \quad 8a_0^2\cot^2\frac{\alpha}{2}.$$

Since $\langle s|\phi_0\rangle = 2a_0\cot\frac{\alpha}{2}$, we can indeed conclude that

$$\frac{|\langle s|\phi_0\rangle|}{\|s\|} \quad \geq \quad \frac{1}{\sqrt{2}}.$$

□

C Proof of Lemma 4.7

Proof. By the definition of α_1 (Lemma 3.11),

$$a_0^2\cot\frac{\alpha_1}{2} + \sum_j a_j^2\left(\cot\left(\frac{\alpha_1 + \theta_j}{2}\right) + \cot\left(\frac{\alpha_1 - \theta_j}{2}\right)\right) \quad = \quad 0. \tag{9}$$

Fix any $\theta \geq 0$ and define the monotonically decreasing and continuous function $f : (0, \theta_1) \mapsto \mathbb{R}$:

$$f(x) \quad = \quad a_0^2\cot\frac{x}{2} + \sum_j a_j^2\left(\cot\left(\frac{x + \theta_j}{2}\right) + \cot\left(\frac{x - \theta_j}{2}\right)\right) - \tan^2\theta\,\tan\frac{x}{2}.$$

We know that $\lim_{x\to 0+} f(x) = +\infty$, $\lim_{x\to\theta_1-} f(x) = -\infty$, and $f(\alpha_1) \leq 0$. Therefore there is a unique $\alpha_1^\theta \in (0, \alpha_1]$ such that $f(\alpha_1^\theta) = 0$.

From the monotonicity of cot, for $x \in (0, \alpha_1]$, we have

$$\sum_j a_j^2 \left(\cot\left(\frac{x+\theta_j}{2}\right) + \cot\left(\frac{x-\theta_j}{2}\right)\right) \quad \geq \quad \sum_j a_j^2 \left(\cot\left(\frac{\alpha_1+\theta_j}{2}\right) + \cot\left(\frac{\alpha_1-\theta_j}{2}\right)\right).$$

Using this inequality together with Eq. (9) and the monotonicity of tan, we bound the function f as follows:

$$\begin{aligned} f(x) &\geq a_0^2 \cot\frac{x}{2} - a_0^2 \cot\frac{\alpha_1}{2} - \tan^2\theta \ \tan\frac{x}{2} \\ &\geq a_0^2 \cot\frac{x}{2} - a_0^2 \cot\frac{\alpha_1}{2} - \tan^2\theta \ \tan\frac{\alpha_1}{2} \\ &\geq a_0^2 \cot\frac{x}{2} - 1.01 \times a_0^2 \cot\frac{\alpha_1}{2}, \end{aligned}$$

where the last inequality comes from the hypothesis $0 \leq \tan\theta \leq a_0 \cot(\alpha_1/2)/10$. Since $f(\alpha_1^\theta) = 0$, we get that $\cot(\alpha_1^\theta/2) \leq 1.01 \times \cot(\alpha_1/2)$.

We now prove that $f(0.77 \times \alpha_1) \geq 0$, which concludes the proof. In the rest of the proof, we restrict the variable x to the interval $[0.77 \times \alpha_1, \alpha_1]$. Let β be the solution of $\tan(\beta/2) = \tan(\alpha_1/2)/1.01$ in $[0, \pi/2)$. Then $f(\beta) \geq 0$, and therefore $\alpha_1^\theta \geq \beta$.

Since $\alpha_1 \geq 0$, we have $\tan(\alpha_1/2) \geq \alpha_1/2$ and

$$\tan\frac{\beta}{2} \quad = \quad \frac{\tan(\frac{\alpha_1}{2})}{1.01} \quad \geq \quad \frac{\alpha_1}{2 \times 1.01}.$$

Moreover since $0 \leq \beta \leq \alpha_1 \leq \pi/4$, we have $\tan(\beta/2) \leq 2\beta/\pi$, and therefore

$$\beta \quad \geq \quad \frac{\pi}{4 \times 1.01} \times \alpha_1 \quad \geq \quad 0.77 \times \alpha_1.$$

□

D Proof of Lemma 4.8

Proof. Since the two vectors $|w_{\pm\alpha_1,\theta}\rangle$ (respectively, $|w_{\pm\alpha_1}\rangle$) have the same norm and are orthogonal, it suffices to upper bound the following squared norm:

$$\|w_{\alpha_1,\theta} - w_{-\alpha_1,\theta}\|^2 \quad = \quad 4\cos^2\theta \ \left[a_0^2 \cot^2\alpha_1^\theta/2 + 2\sum_j a_j^2 \left(\frac{\sin\alpha_1^\theta}{\cos\alpha_1^\theta - \cos\theta_j}\right)^2 + \tan^2\theta \ \tan^2\frac{\alpha_1^\theta}{2}\right] \tag{10}$$

By Lemma 4.7,

$$a_0^2 \cot^2\alpha_1^\theta/2 \quad \leq \quad (1.01)^2 \ a_0^2 \cot^2\alpha_1/2$$

and

$$\tan^2\theta \ \tan^2\frac{\alpha_1^\theta}{2} \quad = \quad 0.01 \ a_0^2 \cot^2\frac{\alpha_1}{2} \ \tan^2\frac{\alpha_1^\theta}{2} \quad \leq \quad 0.01 \ a_0^2$$

by the choice of $\tan\theta = a_0 \cot(\alpha_1/2)/10$ and the monotonicity of $\cot^2 = 1/\tan^2$ on $(0, \pi/2)$. Since

$$\sum_j a_j^2 \left(\frac{\sin\alpha_1^\theta}{\cos\alpha_1^\theta - \cos\theta_j}\right)^2 \quad \leq \quad \sum_j a_j^2 \left(\frac{\sin\alpha_1}{\cos\alpha_1 - \cos\theta_j}\right)^2, \tag{11}$$

the quantity inside of the square brackets of (10) is at most:

$$2\left(1.01^2 \times a_0^2 \cot^2 \alpha_1/2 + 2\sum_j a_j^2 \left(\frac{\sin\alpha_1}{\cos\alpha_1 - \cos\theta_j}\right)^2 + 0.01 \times a_0^2\right).$$

Hence,

$$\|w_{\alpha_1,\theta} - w_{-\alpha_1,\theta}\|^2 \quad \leq \quad 1.0301 \times (8\cos^2\theta) \times \|w_{\alpha_1} - w_{-\alpha_1}\|^2.$$

□