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.

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.

Finally, 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 [19] for the 2D grid. Extending his result, we show that for any state-transitive Markov chain with unique marked state, the quantum hitting time is of the same order for both the detection and finding problems.

1 Introduction

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" [15, 5, 2] and "quantum hitting time" [6, 18, 13] and to develop quantum algorithmic applications to sampling and search problems.

A few years ago, Ambainis [4] 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 [14], matrix product verification [7], and group commutativity testing [12]. 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 [1] were given by Shenvi *et al.* [17] on the hypercube, and by Childs and Goldstone [8] and Ambainis *et al.* [6] on the torus. Szegedy [18] 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 the quantum analogue of any symmetric Markov chain. Later Magniez *et al.* [13] extended this to define

*A full version of the paper with complete proofs can be downloaded at: `http://arxiv.org/abs/0808.0084`

†Research supported in part by the European Commission IST Integrated Project Qubit Applications (QAP) 015848, the ANR Blanc AlgoQP grant of the French Research Ministry, NSERC Canada, CIFAR, an Ontario ERA, QuantumWorks, and ARO/NSA (USA).

‡LRI, Univ Paris-Sud, CNRS; F-91405 Orsay, France; magniez@lri.fr, richterp@lri.fr.

§C&O and IQC, U. Waterloo, and Perimeter Institute, Ontario N2L 3G1, Canada; anayak@uwaterloo.ca. Some of this work was conducted while this author was visiting LRI, Univ Paris-Sud. Research at Perimeter Institute is supported in part by the Government of Canada through Industry Canada and by the Province of Ontario through MRI.

¶LRI, Univ Paris-Sud, CNRS; F-91405 Orsay, France; and Centre for Quantum Technologies, National University of Singapore, Singapore 117543; santha@lri.fr. Research at the Centre for Quantum Technologies is funded by the Singapore Ministry of Education and the National Research Foundation.

the 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? (He 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.* [13], 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 of Ambainis *et al.* [6], Szegedy [18], and Childs and Goldstone [8] 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 in run-time.) For some time it remained unclear if one could do better, until Tulsi [19] 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 [10]. 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?

In this paper we address several questions related to classical and quantum hitting times. 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 2.2).

Within the setting of abstract search algorithms presented by Ambainis *et al.* [6], we introduce quantum analogues of the two classical hitting times (Definition 3.2). The analogue of the Las Vegas version was already present in Szegedy's work [18], 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.* [13]. Our algorithm can detect the presence of a marked element in the starting state. 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 3.3). This is an improvement over the Szegedy detection algorithm whose complexity is related to the potentially larger Las Vegas quantum hitting time.

We then present a variant of the above algorithm, called **Rotate**, which can be used for the more difficult problem of finding, and whose complexity is also related to the Monte Carlo type quantum hitting time (Theorem 3.5). This improves the finding algorithm due to Ambainis *et al.* whose complexity was characterized by a potentially larger quantity, the inverse of the smallest eigenphase of the search algorithm. Our algorithm is also simpler. Combining **Rotate** with the ideas in the Tulsi algorithm for the 2D grid, we can find a 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.

As in the classical case, for some marked elements the two types of the quantum hitting time are of the same order (Fact 3.3 and Theorem 3.6). 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 3.7). 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 paper of Ambainis [3], see also [16]. 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 most 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 3.8), 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 3.5). Curiously, the classical analogue is reversible if and only if the quantum walk is reversible (Lemma 3.4).

2 Classical hitting times

Let P be an ergodic and reversible Markov chain over state space $X = \{1, \ldots, n\}$, which we identify with its transition probability matrix. We suppose that the eigenvalues of P are nonnegative, by replacing P with $(P+I)/2$ if necessary. More generally, one may also assume that the eigenvalues of P are at least α, where $\alpha \in [0,1)$, by replacing P with $((1-\alpha)P+(1+\alpha)I)/2$ if necessary. We make this further assumption when needed, for instance in Section 4. Let π denote the stationary distribution of P. Let P_{-z} be the $(n-1)\times(n-1)$ matrix we get by deleting from P the row and column indexed by z. Similarly, for a vector v, we let v_{-z} stand for the vector obtained by omitting the z-coordinate of v.

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.*

Proof. The proof globally proceeds along the lines of the proof of Lemma 8 in [18]. For $x \in X$ let e_x denote the characteristic vector of x. Let $w_1,\dots,w_n$ be the eigenvectors of P with associated eigenvalues $1=\kappa_1 \geq \dots \geq \kappa_n > 0$. Let v be an arbitrary eigenvector of P_z with eigenvalue λ. Since P is ergodic, $\|P_z\| < 1$, 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 P: let $w = \sum_{k=1}^n \gamma_k w_k$ and $e_z = \sum_{k=1}^n \delta_k w_k$. Then $wP = \lambda w + \nu e_z$ for some real number ν. Moreover, $\nu \neq 0$; otherwise w would have been an eigenvector of P, meaning that $\lambda = \kappa_k$, which contradicts our supposition. For $k=1,\dots,k$, 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 statement then follows since the left hand side of the above equation would be positive if λ were less than κ_n.

Definition 2.1. *For $z \in X$, the* 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.*

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} and S_{-z} is the "symmetrized form" $S_{-z} = \sqrt{\Pi_{-z}}P_{-z}\sqrt{\Pi_{-z}}^{-1}$ of P_{-z} with $\Pi_{-z} = \mathrm{diag}(\pi_x)_{x\neq z}$. The matrices P_{-z} and S_{-z} have the same spectrum since they are similar. Let $\{v_j : j \leq n-1\}$ be the set of normalized 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 $1 > \lambda_1 \geq \dots \geq \lambda_{n-1} \geq 0$. 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:

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

When $0<\theta\leq\pi/2$ then $1-\theta^2/2 \leq \cos\theta \leq 1-\theta^2/4$. 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 can 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. *For $z \in X$ and for $0<\varepsilon<1$, the* ε-error 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 indeed justified (proof in full version). 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 2.1. *For all z and ε, we have*

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

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

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

Proof. The first statement simply follows from the Markov inequality and from the relation $\mathbb{E}[H_z] \le \mathsf{HT}(P,z)/2$. For the second statement, let z be an element such that $\nu_1^2 \ge 1/2$. The existence of such an element is assured by Lemma 8 in [18]. Then $\mathsf{HT}(P,z) \le \sum_j 4\nu_j^2/\theta_j^2 \le 4/\theta_1^2 \le 4\mathsf{HT}_\varepsilon(P,z)$.

3 Quantum hitting times

3.1 Two notions of quantum walk. Let $U = U_2U_1$ be an *abstract search algorithm* as in [6], where $U_1 = I - 2|\mu\rangle\langle\mu|$ for a "target vector" $|\mu\rangle$ with real entries, and U_2 is a real unitary matrix with a unique 1-eigenvector $|\phi_0\rangle$. Without loss of generality we always assume that $|\phi_0\rangle$ has real entries. 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.

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 [18], and corresponds to first making a measurement according $(|\mu\rangle, |\mu\rangle^\perp)$. If the measurement outputs $|\mu\rangle$ we are done. Otherwise we run the abstract search algorithm.

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 paper remain valid if we keep $|\phi_0\rangle$.

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

THEOREM 3.1. ([6]) *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 $U_1 = I - 2|\mu\rangle\langle\mu|$. Let $U = U_2U_1$.*

- *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 $\langle\phi_0|\mu\rangle \ne 0$, then U has no 1-eigenspace.*

Thus one can use U in order to detect if $\langle\phi_0|\mu\rangle \ne 0$. Indeed, in that case, after a certain number T of iterations of U on $|\widetilde{\phi_0}\rangle$, the state moves far from the intial 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 the controlled operator c-V and is better known as the *control test* or the *Hadamard test*. Namely observe that $(H\otimes I)(\text{c-}V)(H\otimes I)|0\rangle|\psi\rangle = \frac{1}{2}|0\rangle(|\psi\rangle + V|\psi\rangle) + \frac{1}{2}|1\rangle(|\psi\rangle - V|\psi\rangle)$. Therefore a measurement of the first register gives outcome 1 with probability $\||\psi\rangle - V|\psi\rangle\|^2/4$.

Szegedy [18] 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 $|\pi\rangle$. The time-reversal P^* of this chain is defined by 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 $\mathcal{H} = \mathbb{C}^{X\times X}$. For a state $|\psi\rangle \in \mathcal{H}$, 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 $\mathcal{H}$. If $\mathcal{K}$ is a subspace of $\mathcal{H}$ spanned by a set of mutually orthogonal 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

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

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. ([18, 13]) *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 of Ambainis *et al.* is made explicit by the following fact.

FACT 3.1. *Let $z \in X$ and $|\mu\rangle = |z\rangle|p_z\rangle$. Let $U_2 = \mathsf{SWAP}\cdot\mathrm{ref}(\mathcal{A})$ and $U_1 = I - 2|\mu\rangle\langle\mu|$. 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 unitary matrix with real entries. The potential eigenvalues of U are then 1, -1, and pairs of conjugate complex numbers $(e^{i\alpha_j}, e^{-i\alpha_j})$ with $0 < \alpha_j < \pi$, for $1 \le j \le J$, for some J.

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

$$(3.1)\quad |\psi\rangle = \delta_0|w_0\rangle + \sum_{1\le j\le J} \delta_j(|w_j^+\rangle + |w_j^-\rangle) + \delta_{-1}|w_{-1}\rangle,$$

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 $e^{i\alpha_j}$ and $e^{-i\alpha_j}$, and $|w_j^-\rangle = \overline{|w_j^+\rangle}$.

We now describe a procedure whose purpose is to detect the state $|\psi\rangle$ has a component orthogonal to the 1-eigenspace of U. In the context of the abstract search algorithm, this is equivalent to $\langle\phi_0|\mu\rangle \neq 0$. The idea, similar to the approach of Magniez *et al.* [13], is to apply the phase estimation algorithm of Kitaev [11] and Cleve *et al.* [9] to U.

THEOREM 3.2. ([11, 9]) *Given an eigenvector $|v\rangle$ of a unitary operator U with eigenvalue $e^{i\alpha}$, the corresponding phase $\alpha \in (-\pi, \pi]$ can be determined with precision Δ and error probability at most $1/3$ by a circuit* **Estimate**. *If $|v\rangle$ is a 1-eigenvector of U, then* **Estimate** *determines $\alpha = 0$ with probability 1. Moreover,* **Estimate** *makes $O(1/\Delta)$ calls to the controlled operator c-U and its inverse, and it contains $O((\log 1/\Delta)^2)$ 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 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, the probabilities in fact sum to $\|\psi\|^2$, since $|\psi\rangle$ is not necessarily normalized, and has norm at most 1.

LEMMA 3.1. *Assume that* $\Pr[QH > 1/\Delta] \le \varepsilon$. *Then the procedure* **Detect**(U, Δ, ε) *accepts $|\psi\rangle$ with probability $\|\psi\|^2 - \delta_0^2 - O(\varepsilon)$, and moreover with probability 0 if $|\delta_0| = \|\psi\|$. In addition, the number of applications of c-U is $O(\log(1/\varepsilon)/\Delta)$.*

Proof. Let us first assume that **Estimate** can compute the eigenphase of any eigenvector with certainty. This assumption is in fact valid when $|\delta_0| = \|\psi\|$. Then the procedure **Detect** rejects exactly with probability δ_0^2.

Assume now that $\Pr[QH > 1/\Delta] \le \varepsilon$, 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 $\alpha_j \ge \Delta$. By hypothesis, the contribution of these eigenphases has squared Euclidean norm $2\sum_j \delta_j^2$. The success probability is then amplified to $1 - O(\varepsilon)$ by checking that all the $O(\log(1/\varepsilon))$ outcomes of **Estimate** are nonzero. For the special case of eigenphase 0, whose contribution has squared Euclidean norm δ_0^2, **Estimate** gives approximation 0 with probability 1.

The contribution of the other eigenphases has squared Euclidean norm less than ε in the vector $|\psi\rangle$. Therefore the overall acceptance probability is $\|\psi\|^2 - \delta_0^2 - O(\varepsilon)$.

In the case of quantum walk, the above theorem justifies the following definitions of quantum hitting times. Let U be some abstract search U_2U_1, where $U_1 = I - 2|\mu\rangle\langle\mu|$, 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. *The* 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 quantum ε-error $|\mu\rangle$-hitting time *of U_2 is defined as*

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

Using Theorem 3.1, Lemma 3.1 and our definition of quantum hitting time, we directly get:

THEOREM 3.3. *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* $\mathrm{O}(\log(1/\varepsilon) \times T)$.

If one would like to deal only with normalized states, and to come back to the original starting state $|\phi_0\rangle$, we can encapsulate the projection to the space orthogonal to $|\mu\rangle$ into our algorithm such as in the following main procedure, and deduce its behavior from the above theorem.

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

1. Make a measurement according $(|\mu\rangle, |\mu\rangle^\perp)$.
2. If the measurement outputs $|\mu\rangle$, `ACCEPT`.
   Otherwise apply **Detect**(U, Δ, ε).

COROLLARY 3.1*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 on 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 3.3 albeit with the parameter $\mathsf{QHT}(P, z)$ for symmetric Markov chains:

THEOREM 3.4. ([18]) *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.* [6] have a similar result in terms of the smallest eigenphase of U_2U_1.

Suppose we wish to not only detect if $\langle\mu|\phi_0\rangle \neq 0$, but also to map $|\psi\rangle$ 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 $|\psi\rangle$ to an orthogonal state that is closer to $|\mu\rangle$.

DEFINITION 3.3. *The U-*rotation *of* $|\psi\rangle$ *is defined as* $\delta_0|w_0\rangle + \sum_j \delta_j(|w_j^+\rangle - |w_j^-\rangle) + \delta_{-1}|w_{-1}\rangle$, *where the decomposition of* $|\psi\rangle$ *in terms of the orthonormal set of eigenvectors* $\{|w_j^+\rangle, |w_j^-\rangle\}$ *of U is given by Eq. (3.1).*

FACT 3.2. *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* $|\psi\rangle$.

This operation can be implemented efficiently by the following procedure with further assumptions on U. Namely, we would like U to avoid having any eigenvalue close to -1. This is naturally the case when we consider the quantum analogue of a reversible Markov chain whose eigenvalues are all positive.

Rotate(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 state $|\psi\rangle$.
2. If the majority of estimated phases are negative
   Perform a Phase a Flip.
   Otherwise do nothing.
3. Undo the Phase Estimations of Step 1.

THEOREM 3.5. *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 3.3.

3.3 Comparison between QHT and QHT$_\varepsilon$.

We assume henceforth that $\langle\phi_0|\mu\rangle \neq 0$; otherwise, the problem is trivial—by our definition $\mathsf{QHT}_\varepsilon(U_2, |\mu\rangle) = \mathsf{QHT}(U_2, |\mu\rangle) = 0$.

The Markov inequality immediately implies the following relationship between these two measures:

FACT 3.3. *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. Writing $|\mu\rangle$ in the eigenspace decomposition of U_2 we get

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

where $|\phi_{-1}\rangle$ is a (-1)-eigenvector of U_2, and $|\phi_j^{\pm}\rangle$ are $\mathrm{e}^{\pm \mathrm{i}\theta_j}$-eigenvectors of U_2 such that a_{-1} and a_j are real, $|\phi_{-1}\rangle$ has real entries, and $|\phi_j^-\rangle = \overline{|\phi_j^+\rangle}$. Since $|\phi_0\rangle$ has real entries, a_0 is also real.

Ambainis *et al.* [6] (see also Tulsi [19]) show the following relation between the spectrum of U_2 and that of U.

LEMMA 3.2. ([6, 19]) *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* $|w'_\alpha\rangle$ *equals*

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

As in the classical case, we are only able to upper bound QHT by QHT_ε for some particular target states $|\mu\rangle$. Therefore, we consider in the following lemma (proof in full version) an arbitrary set of orthonormal vectors $M = \{|\mu_z\rangle\}$ whose span contains $|\phi_0\rangle$. In the case of the quantum analogue of a Markov chain P as in Definition 3.1, a natural choice for $|\mu_z\rangle$ is $|z\rangle|p_z\rangle$ for some z in the state space of the Markov chain. Recall that $|\widetilde{\phi_0}\rangle = |\phi_0\rangle - a_0|\mu\rangle$.

LEMMA 3.3. *Let* $M = \{|\mu_z\rangle\}$ *be a set of orthonormal vectors with real coefficients in the standard basis, such that* $|\phi_0\rangle \in \mathsf{Span}(M)$. *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* $1/\sqrt{2}$.

COROLLARY 3.2. *Let* $M = \{|\mu_z\rangle\}$ *be a set of real orthonormal vectors such that* $|\phi_0\rangle \in \mathsf{Span}(M)$. *For all* U_2 *there exists* z *such that for all* $\varepsilon \le 1/2$,

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

THEOREM 3.6. *Let* $M = \{|\mu_z\rangle\}$ *be a set of real orthonormal vectors such that* $|\phi_0\rangle \in \mathsf{Span}(M)$. *For all* U_2 *there exists* z *such that for all* $\varepsilon \le 1/2$,

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

Proof. This is a consequence of Corollary 3.2 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 $\gamma < 1/2$. Let $z \in X$.

THEOREM 3.7. *Assume that the eigenvalues of* P *are all positive. Then we have the following relations:*

- *For all* z, $\quad \mathsf{QHT}(P, z) \le \sqrt{\mathsf{HT}(P, z)/2}$.
- *For all* z *and* ε, $\quad \mathsf{QHT}_\varepsilon(P, z) = \sqrt{\mathsf{HT}_\varepsilon(P, z)}$.

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 P_{-z} where the eigenvalue of v_j is $\cos\theta_j$, with $0 < \theta_1 \le \ldots \le \theta_{n-1} < \pi/2$. Let $v_j[x]$ denote the x-coordinate of the vector v_j. We set $|\xi_j\rangle = \sum_{x\ne z} v_j[x]|x\rangle|p_x\rangle$ and $|\zeta_j\rangle = \sum_{y \ne z} v_j[y]|p_y^*\rangle|y\rangle$. 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 3.1). 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

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

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

The same quadratic speed-up as above holds when there are multiple marked elements in the state space X. The search algorithm and its analysis are similar and are omitted from this article.

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 3.4 below.

DEFINITION 3.4. *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 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 [3], see also [16]. Szegedy considered for F^x a specific kind of reflection based on Markov chain transition probabilities (see Section 3.1).

DEFINITION 3.5. *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 state:

FACT 3.4. *Let $|\psi^x\rangle = F^x|\phi^x\rangle$. Then $|\phi_0\rangle = \sum_x \sqrt{\pi_x}|\psi^x\rangle|x\rangle$.*

LEMMA 3.4. *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 and only 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 $y \in X$:

$$\begin{aligned} \sum_x \pi_x p_{xy} &= \sum_x \langle xy|\phi_0\rangle^2 \quad \text{by definition of } P \text{ and } |\phi_0\rangle \\ &= \sum_x \pi_y \langle x|\psi^y\rangle^2 \quad \text{by Fact 3.4} \\ &= \pi_y \| |\psi^y\rangle \|^2 = \pi_y. \end{aligned}$$

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 precisely 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 3.8. *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 $\mathcal{B}_{-z} = \mathsf{Span}(|\phi^y\rangle|y\rangle : y \in X \setminus \{z\}) = \mathsf{SWAP}(\mathcal{A})$.

From [18], we know that the spectrum of $(U_2U_1)^2$ is completely defined by the discriminant matrix $D = A^*B$, 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 $\langle xy|\pi\rangle = \langle yx|\pi\rangle$, 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 $\sum_x \sqrt{\pi_x}|x\rangle|p_x\rangle$ to $|\phi_0\rangle$, $|z\rangle|p_z\rangle$ to $|z\rangle|\phi^z\rangle$, and therefore $\sum_{x \neq z} \sqrt{\pi_x}|x\rangle|p_x\rangle$ to $|\widetilde{\phi}_0\rangle$.

4 Finding with constant probability

In this section, we extend a technique devised by Tulsi [19] 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. The technique may be combined with ideas developed in the earlier sections to give an algorithm for the quantum analogue of an arbitrary reversible ergodic Markov chain.

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:

$$(4.2) \qquad |\mu\rangle = a_0|\phi_0\rangle + \sum_{1 \leq j \leq J} a_j(|\phi_j^+\rangle + |\phi_j^-\rangle),$$

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 3.2:* $|\mu\rangle = \sum_\alpha \frac{1}{\|w_\alpha\|^2}|w_\alpha\rangle$*, and* $|\widetilde{\phi}_0\rangle = \sum_\alpha \frac{a_0 \mathrm{i}\cot(\frac{\alpha}{2})}{\|w_\alpha\|^2}|w_\alpha\rangle$.

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

By Lemma 3.2, $\langle\phi_0|w_\alpha\rangle = \langle\phi_0|(|\mu\rangle + \mathrm{i}|w'_\alpha\rangle) = a_0 + a_0\mathrm{i}\cot\frac{\alpha}{2}$. The second equation follows by combining the above with $|\widetilde{\phi}_0\rangle = |\phi_0\rangle - a_0|\mu\rangle$.

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

Theorem 3.7 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 [19] 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:

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

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: $\mathbf{T}(U_1, U_2, \theta) = U_2^\theta U_1^\theta$. This is precisely the circuit used by Tulsi: his rotation $\hat{R}_\theta = R_\theta^\dagger$ in our notation. Tulsi [19] 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 4.1. *The decomposition of* $|1\rangle|\mu\rangle$ *in the eigenvector basis of* U_2^θ *is:*

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

where the coefficients a_0, a_j *are precisely those in Eq. (4.2).*

LEMMA 4.3. *The eigenvalues* $\mathrm{e}^{\pm\mathrm{i}\alpha^\theta}$*, of the operator* $\mathbf{T}(U_1, U_2, \theta)$ *are solutions to the equation*

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

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* $|w'_{\alpha,\theta}\rangle$ *equals*

$$\cos\theta\,|\theta^\perp\rangle\left(a_0\cot\left(\frac{\alpha^\theta}{2}\right)|\phi_0\rangle + \sum_j a_j\left(\cot\left(\frac{\alpha^\theta-\theta_j}{2}\right)|\phi_j^+\rangle + \cot\left(\frac{\alpha^\theta+\theta_j}{2}\right)|\phi_j^-\rangle\right)\right) + \sin\theta\,|\theta\rangle\left(\tan\left(\frac{\alpha^\theta}{2}\right)|\mu\rangle\right).$$

Proof. We apply Lemma 3.2 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 $|\widetilde{\phi}_{0,\theta}\rangle = |\theta^\perp\rangle|\widetilde{\phi}_0\rangle$. The following are analogous to Lemmata 4.1 and 4.2:

COROLLARY 4.1. *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 Corollary 4.3:*

$$|1\rangle|\mu\rangle = \sum_{\alpha^\theta}\frac{1}{\|w_{\alpha,\theta}\|^2}|w_{\alpha,\theta}\rangle, \quad \textit{and}$$

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

COROLLARY 4.2. *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 4.4 (proof in full version) proves that α_1^θ is of the same order as the principal eigenphase α_1 of the original algorithm U_2U_1. Lemma 4.5 (proof in full version) 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 lemmas extend corresponding results by Tulsi in the case of the 2D grid, and lead to the main result of this section.

Lemma 4.4. *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* $0.78 \times \alpha_1 \leq \alpha_1^\theta \leq \alpha_1$.

Lemma 4.5. $\|w_{\pm\alpha_1,\theta}\| \leq (3\cos\theta) \times \|w_{\pm\alpha_1}\|$.

Theorem 4.1. *Let* $\varepsilon > 0$ *be any constant. Suppose that the squared length of the projection of the state* $|\widetilde{\phi_0}\rangle$ *onto the principal eigenspace of* U_2U_1 *is bounded below by* $1-\varepsilon$. *Then, for every* $T \geq \mathsf{QHT}_\varepsilon(U_2, |\widetilde{\phi_0}\rangle)/0.78$, *the procedure* $\mathbf{Rotate}(\mathbf{T}(U_1, U_2, \theta), 1/T, 1/4)$ *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 4.4, $T \leq 1/(0.78\alpha_1) = \mathsf{QHT}_\varepsilon(U_2, |\mu\rangle)/0.78$. We now get our conclusion by applying Corollary 4.2, Lemmata 4.4 and 4.5, and Theorem 3.5.

We combine the above theorem with Lemma 3.3 to get our final result.

Corollary 4.3. *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* $T \geq \mathsf{QHT}_\varepsilon(U_2, |\widetilde{\phi_0}\rangle)/0.78$, *the procedure* $\mathbf{Rotate}(\mathbf{T}(U_1, U_2, \theta), 1/T, 1/4)$ *maps* $|\widetilde{\phi_{0,\theta}}\rangle$ *to a state with constant overlap with the target state* $|1\rangle|\mu\rangle$.

References

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

[2] 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.

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

[4] A. Ambainis. Quantum walk algorithm for Element Distinctness. In *Proceedings of the 45th Symposium on Foundations of Computer Science*, pages 22–31, 2004.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

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

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

[13] 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.

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

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

[16] 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.

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

[18] 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.

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