Algorithmica (2016) 74:851–907
DOI 10.1007/s00453-015-9979-8

Quantum Walks Can Find a Marked Element on Any Graph

Hari Krovi · Frédéric Magniez · Maris Ozols · Jérémie Roland

Received: 13 February 2014 / Accepted: 19 February 2015 / Published online: 3 March 2015

Abstract We solve an open problem by constructing quantum walks that not only detect but also find marked vertices in a graph. In the case when the marked set M consists of a single vertex, the number of steps of the quantum walk is quadratically smaller than the classical hitting time $\mathrm{HT}(P, M)$ of any reversible random walk P on the graph. In the case of multiple marked elements, the number of steps is given in terms of a related quantity $\mathrm{HT}^+(P, M)$ which we call extended hitting time. Our approach is new, simpler and more general than previous ones. We introduce a notion of interpolation between the random walk P and the absorbing walk P', whose marked states are absorbing. Then our quantum walk is simply the quantum analogue of this interpolation. Contrary to previous approaches, our results remain valid when the random walk P is not state-transitive. We also provide algorithms in the cases when only approximations or bounds on parameters p_M (the probability of picking a marked vertex from the stationary distribution) and $\mathrm{HT}^+(P, M)$ are known.

A preliminary version of this work appeared in the *Proceedings of the 37th International Colloquium on Automata, Languages and Programming*, volume 6198 of Lecture Notes in Computer Science, pages 540–551, Springer, 2010.

H. Krovi (✉)
Quantum Information Processing Group, Raytheon BBN Technologies, Cambridge, MA 02138, USA
e-mail: hkrovi@bbn.com; hkrovi@gmail.com

F. Magniez
CNRS, LIAFA, University Paris Diderot, Sorbonne Paris-Cité, 75205 Paris, France

M. Ozols
DAMTP, Centre for Mathematical Sciences, University of Cambridge, Cambridge CB3 0WA, UK
e-mail: marozols@yahoo.com

J. Roland
QuIC, Ecole Polytechnique de Bruxelles, Université Libre de Bruxelles (ULB), 1050 Brussels, Belgium

Keywords Quantum algorithms · Quantum walks · Markov chains · Interpolated quantum walks

1 Introduction

Many randomized classical algorithms rely heavily on random walks or Markov chains. This technique has been extended to the quantum case and is called a *quantum walk*. Ambainis [1] was the first to solve a natural problem—the element distinctness problem—using a quantum walk. Following this, many other quantum walk algorithms were discovered (see, for example, [2–4]).

A common class of problems that are typically solved using a random walk are the so-called *spatial search problems*. In such problems, the displacement constraints are modelled by edges of an undirected graph G, which has some desired subset of vertices M that are marked. The goal of a spatial search problem is to find one of the marked vertices by traversing the graph along its edges. Classically, a simple strategy for finding a marked vertex is to perform a random walk on G, by repeatedly applying some stochastic matrix P until one of the marked vertices is reached (see Sect. 2.5 for more details). The expected running time of this algorithm is called the *hitting time* of P and is denoted by $\mathrm{HT}(P, M)$.

Quantum walk algorithms for the spatial search problem were studied in [5]. This problem has also been considered for several specific graphs, such as the hypercube [6] and the grid [7,8]. The notion of the hitting time has been carried over to the quantum case in [8–14] by generalizing the classical notion in different ways. Usually, the quantum hitting time has a quadratic improvement over the classical one. However, several serious restrictions were imposed for this to be the case. A quantum algorithm could only solve the *detection problem* of deciding whether there are marked vertices or not [10], but for being able to *find* them, the Markov chain had to be reversible, state-transitive, and with a unique marked vertex [13,15]. Recall that a Markov chain P is called *state-transitive* if, given any two states x and y, there exists an automorphism[1] of P that takes x to y. This is analogous to the definition of vertex-transitive graphs and imposes a high degree of symmetry on the Markov chain (intuitively, each state of P locally looks the same). While the detection algorithm [10] is quite intuitive and well understood, the finding algorithm [13,15] requires an elaborate proof whose intuition is not clear. This is due in part to a modification of the quantum walk, so that the resulting walk is not a quantum analogue of a Markov chain anymore.

Whether this quadratic speed-up for finding a marked element also holds for all *reversible* Markov chains (and not merely state-transitive ones) was an open question. In the case of a single marked element, we give a positive answer to this question by providing a quantum algorithm, which *finds* the marked element in time that is quadratically smaller than the classical hitting time for all reversible Markov chains, thus removing the extraneous condition of state-transitivity. While our algorithm also extends to the case of multiple marked elements, the possibility of a general quadratic speed-up still remains open in that case, because of a possible gap between the so-

[1] An *automorphism* of P is a permutation matrix Q such that $QPQ^{\mathsf{T}} = P$.

called extended hitting time $\mathrm{HT}^+(P, M)$, which characterizes the cost of our quantum algorithm, and the standard hitting time $\mathrm{HT}(P, M)$ (see Sect. 2.7 and Appendix C for more details[2]).

1.1 Related Work

Inspired by Ambainis' quantum walk algorithm for solving the element distinctness problem [1], Szegedy [10] has introduced a powerful way of constructing quantum analogues of Markov chains which led to new quantum walk algorithms. He showed that for any symmetric Markov chain a quantum walk could detect the presence of marked vertices in at most the square root of the classical hitting time. However, showing that a marked vertex could also be found in the same time (as is the case for the classical algorithm) proved to be a very difficult task. Magniez et al. [12] extended Szegedy's approach to the larger class of ergodic Markov chains, and proposed a quantum walk algorithm to find a marked vertex, but its complexity may be larger than the square root of the classical hitting time. A typical example where their approach fails to provide a quadratic speed-up is the 2D grid, where their algorithm has complexity $\Theta(n)$, whereas the classical hitting time is $\Theta(n \log n)$. Ambainis et al. [8] and Szegedy's [10] approaches yield a complexity of $\Theta(\sqrt{n} \log n)$ in this special case, for a unique marked vertex. This result was, in fact, first obtained by Childs and Goldstone [7,17] using a continuous-time quantum walk.

However, whether a full quadratic speed-up was possible in the 2D grid case remained an open question, until Tulsi [15] proposed a solution involving a new technique. Magniez et al. [13] extended Tulsi's technique to any reversible state-transitive Markov chain, showing that for such chains, it is possible to find a unique marked vertex with a full quadratic speed-up over the classical hitting time. However, as explained earlier, state-transitivity is a strong symmetry condition, and furthermore their technique cannot deal with multiple marked vertices. Recently, [18] have suggested a modification of the original [8] algorithm in the case of the 2D grid with a single marked element by replacing amplitude amplification with a classical search in a neighbourhood of the final vertex. This results in a $\sqrt{\log n}$ speed-up over the original algorithm from [8] and yields complexity $\mathrm{O}(\sqrt{n \log n})$ as in the case of [13,15].

It seems implausible that one has to rely on involved techniques to solve the finding problem under such restricted conditions in the quantum case, while the classical random walk algorithm (see Sect. 2.5) is conceptually simple and works under general conditions. The classical algorithm simply applies an *absorbing* walk P' obtained from P by turning all outgoing transitions from marked states into self-loops (see Appendix A). Each application of P' results in more probability being absorbed in marked states.

Previous attempts at providing a quantum speed-up over this classical algorithm have followed one of these two approaches:

[2] Note that in the preliminary version of this work [16], a subtle error led to the wrong conclusion that $\mathrm{HT}^+(P, M) = \mathrm{HT}(P, M)$ for all M and reversible P. In general this only holds when $|M| = 1$.

– Combining a quantum version of P with a reflection through marked vertices to mimic a Grover operation [1,8,12].
– Directly applying a quantum version of P' [10,13].

The problem with these approaches is that they would only be able to find marked vertices in very restricted cases. We explain this by the different nature of random and quantum walks: while both have a stable state, i.e., the stationary distribution for the random walk and the eigenstate with eigenvalue 1 for the quantum walk, the way both walks act on other states is dramatically different.

Indeed, an ergodic random walk will converge to its stationary distribution from any initial distribution. This apparent robustness may be attributed to the inherent randomness of the walk, which will smooth out any initial perturbation. After many iterations of the walk, non-stationary contributions of the initial distribution will be damped and only the stationary distribution will survive (this can be attributed to the thermodynamical irreversibility[3] of ergodic random walks).

On the other hand, this is not true for quantum walks, because in the absence of measurements a unitary evolution is deterministic (and in particular thermodynamically reversible): the contributions of the other eigenstates will not be damped but just oscillate with different frequencies, so that the overall evolution is quasi-periodic. As a consequence, while iterations of P' always lead to a marked vertex, it may happen that iterations of the quantum analogue of P' will never lead to a state with a large overlap over marked vertices, unless the walk exhibits a strong symmetry (as is the case for a state-transitive walk with only one marked element, which could be addressed by previous approaches).

1.2 Our Approach and Contributions

Our main result is that a quadratic speed-up for finding a marked element via a quantum walk holds for any reversible Markov chain with a single marked element. We provide several algorithms for different versions of the problem. Compared to previous results, our algorithms are more general and conceptually clean. The intuition behind our main algorithm is based on the adiabatic algorithm from [19]. However, all algorithms presented here are circuit-based and thus do not suffer from the drawbacks of the adiabatic algorithm in [19].

We choose an approach that is different from the ones described above: first, we directly modify the original random walk P, and then construct a quantum analogue of the modified walk. We choose the modified walk to be the interpolated Markov chain $P(s) = (1-s)P + sP'$ that interpolates between P and the absorbing walk P' whose outgoing transitions from marked vertices have been replaced by self-loops. Thus, we can still use our intuition from the classical case, but at the same time also get simpler proofs and more general results in the quantum case.

All of our quantum walk algorithms are based on eigenvalue estimation performed on the operator $W(s)$, a quantum analogue of the Markov chain $P(s)$. We consider

[3] Reversibility of Markov chains (see Appendix A.1.2) is not related to thermodynamical reversibility. Actually, even a "reversible" Markov chain is thermodynamically irreversible.

the $(+1)$-eigenstate $|\Psi_n(s)\rangle$ of $W(s)$, which plays the role of the stationary distribution in the quantum case. We use the interpolation parameter s to tune the length of projections of $|\Psi_n(s)\rangle$ onto marked and unmarked vertices. If both projections are large, our algorithm succeeds with large probability in $\mathrm{O}\big(\sqrt{\mathrm{HT}^+(P, M)}\big)$ steps (Theorem 6), where $\mathrm{HT}^+(P, M)$ is a quantity we call the extended hitting time (see Definition 9 and Prop. 3 for precise statements). In particular, we find that when $|M| = 1$, $\mathrm{HT}^+(P, M) = \mathrm{HT}(P, M)$ and when $|M| > 1$, there exists P such that $\mathrm{HT}^+(P, M) > \mathrm{HT}(P, M)$.

We also provide several modifications of the main algorithm. In particular, we show how to make a suitable choice of s to balance the overlap of $|\Psi_n(s)\rangle$ on marked and unmarked vertices even if some of the parameters required by the main algorithm are unknown and the rest are either approximately known (Theorems 7, 8) or bounded (Theorems 9, 10). In all cases a marked vertex is found in $\tilde{\mathrm{O}}\big(\sqrt{\mathrm{HT}^+(P, M)}\big)$ steps.

In Sect. 2 we introduce several variations of the spatial search problem and provide preliminaries on random and quantum walks and their hitting times. Sect. 3 describes our quantum algorithms and contains the main results. The main algorithm is presented in Sect. 3.1 and is followed by several modifications that execute the main algorithm many times with different parameters.

Technical and background material is provided in several appendices. In Appendix A we describe basic properties of the interpolated Markov chain $P(s)$ and the extended hitting time $\mathrm{HT}^+(P, M)$, which is crucial for the analysis of the algorithms in Sect. 3. In Appendix B we compute the spectrum of the walk operator $W(s)$ and show how it can be implemented for any s. In Appendix C we discuss limitations of our results for the case of multiple marked elements.

2 Preliminaries

2.1 Classical Random Walks

A Markov chain[4] on a discrete state space X of size $n := |X|$ is described by an $n \times n$ *row-stochastic matrix* P where $P_{xy} \in [0, 1]$ is the transition probability from state x to state y and

$$\forall x \in X : \sum_{y \in X} P_{xy} = 1. \tag{1}$$

Such a Markov chain has a corresponding *underlying directed graph* with n vertices labelled by elements of X, and directed arcs labelled by *non-zero* probabilities P_{xy} (see Fig. 1).

We represent probability distributions by *row* vectors whose entries are real, non-negative, and sum to one. When one step of the Markov chain P is applied to a given distribution p, the resulting distribution is pP. A probability distribution π that satisfies $\pi P = \pi$ is called a *stationary distribution* of P. For more background on Markov chains see, e.g., [20–23].

[4] We will use terms "random walk", "Markov chain", and "stochastic matrix" interchangeably. The same holds for "state", "vertex", and "element".

$$P = \begin{pmatrix} 0.7 & 0.3 & 0 \\ 0 & 0 & 1.0 \\ 0 & 0.8 & 0.2 \end{pmatrix}$$

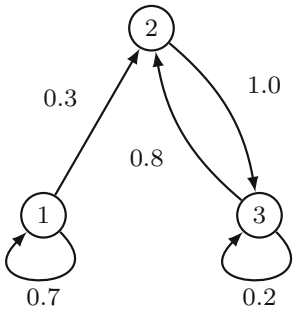

Fig. 1 Markov chain P and the corresponding graph with transition probabilities

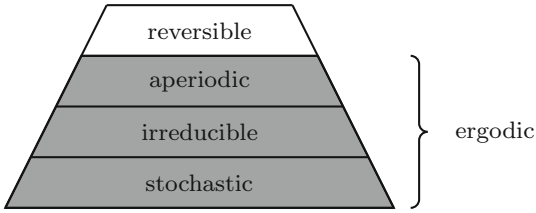

Fig. 2 The order in which Markov chain properties from Definition 1 are typically imposed (*starting from the bottom*). Reversibility is discussed in more detail in Appendix A.1.2

2.1.1 Ergodicity

Let us consider Markov chains with some extra structure.

Definition 1 A Markov chain P is called

- *irreducible*, if any state in the underlying directed graph can be reached from any other by a finite number of steps (i.e., the graph is strongly connected);
- *aperiodic*, if there is no integer $k > 1$ that divides the length of every directed cycle of the underlying directed graph;
- *ergodic*, if it is both irreducible and aperiodic.
- *reversible*, if it is ergodic and satisfies the so called *detailed balance equation* i.e., the stationary distribution π satisfies $\pi_x P_{xy} = \pi_y P_{yx}$.

Equivalently, a Markov chain P is ergodic if there exists some integer $k_0 \geq 1$ such that all entries of P^{k_0} (and, in fact, of P^k for any $k \geq k_0$) are strictly positive (see [23, Prop. 1.7, p. 8] for a proof of this equivalence). Some authors call such chains *regular* and use the term "ergodic" already for irreducible chains [20,21]. From now on, we will exclusively consider Markov chains that are ergodic and reversible (but not necessarily state-transitive).

Even though some of the Markov chain properties in Definition 1 are independent from each other (such as irreducibility and aperiodicity), usually they are imposed in a specific order which is summarized in Fig. 2. As we impose more conditions, more can be said about the spectrum of P as discussed in the next section.

2.1.2 Perron–Frobenius Theorem

The following theorem will be very useful for us. It is essentially the standard Perron–Frobenius theorem [24, Theorem 8.4.4, p. 508], but adapted for Markov chains. (This theorem is also known as the "Ergodic Theorem for Markov chains" [22, Theorem 5.9, p. 72].) The version presented here is based on the extensive overview of Perron–Frobenius theory in [25, Chapter 8].

Theorem 1 (Perron–Frobenius) *Let P be a stochastic matrix. Then*

- *all eigenvalues of P are at most* 1 *in absolute value and* 1 *is an eigenvalue of P;*
- *if P is irreducible, then the* 1*-eigenvector is unique and strictly positive (i.e., it is of the form $c\pi$, where $c > 0$ and π is a probability distribution that is non-zero everywhere);*
- *if in addition to being irreducible, P is also aperiodic (i.e., P is ergodic), then the remaining eigenvalues of P are strictly smaller than* 1 *in absolute value.*

If P is irreducible but not aperiodic, it has some complex eigenvalues on the unit circle (which can be shown to be roots of unity) [25, Chapter 8]. However, when in addition we also impose aperiodicity (and hence ergodicity), we are guaranteed that there is a unique eigenvalue of absolute value 1 and, in fact, it is equal to 1.

2.2 Spatial Search on Graphs

We fix an undirected graph $G = (X, E)$ with $n := |X|$ vertices and a set of edges E. Let $M \subseteq X$ be a set of marked vertices of size $m := |M|$. We insist that during the traversing of the graph the current vertex is stored in a distinguished *vertex register*. Our goal is to find any of the marked vertices in M using only evolutions that preserve the locality of G on the vertex register, i.e., to perform a *spatial search* on G [5] (here we use a notion of locality that is a special case of the one defined in [5] and it is powerful enough for our purpose). Note that algorithms for spatial search cannot simply ignore the vertex register as only the vertex encoded in this register can be checked to be marked or not.

We allow two types of operations on the vertex register:

- *static transformations*, that can be conditioned on the state of the vertex register, but do not modify it;
- SHIFT, that exchanges the value of the vertex register and another register.

To impose locality, we want to restrict the execution of SHIFT only to the edges of G.

Definition 2 *(Shift operation)* Let

$$\text{SHIFT}\colon (x, y) \mapsto \begin{cases} (y, x), & \text{if } (x, y) \in E, \\ (x, y), & \text{otherwise.} \end{cases} \tag{2}$$

In the first case we say that SHIFT *succeeds*, but in the second case it *fails* (we assume that SHIFT always succeeds if $x = y$).

Definition 3 *(Search problems)* Under the restriction that only static transformations and SHIFT are allowed, consider the following problems:

- DETECT(G): Detect if there is a marked vertex in G;
- FIND(G): Find any marked vertex in G, with the promise that $M \neq \emptyset$.

We also define the following variations of the above problems:

- DETECT$^{(k)}$(G): problem DETECT(G) with the promise that either $m = 0$ or $m = k$;
- FIND$^{(k)}$(G): problem FIND(G) with the promise that $m = k$.

Similarly, let DETECT$^{(\geq k)}$(G) and FIND$^{(\geq k)}$(G) denote the corresponding problems with equality $m = k$ replaced by inequality $m \geq k$.

Note that an algorithm for FIND (or its variations) should output a marked element and there are no additional constraints on its output. Our quantum algorithms will solve a slightly stronger version of FIND, which we call SAMPLE- MARKED, where it is necessary to sample marked elements from a specific distribution (see Sect. 2.7).

2.3 Search Via Random Walk

A natural approach to searching on a graph involves using a random walk. Intuitively, a random walk is an alternation of coin flips and shifts. More precisely, a coin is flipped according to the current state $x \in X$ of the vertex register, its value describes the target vertex y, and SHIFT performs a move from x to y. Let P_{xy} be the probability that x is shifted to y. Then SHIFT always succeeds if $P_{xy} = 0$ whenever $(x, y) \notin E$. In such case, we say that $P = (P_{xy})_{x,y \in X}$ is a *Markov chain on graph* G.

From now on, we assume that P is an ergodic Markov chain (see Definition 1). Therefore, by the Perron–Frobenius Theorem, P has a unique stationary distribution π. We also assume that P is reversible: $\pi_x P_{xy} = \pi_y P_{yx}$, for all $x, y \in X$.

To measure the complexity of implementing a random walk corresponding to P, we introduce the following black-box operations:

- `Check`(M): check if a given vertex is marked;
- `Setup`(P): draw a sample from the stationary distribution π of P;
- `Update`(P): perform one step of P.

Each of these black-box operations have the corresponding associated implementation cost, which we denote by C, S, and U, respectively.

2.4 Search Via Quantum Walk

The setup in the quantum case is as follows. As in [19], the evolution takes place in space $\mathcal{H} \otimes \mathcal{H}$ where $\mathcal{H} := \text{span}\{|x\rangle : x \in X\}$ is the n-dimensional complex Euclidean space spanned by elements of set X. The first register stores the current vertex of the walk and is called *vertex register*. We call a unitary transformation *static* if it is controlled by this register, i.e., it is of the form $\sum_{x \in X} |x\rangle\langle x| \otimes U_x$ for some unitaries U_x. The quantum version of the SHIFT operation is obtained by extending the expression in Eq. (2) by linearity.

A *quantum walk* on G is a composition of static unitary transformations and SHIFT. In addition, we require that it respects the local structure of G, i.e., whenever SHIFT is applied to a state, the state must completely lie within the subspace of $\mathcal{H} \otimes \mathcal{H}$ where SHIFT is guaranteed to succeed.

We will only consider quantum walks built from quantum analogues of reversible Markov chains, so we extend the operations `Check`, `Setup`, and `Update` to the quantum setting as follows (we implicitly also allow controlled versions of these operations):

- `Check`(M): map $|x\rangle|b\rangle$ to $|x\rangle|b\rangle$ if $x \notin M$ and $|x\rangle|b \oplus 1\rangle$ if $x \in M$, where $|x\rangle$ is the vertex register and $b \in \{0, 1\}$;
- `Setup`(P): construct the superposition $|\pi\rangle := \sum_{x \in X} \sqrt{\pi_x}|x\rangle$;
- `Update`(P): apply any of $V(P)$, $V(P)^\dagger$, or SHIFT, where $V(P)$ is a unitary operation that satisfies

$$V(P)|x\rangle|\bar{0}\rangle := |x\rangle|p_x\rangle := |x\rangle \sum_{y \in X} \sqrt{P_{xy}}|y\rangle \tag{3}$$

for all $x \in X$ and some fixed reference state $|\bar{0}\rangle \in \mathcal{H}$.

Implicitly, we allow controlled versions of the black-box operations `Check`(M), `Setup`(P), and `Update`(P).

In terms of the number of applications of SHIFT, `Update` has complexity 1 while `Setup` has complexity at least one-half times the diameter of the graph G (this is a lower bound on the mixing time of ergodic Markov chains [23]). Nonetheless, in many algorithmic applications, the situation is more complex and the number of applications of SHIFT is not the only relevant cost; see for instance [1,2].

To define a quantum analogue of a reversible Markov chain P, we follow the construction of Szegedy [10]. Let $\mathcal{X} := \mathcal{H} \otimes \text{span}\{|\bar{0}\rangle\} = \text{span}\{|x\rangle|\bar{0}\rangle : x \in X\}$ and

$$\text{ref}_{\mathcal{X}} := 2 \sum_{x \in X} |x\rangle\langle x| \otimes |\bar{0}\rangle\langle\bar{0}| - I \otimes I = I \otimes (2|\bar{0}\rangle\langle\bar{0}| - I) \tag{4}$$

be the reflection in $\mathcal{H} \otimes \mathcal{H}$ with respect to the subspace $\mathcal{X}$. The *quantum walk operator* corresponding to Markov chain P is[5]

$$W(P) := V(P)^\dagger \cdot \text{SHIFT} \cdot V(P) \cdot \text{ref}_{\mathcal{X}}. \tag{5}$$

Notice that $W(P)$ requires 3 calls to `Update`(P).

Since we always choose an initial state that lies in the subspace $\mathcal{X}$, we can simplify the analysis by restricting the action of $W(P)$ to the smallest subspace that contains $\mathcal{X}$ and is invariant under $W(P)$. We call this subspace the *walk space* of $W(P)$. We show in Appendix B that this subspace is spanned by $\mathcal{X}$ and $W(P)\mathcal{X}$, and that SHIFT is guaranteed to succeed when $W(P)$ is applied to a state in the walk space.

[5] Note that Szegedy [10] uses a different convention and defines the quantum walk operator corresponding to P as $\left(V(P)\, W(P)\, V(P)^\dagger\right)^2$ where $W(P)$ is given in Eq. (5).

2.5 Classical Hitting Time

We define the hitting time of P based on a simple classical random walk algorithm for finding a marked element in the state space X.

Definition 4 Let P be an ergodic Markov chain, and M be a set of marked states. The *hitting time* of P with respect to M, denoted by $\mathrm{HT}(P, M)$, is the expected number of executions of the last step of the **Random Walk Algorithm**, conditioned on the initial vertex being unmarked.

Random Walk Algorithm

1. Generate $x \in X$ according to the stationary distribution π of P using `Setup`(P).
2. Check if x is marked using `Check`(M). If x is marked, output x and exit.
3. Otherwise, update x according to P using `Update`(P) and go back to step 2.

It is straightforward to bound the classical complexity of the DETECT and FIND problems in terms of the hitting time.

Proposition 1 *Let $k \geq 1$.* $\textsc{Detect}^{(\geq k)}(G)$ *can be solved with high probability and classical complexity of order*

$$\mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C}), \quad \textit{where } T = \max_{|M'|=k} \mathrm{HT}(P, M'). \tag{6}$$

$\textsc{Find}(G)$ *can be solved with high probability and expected classical complexity of order*

$$\mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C}), \quad \textit{where } T = \mathrm{HT}(P, M). \tag{7}$$

Note that since the **Random Walk Algorithm** consists in applying the random walk P until hitting a marked vertex, it may be seen as repeated applications of the *absorbing* walk P'.

Definition 5 Let P be an ergodic Markov chain, and M be a set of marked states. The *absorbing* walk P' is the walk obtained from P by replacing all outgoing transitions from marked vertices by self-loops, that is $P'_{xy} = P_{xy}$ for all $x \notin M$, and $P'_{xy} = \delta_{xy}$ for all $x \in M$ (δ_{xy} being the Kronecker delta).

The hitting time $\mathrm{HT}(P, M)$ may be obtained from the spectral properties of the *discriminant matrix* of P', which was introduced by Szegedy in [10].

Definition 6 The *discriminant matrix* $D(P)$ of a Markov chain P is

$$D(P) := \sqrt{P \circ P^{\mathsf{T}}}, \tag{8}$$

where the Hadamard product "$\circ$" and the square root are computed entry-wise.

Proposition 2 *The hitting time of Markov chain P with respect to marked set M is given by*

$$\mathrm{HT}(P, M) = \sum_{k=1}^{n-|M|} \frac{|\langle v'_k|U\rangle|^2}{1-\lambda'_k}, \tag{9}$$

where λ'_k are the eigenvalues of the discriminant matrix $D' = D(P')$ in nondecreasing order, $|v'_k\rangle$ are the corresponding eigenvectors, and $|U\rangle$ is the unit vector

$$|U\rangle := \frac{1}{\sqrt{1-p_M}} \sum_{x\notin M} \sqrt{\pi_x}|x\rangle, \tag{10}$$

p_M being the probability to draw a marked vertex from the stationary distribution π of P.

This proposition is proved in Appendix A.3.

2.6 Quantum Hitting Time

Quantum walks have been successfully used for detecting the presence of marked vertices quadratically faster than random walks [10]. Nonetheless, very little is known about the problem of finding a marked vertex. Below, we describe the understanding of this problem prior to our work.

Theorem 2 ([10]) *Let $k \geq 1$.* $\textsc{Detect}^{(\geq k)}(G)$ *can be solved with high probability and quantum complexity of order*

$$\mathsf{S} + T\cdot(\mathsf{U}+\mathsf{C}), \quad \textit{where} \quad T = \max_{|M'|=k} \sqrt{\mathrm{HT}(P, M')}. \tag{11}$$

When P is state-transitive and there is a unique marked vertex z (i.e., $m = 1$), $\mathrm{HT}(P, \{z\})$ is independent of z and one can also find z:

Theorem 3 ([13,15]) *Assume that P is state-transitive.* $\textsc{Find}^{(1)}(G)$ *can be solved with high probability and quantum complexity of order*

$$\mathsf{S} + T\cdot(\mathsf{U}+\mathsf{C}), \quad \textit{where} \quad T = \sqrt{\mathrm{HT}(P, \{z\})}. \tag{12}$$

Using standard techniques, such as in [5], Theorem 3 can be generalized to any number of marked vertices, with an extra logarithmic multiplicative factor. Nonetheless, the complexities of the corresponding algorithms do not decrease when the size of M increases, contrary to the random walk search algorithm (Prop. 1) and the quantum walk detecting algorithm (Theorem 2).

Corollary 1 *Assume that P is state-transitive.* $\textsc{Find}(G)$ *can be solved with high probability and quantum complexity of order*

$$\log(n)\cdot\big(\mathsf{S} + T\cdot(\mathsf{U}+\mathsf{C})\big), \quad \textit{where} \quad T = \sqrt{\mathrm{HT}(P, \{z\})}, \textit{ for any } z. \tag{13}$$

2.7 Extended Hitting Time

The quantum algorithms leading to the results in the previous subsection are based on quantum analogues of either the Markov chain P or the corresponding absorbing walk P'. However, the algorithms proposed in the present article are based on a quantum analogue of the following *interpolated* Markov chain.

Definition 7 Let P be a Markov chain, M be a set of marked elements and P' be the corresponding absorbing walk. We define the *interpolated* Markov chain $P(s)$ as

$$P(s) := (1-s)P + sP', \quad 0 \leq s \leq 1. \tag{14}$$

We also denote by $D(s)$ the discriminant matrix $D(P(s))$, by $\lambda_k(s)$ its eigenvalues (in nondecreasing order) and by $|v_k(s)\rangle$ its corresponding eigenvectors where $k = 1, \ldots, n$.

Some properties of $P(s)$ are proven in Appendix A.1, in particular, we note that $P(s)$ is ergodic for any $0 \leq s < 1$ as soon as P is (Prop. 7). Moreover, just as $P(s)$ interpolates between P and P', the stationary distribution $\pi(s)$ of $P(s)$ interpolates between the stationary distribution π of P and its restriction to the set of marked vertices, i.e. a stationary distribution for P' (Prop. 11).

This implies that $P(s)$ may be used to solve the following strong version of the FIND problem.

Definition 8 *(Sampling problem)* Let P be an ergodic Markov chain on graph G. Under the restriction that only static transformations and SHIFT are allowed, consider the following problems:

- SAMPLE- MARKED(P): Sample marked vertices in G according to the restriction to set M of the stationary distribution of P, with the promise that $M \neq \emptyset$.
- SAMPLE- MARKED$^{(k)}$(P): problem SAMPLE- MARKED(P) with the promise that $m = k$.

Indeed, since the stationary distribution of $P(s)$ precisely interpolates between π and its restriction to M, we can solve the SAMPLE- MARKED problem by applying Markov chain $P(s)$ for a sufficient number of steps t to approach its stationary distribution, then outputting the current vertex if it is marked, otherwise starting over.

Our new quantum algorithms can be seen as quantum analogues of this classical algorithm, and their cost will be expressed in terms of a quantity which we call the *extended* hitting time.

Definition 9 The *extended hitting time* of P with respect to M is

$$\mathrm{HT}^{+}(P, M) := \lim_{s \to 1} \mathrm{HT}(s), \tag{15}$$

where the *interpolated hitting time* $\mathrm{HT}(s)$ is defined for any $s \in [0, 1)$[6] as

$$\mathrm{HT}(s) := \sum_{k=1}^{n-1} \frac{|\langle v_k(s)|U\rangle|^2}{1-\lambda_k(s)}. \tag{16}$$

The name *extended hitting time* is justified by comparing Eqs. (16) to (9), and noting that $\langle v'_k|U\rangle = 0$ for $k > n - |M|$. In general, the extended hitting time $\mathrm{HT}^+(P, M)$ can be larger than the hitting time $\mathrm{HT}(P, M)$, but they happen to be equal in the case of a single marked element. This implies that when $|M| = 1$, the cost of our quantum algorithms can be expressed in terms of the usual hitting time, which might be attributed to the fact that the SAMPLE- MARKED problem is equivalent to the usual FIND problem in that case.

Proposition 3 *If $|M| = 1$ then $HT^+(P, M) = \mathrm{HT}(P, M)$. However, there exists P and $|M| > 1$ such that $HT^+(P, M) > \mathrm{HT}(P, M)$.*

This proposition is proved in Appendix A.3.1. An alternative expression for $\mathrm{HT}^+(P, M)$ is provided in Appendix C; it allows for an easier comparison with $\mathrm{HT}(P, M)$. The following theorem holds for any number of marked elements and it relates $\mathrm{HT}(s)$ to $\mathrm{HT}^+(P, M)$.

Theorem 4 *For $s < 1$, the interpolated hitting time $\mathrm{HT}(s)$ is related to $HT^+(P, M)$ from Eq. (15) as follows:*

$$\mathrm{HT}(s) = \frac{p_M^2}{(1 - s(1 - p_M))^2} HT^+(P, M) \tag{17}$$

where p_M is the probability to pick a marked state from the stationary distribution π of P. When $|M| = 1$, $HT^+(P, M)$ in Eq. (17) can be replaced by $\mathrm{HT}(P, M)$.

The proof is provided in Appendix A.3.3.

3 Quantum Search Algorithms

In this section we provide several quantum search algorithms. They are all based on a procedure known as *eigenvalue estimation* and essentially run it different numbers of times with different values of parameters. Below is a formal statement of what eigenvalue estimation does. It was discovered by Alexei Kitaev and described in unpublished work (arXiv:quant-ph/9511026, see also [26]).

Theorem 5 (Eigenvalue estimation) *For any unitary operator W and precision $t \in \mathbb{N}$, there exists a quantum circuit **Eigenvalue Estimation**(W, t) that uses 2^t calls to the*

[6] Note that in the case of multiple marked elements this expression cannot be used for $s = 1$, since the numerator and denominator vanish for terms with $k > n - |M|$. We analyze the $s \to 1$ limit in Appendix C.

Table 1 Summary of results on quantum search algorithms

Result	p_M	$\mathrm{HT}^+(P, M)$
Theorem 6	Known	Known
Theorem 7	Approximation known	Known
Theorem 8	Approximation known	Not known
Theorem 9	Bound known	Bound known
Theorem 10	Not known	Bound known

Assumptions on p_M and $\mathrm{HT}^+(P, M)$ are listed in the last two columns

controlled-W operator and $\mathrm{O}(t^2)$ *additional gates, and acts on eigenstates* $|\Psi_k\rangle$ *of* W *as*

$$|\Psi_k\rangle \mapsto |\Psi_k\rangle \frac{1}{2^t} \sum_{l,m=0}^{2^t-1} e^{-\frac{2\pi i l m}{2^t}} e^{i\varphi_k l} |m\rangle, \tag{18}$$

where $e^{i\varphi_k}$ *is the eigenvalue of* W *corresponding to* $|\Psi_k\rangle$.

By linearity, **Eigenvalue Estimation**(W, t) resolves any state as a linear combination of the eigenstates of W and attaches to each term a second register holding an approximation of the first t bits of the binary decomposition of $\frac{1}{2\pi}\varphi_k$, where φ_k is the phase of the corresponding eigenvalue. We will mostly be interested in the component along the eigenvector $|\Psi_n\rangle$ which corresponds to the phase $\varphi_n = 0$. In that case, the second register is in the state $|0^t\rangle$ and the estimation is exact.

Our search algorithms will be based on **Eigenvalue Estimation**$(W(s), t)$ for some values of parameters s and t. Here, $W(s) := W(P(s))$ is the quantum analogue of the interpolated Markov chain $P(s)$, following Szegedy's construction as described in Sect. 2.4 (a quantum circuit implementing $W(s)$ is also provided by Lemma 3 in Appendix B.2). The value of the interpolation parameter $s \in [0, 1]$ will be related to p_M, the probability to pick a marked vertex from the stationary distribution π of P. Precision $t \in \mathbb{N}$, or the number of binary digits in eigenvalue estimation, will be related to $\mathrm{HT}^+(P, M)$, the extended hitting time of P.

We consider several scenarios where different knowledge of the values of parameters p_M and $\mathrm{HT}^+(P, M)$ is available, and for each case we provide an algorithm. The list of all results and the corresponding assumptions is given in Table 1.

Throughout the rest of this section we assume that all eigenvalues of P are between 0 and 1. If this is not the case, we can guarantee it by replacing P with $(P + I)/2$, which makes P "lazy" and affects the hitting time only by a factor of 2 (see Prop. 20).

3.1 Algorithm with Known Values of p_M and $\mathrm{HT}^+(P, M)$

For simplicity, let us first assume that the values of p_M and $\mathrm{HT}^+(P, M)$ are known. In this case we provide a quantum algorithm that solves $\textsc{Find}(G)$ (i.e., outputs a marked vertex if there is any) with success probability and running time that depends on two parameters ε_1 and ε_2.

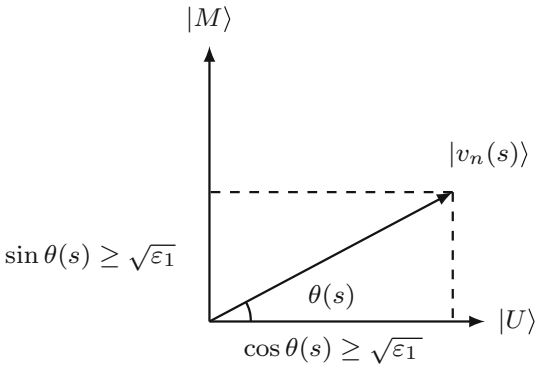

Fig. 3 Vectors $|U\rangle$, $|M\rangle$, and $|v_n(s)\rangle = \cos\theta(s)|U\rangle + \sin\theta(s)|M\rangle$. We want to choose s so that $\langle U|v_n(s)\rangle = \cos\theta(s) \geq \sqrt{\varepsilon_1}$ and $\langle M|v_n(s)\rangle = \sin\theta(s) \geq \sqrt{\varepsilon_1}$

Let us first recall how the classical **Random Walk Algorithm** from Sect. 2.5 works. It starts with the stationary distribution π of P and applies the absorbing walk P' until most of the probability is absorbed in marked vertices and thus the state is close to a stationary distribution of P'.

In the quantum case a natural starting state is $|\pi\rangle|\bar{0}\rangle = |v_n(0)\rangle|\bar{0}\rangle$, which is a stationary state of $W(P)$ (see Eq. (26) below). By analogy, we would like to end up in its projection onto marked vertices, namely $|M\rangle|\bar{0}\rangle$, where

$$|M\rangle := \frac{1}{\sqrt{p_M}} \sum_{x \in M} |x\rangle, \tag{19}$$

which is also a stationary state of $W(P')$. However, at this point the analogy breaks down, since we do not want to apply $W(P')$ to reach the final state. The reason is that in many cases, including the 2D grid, every iteration of $W(P')$ on $|\pi\rangle|\bar{0}\rangle$ may remain far from $|M\rangle|\bar{0}\rangle$. Instead, our approach consists of quantizing a new random walk, namely an interpolation $P(s)$ between P and P'. This technique is drastically different from the approach of [13,15] and, to our knowledge, new.

Intuitively, our quantum algorithm works as follows. We first prepare the initial state $|\pi\rangle$ and check whether the vertex register corresponds to a marked vertex. If so, we are done. If not, we have projected the initial state onto the state $|U\rangle$ from Prop. 2:

$$|U\rangle := \frac{1}{\sqrt{1-p_M}} \sum_{x \notin M} \sqrt{\pi_x}|x\rangle. \tag{20}$$

Now, we fix some value of $s \in [0, 1]$ and map $|U\rangle$ to $|v_n(s)\rangle$ using a quantum walk based on $P(s)$, and then measure $|v_n(s)\rangle$ in the standard basis to get a marked vertex. For this to work with a good probability of success, we have to choose the interpolation parameter s so that $|v_n(s)\rangle$ has a large overlap with both $|U\rangle$ and $|M\rangle$ (see Fig. 3). In that context, the following proposition, proved in Appendix A.2.2, will be useful.

Proposition 4 $|v_n(s)\rangle = \cos\theta(s)|U\rangle + \sin\theta(s)|M\rangle$ *where*

$$\cos\theta(s) = \sqrt{\frac{(1-s)(1-p_M)}{1-s(1-p_M)}}, \qquad \sin\theta(s) = \sqrt{\frac{p_M}{1-s(1-p_M)}}. \tag{21}$$

Therefore, for $|v_n(s)\rangle$ to have a large overlap on both $|U\rangle$ and $|M\rangle$, we will demand that $\cos\theta(s)\sin\theta(s) \geq \varepsilon_1$ for some parameter ε_1. A second parameter ε_2 controls the precision of phase estimation.

Theorem 6 *Assume that the values of* p_M *and* $HT^+(P, M)$ *are known, and let* $s \in [0, 1)$, $T \geq 1$, *and* $\frac{1}{2} \geq \varepsilon_1 \geq \varepsilon_2 \geq 0$ *be some parameters. If*

$$\cos\theta(s)\sin\theta(s) \geq \varepsilon_1 \qquad \text{and} \qquad T \geq \frac{\pi}{\sqrt{2}\varepsilon_2}\sqrt{\mathrm{HT}(s)} \tag{22}$$

where $\cos\theta(s)$ *and* $\sin\theta(s)$ *are defined in Eq.* (21) *and* $\mathrm{HT}(s)$ *is the interpolated hitting time (see Definition 9), then* ***Search***$(P, M, s, \lceil \log T \rceil)$ *(defined below in the proof) solves* FIND(G) *with success probability at least*

$$p_M + (1 - p_M)(\varepsilon_1 - \varepsilon_2)^2 \tag{23}$$

and complexity of order $\mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C})$.

The proof of this theorem relies on the following result, originally due to Szegedy [10], which provides the spectral decomposition of the quantum walk operator $W(s)$ in terms of that of the discriminant matrix $D(s)$. Recall from Definition 7 that $D(s) = \sum_{k=1}^{n} \lambda_k(s)|v_k(s)\rangle\langle v_k(s)|$ is the spectral decomposition of $D(s)$, and define phases $\varphi_k(s) \in [0, \pi]$ such that

$$\lambda_k(s) = \cos\varphi_k(s). \tag{24}$$

Then the walk space of $W(s)$ has the following eigenvalues and eigenvectors:

$$e^{\pm i\varphi_k(s)}, \qquad |\Psi_k^{\pm}(s)\rangle := \frac{|v_k(s), \bar{0}\rangle \pm i|v_k(s), \bar{0}\rangle^{\perp}}{\sqrt{2}} \quad (k = 1, \ldots, n-1), \tag{25}$$

$$1, \qquad |\Psi_n(s)\rangle := |v_n(s), \bar{0}\rangle, \tag{26}$$

where the precise definition of vectors $|v_k(s), \bar{0}\rangle^{\perp}$ is not important (see Appendix B.1 for precise definitions and Lemma 2 for a precise statement and a full proof). We can now prove Theorem 6.

Proof (of Theorem 6) Let $t = \lceil \log T \rceil$ be the precision in the eigenvalue estimation. Our algorithm uses two registers: R_1 and R_2 with underlying state space $\mathcal{H}$ each. Occasionally we will attach the third register R_3 initialized in $|0\rangle \in \mathbb{C}^2$ to check if the current vertex is marked.

Search(P, M, s, t)

1. Use `Setup`(P) to prepare the state $|\pi\rangle|\bar{0}\rangle$.
2. Attach R_3, apply `Check`(M) to $\mathsf{R}_1\mathsf{R}_3$, and measure R_3.
3. If $\mathsf{R}_3 = 1$, measure R_1 (in the vertex basis) and output the outcome.
4. Otherwise, discard R_3 and:
   (a) Apply **Eigenvalue Estimation**$(W(s), t)$ on $\mathsf{R}_1\mathsf{R}_2$.
   (b) Attach R_3, apply `Check`(M) to $\mathsf{R}_1\mathsf{R}_3$, and measure R_3.
   (c) If $\mathsf{R}_3 = 1$, measure R_1 (in the vertex basis) and output the outcome. Otherwise, output: `No marked vertex`.

Notice that step 1 has complexity S, but **Eigenvalue Estimation**$(W(s), t)$ in step 4a has complexity of the order $2^t \cdot (\mathsf{U} + \mathsf{C})$ according to Theorem 5 and Lemma 3. Thus, the total complexity is of the order $\mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C})$, and it only remains to bound the success probability.

Observe that the overall success probability is of the form $p_M + (1 - p_M)q$ where q is the probability to find a marked vertex in step 4. Thus, it remains to show that $q \geq (\varepsilon_1 - \varepsilon_2)^2$.

We assume that **Search**(P, M, s, t) reaches step 4a, otherwise a marked vertex is already found. At this point the state is $|U\rangle|\bar{0}\rangle$. Let us expand the first register of this state in the eigenbasis of the discriminant matrix $D(s)$. From now on we will omit the explicit dependence on s when there is no ambiguity. Let

$$\alpha_k := \langle v_k|U\rangle \tag{27}$$

and observe from Eq. (25) that $|v_k\rangle|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|\Psi_k^+\rangle + |\Psi_k^-\rangle)$. Then

$$|U\rangle|\bar{0}\rangle = \alpha_n|v_n\rangle|\bar{0}\rangle + \sum_{k=1}^{n-1}\alpha_k|v_k\rangle|\bar{0}\rangle = \alpha_n|\Psi_n\rangle + \frac{1}{\sqrt{2}}\sum_{k=1}^{n-1}\alpha_k\big(|\Psi_k^+\rangle + |\Psi_k^-\rangle\big). \tag{28}$$

According to Eqs. (26) and (25), the eigenvalues corresponding to $|\Psi_n\rangle$ and $|\Psi_k^\pm\rangle$ are 1 and $e^{\pm i\varphi_k}$, respectively. From Eq. (18) we see that **Eigenvalue Estimation**$(W(s), t)$ in step 4a acts as follows:

$$|\Psi_n\rangle \mapsto |\Psi_n\rangle|0^t\rangle, \tag{29}$$

$$|\Psi_k^\pm\rangle \mapsto |\Psi_k^\pm\rangle|\xi_k^\pm\rangle, \tag{30}$$

where $|\xi_k^\pm\rangle$ is a t-qubit state that satisfies

$$\langle 0^t|\xi_k^\pm\rangle = \frac{1}{2^t}\sum_{l=0}^{2^t-1} e^{\pm i\varphi_k l} =: \delta_k^\pm. \tag{31}$$

Thus, the state after eigenvalue estimation lies in $\mathcal{H} \otimes \mathcal{H} \otimes \mathbb{C}^{2^t}$ and is equal to

$$|\Phi\rangle := \alpha_n |\Psi_n\rangle|0^t\rangle + \frac{1}{\sqrt{2}} \sum_{k=1}^{n-1} \alpha_k \big(|\Psi_k^+\rangle|\xi_k^+\rangle + |\Psi_k^-\rangle|\xi_k^-\rangle\big). \tag{32}$$

Recall that q denotes the probability to obtain a marked vertex by measuring the first register of $|\Phi\rangle$ in step 4c. To lower bound q, we require that the last register of $|\Phi\rangle$ is in the state $|0^t\rangle$ (i.e., the phase is estimated to be 0). Then

$$\begin{aligned}
\sqrt{q} &= \|(\Pi_M \otimes I \otimes I)|\Phi\rangle\| && (33)\\
&\geq \|(\Pi_M \otimes I \otimes |0^t\rangle\langle 0^t|)|\Phi\rangle\| && (34)\\
&\geq \|\alpha_n(\Pi_M \otimes I)|\Psi_n\rangle\| - \frac{1}{\sqrt{2}} \left\| (\Pi_M \otimes I) \sum_{k=1}^{n-1} \alpha_k \big(\delta_k^+ |\Psi_k^+\rangle + \delta_k^- |\Psi_k^-\rangle\big) \right\| && (35)\\
&\geq \|\alpha_n(\Pi_M \otimes I)|\Psi_n\rangle\| - \frac{1}{\sqrt{2}} \left\| \sum_{k=1}^{n-1} \alpha_k \big(\delta_k^+ |\Psi_k^+\rangle + \delta_k^- |\Psi_k^-\rangle\big) \right\|. && (36)
\end{aligned}$$

From Eq. (26) and Prop. 4 we know that $|\Psi_n\rangle = |v_n\rangle|\bar{0}\rangle = (\cos\theta|U\rangle + \sin\theta|M\rangle)|\bar{0}\rangle$. Hence, we find that

$$\alpha_n = \langle v_n|U\rangle = \cos\theta \tag{37}$$

and $\|(\Pi_M \otimes I)|\Psi_n\rangle\| = \sin\theta$. Moreover, from Eq. (25) we know that vectors $|\Psi_1^\pm\rangle, \ldots, |\Psi_k^\pm\rangle$ are mutually orthogonal. We use this to simplify Eq. (36):

$$\sqrt{q} \geq \cos\theta \sin\theta - \sqrt{\sum_{k=1}^{n-1} |\alpha_k|^2 \delta_k^2} \tag{38}$$

where $\delta_k := |\delta_k^+| = |\delta_k^-|$ (note from Eq. (31) that δ_k^+ and δ_k^- are complex conjugates). Now we will bound the second term in Eq. (38).

Let us compute the sum of the geometric series in Eq. (31):

$$\delta_k^2 = \left| \frac{1}{2^t} \sum_{l=0}^{2^t-1} e^{i\varphi_k l} \right|^2 = \frac{1}{2^{2t}} \left| \frac{1 - e^{i\varphi_k 2^t}}{1 - e^{i\varphi_k}} \right|^2 = \frac{1}{2^{2t}} \left| \frac{e^{-i\frac{\varphi_k}{2}2^t} - e^{i\frac{\varphi_k}{2}2^t}}{e^{-i\frac{\varphi_k}{2}} - e^{i\frac{\varphi_k}{2}}} \right|^2. \tag{39}$$

The imaginary parts cancel out and we get

$$\delta_k^2 = \frac{\sin^2\left(\frac{\varphi_k}{2}2^t\right)}{2^{2t}\sin^2\left(\frac{\varphi_k}{2}\right)}. \tag{40}$$

We can upper bound the numerator in this expression by one. To bound the denominator, we use $\sin\frac{x}{2} \geq \frac{x}{\pi}$ for $x \in [0, \pi]$. Hence, we get

$$\delta_k^2 \leq \frac{\pi^2}{2^{2t}\varphi_k^2} \leq \frac{\pi^2}{T^2\varphi_k^2} \tag{41}$$

since we chose $t = \lceil \log T \rceil$.

The interpolated hitting time is given by Definition 9:

$$\mathrm{HT}(s) = \sum_{k=1}^{n-1} \frac{|\langle v_k(s)|U\rangle|^2}{1-\lambda_k(s)}. \tag{42}$$

If we substitute $\langle v_k(s)|U\rangle = \alpha_k(s)$ and $\lambda_k(s) = \cos\varphi_k(s)$ from Eqs. (31) and (24), and omit the dependence on s, we get

$$\mathrm{HT}(s) = \sum_{k=1}^{n-1} \frac{|\alpha_k|^2}{1-\cos\varphi_k} = \sum_{k=1}^{n-1} \frac{|\alpha_k|^2}{2\sin^2(\frac{\varphi_k}{2})} \geq 2\sum_{k=1}^{n-1} \frac{|\alpha_k|^2}{\varphi_k^2} \tag{43}$$

since $x \geq \sin x$ for $x \in [0, \pi]$.

By combining Eqs. (41) and (43) we get

$$\sum_{k=1}^{n-1} |\alpha_k|^2 \delta_k^2 \leq \sum_{k=1}^{n-1} |\alpha_k|^2 \frac{\pi^2}{T^2\varphi_k^2} = \frac{\pi^2}{T^2} \sum_{k=1}^{n-1} \frac{|\alpha_k|^2}{\varphi_k^2} \leq \frac{\pi^2}{2} \frac{\mathrm{HT}(s)}{T^2}. \tag{44}$$

Thus, Eq. (38) becomes

$$\sqrt{q} \geq \cos\theta(s)\sin\theta(s) - \frac{\pi}{\sqrt{2}} \frac{\sqrt{\mathrm{HT}(s)}}{T} \geq \varepsilon_1 - \varepsilon_2, \tag{45}$$

where the last inequality follows from our assumptions. Thus $q \geq (\varepsilon_1 - \varepsilon_2)^2$, which was required to complete the proof. □

3.2 Algorithms with Approximately Known p_M

In this section we show that a good approximation p^* of p_M suffices to guarantee that the constraint $\cos\theta(s)\sin\theta(s) \geq \varepsilon_1$ in Theorem 6 is satisfied. Our strategy is to make a specific choice of the interpolation parameter s, based on p^*.

Intuitively, we want to choose s so that $\cos\theta(s)\sin\theta(s)$ is large (recall Fig. 3), since this will increase the success probability according to Eq. (45), and make it easier to satisfy the constraint on ε_1 in Theorem 6. The maximal value of $\cos\theta(s)\sin\theta(s)$ is achieved when $\sin\theta(s) = \cos\theta(s) = 1/\sqrt{2}$, and from Eq. (21) we get that the optimal value of s as a function of p_M is

$$s(p_M) := 1 - \frac{p_M}{1-p_M}. \tag{46}$$

Thus, when only an approximation p^* of p_M is known, we will choose the interpolation parameter to be

$$s^* := s(p^*) = 1 - \frac{p^*}{1 - p^*}. \tag{47}$$

If we substitute this in Eq. (21), we get the following expressions for $\cos\theta(s^*)$ and $\sin\theta(s^*)$ in terms of p_M and p^*:

$$\cos\theta(s^*) = \sqrt{\frac{(1-p_M)p^*}{p_M + p^* - 2p_M p^*}}, \quad \sin\theta(s^*) = \sqrt{\frac{p_M(1-p^*)}{p_M + p^* - 2p_M p^*}}. \tag{48}$$

Since we want $s^* \geq 0$, we have to always make sure that $p^* \leq 1/2$. In fact, from now we will also assume that $p_M \leq 1/2$. This is without loss of generality, since one can always prepare the initial state $|\pi\rangle$ at cost S and measure it in the standard basis. If $p_M \geq 1/2$, this yields a marked vertex with probability at least $1/2$.

Proposition 5 *If $p_M, \varepsilon_1 \in [0, \frac{1}{2}]$ and p^* satisfy*

$$2\varepsilon_1 p_M \leq p^* \leq 2(1-\varepsilon_1)p_M, \tag{49}$$

then $\cos\theta(s^*)\sin\theta(s^*) \geq \varepsilon_1$ where $s^* := 1 - \frac{p^*}{1-p^*}$.

Proof To get the desired result, we will show that the two inequalities in Eq. (49) imply that $\cos^2\theta(s^*) \geq \varepsilon_1$ and $\sin^2\theta(s^*) \geq \varepsilon_1$, respectively.

From Eq. (48), we have $\sin^2\theta(s^*) \geq \varepsilon_1$ if and only if

$$p^* \leq \frac{(1-\varepsilon_1)p_M}{\varepsilon_1 + p_M - 2\varepsilon_1 p_M}. \tag{50}$$

Since $p_M, \varepsilon_1 \leq 1/2$, the denominator is upper bounded as

$$\varepsilon_1 + (1-2\varepsilon_1)p_M \leq \varepsilon_1 + \frac{1-2\varepsilon_1}{2} = \frac{1}{2}. \tag{51}$$

Therefore, $p^* \leq 2(1-\varepsilon_1)p_M$ implies Eq. (50), which in turn is equivalent to $\sin^2\theta(s^*) \geq \varepsilon_1$.

Similarly from Eq. (48) we have $\cos^2\theta(s^*) \geq \varepsilon_1$ if and only if

$$p^* \geq \frac{\varepsilon_1 p_M}{1 - \varepsilon_1 - p_M + 2\varepsilon_1 p_M}, \tag{52}$$

where the denominator is lower bounded as

$$1 - \varepsilon_1 - (1-2\varepsilon_1)p_M \geq 1 - \varepsilon_1 - \frac{1-2\varepsilon_1}{2} = \frac{1}{2}. \tag{53}$$

Therefore, $p^* \geq 2\varepsilon_1 p_M$ implies Eq. (52), which in turn is equivalent to the second desired inequality, namely $\cos^2\theta(s^*) \geq \varepsilon_1$. □

3.2.1 Known $HT^+(P, M)$

Now we will use Prop. 5 to show how an approximation p^* of p_M can be used to make a specific choice of the parameters ε_1, ε_2, s, and T in Theorem 6, so that our quantum search algorithm succeeds with constant probability.

To be more specific, we assume that we have an approximation p^* of p_M such that

$$|p^* - p_M| \leq \frac{1}{3} p_M, \tag{54}$$

where the constant $1/3$ is an arbitrary choice. Notice that

$$\frac{1}{3} p_M \geq p^* - p_M \quad \Longleftrightarrow \quad \frac{4}{3} p_M \geq p^*, \tag{55}$$

$$\frac{1}{3} p_M \geq p_M - p^* \quad \Longleftrightarrow \quad p^* \geq \frac{2}{3} p_M, \tag{56}$$

so Eq. (54) is equivalent to

$$\frac{2}{3} p_M \leq p^* \leq \frac{4}{3} p_M. \tag{57}$$

If we are given such p^* and we choose s^* according to Eq. (47), then our algorithm succeeds with constant probability if T is sufficiently large.

Theorem 7 *Assume that we know the value of $HT^+(P, M)$ and an approximation p^* of p_M such that $|p^* - p_M| \leq p_M/3$. If $T \geq 14\sqrt{HT^+(P, M)}$ then **Search**$(P, M, s^*, \lceil \log T \rceil)$ solves* FIND(G) *with probability at least* $1/36$ *and complexity of order* $\mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C})$.

Proof We are given p^* that satisfies Eq. (57). This is equivalent to Eq. (49) if we choose $\varepsilon_1 := 1/3$. Without loss of generality $p_M \leq 1/2$, so from Prop. 5 we get that $\cos\theta(s^*) \sin\theta(s^*) \geq \varepsilon_1$. Thus, the first condition in Eq. (22) of Theorem 6 is satisfied.

Next, we choose $\varepsilon_2 := 1/6$ somewhat arbitrarily. According to Theorem 4, $\mathrm{HT}(s^*) \leq \mathrm{HT}^+(P, M)$. Thus

$$\frac{\pi}{\sqrt{2}} \frac{1}{\varepsilon_2} \sqrt{\mathrm{HT}(s^*)} \leq \pi\, 3\sqrt{2} \sqrt{\mathrm{HT}^+(P, M)} \leq 14 \sqrt{\mathrm{HT}^+(P, M)} \leq T, \tag{58}$$

so the second condition in Eq. (22) is also satisfied.

Hence, according to Theorem 6, **Search**$(P, M, s^*, \lceil \log T \rceil)$ solves FIND(G) with success probability at least

$$p_M + (1 - p_M)(\varepsilon_1 - \varepsilon_2)^2 \geq (\varepsilon_1 - \varepsilon_2)^2 = \left(\frac{1}{3} - \frac{1}{6}\right)^2 = \frac{1}{36} \tag{59}$$

and complexity of order $\mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C})$. □

3.2.2 Unknown $HT^+(P, M)$

Recall from Theorem 7 in previous section that a marked vertex can be found if p^*, an approximation of p_M, and $\mathrm{HT}^+(P, M)$ are known. In this section we show that a marked vertex can still be found (with essentially the same expected complexity), even if the requirement that $\mathrm{HT}^+(P, M)$ be known is relaxed.

Theorem 8 *Assume that we are given p^* such that $|p^* - p_M| \leq p_M/3$, then* ***Incremental Search***$(P, M, s^*, 50)$ *solves* FIND(G) *with expected quantum complexity of order*

$$\log(T) \cdot \mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C}), \quad \textit{where} \quad T = \sqrt{HT^+(P, M)}. \tag{60}$$

Proof The idea is to repeatedly use **Search**(P, M, s^*, t) with increasing accuracy of the eigenvalue estimation. We start with $t = 1$ and in every iteration increase it by one. Once t is above some threshold t_0, any subsequent iteration outputs a marked element with probability that is at least a certain constant. To boost the success probability of the **Search**(P, M, s^*, t) subroutine, for each value of t we call it $k = 50$ times.

Incremental Search(P, M, s^*, k)

1. Let $t = 1$.
2. Call k times **Search**(P, M, s^*, t).
3. If no marked vertex is found, set $t \leftarrow t + 1$ and go back to step 2.

Let t_0 be the smallest integer that satisfies

$$14\sqrt{\mathrm{HT}^+(P, M)} \leq 2^{t_0}. \tag{61}$$

Assume that variable t has reached value $t \geq t_0$, but the execution of **Incremental Search**$(P, M, s^*, 50)$ has not terminated yet. By Theorem 7, each execution of **Search**(P, M, s^*, t) outputs a marked vertex with probability at least $1/36$. Let p_{fail} be the probability that none of the $k = 50$ executions in step 2 succeeds. Notice that

$$p_{\mathrm{fail}} \leq (1 - 1/36)^{50} \leq 1/4. \tag{62}$$

Let us assume that **Incremental Search**$(P, M, s^*, 50)$ terminates with the final value of t equal to t_f. Recall from Theorem 6 that **Search**(P, M, s^*, t) has complexity of order $\mathsf{S} + 2^t \cdot (\mathsf{U} + \mathsf{C})$, so the expected complexity of **Incremental Search**$(P, M, s^*, 50)$ is of order

$$N_1 \cdot \mathsf{S} + N_2 \cdot (\mathsf{U} + \mathsf{C}), \tag{63}$$

where N_1 is the expectation of t_f, and N_2 is the expectation of $2 + 4 + \cdots + 2^{t_f}$.

To upper bound N_1, we assume that the first $t_0 - 1$ iterations fail. Since each of the remaining iterations fails with probability at most p_{fail}, we get

$$N_1 \le (t_0 - 1) + \sum_{t=t_0}^{\infty} p_{\text{fail}}^{1+(t-t_0)} \tag{64}$$

$$= (t_0 - 1) + \frac{p_{\text{fail}}}{1 - p_{\text{fail}}} \tag{65}$$

$$\le (t_0 - 1) + \frac{1/4}{3/4} \tag{66}$$

$$\le t_0. \tag{67}$$

We use the same strategy to upper bound N_2:

$$N_2 \le \sum_{t=1}^{t_0-1} 2^t + \sum_{t=t_0}^{\infty} p_{\text{fail}}^{1+(t-t_0)} 2^t \tag{68}$$

$$= (2^{t_0} - 2) + p_{\text{fail}} \cdot \sum_{t=0}^{\infty} p_{\text{fail}}^{t} 2^{t+t_0} \tag{69}$$

$$\le (2^{t_0} - 2) + \frac{1}{4} \cdot \sum_{t=0}^{\infty} \left(\frac{1}{4} \cdot 2\right)^t \cdot 2^{t_0} \tag{70}$$

$$= (2^{t_0} - 2) + \frac{1}{4} \cdot 2 \cdot 2^{t_0} \tag{71}$$

$$\le 2 \cdot 2^{t_0}. \tag{72}$$

We plug the bounds on N_1 and N_2 in Eq. (63) and get that the expected complexity is of order $t_0 \cdot \mathsf{S} + 2^{t_0+1} \cdot (\mathsf{U} + \mathsf{C})$. Since t_0 satisfies Eq. (61), this concludes the proof. □

3.3 Algorithms with a Given Bound on p_M or $\text{HT}^+(P, M)$

In previous section, we considered the case when we know a *relative* approximation of p_M, i.e., a value p^* such that $|p^* - p_M| \le p_M/3$. In this section, we consider the case when we are given an *absolute* lower bound $p_{\min}$ such that $p_{\min} \le p_M$, or an *absolute* upper bound $\text{HT}_{\max} \ge \text{HT}^+(P, M)$, or both. In particular, for problem $\text{FIND}(G)^{(\ge k)}$ we can set $p_{\min} := \min_{M':|M'|=k} p_{M'}$ and $\text{HT}_{\max} := \max_{M':|M'|\ge k} \text{HT}^+(P, M')$.

3.3.1 Assuming a Bound on p_M

Theorem 9 *Given $p_{\min}$ such that $p_{\min} \le p_M$, $\text{FIND}(G)$ can be solved with expected quantum complexity of order*

$$\sqrt{\log(1/p_{\min})} \cdot \left[\log(T) \cdot \mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C})\right], \quad \textit{where} \quad T = \sqrt{HT^+(P, M)}. \tag{73}$$

Moreover, given $\mathrm{HT}_{\max}$ *such that* $\mathrm{HT}_{\max} \geq HT^+(P, M)$*, we can solve* FIND$(G)$ *with quantum complexity of order*

$$\sqrt{\log(1/p_{\min})} \cdot \left[\mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C})\right], \quad \textit{where} \quad T = \sqrt{\mathrm{HT}_{\max}}. \tag{74}$$

Proof We prove only the first part; the second part is similar except one has to use **Search**(P, M, s^*, T) instead of **Incremental Search**$(P, M, s^*, 50)$.

To apply Theorem 8, it is enough to obtain an approximation p^* of p_M such that $|p^* - p_M| \leq p_M/3$. Recall from Eq. (57) that this is equivalent to finding p^* such that

$$\frac{2}{3} p_M \leq p^* \leq \frac{4}{3} p_M. \tag{75}$$

Let l be the largest integer such that $p_M \leq 2^{-l}$. Then

$$\frac{1}{2} \cdot 2^{-l} \leq p_M \leq 2^{-l} \tag{76}$$

and hence

$$\frac{2}{3} p_M \leq \frac{2}{3} \cdot 2^{-l} = \frac{4}{3} \cdot \left(\frac{1}{2} \cdot 2^{-l}\right) \leq \frac{4}{3} p_M. \tag{77}$$

We can make sure that Eq. (75) is satisfied by choosing $p^* := \frac{2}{3} \cdot 2^{-l}$. Unfortunately, we do not know the value of l. However, we know that $p_{\min} \leq p_M$ and without loss of generality we can assume that $p_M \leq 1/2$. Thus, it only suffices to check all values of l from 1 to $\lfloor \log(1/p_{\min}) \rfloor$.

To find a marked vertex, we replace step 2 in the **Incremental Search** algorithm by a loop over the $\lfloor \log(1/p_{\min}) \rfloor$ possible values of p^*:

For $l = 1$ to $\lfloor \log(1/p_{\min}) \rfloor$ do:

- Let $p^* := \frac{2}{3} \cdot 2^{-l}$.
- Call k times **Search**$(P, M, s(p^*), t)$.

Recall from Theorem 6 that the complexity of **Search**(P, M, s^*, t) depends only on t. Hence, the analysis of the modified algorithm is the same, except that now the complexity of step 2 is multiplied by a factor of order $\log(1/p_{\min})$. In fact, this is the only non-trivial step of the **Incremental Search** algorithm, so the overall complexity increases by this multiplicative factor. Finally, note that instead of trying all possible values of p^*, we can search for the right value using Grover's algorithm, following the approach of [27], therefore reducing the multiplicative factor to $\sqrt{\log(1/p_{\min})}$. □

3.3.2 Assuming a Bound on $HT^+(P, M)$

Theorem 10 *Given* $\mathrm{HT}_{\max}$ *such that* $\mathrm{HT}_{\max} \geq HT^+(P, M)$*,* FIND$(G)$ *can be solved with expected quantum complexity of order*

$$\log(1/p_M) \cdot \left[\mathsf{S} + T \cdot (\mathsf{U} + \mathsf{C})\right], \quad \textit{where} \quad T = \sqrt{\mathrm{HT}_{\max}}. \tag{78}$$

The proof of this theorem relies on the following procedure, which tests a candidate value p^* for p_M and, in case it fails, concludes that this candidate value was either too high or too low.

Test(P, M, p^*, t)

1. Call 300 times **Search**$(P, M, s(p^*), t)$;
   if a marked vertex is found, output it and stop.
2. Measure the last register of all 300 output states produced by **Eigenvalue Estimation**$(W(s(p^*)), t)$ within the **Search** subroutine above;
   if a minority of 0^ts is found, then output "$p^* \leq 2p_M/3$", else output "$p^* \geq 4p_M/3$".

The above procedure will be used to "query" the value of p_M. However, rather than finding the precise value of p_M, we only care about establishing that $2p_M/3 \leq p^* \leq 4p_M/3$. Whenever p^* is in this range, the first step of **Test**$(P, M, s(p^*), t)$ will succeed with probability at least $99/100$ for appropriately chosen value of t. If it fails, then with high probability it is because p^* is not within $2p_M/3$ and $4p_M/3$. One can decide which of the two cases it is by measuring the last register of the output state of **Search**$(P, M, s(p^*), t)$, which stores the value of the phase computed by the phase estimation subroutine. Indeed, if it turns out that $p^* \geq 4p_M/3$, then this register will be in the state $|0^t\rangle$ with high probability. On the other hand, if $p^* \leq 2p_M/3$, then it will be in the state $|0^t\rangle$ with low probability.

Proposition 6 *For* $t := \lceil \log(14\sqrt{\mathrm{HT}_{\max}}) \rceil$, *the procedure* ***Test***(P, M, p^*, t) *runs in time of order* $\mathsf{S} + \sqrt{\mathrm{HT}_{\max}} \cdot (\mathsf{U} + \mathsf{C})$ *and produces the following output:*

- *If* $2p_M/3 \leq p^* \leq 4p_M/3$, *then with probability at least* $99/100$ *the output is a marked element.*
- *If* $p^* \leq 2p_M/3$, *then with probability at least* $2/3$ *the output is either a marked element or "*$p^* \leq 2p_M/3$*".*
- *If* $p^* \geq 4p_M/3$, *then with probability at least* $2/3$ *the output is either a marked element or "*$p^* \geq 4p_M/3$*".*

Proof From Theorem 7, the procedure **Search**$(P, M, s(p^*), t)$ has a cost of order $\mathsf{S} + \sqrt{\mathrm{HT}_{\max}} \cdot (\mathsf{U} + \mathsf{C})$, hence repeating it 300 times yields an overall cost of the same order.

When $2p_M/3 \leq p^* \leq 4p_M/3$, Theorem 7 also implies that the procedure **Search**$(P, M, s(p^*), t)$ outputs a marked element with probability at least $1/36$. Since this is repeated 300 times, we conclude that the test procedure outputs a marked element with probability at least $1 - (1 - 1/36)^{300} \geq 99/100$.

For the two other cases, let us first recall the main steps of the procedure **Search**$(P, M, s(p^*), t)$. We prepare the initial state $|\pi\rangle$, and then check wether the vertex register is marked. This either yields a marked vertex with probability p_M, or projects onto the state $|U\rangle$. We then apply **Eigenvalue Estimation**$(W(s(p^*)), t)$ on this state, which prepares the state $|\Phi\rangle$ given by Eq. (32). We finally check whether

the first register of this output state is marked, which happens with probability

$$p_1 := \left\| \left(\Pi_M \otimes I \otimes I\right) |\Phi\rangle \right\|^2 . \tag{79}$$

Overall, the probability to obtain a marked vertex from one execution of **Search** $(P, M, s(p^*), t)$ is then given by

$$p_1' := p_M + (1 - p_M) \cdot p_1 \geq p_1 \tag{80}$$

Let us note that p_1 depends on p^*. We first consider the case where $p_1 > 0.004$. In that case, the 300 repetitions of **Search**$(P, M, s(p^*), t)$ in the procedure **Test**(P, M, p^*, t) will output at least one marked vertex with probability

$$1 - (1 - p_1')^{300} \geq 1 - (1 - p_1)^{300} \geq 2/3, \tag{81}$$

which is sufficient for the last two cases of the proposition.

It then remains to analyze the case where $p_1 \leq 0.004$. We show that if none of the 300 repetitions of **Search**$(P, M, s(p^*), t)$ find a marked vertex, measuring the last register of the output states yields with probability at least $2/3$ either a minority of 0^t's (when $p^* \leq 2p_M/3$) or a majority of 0^t's (when $p^* \geq 4p_M/3$).

When the procedure **Search**$(P, M, s(p^*), t)$ does not find a marked vertex, its output state is

$$\frac{\left((I - \Pi_M) \otimes I \otimes I\right) |\Phi\rangle}{\sqrt{1 - p_1}}. \tag{82}$$

Therefore, the probability that the last register of this state is found in state 0^t is

$$q_1 := \frac{\left\| \left((I - \Pi_M) \otimes I \otimes |0^t\rangle\langle 0^t|\right) |\Phi\rangle \right\|^2}{1 - p_1}. \tag{83}$$

Defining

$$q_1' := \left\| \left(I \otimes I \otimes |0^t\rangle\langle 0^t|\right) |\Phi\rangle \right\|^2 , \tag{84}$$

we can bound the numerator in Eq. (83) as

$$q_1' - p_1 \leq \left\| \left((I - \Pi_M) \otimes I \otimes |0^t\rangle\langle 0^t|\right) |\Phi\rangle \right\|^2 \leq q_1' \tag{85}$$

and in turn q_1 itself as

$$q_1' - p_1 \leq q_1 \leq \frac{q_1'}{1 - p_1}. \tag{86}$$

Recall that we have assumed that $p_1 \leq 0.004$. It remains to compute q_1'. From Eq. (32), we have

$$q_1' = \|(I \otimes I \otimes |0^t\rangle\langle 0^t|)|\Phi\rangle\|^2 \tag{87}$$

$$= \left\| \alpha_n |\Psi_n\rangle + \frac{1}{\sqrt{2}} \sum_{k=1}^{n-1} \alpha_k \left(\delta_k^+ |\Psi_k^+\rangle + \delta_k^- |\Psi_k^-\rangle\right) \right\|^2 \tag{88}$$

$$= \alpha_n^2 + \sum_{k=1}^{n-1} |\alpha_k|^2 \delta_k^2. \tag{89}$$

Recall from Eq. (37) that $\alpha_n = \langle v_n(s^*)|U\rangle = \cos\theta(s^*)$. Using Eq. (44) and our choice of $t = \lceil \log T \rceil$ where $T := 14\sqrt{\mathrm{HT}_{\max}}$, we can bound the remaining terms in Eq. (87) as follows:

$$\sum_{k=1}^{n-1} |\alpha_k|^2 \delta_k^2 \leq \frac{\pi^2}{2} \frac{\mathrm{HT}(s^*)}{T^2} \leq \frac{\pi^2}{2} \frac{\mathrm{HT}(s^*)}{(14\sqrt{\mathrm{HT}_{\max}})^2} \leq \frac{\pi^2}{2 \cdot 14^2} \leq \frac{1}{36}, \tag{90}$$

where we relied on $\mathrm{HT}_{\max} \geq \mathrm{HT}^+(P, M) \geq \mathrm{HT}(s^*)$ (see Theorem 4). This and Eq. (87) gives the following bounds on q_1':

$$\cos^2\theta(s^*) \leq q_1' \leq \cos^2\theta(s^*) + \frac{1}{36}. \tag{91}$$

Recall from Eq. (48) that

$$\cos^2\theta(s^*) = \frac{1 - p_M}{\frac{p_M}{p^*} + 1 - 2p_M}. \tag{92}$$

Let us now consider the case $p^* \leq 2p_M/3$. Plugging $\frac{p_M}{p^*} \geq \frac{3}{2}$ into the last equation, we find the bound

$$\cos^2\theta(s^*) \leq \frac{1 - p_M}{\frac{5}{2} - 2p_M} \leq \frac{2}{5}. \tag{93}$$

Combining this bound with Eqs. (91) and (86), we obtain that the probability of observing the last register of the output state of an unsuccessful application of **Search**$(P, M, s(p^*), t)$ in the state 0^t is bounded as

$$q_1 \leq \frac{\cos^2\theta(s^*) + \frac{1}{36}}{1 - p_1} \leq \frac{\frac{2}{5} + \frac{1}{36}}{1 - 0.004} \leq 0.4295. \tag{94}$$

It remains to bound the probability to obtain a minority of 0^t's for 300 repetitions of this measurement.

According to the Chernoff bound, if an experiment produces a desirable outcome with probability at least $q > 1/2$, then for k independent repetitions of the experiment

a majority of outcomes are desirable with probability at least $1 - e^{-\frac{k}{2q}(q-\frac{1}{2})^2}$. In this case, the desirable outcome is to not obtain 0^t, hence we have $q := 1 - q_1 \geq 0.570$, and for $k = 300$, the expression is indeed larger than $2/3$.

For the final case $p^* \geq 4p_M/3$, we obtain from Eq. (92) that

$$\cos^2 \theta(s^*) \geq \frac{1 - p_M}{\frac{7}{4} - 2p_M} \geq \frac{4}{7} \tag{95}$$

(recall that we can always assume $p_M \leq 1/2$ as explained in the beginning of Sect. 3.2). Together with Eqs. (91) and (86), we obtain the bound

$$q_1 \geq \cos^2 \theta(s^*) - p_1 \geq \frac{4}{7} - 0.004 \geq 0.567. \tag{96}$$

In this case the desirable outcome for the Chernoff bound is precisely 0^t, which happens with probability $q := q_1$, so after 300 repetitions we obtain a majority of 0^t's with probability at least $2/3$. □

We are now ready to prove Theorem 10.

Proof (of Theorem 10) The general idea is to use **Search**$(P, M, s(p^*), t)$ with $t := \lceil \log(14\sqrt{\mathrm{HT}_{\max}}) \rceil$ and perform a dichotomic search for an appropriately chosen value of p^*, using the procedure **Test**(P, M, p^*, t). This dichotomic search uses backtracking, since the branching in the dichotomy is with bounded error, similar to the situation in [28].

Let us first describe the robust binary search of [28]. Let $x \neq 0^n$ be an n-bit string of 0's followed by some 1's. An algorithm can only access x by querying its bits as follows: the answer to a query $i \in \{1, \ldots, n\}$ is a random and independent bit which takes value x_i with probability at least $2/3$.

When there is no error, finding the largest i such that $x_i = 0$ can be done using the usual binary search. Start with $a = 1$ and $b = n$. At each step, query x_i with $i = \lceil (a + b)/2 \rceil$. Then set $a = i$ if $x_i = 0$, and $b = i$ otherwise. The procedure stops when $a + 1 = b$, which happens after $\Theta(\log n)$ steps.

In our error model, the above algorithm can be made robust by adding a sanity check. Before querying x_i, bits x_a and x_b are also queried. If one of the two answers is inconsistent (i.e., $x_a = 1$ or $x_b = 0$), the algorithm backtracks to the previous values of a and b. It is proven in [28] that this procedure converges with expected time $\Theta(\log n)$ and outputs a correct value with high probability, say at least $2/3$.

For our problem, we conduct a search similar to the one in [28], starting with $a = 0$ and $b = 1$. The only difference is that the search stops when a marked element is found. At each step, we check the consistency of a and b by running **Test**(P, M, a, t) and **Test**(P, M, b, t). If there is a contradiction, we backtrack to the previous values of a and b. Otherwise we conduct the dichotomy search by running **Test**(P, M, p^*, t) with $p^* = (a + b)/2$ (in order to set either $a = p^*$ or $b = p^*$). The search stops when a marked element is found.

Our procedure behaves similar to the one in [28]. Indeed, it follows from Prop. 6 that our algorithm converges even faster since it stops with probability at least $99/100$ when

$p^* \in [2p_M/3, 4p_M/3]$. Therefore it ends after $O(\log(1/p_M))$ expected iterations of **Test**. Taking into account the cost of **Test**(P, M, p^*, t), we see that the total number of steps is as stated in the theorem. □

Acknowledgments MO would like to acknowledge Andrew Childs for many helpful discussions. The authors would also like to thank Andris Ambainis for useful comments. Part of this work was done while HK, MO, and JR were at NEC Laboratories America in Princeton. MO also was affiliated with University of Waterloo and Institute for Quantum Computing (supported by QuantumWorks) and IBM TJ Watson Research Center (supported by DARPA QUEST program under Contract No. HR0011-09-C-0047) during this project. Presently FM, MO and JR are supported by the European Union Seventh Framework Programme (FP7/2007-2013) under Grant Agreement No. 600700 (QALGO). FM is also supported by the French ANR Blanc project ANR-12-BS02-005 (RDAM). Last, JR acknowledges support from the Belgian ARC project COPHYMA.

Appendix A: Semi-Absorbing Markov Chains

In this appendix we study a special type of Markov chains described by a one-parameter family $P(s)$ corresponding to convex combinations of P and the associated absorbing chain P'. Intuitively, some states of $P(s)$ are hard to escape and the interpolation parameter s controls how absorbing they are. For this reason we call such chains *semi-absorbing*. In this appendix we consider various properties of semi-absorbing Markov chains as a function of the interpolation parameter s. The main result of this appendix is Theorem 4 which is of central importance in Sect. 3.

We discussed some preliminaries on Markov chains and defined basic concepts such as ergodicity in Sect. 2.1. Here we begin by defining the interpolated Markov chain $P(s)$ and considering its properties, such as the stationary distribution and reversibility (Appendix A.1). We proceed by applying these concepts to define and study the discriminant matrix of $P(s)$ which encodes all relevant properties of $P(s)$, such as eigenvalues and the principal eigenvector, but has a much more convenient form (Appendix A.2). Finally, we define the hitting time HT and the interpolated hitting time HT(s) and relate the two in the case of a single marked element via Theorem 4, which is our main result regarding semi-absorbing Markov chains (Appendix A.3).

Results from this appendix are used in Sect. 3 to construct quantum search algorithms based on discrete-time quantum walks.

Appendix A.1: Basic Properties of Semi-Absorbing Markov Chains

Assume that a subset $M \subset X$ of size $m := |M|$ of the states are marked (we assume that M is not empty). (see [21, Chapter III] and [20, Sect. 11.2]). Note that P' differs from P only in the rows corresponding to the marked states (where it contains all zeros on non-diagonal elements, and ones on the diagonal). If we arrange the states of X so that the unmarked states $U := X \setminus M$ come first, matrices P and P' have the following block structure:

$$P := \begin{pmatrix} P_{UU} & P_{UM} \\ P_{MU} & P_{MM} \end{pmatrix}, \qquad P' := \begin{pmatrix} P_{UU} & P_{UM} \\ 0 & I \end{pmatrix}, \tag{97}$$

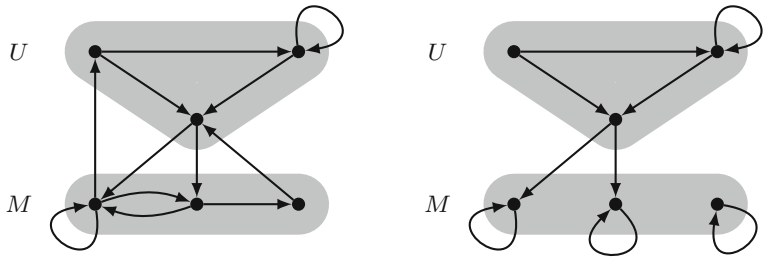

Fig. 4 Directed graphs underlying Markov chain P (*left*) and the corresponding absorbing chain P' (*right*). Outgoing arcs from vertices in the marked set M have been turned into self-loops in P'

where P_{UU} and P_{MM} are square matrices of size $(n-m)\times(n-m)$ and $m\times m$, respectively, while P_{UM} and P_{MU} are matrices of size $(n-m)\times m$ and $m\times(n-m)$, respectively (Fig. 4).

Recall that we have defined an *interpolated* Markov chain that interpolates between P and P':

$$P(s) := (1-s)P + sP', \quad 0 \le s \le 1. \tag{98}$$

This expression has some resemblance with adiabatic quantum computation where similar interpolations are usually defined for quantum Hamiltonians [29]. Indeed, the interpolated Markov chain $P(s)$ was used in [19] to construct an adiabatic quantum search algorithm. Note that $P(0) = P$, $P(1) = P'$, and $P(s)$ has the following block structure:

$$P(s) = \begin{pmatrix} P_{UU} & P_{UM} \\ (1-s)P_{MU} & (1-s)P_{MM} + sI \end{pmatrix}. \tag{99}$$

Proposition 7 *If P is ergodic then so is $P(s)$ for $s \in [0,1)$. $P(1)$ is not ergodic.*

Proof Recall from Definition 1 that ergodicity of a Markov chain can be established just by looking at its underlying graph. A non-zero transition probability in P remains non-zero also in $P(s)$ for $s \in [0,1)$. Thus the ergodicity of P implies that $P(s)$ is also ergodic for $s \in [0,1)$. However, $P(1)$ is not irreducible, since states in U are not reachable from M. Thus $P(1)$ is *not* ergodic. □

Proposition 8 $(P'^t)_{UU} = P_{UU}^t$.

Proof Let us derive an expression for P'^t, the matrix of transition probabilities corresponding to t applications of P'. Notice that $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} ac & ad+b \\ 0 & 1 \end{smallmatrix}\right)$. By induction,

$$P'^t = \begin{pmatrix} P_{UU}^t & \sum_{k=0}^{t-1} P_{UU}^k P_{UM} \\ 0 & I \end{pmatrix}. \tag{100}$$

When restricted to U, it acts as P_{UU}^t. □

Proposition 9 ([20, Theorem 11.3, p. 417]) *If P is irreducible then* $\lim_{k\to\infty} P_{UU}^k = 0$.

Intuitively this means that the sub-stochastic process defined by P_{UU} eventually dies out or, equivalently, that the unmarked states of P' eventually get absorbed (by Prop. 8).

Proof Let us fix an unmarked initial state x. Since P is irreducible, we can reach a marked state from x in a finite number of steps. Note that this also holds true for P'. Let us denote the smallest number of steps by l_x and the corresponding probability by $p_x > 0$. Thus in $l := \max_x l_x$ steps of P' we are guaranteed to reach a marked state with probability at least $p := \min_x p_x > 0$, independently of the initial state $x \in U$. Notice that the probability to still be in an unmarked state after kl steps is at most $(1-p)^k$ which approaches zero as we increase k. □

Proposition 10 ([21, Theorem 3.2.1,p. 46]) *If P is irreducible then $I - P_{UU}$ is invertible.*

Proof Notice that

$$(I - P_{UU}) \cdot (I + P_{UU} + P_{UU}^2 + \cdots + P_{UU}^{k-1}) = I - P_{UU}^k \tag{101}$$

and take the determinant of both sides. From Prop. 9 we see that $\lim_{k\to\infty} \det(I - P_{UU}^k) = 1$. By continuity, there exists k_0 such that $\det(I - P_{UU}^{k_0}) > 0$, so the determinant of the left-hand side is non-zero as well. Using multiplicativity of the determinant, we conclude that $\det(I - P_{UU}) \neq 0$ and thus $I - P_{UU}$ is invertible. □

In the Markov chain literature $(I - P_{UU})^{-1}$ is called the *fundamental matrix* of P.

Appendix A.1.1: Stationary Distribution

From now on let us demand that P is ergodic. Then according to the Perron–Frobenius Theorem it has a unique stationary distribution π that is non-zero everywhere. Let π_U and π_M be row vectors of length $n - m$ and m that are obtained by restricting π to sets U and M, respectively. Then

$$\pi = \begin{pmatrix}\pi_U & \pi_M\end{pmatrix}, \qquad \pi' := \begin{pmatrix}0_U & \pi_M\end{pmatrix} \tag{102}$$

where 0_U is the all-zeroes row vector indexed by elements of U and π' satisfies $\pi' P' = \pi'$.

Let $p_M := \sum_{x\in M} \pi_x$ be the probability to pick a marked element from the stationary distribution. In analogy to the definition of $P(s)$ in Eq. (98), let $\pi(s)$ be a convex combination of π and π', appropriately normalized:

$$\pi(s) := \frac{(1-s)\pi + s\pi'}{(1-s) + sp_M} = \frac{1}{1 - s(1-p_M)} \begin{pmatrix}(1-s)\pi_U & \pi_M\end{pmatrix}. \tag{103}$$

Proposition 11 *$\pi(s)$ is the unique stationary distribution of $P(s)$ for $s \in [0, 1)$. At $s = 1$ any distribution with support only on marked states is stationary, including $\pi(1)$.*

Proof Notice that

$$(\pi - \pi')(P - P') = \begin{pmatrix}\pi_U & 0\end{pmatrix} \begin{pmatrix} 0 & 0 \\ P_{MU} & P_{MM} - I \end{pmatrix} = 0 \tag{104}$$

which is equivalent to

$$\pi P' + \pi' P = \pi P + \pi' P'. \tag{105}$$

Using this equation we can check that $\pi(s)P(s) = \pi(s)$ for any $s \in [0, 1]$:

$$\begin{aligned}
&\big((1-s)\pi + s\pi'\big)\big((1-s)P + sP'\big) && (106)\\
&= (1-s)^2\pi P + (1-s)s(\pi P' + \pi' P) + s^2\pi' P' && (107)\\
&= (1-s)^2\pi + (1-s)s(\pi + \pi') + s^2\pi' && (108)\\
&= \big((1-s)\pi + s\pi'\big)\big((1-s) + s\big) && (109)\\
&= (1-s)\pi + s\pi'. && (110)
\end{aligned}$$

Recall from Prop. 7 that $P(s)$ is ergodic for $s \in [0, 1)$ so $\pi(s)$ is the unique stationary distribution by Perron–Frobenius Theorem. Since P' acts trivially on marked states, any distribution with support only on marked states is stationary for $P(1)$. □

Appendix A.1.2: Reversibility

Definition 10 Markov chain P is called *reversible* if it is ergodic and satisfies the so-called *detailed balance condition*

$$\forall x,\ y \in X\colon \pi_x P_{xy} = \pi_y P_{yx} \tag{111}$$

where π is the unique stationary distribution of P.

Intuitively this means that the net flow of probability in the stationary distribution between every pair of states is zero. Note that Eq. (111) is equivalent to

$$\operatorname{diag}(\pi)\, P = P^{\mathsf{T}} \operatorname{diag}(\pi) = \big(\operatorname{diag}(\pi) P\big)^{\mathsf{T}} \tag{112}$$

where $\operatorname{diag}(\pi)$ is a diagonal matrix whose diagonal is given by vector π. Thus Eq. (111) is equivalent to saying that matrix $\operatorname{diag}(\pi)P$ is symmetric.

Proposition 12 *If P is reversible then so is $P(s)$ for any $s \in [0, 1]$. Hence, $P(s)$ satisfies the interpolated detailed balance equation*

$$\forall s \in [0, 1],\ \forall x, y \in X\colon \pi_x(s) P_{xy}(s) = \pi_y(s) P_{yx}(s). \tag{113}$$

Proof First, notice that the absorbing walk P' is reversible[7] since $\operatorname{diag}(\pi')P'$ is a symmetric matrix:

$$\operatorname{diag}(\pi')P' = \begin{pmatrix} 0 & 0 \\ 0 & \operatorname{diag}(\pi_M) \end{pmatrix} \begin{pmatrix} P_{UU} & P_{UM} \\ 0 & I \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & \operatorname{diag}(\pi_M) \end{pmatrix} = \operatorname{diag}(\pi'). \tag{114}$$

[7] Strictly speaking, the definition of reversibility also includes ergodicity for the stationary distribution to be uniquely defined. However, we will relax this requirement for P' since, by continuity, π' is the natural choice of the "unique" stationary distribution.

Next, notice that

$$\operatorname{diag}(\pi - \pi')(P - P') = \begin{pmatrix} \operatorname{diag}(\pi_U) & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ P_{MU} & P_{MM} - I \end{pmatrix} = 0 \tag{115}$$

which gives us an analogue of Eq. (105):

$$\operatorname{diag}(\pi')P + \operatorname{diag}(\pi)P' = \operatorname{diag}(\pi)P + \operatorname{diag}(\pi')P'. \tag{116}$$

Here the right-hand side is symmetric due to reversibility of P and P', thus so is the left-hand side. Using this we can check that $P(s)$ is reversible:

$$\operatorname{diag}\big((1-s)\pi + s\pi'\big)\big((1-s)P + sP'\big) \tag{117}$$

$$= (1-s)^2 \operatorname{diag}(\pi)P + (1-s)s\big(\operatorname{diag}(\pi)P' + \operatorname{diag}(\pi')P\big) + s^2 \operatorname{diag}(\pi')P' \tag{118}$$

where the first and last terms are symmetric since P and P' are reversible, but the middle term is symmetric due to Eq. (116). □

Appendix A.2: Discriminant Matrix

Recall from Definition 6 that the *discriminant matrix* of a Markov chain $P(s)$ is

$$D(s) := \sqrt{P(s) \circ P(s)^{\mathsf{T}}}, \tag{119}$$

where the Hadamard product "$\circ$" and the square root are computed entry-wise. This matrix was introduced by Szegedy in [10]. We prefer to work with $D(s)$ rather than $P(s)$ since the matrix of transition probabilities is not necessarily symmetric while its discriminant matrix is.

Proposition 13 *If P is reversible then*

$$D(s) = \operatorname{diag}\big(\sqrt{\pi(s)}\big)\, P(s)\, \operatorname{diag}\big(\sqrt{\pi(s)}\big)^{-1}, \qquad \forall s \in [0, 1); \tag{120}$$

$$D(1) = \begin{pmatrix} \operatorname{diag}\big(\sqrt{\pi_U}\big)\, P_{UU}\, \operatorname{diag}\big(\sqrt{\pi_U}\big)^{-1} & 0 \\ 0 & I \end{pmatrix}. \tag{121}$$

Here the square roots are also computed entry-wise and M^{-1} denotes the matrix inverse of M. Notice that for $s \in [0, 1)$ the right-hand side of Eq. (120) is well-defined, since $P(s)$ is ergodic by Prop. 7 and thus according to the Perron–Frobenius Theorem has a unique and non-vanishing stationary distribution. However, recall from Prop. 11 that $\pi(1)$ vanishes on U, so the right-hand side of Eq. (120) is no longer well-defined at $s = 1$. For this reason we have an alternative expression for $D(1)$.

Proof (of Prop. 13) For a reversible Markov chain P the interpolated detailed balance condition in Eq. (113) implies that $D_{xy}(s) = \sqrt{P_{xy}(s)P_{yx}(s)} = P_{xy}(s)\sqrt{\pi_x(s)/\pi_y(s)}$. This is equivalent to Eq. (120).

At $s = 1$ from Eq. (119) we have:

$$D(1) = \sqrt{P(1) \circ P(1)^{\mathsf{T}}} = \sqrt{\begin{pmatrix} P_{UU} \circ P_{UU}^{\mathsf{T}} & 0 \\ 0 & I \end{pmatrix}} = \begin{pmatrix} \sqrt{P_{UU} \circ P_{UU}^{\mathsf{T}}} & 0 \\ 0 & I \end{pmatrix}. \tag{122}$$

It remains to verify that the upper left block of $D(1)$ agrees with Eq. (121). Using Eq. (119) we compute that

$$D_{UU}(s) = \sqrt{P_{UU} \circ P_{UU}^{\mathsf{T}}} = D_{UU}(0) = \operatorname{diag}\left(\sqrt{\pi_U}\right) P_{UU} \operatorname{diag}\left(\sqrt{\pi_U}\right)^{-1} \tag{123}$$

where the last equality follows from Eq. (120) at $s = 0$. Together with Eq. (122) this gives us the desired expression in Eq. (121). □

Appendix A.2.1: Spectral Decomposition

Recall from Eq. (119) that $D(s)$ is real and symmetric. Therefore, its eigenvalues are real and it has an orthonormal set of real eigenvectors. Let

$$D(s) = \sum_{i=1}^{n} \lambda_i(s) |v_i(s)\rangle\langle v_i(s)| \tag{124}$$

be the spectral decomposition of $D(s)$ with eigenvalues $\lambda_i(s)$ and eigenvectors[8] $|v_i(s)\rangle$. Moreover, let us arrange the eigenvalues so that

$$\lambda_1(s) \leq \lambda_2(s) \leq \cdots \leq \lambda_n(s). \tag{125}$$

From now on we will assume that P is reversible (and hence ergodic) without explicitly mentioning it. Under this assumption the matrices $P(s)$ and $D(s)$ are similar (see Prop. 14 below). This means that $D(s)$ essentially has the same properties as $P(s)$, but in addition it also admits a spectral decomposition with orthogonal eigenvectors. This will be very useful in Appendix B.1, where we find the spectral decomposition of the quantum walk operator $W(s)$ in terms of that of $D(s)$, and use it to relate properties of $W(s)$ and $P(s)$.

Proposition 14 *Assume P is reversible. The matrices $P(s)$ and $D(s)$ are similar for any $s \in [0, 1]$ and therefore have the same eigenvalues. In particular, the eigenvalues of $P(s)$ are real.*

Proof From Eq. (120) we see that the matrices $D(s)$ and $P(s)$ are similar for $s \in [0, 1)$. From Eq. (121) we see that $D(1)$ is similar to $\tilde{P} := \left(\begin{smallmatrix} P_{UU} & 0 \\ 0 & I \end{smallmatrix}\right)$. To verify that $\tilde{P}$ and $P(1) = \left(\begin{smallmatrix} P_{UU} & P_{UM} \\ 0 & I \end{smallmatrix}\right)$ are similar, let $M := \left(\begin{smallmatrix} P_{UU} - I & P_{UM} \\ 0 & I \end{smallmatrix}\right)$. One can check that

[8] There is no need to use bra-ket notation at this point; nevertheless we adopt it since vectors $|v_i(s)\rangle$ later will be used as quantum states.

$MP(1)M^{-1} = \tilde{P}$ where $M^{-1} = \begin{pmatrix} (P_{UU}-I)^{-1} & -(P_{UU}-I)^{-1}P_{UM} \\ 0 & I \end{pmatrix}$ exists, since $P_{UU} - I$ is invertible according to Prop. 10. By transitivity, $D(1)$ is also similar to $P(1)$. □

Proposition 15 *The largest eigenvalue of $D(s)$ is 1. It has multiplicity 1 when $s \in [0, 1)$ and multiplicity m when $s = 1$. In other words,*

$$\lambda_{n-1}(s) < \lambda_n(s) = 1, \quad \forall s \in [0, 1), \tag{126}$$

$$\lambda_{n-m}(1) < \lambda_{n-m+1}(1) = \cdots = \lambda_n(1) = 1. \tag{127}$$

Proof Let us argue about $P(s)$, since it has the same eigenvalues as $D(s)$ by Prop. 14. From the Perron–Frobenius Theorem we have that $\forall i: \lambda_i(s) \leq 1$ and $\lambda_n(s) = 1$. In addition, by Prop. 7 the Markov chain $P(s)$ is ergodic for any $s \in [0, 1)$, so $\forall i \neq n: \lambda_i(s) < 1$. Finally, note by Eq. (121) that for $s = 1$ eigenvalue 1 has multiplicity at least m. Recall from Eq. (123) that $D_{UU}(1)$ and P_{UU} are similar. From Prop. 10 we conclude that all eigenvalues of P_{UU} are strictly less than 1. Thus the multiplicity of eigenvalue 1 of $D(1)$ is exactly m. □

Appendix A.2.2: Principal Eigenvector

Let us prove an analogue of Prop. 11 for the matrix $D(s)$.

Proposition 16 *$\sqrt{\pi(s)}^{\mathsf{T}}$ is the unique $(+1)$-eigenvector of $D(s)$ for $s \in [0, 1)$. At $s = 1$ any vector with support only on marked states is a $(+1)$-eigenvector, including $\sqrt{\pi(1)}^{\mathsf{T}}$.*

Proof Since $P(s)$ is row-stochastic, $P(s)\ 1_X^{\mathsf{T}} = 1_X^{\mathsf{T}}$ where 1_X is the all-ones row vector. Thus we can check that for $s \in [0, 1)$,

$$D(s)\sqrt{\pi(s)}^{\mathsf{T}} = \operatorname{diag}\left(\sqrt{\pi(s)}\right) P(s)\ \operatorname{diag}\left(\sqrt{\pi(s)}\right)^{-1} \sqrt{\pi(s)}^{\mathsf{T}} \tag{128}$$

$$= \operatorname{diag}\left(\sqrt{\pi(s)}\right) P(s)\ 1_X^{\mathsf{T}} \tag{129}$$

$$= \operatorname{diag}\left(\sqrt{\pi(s)}\right) 1_X^{\mathsf{T}} \tag{130}$$

$$= \sqrt{\pi(s)}^{\mathsf{T}}. \tag{131}$$

Uniqueness for $s \in [0, 1)$ follows by the uniqueness of $\pi(s)$ and Prop. 14. For the $s = 1$ case, notice from Eq. (121) that $D(1)$ acts trivially on marked elements and recall from Eq. (103) that $\pi(1) = (0_U\ \ \pi_M)/p_M$. □

According to the above Proposition, for any $s \in [0, 1]$ we can choose the principal eigenvector $|v_n(s)\rangle$ in the spectral decomposition of $D(s)$ in Eq. (124) to be

$$|v_n(s)\rangle := \sqrt{\pi(s)}^{\mathsf{T}}. \tag{132}$$

We would like to have an intuitive understanding of how $|v_n(s)\rangle$ evolves as a function of s. Let us introduce some useful notation that we will also need later.

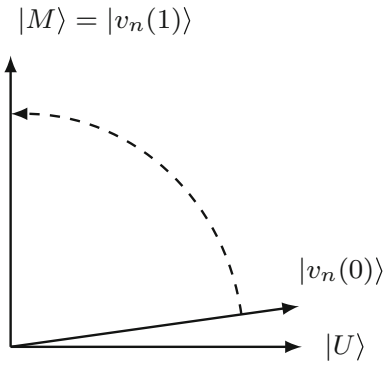

Fig. 5 As s changes from zero to one, the evolution of the principal eigenvector $|v_n(s)\rangle$ corresponds to a rotation in the two-dimensional subspace $\mathrm{span}\{|U\rangle, |M\rangle\}$

Let 0_U and 1_U (respectively, 0_M and 1_M) be the all-zeros and all-ones row vectors of dimension $n - m$ (respectively, m) whose entries are indexed by elements of U (respectively, M). Furthermore, let

$$\tilde{\pi}_U := \pi_U/(1 - p_M), \qquad \tilde{\pi}_M := \pi_M/p_M \tag{133}$$

be the normalized row vectors describing the stationary distribution π restricted to unmarked and marked states. Let us also define the following unit vectors in $\mathbb{R}^n$:

$$|U\rangle := \sqrt{(\tilde{\pi}_U \;\; 0_M)^{\mathsf{T}}} = \frac{1}{\sqrt{1 - p_M}} \sum_{x \in U} \sqrt{\pi_x}|x\rangle, \tag{134}$$

$$|M\rangle := \sqrt{(0_U \;\; \tilde{\pi}_M)^{\mathsf{T}}} = \frac{1}{\sqrt{p_M}} \sum_{x \in M} \sqrt{\pi_x}|x\rangle. \tag{135}$$

Then we can express $|v_n(s)\rangle$ as a linear combination of $|U\rangle$ and $|M\rangle$.

Now we prove Prop. 4.

Proof By substituting $\pi(s)$ from Eq. (103) into Eq. (132) we get

$$|v_n(s)\rangle = \sqrt{\pi(s)^{\mathsf{T}}} = \sqrt{\frac{\big((1-s)\pi_U \;\; \pi_M\big)^{\mathsf{T}}}{1 - s(1 - p_M)}} = \sqrt{\frac{\big((1-s)(1-p_M)\tilde{\pi}_U \;\; p_M\tilde{\pi}_M\big)^{\mathsf{T}}}{1 - s(1 - p_M)}} \tag{136}$$

which is the desired expression. □

Thus $|v_n(s)\rangle$ lies in the two-dimensional subspace $\mathrm{span}\{|U\rangle, |M\rangle\}$ and is subject to a rotation as we change the parameter s (see Fig. 5). In particular,

$$|v_n(0)\rangle = \sqrt{1 - p_M}|U\rangle + \sqrt{p_M}|M\rangle, \qquad |v_n(1)\rangle = |M\rangle. \tag{137}$$

Proposition 17 *$\theta(s)$ and its derivative $\dot{\theta}(s) := \frac{d}{ds}\theta(s)$ are related as follows:*

$$2\dot{\theta}(s) = \frac{\sin\theta(s)\cos\theta(s)}{1-s}. \tag{138}$$

Proof Notice that

$$\frac{d}{ds}\big(\sin^2\theta(s)\big) = 2\dot{\theta}(s)\sin\theta(s)\cos\theta(s). \tag{139}$$

On the other hand, according to Eq. (21) we have

$$\frac{d}{ds}\big(\sin^2\theta(s)\big) = \frac{d}{ds}\left(\frac{p_M}{1-s(1-p_M)}\right) = \frac{p_M(1-p_M)}{(1-s(1-p_M))^2} = \frac{\sin^2\theta(s)\cos^2\theta(s)}{1-s}. \tag{140}$$

By comparing both equations we get the desired result. □

Appendix A.2.3: Derivative

Proposition 18 *$D(s)$ and its derivative $\dot{D}(s) := \frac{d}{ds}D(s)$ are related as follows:*

$$\dot{D}(s) = \frac{1}{2(1-s)}\big\{\Pi_M, I - D(s)\big\} \tag{141}$$

where $\{X, Y\} := XY + YX$ is the anticommutator of X and Y, and $\Pi_M := \sum_{x\in M}|x\rangle\langle x|$ is the projector onto the m-dimensional subspace spanned by marked states M.

Proof Recall from Eq. (119) that $D(s) = \sqrt{P(s)\circ P(s)^{\mathsf{T}}}$. The block structure of $P(s)$ is given in Eq. (99). First, let us derive an expression for $D_{MM}(s)$, the lower right block of $D(s)$:

$$D_{MM}(s) = \sqrt{P_{MM}(s)\circ P_{MM}(s)^{\mathsf{T}}} \tag{142}$$

$$= \sqrt{\big((1-s)P_{MM} + sI\big)\circ\big((1-s)P_{MM}^{\mathsf{T}} + sI\big)}. \tag{143}$$

Let us separately consider the diagonal and off-diagonal entries of $D_{MM}(s)$. For $x, y \in M$ we have

$$D_{xy}(s) = \begin{cases} (1-s)\sqrt{P_{xy}P_{yx}} & \text{if } x \neq y, \\ (1-s)P_{xx} + s & \text{if } x = y. \end{cases} \tag{144}$$

Thus we can write $D_{MM}(s)$ as

$$D_{MM}(s) = (1-s)\sqrt{P_{MM}\circ P_{MM}^{\mathsf{T}}} + sI. \tag{145}$$

Expressions for the remaining blocks of $D(s)$ can be derived in a straightforward way. By putting all blocks together we get

$$D(s) = \begin{pmatrix} \sqrt{P_{UU} \circ P_{UU}^{\mathsf{T}}} & \sqrt{(1-s)(P_{UM} \circ P_{MU}^{\mathsf{T}})} \\ \sqrt{(1-s)(P_{MU} \circ P_{UM}^{\mathsf{T}})} & (1-s)\sqrt{P_{MM} \circ P_{MM}^{\mathsf{T}}} + sI \end{pmatrix}. \tag{146}$$

When we take the derivative with respect to s we find

$$\dot{D}(s) = \begin{pmatrix} 0 & -\frac{1}{2\sqrt{1-s}}\sqrt{P_{UM} \circ P_{MU}^{\mathsf{T}}} \\ -\frac{1}{2\sqrt{1-s}}\sqrt{P_{MU} \circ P_{UM}^{\mathsf{T}}} & I - \sqrt{P_{MM} \circ P_{MM}^{\mathsf{T}}} \end{pmatrix}. \tag{147}$$

To relate $\dot{D}(s)$ and the original matrix $D(s)$, observe that

$$\Pi_M D(s) + D(s)\Pi_M = \begin{pmatrix} 0 & \sqrt{(1-s)(P_{UM} \circ P_{MU}^{\mathsf{T}})} \\ \sqrt{(1-s)(P_{MU} \circ P_{UM}^{\mathsf{T}})} & 2(1-s)\sqrt{P_{MM} \circ P_{MM}^{\mathsf{T}}} + 2sI \end{pmatrix} \tag{148}$$

which can be seen by overlaying the second column and row of $D(s)$ given in Eq. (146). When we rescale this by an appropriate constant, we get

$$-\frac{1}{2(1-s)}\{\Pi_M, D(s)\} = \begin{pmatrix} 0 & -\frac{1}{2\sqrt{1-s}}\sqrt{P_{UM} \circ P_{MU}^{\mathsf{T}}} \\ -\frac{1}{2\sqrt{1-s}}\sqrt{P_{MU} \circ P_{UM}^{\mathsf{T}}} & -\sqrt{P_{MM} \circ P_{MM}^{\mathsf{T}}} - \frac{s}{1-s}I \end{pmatrix}. \tag{149}$$

This is very similar to the expression for $\dot{D}(s)$ in Eq. (147), except for a slightly different coefficient for the identity matrix in the lower right corner. We can correct this by adding Π_M with an appropriate constant: $-\frac{1}{2(1-s)}\{\Pi_M, D(s)\} + \frac{1}{1-s}\Pi_M = \dot{D}(s)$. □

Appendix A.3: Hitting Time

From now on we assume that P is ergodic and reversible. Recall from Definition 4 that $\mathrm{HT}(P, M)$ is the expected number of steps it takes for the **Random Walk Algorithm** to find a marked vertex, starting from the stationary distribution of P restricted to unmarked vertices. We now prove Prop. 2 which expresses the hitting time of P in terms of the spectral properties of the discriminant matrix of the absorbing walk P'.

Proposition 2 *The hitting time of Markov chain P with respect to marked set M is given by*

$$\mathrm{HT}(P, M) = \sum_{k=1}^{n-|M|} \frac{|\langle v'_k|U\rangle|^2}{1-\lambda'_k}, \tag{9}$$

where λ'_k are the eigenvalues of the discriminant matrix $D' = D(P')$ in nondecreasing order, $|v'_k\rangle$ are the corresponding eigenvectors, and $|U\rangle$ is the unit vector

$$|U\rangle := \frac{1}{\sqrt{1-p_M}} \sum_{x \notin M} \sqrt{\pi_x}|x\rangle, \tag{10}$$

p_M being the probability to draw a marked vertex from the stationary distribution π of P.

Proposition 19 *The hitting time of Markov chain P with respect to marked set M is given by*

$$\mathrm{HT}(P, M) = \sum_{k=1}^{n-|M|} \frac{|\langle v'_k|U\rangle|^2}{1-\lambda'_k}, \tag{150}$$

where λ'_k are the eigenvalues of the discriminant matrix $D' = D(P')$ in nondecreasing order, $|v'_k\rangle$ are the corresponding eigenvectors, and $|U\rangle$ is the unit vector

$$|U\rangle := \frac{1}{\sqrt{1-p_M}} \sum_{x \notin M} \sqrt{\pi_x}|x\rangle, \tag{151}$$

p_M being the probability to draw a marked vertex from the stationary distribution π of P.

Proof The expected number of iterations in the **Random Walk Algorithm** is

$$\begin{aligned}
\mathrm{HT}(P, M) &:= \sum_{l=1}^{\infty} l \cdot \Pr[\text{need } \textit{exactly } l \text{ steps}] && (152)\\
&= \sum_{l=1}^{\infty} \sum_{t=1}^{l} \Pr[\text{need } \textit{exactly } l \text{ steps}] && (153)\\
&= \sum_{t=1}^{\infty} \sum_{l=t}^{\infty} \Pr[\text{need } \textit{exactly } l \text{ steps}] && (154)\\
&= \sum_{t=1}^{\infty} \Pr[\text{need } \textit{at least } t \text{ steps}] && (155)\\
&= \sum_{t=0}^{\infty} \Pr[\text{need } \textit{more} \text{ than } t \text{ steps}]. && (156)
\end{aligned}$$

The region corresponding to the double sums in Eqs. (153) and (154) is shown in Fig. 6.

It remains to determine the probability that no marked vertex is found after t steps, starting from an unmarked vertex distributed according to $\tilde{\pi}_U = \pi_U/(1-p_M)$. The

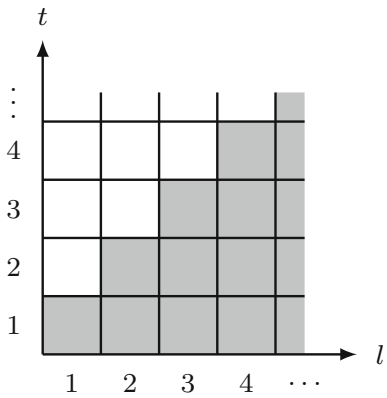

Fig. 6 Range of variables l and t in the double sums of Eqs. (153) and (154)

distribution of vertices at the first execution of step 3 of the **Random Walk Algorithm** is $(\tilde{\pi}_U \;\; 0_M)$, hence

$$\Pr[\text{need } \textit{more} \text{ than } t \text{ steps}] = (\tilde{\pi}_U \;\; 0_M) P'^t (1_U \;\; 0_M)^{\mathsf{T}}. \tag{157}$$

Recall from Prop. 8 that $(P'^t)_{UU} = P^t_{UU}$ so we can simplify Eq. (157) as follows:

$$\begin{aligned}
\Pr[\text{need } \textit{more} \text{ than } t \text{ steps}] &= (\tilde{\pi}_U \;\; 0_M) P'^t (1_U \;\; 0_M)^{\mathsf{T}} && (158)\\
&= \frac{\pi_U}{1-p_M} P^t_{UU} 1_U^{\mathsf{T}} && (159)\\
&= \sqrt{\tfrac{\pi_U}{1-p_M}}\, \mathrm{diag}\big(\sqrt{\pi_U}\big) P^t_{UU}\, \mathrm{diag}\big(\sqrt{\pi_U}\big)^{-1} \sqrt{\tfrac{\pi_U^{\mathsf{T}}}{1-p_M}} && (160)\\
&= \langle U | D'^t | U \rangle, && (161)
\end{aligned}$$

where the last equality follows from the expression for the discriminant matrix $D' = D(1)$ in Eq. (121). By plugging this back in Eq. (156) we get

$$\mathrm{HT}(P, M) = \sum_{t=0}^{\infty} \langle U | D'^t | U \rangle. \tag{162}$$

From the spectral decomposition $D' = \sum_{k=1}^{n} \lambda'_k |v'_k\rangle$, this may be rewritten as

$$\mathrm{HT}(P, M) = \sum_{t=0}^{\infty} \sum_{k=1}^{n} \lambda'^t_k |\langle v'_k | U \rangle|^2. \tag{163}$$

Let $m := |M|$ be the number of marked elements. Recall from Eq. (121) that $D' = D(1)$ is block-diagonal and acts as identity matrix in the m-dimensional marked subspace. Furthermore, all 1-eigenvectors of D' lie in the marked subspace, since

eigenvalue 1 has multiplicity m (recall from Prop. 15 that $\lambda'_k = 1$ when $k > n - m$). Therefore, the terms in Eq. (163) with $k > n - m$ disappear since $\langle v'_k | U \rangle = 0$, and we get the desired expression by exchanging the two sums in Eq. (163) and using the expansion $(1 - x)^{-1} = \sum_{t=0}^{\infty} x^t$ where $|x| < 1$. □

Note that the two sums in Eq. (163) may not be exchanged before removing the terms with $k > n - m$: they do not commute in the presence of these extra terms since $\lambda'_k = 1$ for $k > n - m$ and therefore $\sum_{t=0}^{\infty} |\lambda'_k|^t$ diverges. This subtlety had unfortunately been overlooked in [16,19], and is at the source of the distinction between the hitting time $\mathrm{HT}(P, M)$ and the extended hitting time $\mathrm{HT}^+(P, M)$ (see Appendix C).

Appendix A.3.1: Extended Hitting Time

We now prove Prop. 3, which states that the extended hitting time reduces to the usual hitting time in the case of a single marked element, even though they may differ in general.

Proof The fact that $\mathrm{HT}^+(P, M) = \mathrm{HT}(P, M)$ when $|M| = 1$ follows immediately from the expression for $\mathrm{HT}(P, M)$ in Prop. 2 and Definition 9.

For the second part, choose

$$P = \frac{1}{4} \begin{pmatrix} 3 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 3 \end{pmatrix} \tag{164}$$

and let the last two elements be marked. If we explicitly compute the eigenvalues and eigenvectors of $D(s)$, then from Definition 9 we get that $\mathrm{HT}(s) = \frac{20}{(3-s)^2}$ for $s \in [0, 1)$ and thus $\mathrm{HT}^+(P, M) = 5$. However, $\mathrm{HT}(P, M) = 4$. One can also use the formulas from Lemma 4 in Appendix C to verify this. □

This proposition implies that in the case of a single marked element, the quantum search algorithms in Sect. 3 provide a quadratic speedup over the classical hitting time. In the general case of multiple marked elements, these quantum algorithms still solve the search problems but their cost is given in terms of the extended hitting time rather than the standard one.

Appendix A.3.2: Lazy Walk

For technical reasons, in Sect. 3 it is important that all eigenvalues of $P(s)$ are non-negative. We can guarantee this using a standard trick—replacing the original Markov chain P with a "lazy" walk $(P + I)/2$ where I is the $n \times n$ identity matrix. In fact, we can assume without loss of generality that the original Markov chain already is "lazy", since this affects the hitting time only by a constant factor, as shown below.

Proposition 20 *Let P be an ergodic and reversible Markov chain. Then for any $s \in [0, 1]$ the eigenvalues of $(P(s)+I)/2$ are between 0 and 1. Moreover, if the interpolated hitting time of P is $\mathrm{HT}(s)$, then the interpolated hitting time of $(P + I)/2$ is $2\,\mathrm{HT}(s)$.*

Proof Since P is reversible, so is $P(s)$ by Prop. 12. Thus the eigenvalues of $P(s)$ are real by Prop. 14. If $\lambda_k(s)$ is an eigenvalue of $P(s)$ then $\lambda_k(s) \in [-1, 1]$ according to Perron–Frobenius Theorem. Thus, the eigenvalues of $(P(s) + I)/2$ satisfy $(\lambda_k(s) + 1)/2 \in [0, 1]$.

Recall from Prop. 14 that $P(s)$ and $D(s)$ are similar. Thus, the discriminant matrix of $(P(s) + I)/2$ is $(D(s) + I)/2$, which has the same eigenvectors as $D(s)$. By Definition 9, the interpolated hitting time of $(P(s) + I)/2$ is

$$\sum_{k=1}^{n-1} \frac{|\langle v_k(s)|U\rangle|^2}{1 - \frac{\lambda_k(s)+1}{2}}. \tag{165}$$

Since $1 - \frac{\lambda_k(s)+1}{2} = \frac{1-\lambda_k(s)}{2}$, the above expression is equal to $2\,\mathrm{HT}(s)$ as claimed. □

Appendix A.3.3: Relationship Between $\mathrm{HT}(s)$ *and* $HT^+(P, M)$

In this section we express $\mathrm{HT}(s)$ as a function of s and $\mathrm{HT}^+(P, M)$, which is the main result of this appendix. The main idea is to relate $\frac{d}{ds}\mathrm{HT}(s)$ to $\mathrm{HT}(s)$. When we solve the resulting differential equation, the boundary condition at $s = 1$ gives the desired result.

First, note that by Definition 9, $\mathrm{HT}(s)$ may be written as $\mathrm{HT}(s) = \langle U|A(s)|U\rangle$, where

$$A(s) := \sum_{k=1}^{n-1} \frac{|v_k(s)\rangle\langle v_k(s)|}{1 - \lambda_k(s)}. \tag{166}$$

The following property of $A(s)$ will be useful on several occasions.

Proposition 21 $A(s)|M\rangle = -\frac{\cos\theta(s)}{\sin\theta(s)} A(s)|U\rangle$.

Proof Recall from Prop. 15 that $|v_n(s)\rangle$ is orthogonal to $|v_k(s)\rangle$ for all $k \neq n$. So, we have $A(s)|v_n(s)\rangle = 0$ by the definition of $A(s)$. If we substitute $|v_n(s)\rangle = \cos\theta(s)|U\rangle + \sin\theta(s)|M\rangle$ from Prop. 4 in this equation, we get the desired formula. □

Lemma 1 *For* $s < 1$, *the derivative of* $\mathrm{HT}(s)$ *is related to* $\mathrm{HT}(s)$ *as*

$$\frac{d}{ds}\mathrm{HT}(s) = \frac{2(1 - p_M)}{1 - s(1 - p_M)}\mathrm{HT}(s) \tag{167}$$

where p_M *is the probability to pick a marked state from the stationary distribution* π *of* P.

Proof Recall that $\mathrm{HT}(s) = \langle U|A(s)|U\rangle$ where $A(s)$ may be written as

$$A(s) = B(s)^{-1} - \Pi_n(s) \text{ where } B(s) := I - D(s) + \Pi_n(s),\ \Pi_n(s) := |v_n(s)\rangle\langle v_n(s)|. \tag{168}$$

Recall from Appendix A.2.1 that $|v_n(s)\rangle$ is the unique $(+1)$-eigenvector of $D(s)$ for $s \in [0, 1)$, thus $B(s)$ is indeed invertible when s is in this range.

From now on we will not write the dependence on s explicitly. We will also often use $\dot{f}(s)$ as a shorthand form of $\frac{d}{ds} f(s)$. Let us start with

$$\frac{d}{ds}\,\mathrm{HT} = \langle U|\dot{A}|U\rangle \tag{169}$$

and expand $\dot{A}$ using Eq. (168). To find $\frac{d}{ds}(B^{-1})$, take the derivative of both sides of $B^{-1}B = I$ and get $\frac{d}{ds}(B^{-1})\cdot B + B^{-1}\cdot\frac{d}{ds}B = 0$. Thus $\frac{d}{ds}(B^{-1}) = -B^{-1}\dot{B}B^{-1}$ and

$$\dot{A} = -B^{-1}\dot{B}B^{-1} - \dot{\Pi}_n. \tag{170}$$

Notice from Eq. (168) that $\dot{B} = -\dot{D} + \dot{\Pi}_n$, thus $\dot{A} = -B^{-1}(-\dot{D} + \dot{\Pi}_n)B^{-1} - \dot{\Pi}_n$ and $\frac{d}{ds}\,\mathrm{HT} = h_1 + h_2 + h_3$ where

$$h_1 := \langle U|B^{-1}\dot{D}B^{-1}|U\rangle, \tag{171}$$

$$h_2 := -\langle U|B^{-1}\dot{\Pi}_n B^{-1}|U\rangle, \tag{172}$$

$$h_3 := -\langle U|\dot{\Pi}_n|U\rangle. \tag{173}$$

Let us evaluate each of these terms separately.

To evaluate the first term h_1, we substitute $\dot{D} = \frac{1}{2(1-s)}\{\Pi_M, I - D\}$ from Prop. 18 and replace $I - D$ by $B - \Pi_n$ according to Eq. (168):

$$2(1-s)h_1 = \langle U|B^{-1}\{\Pi_M, B - \Pi_n\}B^{-1}|U\rangle \tag{174}$$

$$= \langle U|B^{-1}\big(\{\Pi_M, B\} - \{\Pi_M, \Pi_n\}\big)B^{-1}|U\rangle \tag{175}$$

$$= \langle U|\{B^{-1}, \Pi_M\}|U\rangle - \langle U|B^{-1}\{\Pi_M, \Pi_n\}B^{-1}|U\rangle. \tag{176}$$

Recall that $\Pi_M = \sum_{x\in M}|x\rangle\langle x|$ is the projector onto the marked states. Thus $\Pi_M|U\rangle = 0$ and the first term vanishes. Note that B has the same eigenvectors as D. In particular, $B^{-1}|v_n\rangle = |v_n\rangle$ and thus $B^{-1}\Pi_n = \Pi_n = \Pi_n B^{-1}$. Using this we can expand the anti-commutator in the second term: $B^{-1}\{\Pi_M, \Pi_n\}B^{-1} = B^{-1}\Pi_M\Pi_n + \Pi_n\Pi_M B^{-1}$. Since all three matrices in this expression are real and symmetric and $|U\rangle$ is also real, both terms of the anti-commutator have the same contribution, so we get

$$2(1-s)h_1 = -2\langle U|B^{-1}\Pi_M\Pi_n|U\rangle. \tag{177}$$

Recall from Prop. 4 that $|v_n\rangle = \cos\theta|U\rangle + \sin\theta|M\rangle$, so we see that $\Pi_M\Pi_n|U\rangle = \Pi_M|v_n\rangle\cdot\langle v_n|U\rangle = \sin\theta|M\rangle\cdot\cos\theta$. Moreover, $B^{-1} = A + \Pi_n$ according to Eq. (168), so

$$2(1-s)h_1 = -2\sin\theta\cos\theta\langle U|(A + \Pi_n)|M\rangle. \tag{178}$$

Recall from Prop. 21 that $\sin\theta\langle U|A|M\rangle = \cos\theta\langle U|A|U\rangle$. To simplify the second term, notice that $\langle U|\Pi_n|M\rangle = \langle U|v_n\rangle\cdot\langle v_n|M\rangle = \cos\theta\cdot\sin\theta$. When we put this together, we get

$$2(1-s)h_1 = 2\cos^2\theta\langle U|A|U\rangle - 2\sin^2\theta\cos^2\theta \tag{179}$$

or simply

$$h_1 = \frac{\cos^2\theta}{1-s}\big(\langle U|A|U\rangle - \sin^2\theta\big). \tag{180}$$

Let us now consider the second term $h_2 = -\langle U|B^{-1}\dot{\Pi}_n B^{-1}|U\rangle$. First, we compute $\dot{\Pi}_n = |\dot{v}_n\rangle\langle v_n| + |v_n\rangle\langle\dot{v}_n|$. Using $B^{-1}|v_n\rangle = |v_n\rangle$ we get $B^{-1}\dot{\Pi}_n B^{-1} = B^{-1}|\dot{v}_n\rangle\langle v_n| + |v_n\rangle\langle\dot{v}_n|B^{-1}$. Since $\langle v_n|U\rangle = \cos\theta$ we have

$$h_2 = -2\langle U|B^{-1}|\dot{v}_n\rangle\cos\theta \tag{181}$$

where the factor two comes from the fact that all vectors involved are real and matrix B^{-1} is real and symmetric. Let us compute

$$|\dot{v}_n\rangle = \dot{\theta}\big(-\sin\theta|U\rangle + \cos\theta|M\rangle\big). \tag{182}$$

Notice that $\langle v_n|\dot{v}_n\rangle = 0$ and thus $\Pi_n|\dot{v}_n\rangle = 0$. By substituting $B^{-1} = A + \Pi_n$ from Eq. (168) we get

$$h_2 = -2\langle U|A|\dot{v}_n\rangle\cos\theta. \tag{183}$$

Next, we substitute $|\dot{v}_n\rangle$ and get

$$h_2 = -2\dot{\theta}\big(-\sin\theta\langle U|A|U\rangle + \cos\theta\langle U|A|M\rangle\big)\cos\theta. \tag{184}$$

Now we use Prop. 21 to substitute $A|M\rangle$ by $A|U\rangle$:

$$h_2 = -2\dot{\theta}\left(-\sin\theta - \frac{\cos^2\theta}{\sin\theta}\right)\langle U|A|U\rangle\cos\theta = 2\dot{\theta}\frac{\cos\theta}{\sin\theta}\langle U|A|U\rangle. \tag{185}$$

Finally, we substitute $2\dot{\theta} = \frac{\sin\theta\cos\theta}{1-s}$ from Eq. (138) and get

$$h_2 = \frac{\cos^2\theta}{1-s}\langle U|A|U\rangle. \tag{186}$$

For the last term $h_3 = -\langle U|\dot{\Pi}_n|U\rangle$ we observe that $\langle U|\dot{v}_n\rangle\langle v_n|U\rangle = -\dot{\theta}\sin\theta\cdot\cos\theta$ thus $h_3 = 2\dot{\theta}\sin\theta\cos\theta$ where the factor two comes from symmetry. After substituting $2\dot{\theta}$ from Eq. (138) we get

$$h_3 = \frac{\cos^2\theta}{1-s}\sin^2\theta. \tag{187}$$

When we compare Eqs. (180), (186), and (187) we notice that $h_2 = h_1 + h_3$. Thus the derivative of the hitting time is $\frac{d}{ds}\mathrm{HT} = h_1 + h_2 + h_3 = 2h_2$. Recall from Definition 9 that $\mathrm{HT} = \langle U|A|U\rangle$. Thus

$$\frac{d}{ds}\,\mathrm{HT}(s) = 2\frac{\cos^2\theta(s)}{1-s}\,\mathrm{HT}(s). \tag{188}$$

By substituting $\cos\theta(s)$ from Eq. (21) we get the desired result. □

We now prove Theorem 4, which relates $\mathrm{HT}(s)$ to $\mathrm{HT}^+(P, M)$.

Proof When the marked element is unique, $\mathrm{HT}^+(P, M) = \mathrm{HT}(P, M)$ by Prop. 3. This gives the second part.

We will prove the first part by solving the differential equation obtained in Lemma 1. Consider Eq. (188) and recall from Eq. (138) that $2\dot{\theta} = \frac{\sin\theta\cos\theta}{1-s}$. We can rewrite the coefficient in Eq. (188) as

$$2\frac{\cos^2\theta}{1-s} = 2\cdot\frac{\sin\theta\cos\theta}{1-s}\cdot\frac{\cos\theta}{\sin\theta} = 4\dot{\theta}\frac{\cos\theta}{\sin\theta} = 4\frac{\frac{d}{ds}(\sin\theta)}{\sin\theta}. \tag{189}$$

Then the differential equation becomes

$$\frac{\frac{d}{ds}\,\mathrm{HT}(s)}{\mathrm{HT}(s)} = 4\frac{\frac{d}{ds}(\sin\theta(s))}{\sin\theta(s)}. \tag{190}$$

By integrating both sides we get

$$\ln|\mathrm{HT}(s)| = 4\ln|\sin\theta(s)| + C \tag{191}$$

for some constant C. Recall from Eq. (21) that $\sin\theta(1) = 1$, so the boundary condition at $s = 1$ gives us $C = \ln|\mathrm{HT}^+(P, M)|$. Since all quantities are non-negative, we can omit the absolute value signs. After exponentiating both sides we get

$$\mathrm{HT}(s) = \sin^4\theta(s)\cdot\mathrm{HT}^+(P, M). \tag{192}$$

We get the desired expression when we substitute $\sin\theta(s)$ from Eq. (21). □

In Sect. 3 we consider several quantum search algorithms whose running time depends on $\mathrm{HT}(s)$ for some values of s. Theorem 4 is a crucial ingredient in analysis of these algorithms: when the marked element is unique, it expresses $\mathrm{HT}(s)$ as a function of s and the usual hitting time $\mathrm{HT}(P, M)$. In particular, we see that $\mathrm{HT}(s)$ is monotonically increasing as a function of s and it reaches maximum value at $s = 1$ (some example plots of $\mathrm{HT}(s)$ are shown in Fig. 7). This observation is crucial, for example, in the proof of Theorem 7.

Appendix B: Spectrum and Implementation of $W(s)$

Szegedy [10] proposed a general method to map a random walk to a unitary operator that defines a quantum walk. The first step of Szegedy's construction is to map the rows of $P(s)$ to quantum states. Let X be the state space of $P(s)$ and $\mathcal{H} := \mathrm{span}\{|x\rangle : x \in X\}$

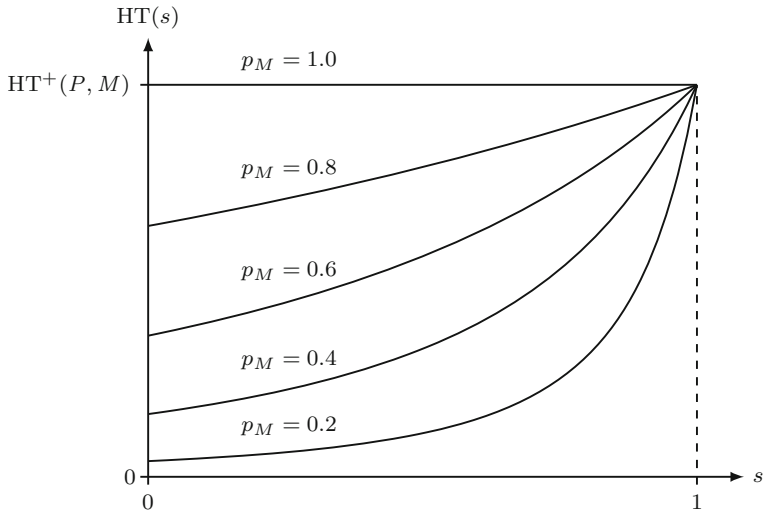

Fig. 7 The interpolated hitting time HT(s) as a function of s for several values of p_M according to Theorem 4

be a complex Euclidean space of dimension $n := |X|$ with basis states labelled by elements of X. For every $x \in X$ we define the following state in $\mathcal{H}$:

$$|p_x(s)\rangle := \sum_{y \in X} \sqrt{P_{xy}(s)}|y\rangle. \tag{193}$$

Notice that these states are correctly normalized, since $P(s)$ is row-stochastic. Following the approach of Szegedy [10], we define a unitary operator $V(s)$ acting on $\mathcal{H} \otimes \mathcal{H}$ as

$$V(s)|x, \bar{0}\rangle := |x\rangle|p_x(s)\rangle = \sum_{y \in X} \sqrt{P_{xy}(s)}|x, y\rangle, \tag{194}$$

when the second register is in some reference state $|\bar{0}\rangle \in \mathcal{H}$, and arbitrarily otherwise. It will not be relevant to us how $V(s)$ is extended from $\mathcal{H} \otimes |\bar{0}\rangle$ to $\mathcal{H} \otimes \mathcal{H}$. The only constraint we impose is that $V(s)$ is continuous as a function of s, which is a reasonable assumption from a physical point of view.

Let SHIFT be the operation defined in Eq. (2). Let $\Pi_0 := I \otimes |\bar{0}\rangle\langle\bar{0}|$ be the projector that keeps only the component containing the reference state $|\bar{0}\rangle$ in the second register and let $\mathrm{ref}_{\mathcal{X}} := 2\Pi_0 - I \otimes I$. The goal of this section is to find the spectral decomposition of the quantum walk operator corresponding to $P(s)$:

$$W(s) := V(s)^{\dagger} \cdot \textsc{Shift} \cdot V(s) \cdot \mathrm{ref}_{\mathcal{X}} \tag{195}$$

where $V(s) := V(P(s))$. Recall from Appendix A.2.1 that $\lambda_k(s)$ and $|v_k(s)\rangle$ are the eigenvalues and eigenvectors of the discriminant matrix $D(s)$ of $P(s)$.

Appendix B.1: Spectral Decomposition of $W(s)$

In this section we determine the invariant subspaces of $W(s)$ and find its eigenvectors and eigenvalues. First, observe that on certain states SHIFT acts as the swap gate.

Proposition 22 *If P is a Markov chain on graph G then* SHIFT $|x, p_x(s)\rangle = |p_x(s), x\rangle$, *i.e.,* SHIFT *always succeeds on states of the form $|x, p_x(s)\rangle$ for any $x \in X$.*

Proof From Eq. (194) we get

$$\text{SHIFT}\,|x, p_x(s)\rangle = \text{SHIFT} \sum_{y\in X} \sqrt{P_{xy}(s)}|x, y\rangle \tag{196}$$

$$= \sum_{y\in X} \sqrt{P_{xy}(s)}|y, x\rangle \tag{197}$$

$$= |p_x(s), x\rangle, \tag{198}$$

where the second equality holds since $P(s)$ is a Markov chain on G and thus $P_{xy}(s) = 0$ when xy is not an edge of G. □

It follows from Prop. 22 that SHIFT always succeeds when $V^\dagger(s)\,\text{SHIFT}\,V(s)$ acts on any state that has $|\bar{0}\rangle$ in the second register. In fact, we can say even more.

Proposition 23 *If P is a Markov chain on graph G then the operator $V^\dagger(s)\,\text{SHIFT}\,V(s)$ acts as the discriminant matrix $D(s)$ (see Appendix A.2) when restricted to $|\bar{0}\rangle$ in the second register, i.e.,*

$$\Pi_0 V^\dagger(s)\,\text{SHIFT}\,V(s)\Pi_0 = D(s) \otimes |\bar{0}\rangle\langle\bar{0}|. \tag{199}$$

Proof From Eq. (194) and Prop. 22 we get

$$\langle x, \bar{0}|V^\dagger(s)\,\text{SHIFT}\,V(s)|y, \bar{0}\rangle = \langle x, p_x(s)|\,\text{SHIFT}\,|y, p_y(s)\rangle \tag{200}$$

$$= \langle x, p_x(s)|p_y(s), y\rangle \tag{201}$$

$$= \langle p_x(s)|y\rangle\langle x|p_y(s)\rangle \tag{202}$$

$$= \sqrt{P_{xy}(s)P_{yx}(s)} \tag{203}$$

$$= D_{xy}(s) \tag{204}$$

where last equality follows from Eq. (119). □

This suggests a close relationship between the operators $D(s)$ and $V^\dagger(s)\,\text{SHIFT}\,V(s)$. We want to extend this and relate the spectral decompositions of $D(s)$ and $W(s)$ from Eq. (195). Recall from Eq. (124) the spectral decomposition $D(s) = \sum_{k=1}^{n} \lambda_k(s)|v_k(s)\rangle\langle v_k(s)|$.

Definition 11 We define the following subspaces of $\mathcal{H}\otimes\mathcal{H}$ in terms of the eigenvectors of $D(s)$ and the operator $V^\dagger(s)\,\text{SHIFT}\,V(s)$:

$$\mathcal{B}_k(s) := \operatorname{span}\{|v_k(s), \bar{0}\rangle,\ V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle\}, \quad k \in \{1, \ldots, n-1\}, \tag{205}$$

$$\mathcal{B}_n(s) := \operatorname{span}\{|v_n(s), \bar{0}\rangle\}, \tag{206}$$

$$\mathcal{B}^\perp(s) := \left(\bigoplus_{k=1}^n \mathcal{B}_k(s)\right)^\perp. \tag{207}$$

Let us first understand how $V^\dagger(s)\ \textsc{Shift}\ V(s)$ acts on vectors defining the subspaces in Definition 11. Let us consider $s < 1$ and $k < n$. Then $\lambda_k(s) \neq 1$ by Prop. 15. By unitarity of $V^\dagger(s)\textsc{Shift}\ V(s)$ and Prop. 23,

$$V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle = \lambda_k(s)|v_k(s), \bar{0}\rangle + \sqrt{1-\lambda_k(s)^2}|v_k(s), \bar{0}\rangle^\perp \tag{208}$$

for some unit vector $|v_k(s), \bar{0}\rangle^\perp$ orthogonal to $|v_k(s), \bar{0}\rangle$ and lying in the subspace $\mathcal{B}_k(s)$. In particular, $\mathcal{B}_k(s)$ is two-dimensional. Note that $|v_k(s), \bar{0}\rangle^\perp$ depends on how the operator $V(s)$, defined in Eq. (194), is extended to the rest of the space $\mathcal{H} \otimes \mathcal{H}$.

Let us also find how $V^\dagger(s)\ \textsc{Shift}\ V(s)$ acts on $|v_k(s), \bar{0}\rangle^\perp$. If we apply $V^\dagger(s)$ $\textsc{Shift}\ V(s)$ to both sides of Eq. (208), we get

$$\begin{aligned}|v_k(s), \bar{0}\rangle = {} & \lambda_k(s) V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle \\ & + \sqrt{1-\lambda_k(s)^2} V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle^\perp.\end{aligned} \tag{209}$$

We regroup the terms and substitute Eq. (208):

$$\sqrt{1-\lambda_k(s)^2} V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle^\perp \tag{210}$$

$$= |v_k(s), \bar{0}\rangle - \lambda_k(s) V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle \tag{211}$$

$$= |v_k(s), \bar{0}\rangle - \lambda_k(s)\Big(\lambda_k(s)|v_k(s), \bar{0}\rangle + \sqrt{1-\lambda_k(s)^2}|v_k(s), \bar{0}\rangle^\perp\Big). \tag{212}$$

After cancellation we get

$$V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle^\perp = \sqrt{1-\lambda_k(s)^2}|v_k(s), \bar{0}\rangle - \lambda_k(s)|v_k(s), \bar{0}\rangle^\perp. \tag{213}$$

Proposition 24 *Subspaces $\mathcal{B}_1(s), \ldots, \mathcal{B}_n(s)$, and $\mathcal{B}^\perp(s)$ are mutually orthogonal and invariant under $W(s)$ for all $s \in [0, 1]$.*

Proof Clearly, $\mathcal{B}^\perp(s)$ is orthogonal to the other subspaces. Vectors $|v_k(s), \bar{0}\rangle$ are also mutually orthogonal for $k \in \{1, \ldots, n\}$, since they form an orthonormal basis of $\mathcal{H} \otimes |\bar{0}\rangle$. Finally, note from Prop. 23 that

$$\langle v_j(s), \bar{0}| \cdot V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle = \langle v_j(s)|D(s)|v_k(s)\rangle = \delta_{jk}\lambda_k(s), \tag{214}$$

so $V^\dagger(s)\ \textsc{Shift}\ V(s)|v_k(s), \bar{0}\rangle$ is orthogonal to $|v_j(s), \bar{0}\rangle$ for any $j \neq k$. Thus all of the above subspaces are mutually orthogonal.

Let us show that these subspaces are invariant under $W(s)$. From the definition of $W(s)$ in Eq. (195) we see that it suffices to check the invariance of each subspace under $V^\dagger(s)\ \textsc{Shift}\ V(s)$ and Π_0 separately.

First, let us argue the invariance under $V^\dagger(s)\,\textsc{Shift}\,V(s)$. Since $\textsc{Shift}^2$ acts as identity according to Eq. (2), then so does $V^\dagger(s)\,\textsc{Shift}\,V(s)$ and hence $\mathcal{B}_k(s)$ is invariant under $V^\dagger(s)\,\textsc{Shift}\,V(s)$ for any $k < n$. Next, $\mathcal{B}_n(s)$ is invariant, since $V^\dagger(s)\,\textsc{Shift}\,V(s)$ acts trivially on $|v_n(s), \bar{0}\rangle$ by Prop. 23. Finally, $\mathcal{B}^\perp(s)$ is invariant, since it is the orthogonal complement of invariant subspaces.

Let us now show the invariance under Π_0. First, let us argue that

$$\langle v_j(s), \bar{0}|v_k(s), \bar{0}\rangle^\perp = 0, \quad \forall j \in \{1, \ldots, n\}. \tag{215}$$

These vectors lie in subspaces $\mathcal{B}_j(s)$ and $\mathcal{B}_k(s)$ that are mutually orthogonal when $j \neq k$. For $j = k$ this holds by definition of $|v_k(s), \bar{0}\rangle^\perp$. Since $\text{span}\{|v_k(s), \bar{0}\rangle\}_{k=1}^n = \mathcal{H} \otimes |\bar{0}\rangle$, we conclude that

$$\Pi_0|v_k(s), \bar{0}\rangle^\perp = 0. \tag{216}$$

From Eq. (208) we get

$$\Pi_0 V^\dagger(s)\,\textsc{Shift}\,V(s)|v_k(s), \bar{0}\rangle = \lambda_k(s)|v_k(s), \bar{0}\rangle, \tag{217}$$

hence $\mathcal{B}_k(s)$ is invariant under Π_0 for $k < n$. Next, $\mathcal{B}_n(s)$ is invariant since $\Pi_0|v_n(s), \bar{0}\rangle = |v_n(s), \bar{0}\rangle$. Finally, $\mathcal{B}^\perp(s)$ is invariant by being the orthogonal complement of invariant subspaces. □

We now prove Lemma 2 by Szegedy [10], which provides the spectral decomposition of $W(s)$ in terms of that of $D(s)$. Note that we can guarantee that all eigenvalues of $D(s)$ are in $[0, 1]$ via Prop. 20.

Lemma 2 (Szegedy [10]) *Let $\mathcal{B}_k(s)$ for $k = 1, \ldots, n$ be the subspaces from Definition 11. Assume that all eigenvalues $\lambda_k(s)$ of $D(s)$ are between 0 and 1, and let $\varphi_k(s) \in [0, \pi]$ be such that*

$$\lambda_k(s) = \cos\varphi_k(s). \tag{218}$$

Then $W(s)$ has the following eigenvalues and eigenvectors.

$$\text{On } \mathcal{B}_k(s): \quad e^{\pm i\varphi_k(s)}, \quad |\Psi_k^\pm(s)\rangle := \frac{|v_k(s), \bar{0}\rangle \pm i|v_k(s), \bar{0}\rangle^\perp}{\sqrt{2}}. \tag{219}$$

$$\text{On } \mathcal{B}_n(s): \quad 1, \quad |\Psi_n(s)\rangle := |v_n(s), \bar{0}\rangle. \tag{220}$$

In particular, $\bigcup_{k=1}^n \mathcal{B}_k(s)$ is the walk space of $W(s)$ and the remaining eigenvectors of $W(s)$ lie in the orthogonal complement $\mathcal{B}^\perp(s)$.

Proof Recall Eqs. (208) and (213):

$$V^\dagger(s)\,\textsc{Shift}\,V(s) \cdot |v_k(s), \bar{0}\rangle = \lambda_k(s)|v_k(s), \bar{0}\rangle + \sqrt{1-\lambda_k(s)^2}|v_k(s), \bar{0}\rangle^\perp, \tag{221}$$

$$V^\dagger(s)\,\textsc{Shift}\,V(s) \cdot |v_k(s), \bar{0}\rangle^\perp = \sqrt{1-\lambda_k(s)^2}|v_k(s), \bar{0}\rangle - \lambda_k(s)|v_k(s), \bar{0}\rangle^\perp. \tag{222}$$

Clearly, $\text{ref}_{\mathcal{X}}|v_k(s), \bar{0}\rangle = |v_k(s), \bar{0}\rangle$ from Eq. (4). Recall from Eq. (216) that $\Pi_0|v_k(s), \bar{0}\rangle^\perp = 0$, so $\text{ref}_{\mathcal{X}}|v_k(s), \bar{0}\rangle^\perp = -|v_k(s), \bar{0}\rangle^\perp$. Thus, Eqs. (221) and (222) give us

$$W(s)\cdot|v_k(s),\bar{0}\rangle = \lambda_k(s)|v_k(s),\bar{0}\rangle + \sqrt{1-\lambda_k(s)^2}|v_k(s),\bar{0}\rangle^{\perp}, \tag{223}$$

$$W(s)\cdot|v_k(s),\bar{0}\rangle^{\perp} = -\sqrt{1-\lambda_k(s)^2}|v_k(s),\bar{0}\rangle + \lambda_k(s)|v_k(s),\bar{0}\rangle^{\perp}. \tag{224}$$

Recall from Prop. 24 that subspaces $\mathcal{B}_k(s)$ are mutually orthogonal and invariant under $W(s)$. In fact, $W(s)$ acts in the basis $\{|v_k(s),\bar{0}\rangle, |v_k(s),\bar{0}\rangle^{\perp}\}$ of $\mathcal{B}_k(s)$ as

$$\begin{pmatrix} \lambda_k(s) & -\sqrt{1-\lambda_k(s)^2} \\ \sqrt{1-\lambda_k(s)^2} & \lambda_k(s) \end{pmatrix} = \lambda_k(s) I + i\sqrt{1-\lambda_k(s)^2}\,\sigma_y \tag{225}$$

where $\sigma_y := \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$ is the Pauli y matrix. The matrix in Eq. (225) has the same eigenvectors as σ_y and its eigenvalues are given by

$$\lambda_k(s) \pm i\sqrt{1-\lambda_k(s)^2} = e^{\pm i\varphi_k(s)}. \tag{226}$$

This shows Eq. (219). To obtain Eq. (220), we use Prop. 23:

$$\langle v_n(s),\bar{0}|\cdot V^{\dagger}(s)\,\textsc{Shift}\,V(s)\cdot|v_n(s),\bar{0}\rangle = 1, \tag{227}$$

so $|v_n(s),\bar{0}\rangle$ is an eigenvector of $W(s)$ with eigenvalue 1. □

Appendix B.2: Quantum Circuit for $W(s)$

Recall that $\texttt{Update}(P)$ can be used to implement the quantum walk operator $W(P)$. However, we would also like to be able to implement the quantum analogue of $P(s)$ for any $s \in [0,1]$. Recall from Eq. (195) that it is given by

$$W(s) = V(s)^{\dagger}\,\textsc{Shift}\,V(s)\cdot \mathrm{ref}_{\mathcal{X}}. \tag{228}$$

We know how to implement Shift and $\mathrm{ref}_{\mathcal{X}}$, so we only need to understand how to implement $V(s)$ using $V(P)$. Recall from Eq. (3) that

$$V(s)|x\rangle|\bar{0}\rangle = |x\rangle|p_x(s)\rangle = |x\rangle\sum_{y\in X}\sqrt{P_{xy}(s)}|y\rangle. \tag{229}$$

In the following lemma, we assume that we know p_{xx} for every x. This is reasonable since in practice the probability of self-loops is known. In many cases, it is even independent of x. For the rest of this chapter, we assume that this is not an obstacle (we can assume that one call to $\texttt{Update}(P)$ allows to learn p_{xx} for any x).

Lemma 3 *Assuming that p_{xx} is known for every x, **Interpolation**(P, M, s) implements $V(s)$ with quantum complexity $2\mathsf{C}+\mathsf{U}$. Thus, $\texttt{Update}(P(s))$ has quantum complexity of order $\mathsf{C}+\mathsf{U}$.*

Proof We explain only how to implement $V(s)$ using one call to $V(P)$ and two calls to $\texttt{Check}(M)$. The algorithm for $V(s)^{\dagger}$ is obtained from the reverse algorithm.

Our algorithm uses four registers: R_1, R_2, R_3, R_4. The first two registers have underlying state space $\mathcal{H}$ each, but the last two store a qubit in $\mathbb{C}^2$ each. Register R_3 is used to store if the current vertex x is marked, but R_4 is used for performing rotations. Let

$$R_\alpha := \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \tag{230}$$

denote the rotation by angle α. An algorithm for implementing the transformation $|x\rangle|\bar{0}\rangle \mapsto |x\rangle|p_x(s)\rangle$ is given below.

Interpolation(P, M, s)

1. Let the initial state be $|x\rangle|\bar{0}\rangle|0\rangle|0\rangle$.
2. Apply `Check`(M) to $\mathsf{R}_1\mathsf{R}_3$ (then $\mathsf{R}_3 = 1$ if and only if $x \in M$).
3. If $\mathsf{R}_3 = 0$, apply $V(P)$ to $\mathsf{R}_1\mathsf{R}_2$ and get $|x\rangle|p_x\rangle|0\rangle|0\rangle$.
4. Otherwise:
   (a) The state is $|x\rangle|\bar{0}\rangle|1\rangle|0\rangle$ where $x \in M$.
   (b) Apply R_α with $\alpha = \arcsin\sqrt{s}$ on R_4: $|x\rangle|\bar{0}\rangle|1\rangle(\sqrt{1-s}|0\rangle + \sqrt{s}|1\rangle)$.
   (c) If $\mathsf{R}_4 = 0$, apply $V(P)$ on $\mathsf{R}_1\mathsf{R}_2$. Otherwise, use CNOT to copy R_1 to R_2 in the standard basis: $|x\rangle(\sqrt{1-s}|p_x\rangle|1\rangle|0\rangle + \sqrt{s}|x\rangle|1\rangle|1\rangle)$.
   (d) If $\mathsf{R}_1 = \mathsf{R}_2$, apply R_α with $\alpha = -\arcsin\sqrt{s/((1-s)P_{xx}+s)}$ to R_4. Otherwise, do nothing: $|x\rangle|p_x(s)\rangle|1\rangle|0\rangle$.
5. Apply `Check`(M) to $\mathsf{R}_1\mathsf{R}_3$ to uncompute R_3 and get $|x\rangle|p_x(s)\rangle|0\rangle|0\rangle$.

Recall from Eq. (98) that $P(s)$ has the following block structure:

$$P(s) = \begin{pmatrix} P_{UU} & P_{UM} \\ (1-s)P_{MU} & (1-s)P_{MM} + sI \end{pmatrix}. \tag{231}$$

We will analyze the cases $x \in M$ and $x \in U$ separately. Then the general case will hold by linearity.

If $x \in U$ then the corresponding row of $P(s)$ does not depend on s, so $|p_x(s)\rangle = |p_x\rangle$. In this case step 4 of the above algorithm is never executed and the remaining steps effectively apply $V(P)$ to produce the correct state.

When $x \in M$ the algorithm is more involved. Let us analyze only step 4 where most of the work is done. During this step the state gets transformed as follows:

$$|x\rangle|\bar{0}\rangle|1\rangle|0\rangle \mapsto |x\rangle|\bar{0}\rangle|1\rangle(\sqrt{1-s}|0\rangle + \sqrt{s}|1\rangle) \tag{232}$$

$$\mapsto |x\rangle\big(\sqrt{1-s}|p_x\rangle|1\rangle|0\rangle + \sqrt{s}|x\rangle|1\rangle|1\rangle\big) \tag{233}$$

$$\mapsto |x\rangle|p_x(s)\rangle|1\rangle|0\rangle. \tag{234}$$

The first two transformations are straightforward, so let us focus only on the last one which corresponds to step 4d. The state at the beginning of this step is

$$|x\rangle\big(\sqrt{1-s}|p_x\rangle|1\rangle|0\rangle + \sqrt{s}|x\rangle|1\rangle|1\rangle\big) \tag{235}$$

$$= |x\rangle\left[\sqrt{1-s}\sum_{y\in X\setminus\{x\}}\sqrt{P_{xy}}|y\rangle|1\rangle|0\rangle + |x\rangle|1\rangle\Big(\sqrt{(1-s)P_{xx}}|0\rangle + \sqrt{s}|1\rangle\Big)\right]. \tag{236}$$

Note from the second row of matrix $P(s)$ in Eq. (231) that all its elements have acquired a factor of $1-s$, except the diagonal ones. Thus in step 4d we perform a rotation only when $\mathsf{R}_1 = \mathsf{R}_2$. This rotation affects only the second half of the state in Eq. (236) and transfers all amplitude to $|0\rangle$ in the last register:

$$|x\rangle\left[\sqrt{1-s}\sum_{y\in X\setminus\{x\}}\sqrt{P_{xy}}|y\rangle + \sqrt{(1-s)P_{xx}+s}|x\rangle\right]|1\rangle|0\rangle = |x\rangle|p_x(s)\rangle|1\rangle|0\rangle. \tag{237}$$

Finally, step 5 uncomputes R_3 to $|0\rangle$ and the final state is $|x\rangle|p_x(s)\rangle|0\rangle|0\rangle$ as desired. □

Appendix C: An Explicit Formula for $\mathrm{HT}^+(P, M)$

Recall from Definition 9 that $\mathrm{HT}^+(P, M)$ is defined as the $s \to 1$ limit of $\mathrm{HT}(s)$. In this appendix we derive an alternative expression for $\mathrm{HT}^+(P, M)$. This formula explicitly expresses $\mathrm{HT}^+(P, M)$ in terms of the Markov chain P and its stationary distribution π, and makes it easier to evaluate this quantity and compare it to the regular hitting time $\mathrm{HT}(P, M)$.

Let us define unit vectors $|\tilde{U}\rangle \in \mathbb{R}^{|U|}$ and $|\tilde{M}\rangle \in \mathbb{R}^{|M|}$ as follows:

$$|\tilde{U}\rangle := \sqrt{\tilde{\pi}_U^{\mathsf{T}}}, \qquad |\tilde{M}\rangle := \sqrt{\tilde{\pi}_M^{\mathsf{T}}}, \tag{238}$$

where $\tilde{\pi}_U$ and $\tilde{\pi}_M$ are defined in Eq. (133) in terms of the stationary distribution $\pi = (\pi_U\ \pi_M)$ of P. Note from Eq. (134) that $|\tilde{U}\rangle$ and $|\tilde{M}\rangle$ are the restrictions of $|U\rangle$ and $|M\rangle$ to the unmarked and marked subspaces. Furthermore, let

$$\begin{pmatrix} D_{UU} & D_{UM} \\ D_{MU} & D_{MM} \end{pmatrix} := \begin{pmatrix} \sqrt{P_{UU} \circ P_{UU}^{\mathsf{T}}} & \sqrt{P_{UM} \circ P_{MU}^{\mathsf{T}}} \\ \sqrt{P_{MU} \circ P_{UM}^{\mathsf{T}}} & \sqrt{P_{MM} \circ P_{MM}^{\mathsf{T}}} \end{pmatrix} \tag{239}$$

be the blocks of the discriminant matrix $D(P)$ of P (see Definition 6).

Lemma 4 *If* $\mathrm{HT}(P, M)$ *is the hitting time of* P *(see Definition 4) and* $\mathrm{HT}^+(P, M)$ *is the extended hitting time (see Definition 9) then*

$$\mathrm{HT}(P, M) = \langle \tilde{U}|(I - D_{UU})^{-1}|\tilde{U}\rangle, \tag{240}$$

$$HT^{+}(P, M) = \langle \tilde{U}|(I - D_{UU} - S)^{-1}|\tilde{U}\rangle, \tag{241}$$

where

$$S := D_{UM}\left[(I - D_{MM})^{-1} - \frac{(I-D_{MM})^{-1}|\tilde{M}\rangle\langle\tilde{M}|(I - D_{MM})^{-1}}{\langle\tilde{M}|(I-D_{MM})^{-1}|\tilde{M}\rangle}\right]D_{MU}. \tag{242}$$

Vectors $|\tilde{U}\rangle$ *and* $|\tilde{M}\rangle$ *are defined in Eq.* (238) *and matrices* D_{UU}, D_{UM}, D_{MU}, D_{MM} *in Eq.* (239).

Proof Let us first derive Eq. (240). Recall from Eq. (243) that $\mathrm{HT}(P, M)$ can be written as

$$\mathrm{HT}(P, M) = \sum_{t=0}^{\infty}\langle U|D(1)^t|U\rangle, \tag{243}$$

where $D(1)$ is the discriminant matrix of $P(1) = P'$. Recall from Eq. (122) that

$$D(1) = \begin{pmatrix} \sqrt{P_{UU} \circ P_{UU}^{\mathsf{T}}} & 0 \\ 0 & I \end{pmatrix}. \tag{244}$$

Since $D(1)$ is block diagonal and $|U\rangle$ acts only on the unmarked states U, we can restrict each term in Eq. (245) to the unmarked subspace and bring the summation inside:

$$\mathrm{HT}(P, M) = \langle\tilde{U}|\sum_{t=0}^{\infty} D(1)_{UU}^t|\tilde{U}\rangle. \tag{245}$$

Recall from Eq. (146) that the UU block of $D(s)$ is independent of s, hence $D(1)_{UU} = D_{UU}$, the UU block of $D(0)$ given in Eq. (239). Recall from Prop. 10 that $I - P_{UU}$ is invertible. Furthermore, due to Prop. 9 we can write $(I - P_{UU})^{-1} = \sum_{t=0}^{\infty} P_{UU}^t$. As D_{UU} and P_{UU} are similar according to Eq. (123), $I - D_{UU}$ is also invertible and $(I - D_{UU})^{-1} = \sum_{t=0}^{\infty} D_{UU}^t$. If we substitute this in Eq. (245), we get Eq. (240) and thus prove the first half of the lemma.

For the second half, recall from Eq. (16) that for $s \in [0, 1)$,

$$\mathrm{HT}(s) = \sum_{k=1}^{n-1}\frac{|\langle v_k(s)|U\rangle|^2}{1 - \lambda_k(s)}, \tag{246}$$

where $\lambda_k(s)$ and $|v_k(s)\rangle$ are the eigenvalues and eigenvectors of the discriminant matrix $D(s)$. By Prop. 15, for any $s \in [0, 1)$, $\lambda_n(s) = 1$ and $\lambda_k(s) < 1$ for all $k \neq n$. Let $\Pi_n(s) := |v_n(s)\rangle\langle v_n(s)|$, where $|v_n(s)\rangle$ is given by Prop. 4:

$$|v_n(s)\rangle = \cos\theta(s)|U\rangle + \sin\theta(s)|M\rangle. \tag{247}$$

With this in mind, we can rewrite Eq. (246) as follows:

$$\mathrm{HT}(s) = \langle U| \left[\sum_{k=1}^{n-1} \sum_{t=0}^{\infty} \lambda_k^t(s) |v_k(s)\rangle\langle v_k(s)| \right] |U\rangle \tag{248}$$

$$= \langle U| \sum_{t=0}^{\infty} \big(D^t(s) - \Pi_n(s)\big) |U\rangle \tag{249}$$

$$= \langle U| \left[I + \sum_{t=1}^{\infty} \big(D(s) - \Pi_n(s)\big)^t - \Pi_n(s) \right] |U\rangle \tag{250}$$

$$= \langle U| \Big[\big(I - D(s) + \Pi_n(s)\big)^{-1} - \Pi_n(s) \Big] |U\rangle \tag{251}$$

$$= \langle U| \big(I - D(s) + \Pi_n(s)\big)^{-1} |U\rangle - \cos^2\theta(s), \tag{252}$$

where the last equality follows from Eq. (247).

Our goal is to compute $\lim_{s\to 1} \mathrm{HT}(s)$. Recall from Prop. 15 that $D(1)$ has eigenvalue 1 with multiplicity $|M|$. Thus, if $|M| > 1$, the matrix $I - D(s) + \Pi_n(s)$ in Eq. (252) is not invertible at $s = 1$, hence we cannot compute the limit by simply substituting $s = 1$. Let us rewrite this expression before we take the limit.

Note that the discriminant matrix $D(s)$ at $s = 0$ agrees with $D(P)$. Using Eq. (146) that relates $D(s)$ and $D(P)$, we can write

$$I - D(s) = \begin{pmatrix} I - D_{UU} & -\sqrt{1-s}\, D_{UM} \\ -\sqrt{1-s}\, D_{MU} & (1-s)(I - D_{MM}) \end{pmatrix}, \tag{253}$$

where $\left(\begin{smallmatrix} D_{UU} & D_{UM} \\ D_{MU} & D_{MM} \end{smallmatrix}\right)$ are the blocks of $D(P)$ given in Eq. (239). Next, note that

$$|v_n(s)\rangle = \begin{pmatrix} \cos\theta(s) |\tilde{U}\rangle \\ \sin\theta(s) |\tilde{M}\rangle \end{pmatrix}, \tag{254}$$

so we can write

$$\Pi_n(s) = \begin{pmatrix} \cos^2\theta(s) |\tilde{U}\rangle\langle\tilde{U}| & \cos\theta(s)\sin\theta(s) |\tilde{U}\rangle\langle\tilde{M}| \\ \cos\theta(s)\sin\theta(s) |\tilde{M}\rangle\langle\tilde{U}| & \sin^2\theta(s) |\tilde{M}\rangle\langle\tilde{M}| \end{pmatrix}. \tag{255}$$

Putting the two equations together, we can write $I - D(s) + \Pi_n(s)$ as

$$\begin{pmatrix} I - D_{UU} + \cos^2\theta(s) |\tilde{U}\rangle\langle\tilde{U}| & -\sqrt{1-s}\, D_{UM} + \cos\theta(s)\sin\theta(s) |\tilde{U}\rangle\langle\tilde{M}| \\ -\sqrt{1-s}\, D_{MU} + \cos\theta(s)\sin\theta(s) |\tilde{M}\rangle\langle\tilde{U}| & (1-s)(I - D_{MM}) + \sin^2\theta(s) |\tilde{M}\rangle\langle\tilde{M}| \end{pmatrix}. \tag{256}$$

In Eq. (252) we need only the upper left block of the inverse of the above matrix, since $|U\rangle$ is non-zero only on the U block. According to the block-wise inversion formula,

$$\begin{pmatrix} A & B \\ B^{\mathsf{T}} & C \end{pmatrix}^{-1} = \begin{pmatrix} (A - BC^{-1}B^{\mathsf{T}})^{-1} & \dots \\ \dots & \dots \end{pmatrix}. \tag{257}$$

Thus, Eq. (252) becomes

$$\mathrm{HT}(s) = \langle \tilde{U}| \big(A(s) - B(s)C(s)^{-1}B(s)^{\mathsf{T}}\big)^{-1} |\tilde{U}\rangle - \cos^2\theta(s), \tag{258}$$

where $A(s)$, $B(s)$, and $C(s)$ are the blocks in Eq. (256). We can further rewrite this as follows:

$$\mathrm{HT}(s) = \langle \tilde{U}| \left[A(s) - \frac{B(s)}{\sqrt{1-s}} \left(\frac{C(s)}{1-s}\right)^{-1} \frac{B(s)^{\mathsf{T}}}{\sqrt{1-s}} \right]^{-1} |\tilde{U}\rangle - \cos^2\theta(s), \tag{259}$$

where the extra factors will allows us to deal with the fact that $C(1)$ is singular.

Now we can compute $\lim_{s\to 1} \mathrm{HT}(s)$ for each piece of Eq. (259) separately. Note from Eq. (21) that $\cos^2\theta(s)$ vanishes as $s \to 1$. Similarly, we also get that

$$A' := \lim_{s\to 1} A(s) = I - D_{UU}, \tag{260}$$

$$B' := \lim_{s\to 1} \frac{B(s)}{\sqrt{1-s}} = -D_{UM} + \sqrt{\frac{1-p_M}{p_M}} |\tilde{U}\rangle\langle\tilde{M}|. \tag{261}$$

Finally, notice that $\lim_{s\to 1} C(s)/(1-s)$ does not exist. Nevertheless, the limit of the inverse exists (in particular, it is a singular matrix) and we can compute it using the Sherman–Morrison formula:

$$\big(X + |\psi\rangle\langle\psi|\big)^{-1} = X^{-1} - \frac{X^{-1}|\psi\rangle\langle\psi|X^{-1}}{1 + \langle\psi|X^{-1}|\psi\rangle}. \tag{262}$$

For $s < 1$, we get

$$\left(\frac{C(s)}{1-s}\right)^{-1} = \left(I - D_{MM} + \frac{\sin^2\theta(s)}{1-s} |\tilde{M}\rangle\langle\tilde{M}|\right)^{-1} \tag{263}$$

$$= (I - D_{MM})^{-1} - \frac{(I - D_{MM})^{-1}|\tilde{M}\rangle\langle\tilde{M}|(I - D_{MM})^{-1}}{\frac{1-s}{\sin^2\theta(s)} + \langle\tilde{M}|(I - D_{MM})^{-1}|\tilde{M}\rangle}, \tag{264}$$

so the limit is

$$C' := \lim_{s\to 1} \left(\frac{C(s)}{1-s}\right)^{-1} = (I - D_{MM})^{-1} - \frac{(I - D_{MM})^{-1}|\tilde{M}\rangle\langle\tilde{M}|(I - D_{MM})^{-1}}{\langle\tilde{M}|(I - D_{MM})^{-1}|\tilde{M}\rangle}. \tag{265}$$

Let $S(s) := B(s)C(s)^{-1}B(s)^{\mathsf{T}}$ be the matrix that appears in Eq. (258). Since it also appears in Eq. (259), we find that

$$S' := \lim_{s\to 1} S(s) = B'C'B'^{\mathsf{T}} \tag{266}$$

by substituting B' and C' from Eqs. (261) and (265), respectively. Note from Eq. (265) that $C'|\tilde{M}\rangle = 0$, so Eq. (266) simplifies to

$$S' = D_{UM} C' D_{MU} \tag{267}$$

after we substitute B' from Eq. (261). Note that S' agrees with Eq. (242) and that

$$\mathrm{HT}^+(P, M) = \lim_{s \to 1} \mathrm{HT}(s) = \langle \tilde{U}|(A' - S')^{-1}|\tilde{U}\rangle, \tag{268}$$

where A' and S' are given in Eqs. (260) and (267), respectively. □

References

1. Ambainis, A.: Quantum walk algorithm for element distinctness. SIAM J. Comput. **37**(1), 210–239 (2007)
2. Magniez, F., Santha, M., Szegedy, M.: Quantum algorithms for the triangle problem. SIAM J. Comput. **37**(2), 413–424 (2007)
3. Buhrman, H., Špalek, R: Quantum verification of matrix products. In: Proceedings of the 17th ACM-SIAM symposium on discrete algorithms (SODA'06), pp. 880–889. ACM (2006)
4. Magniez, F., Nayak, A.: Quantum complexity of testing group commutativity. Algorithmica **48**(3), 221–232 (2007)
5. Aaronson, S., Ambainis, A.: Quantum search of spatial regions. Theory Comput. **1**(4), 47–79 (2005)
6. Shenvi, N., Kempe, J., Whaley, B.K.: Quantum random-walk search algorithm. Phys. Rev. A **67**(5), 052307 (2003)
7. Childs, A.M., Goldstone, J.: Spatial search and the Dirac equation. Phys. Rev. A **70**(4), 042312 (2004)
8. Ambainis, A., Kempe, J., Rivosh, A.: Coins make quantum walks faster. In: Proceedings of the 16th ACM-SIAM symposium on discrete algorithms (SODA'05), pp. 1099–1108. SIAM (2005)
9. Kempe, J.: Discrete quantum walks hit exponentially faster. Probab. Theory Relat. Fields **133**(2), 215–235 (2005)
10. Szegedy, M.: Quantum speed-up of Markov chain based algorithms. In: Proceedings of the 45th IEEE symposium on foundations of computer science (FOCS'04), pp. 32–41. IEEE Computer Society Press (2004)
11. Krovi, H., Brun, T.A.: Hitting time for quantum walks on the hypercube. Phys. Rev. A **73**(3), 032341 (2006)
12. Magniez, F., Nayak, A., Roland, J., Santha, M.: Search via quantum walk. In: Proceedings of the 39th ACM symposium on theory of computing (STOC'07), pp. 575–584. ACM Press (2007)
13. Magniez, F., Nayak, A., Richter, P., Santha, M.: On the hitting times of quantum versus random walks. Algorithmica **63**(1), 91–116 (2012)
14. Varbanov, M., Krovi, H., Brun, T.A.: Hitting time for the continuous quantum walk. Phys. Rev. A **78**(2), 022324 (2008)
15. Tulsi, A.: Faster quantum-walk algorithm for the two-dimensional spatial search. Phys. Rev. A **78**(1), 012310 (2008)
16. Krovi, H., Magniez, F., Ozols, M., Roland, J.: Finding is as easy as detecting for quantum walks. In: Automata, Languages and Programming, Lecture Notes in Computer Science, vol. 6198, pp. 540–551. Springer, Berlin-Heidelberg (2010)
17. Childs, A.M., Goldstone, J.: Spatial search by quantum walk. Phys. Rev. A **70**(2), 022314 (2004)
18. Ambainis, A., Bačkurs, A., Nahimovs, N., Ozols, R., Rivosh, A.: Lecture Notes in Computer Science, vol. 7582. Springer, Berlin (2013)
19. Krovi, H., Ozols, M., Roland, J.: Adiabatic condition and the quantum hitting time of Markov chains. Phys. Rev. A **82**(2), 022333 (2010)
20. Grinstead, C.M., Snell, J.L.: Introduction to Probability, 2nd edn. American Mathematical Society, Providence (1997)

21. Kemeny, J.G., Snell, J.L.: Finite Markov Chains. Undergraduate Texts in Mathematics. Springer, Berlin (1960)
22. Koralov, L.B., Sinai, Y.G.: Theory of Probability and Random Processes. Springer, Berlin (2007)
23. Levin, D.A., Peres, Y., Wilmer, E.L.: Markov Chains and Mixing Times. American Mathematical Society, Providence (2009)
24. Horn, R.A., Johnson, C.R.: Matrix Analysis. Cambridge University Press, Cambridge (1990)
25. Meyer, C.D.: Matrix Analysis and Applied Linear Algebra, vol. 1. SIAM (Society for Industrial and Applied Mathematics), Philadelphia (2000)
26. Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Quantum algorithms revisited. Proc. R. Soc. Lond. **454**(1969), 339–354 (1998)
27. Høyer, P., Mosca, M., de Wolf, R.: Quantum search on bounded-error inputs. In: Proceedings of the 30th international colloquium on automata, languages and programming (ICALP'03), volume 2719 of lecture notes in computer science, pp. 291–299. Springer (2003)
28. Feige, U., Raghavan, P., Peleg, D., Upfal, E.: Computing with noisy information. SIAM J. Comput. **23**(5), 1001–1018 (1994)
29. Farhi, E., Goldstone, J., Gutmann, S., Lapan, J., Lundgren, A., Preda, D.: A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. Science **292**(5516), 472–475 (2001)