Coins Make Quantum Walks Faster

Andris Ambainis
School of Mathematics,
Institute for Advanced Study,
Princeton, NJ 08540
ambainis@ias.edu

Julia Kempe
CNRS-LRI UMR 8623
Université de Paris-Sud
91405 Orsay, France
and UC Berkeley, Berkeley, CA 94720
kempe@lri.fr

Alexander Rivosh
Institute of Mathematics and Computer Science
University of Latvia
Raina bulv.29, Riga, LV-1459, Latvia
vbug@solutions.lv

May 26, 2006

Abstract

We show how to search N items arranged on a $\sqrt{N} \times \sqrt{N}$ grid in time $O(\sqrt{N} \log N)$, using a discrete time quantum walk. This result for the first time exhibits a significant difference between discrete time and continuous time walks without coin degrees of freedom, since it has been shown recently that such a continuous time walk needs time $\Omega(N)$ to perform the same task. Our result furthermore improves on a previous bound for quantum local search by Aaronson and Ambainis. We generalize our result to 3 and more dimensions where the walk yields the optimal performance of $O(\sqrt{N})$ and give several extensions of quantum walk search algorithms for general graphs. The coin-flip operation needs to be chosen judiciously: we show that another "natural" choice of coin gives a walk that takes $\Omega(N)$ steps. We also show that in 2 dimensions it is sufficient to have a two-dimensional coin-space to achieve the time $O(\sqrt{N} \log N)$.

1 Introduction

Quantum walks are quantum counterparts of classical random walks. Classical random walks have many applications in randomized algorithms [MR95] and we hope that quantum walks would have similar applications in quantum algorithms. Both discrete-time [Mey96, AAKV01, ABN$^+$01] and continous time [FG98, CFG02] quantum walks have been introduced[1]. The definitions of the two are quite different. In continous time, one can directly define the walk on the vertices of the graph. In discrete time, it is necessary to introduce an extra "coin" register storing the direction in which the walk is moving.

Because of this difference in the definitions, it has been open what the relation between discrete and continous walk is. In the classical world, the continous walk is the limit of the discrete walk

[1]For an introduction to quantum walks see [Kem03a].

when the length of the time step approaches 0. In the quantum case, this is no longer true. Even if we make the time-steps of the discrete walk smaller and smaller, the "coin" register remains. Therefore, the limit cannot be the continous walk without the "coin" register. This means that one variant of quantum walks could be more powerful than the other in some context, but so far all known examples have given similar behavior of the two walks (see e.g. [CFG02, Kem03b, CCD$^+$03]).

In this paper, we present the first example where the discrete walk (with "coin") outperforms the continous walk (with no "coin"). Our example is the spatial search [Ben02, AA03] variant of Grover's search problem. In the usual Grover's search problem [Gro96], we have N items, one of which is marked. Then, we can find the marked item in $O(\sqrt{N})$ quantum steps, with one quantum step querying a superposition of items. In contrast, classically $\Omega(N)$ queries are required. In the "spatial search" variant, we have the extra constraint that the N items are stored in N different memory locations and we need time to move betwen locations. This may increase the running time of a quantum algorithm.

The first "spatial" version of Grover's algorithms with optimal performance was given by [SKW03] who showed how to search N items arranged on the n-dimensional hypercube, using a discrete quantum walk.

In this paper, we consider the 2-dimensional arrangement where N memory locations are arranged in an $\sqrt{N} \times \sqrt{N}$ grid. This was first studied by Benioff [Ben02] who observed that the usual Grover's search algorithm takes $\Omega(N)$ steps. It uses $\Theta(\sqrt{N})$ query steps but, between each two queries, it might move a distance of $\Theta(\sqrt{N})$. Thus, the total time becomes $\Theta(N)$ and the quantum speedup disappears. Aaronson and Ambainis [AA03] fixed this problem by giving an algorithm for searching the 2-dimensional grid in $O(\sqrt{N}\log^2 N)$ total steps[2] (counting both queries and moving steps) and the 3-dimensional grid in $O(\sqrt{N})$ steps, using Grover's algorithm together with multi-level recursion. Quantum walks were first applied to this problem by Childs and Goldstone [CG03] who studied the search on the grid by a continous quantum walk. They discovered that the continous walk provides an alternative search algorithm with optimal performance of $O(\sqrt{N})$ in 5 and more dimensions, but not in 2 or 3 dimensions, where the continuous walk takes $\Omega(N)$ and $\Omega(N^{5/6})$, respectively. In 4 dimensions the continuous time walk algorithm performs as $O(\sqrt{N}\log N)$.

In this paper, we use discrete-time quantum walks to design an algorithm that searches the grid in $O(\sqrt{N}\log N)$ time in 2 dimensions and $O(\sqrt{N})$ time in 3 and more dimensions. Thus, our algorithm is faster than both the non-walk quantum algorithm of [AA03] and the algorithm based on the continous time quantum walk [CG03]. In addition to having a very simple structure our algorithm also uses only 1 or 2 qubits of extra memory (or $log2d$ qubits for the d-dimensional grid), besides the current location. (The previous algorithm of [AA03] uses $O(\log^c n)$ qubits of extra memory.)

Besides improving the running time, we present several interesting features of quantum walks. The first feature is that the discrete-time walk succeeds while the continous walk does not. Secondly, the behavior of the discrete quantum walk on the grid crucially depends on the choice of the "coin"

[2]The running times for the 2-dimensional grid are for the case when the grid contains one marked item. The general case (an arbitrary number of marked items) can be reduced to the one item case with a $\log N$ increase of the running time [AA03]. That would result in a running time of $O(\sqrt{N}\log^3 N)$ for the algorithm of [AA03] and $O(\sqrt{N}\log^2 N)$ for our algorithm which we present in this paper. For 3 and higher dimensions, the general case can be reduced to the one item case with just a constant factor increase [AA03]. Thus, the asymptotic running times stay the same.

transformation. One natural choice, discovered numerically by Neil Shenvi [She03], leads to our algorithm while some other natural choices fail to produce a good algorithm. Thus, the "coin" transformation could be a resource which affects the algorithm profoundly. We give both upper and lower bounds for the performance of some natural choices of the "coin". Surprisingly we show that in the case of the 2-dimensional grid only 2 (and not the standard 4) coin-degrees of freedom are sufficient to achieve the quantum speed-up. The insights gained from our study might aid in the design of future discrete quantum walk based algorithms. Several such algorithms have recently been discovered [CCD$^+$03, Amb03, MSS03, CE03, Sze04].

Our presentation allows a fairly general approach to quantum walk search algorithms on graphs. In particular it simplifies the proof of [SKW03], where the relevant eigenvectors had to be "guessed". We also give a discrete walk search algorithm on the complete graph and show its equivalence to Grover's algorithm and outline several generalizations of our results.

2 Preliminaries and Notation

2.1 Model

Our model is similar to the one in [AA03]. We have an *undirected graph* $G = (V, E)$. Each vertex v stores a variable $a_v \in \{0, 1\}$. Our goal is to find a vertex v for which $a_v = 1$ (assuming such vertex exists). We will often call such vertices marked and vertices for which $a_v = 0$ unmarked.

In one step, an algorithm can examine the current vertex or move to a neighboring vertex in the graph G. The goal is to find a marked vertex in as few steps as possible.

More formally, a quantum algorithm is a sequence of unitary transformations on a Hilbert space $\mathcal{H}_i \otimes \mathcal{H}_V$. $\mathcal{H}_V$ is a Hilbert space spanned by states $|v\rangle$ corresponding to vertices of G. $\mathcal{H}_i$ represents the algorithm's internal state and can be of arbitrary fixed dimension. A t-step quantum algorithm is a sequence U_1, U_2, ..., U_t where each U_i is either a *query* or a *local transformation*. A query U_i consists of two transformations (U_i^0, U_i^1). $U_i^0 \otimes I$ is applied to all $\mathcal{H}_i \otimes |v\rangle$ for which $a_v = 0$ and $U_i^1 \otimes I$ is applied to all $\mathcal{H}_i \otimes |v\rangle$ for which $a_v = 1$.

A local transformation can be defined in several ways [AA03]. In this paper, we require them to be Z-local. A transformation U_i is Z-local if, for any $v \in V$ and $|\psi\rangle \in \mathcal{H}_i$, the state $U_i(|\psi\rangle \otimes |v\rangle)$ is contained in the subspace $\mathcal{H}_i \otimes \mathcal{H}_{\Gamma(v)}$ where $\mathcal{H}_{\Gamma(v)} \subset \mathcal{H}_V$ is spanned by the state $|v\rangle$ and the states $|v'\rangle$ for all v' adjacent to v. Our results also apply if the local transformations are C-local (another locality definition introduced in [AA03]).

The algorithm starts in a fixed starting state $|\psi_{start}\rangle$ and applies U_1, ..., U_t. This results in a final state $|\psi_{final}\rangle = U_t U_{t-1} \dots U_1 |\psi_{start}\rangle$. Then, we measure $|\psi_{start}\rangle$. The algorithm succeeds if measuring the $\mathcal{H}_V$ part of the final state gives $|g\rangle$ such that $a_g = 1$.

For more details on this model, see [AA03].

2.2 Search by quantum walk

In what follows we will assume that G is *undirected* and *d-regular*, i.e. has constant degree d. To each vertex we can associate a labeling $\{1, \dots, d\}$ of the d edges (directions) adjacent to it and an auxiliary "coin"-Hilbert space $\mathcal{H}_d = \{|1\rangle, \dots, |d\rangle\}$. Let $\mathcal{H}_N$ be the Hilbert space spanned by the vertices of the graph, then the walk takes place in the joint space of coin and graph $\mathcal{H} = \mathcal{H}_d \otimes \mathcal{H}_N$.

Definition 1 *[Discrete Quantum Walk on G:] The discrete quantum walk is an alternation of coin flip and moving step: $U = S \cdot C$, where S is a shift controlled by the coin register*

$$S : |i\rangle \otimes |x\rangle \longrightarrow |\pi(i)\rangle \otimes |\tilde{x}\rangle \tag{1}$$

$i = 1, \ldots, d$ and $x, \tilde{x} \in V$, x and $\tilde{x}$ are connected by the edge labelled "i" on x's side and π is a permutation of the d basis states of the coin space $\mathcal{H}_d$, and the coin $C = C_0 \otimes I_N$ where I_N acts as identity on $\mathcal{H}_N$ and C_0 is a "coin-flip" acting on $\mathcal{H}_d$

$$C_0 = 2|s\rangle\langle s| - I_d \quad \texttt{where} \quad |s\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle. \tag{2}$$

For a given i S permutes the vertices of the graph, hence S is a unitary operation. The permutation π allows us to specify shift operations that act differently on the coin space $\mathcal{H}_d$. Note that the coin is *symmetric* in that it treats all d directions equally, and among all such coins C_0 is the one farthest away from identity.

Remark: The uniform superposition $|\Phi_0\rangle = \frac{1}{\sqrt{dN}} \sum_{i=1}^{d} \sum_{x=1}^{N} |i\rangle \otimes |x\rangle$ is an eigenvector of U with eigenvalue 1 ($U|\Phi_0\rangle = |\Phi_0\rangle$); if we start the walk in $|\Phi_0\rangle$ it will never change this state.

To introduce a marked item in the graph we need to have an inhomogeneity in the quantum walk by using the coin to "mark" a vertex v, which gives rise to the following:

Definition 2 *[Perturbed Quantum Walk:] The perturbed walk with marked vertex v and "marking coin" $C_1 = -I_d$ is $U' = S \cdot C'$, where*

$$C' = C_0 \otimes (I - |v\rangle\langle v|) + C_1 \otimes |v\rangle\langle v| = C - (C_0 - C_1) \otimes |v\rangle\langle v|. \tag{3}$$

We will think of U' as the random walk with one (or several) marked coins. This means that instead of one coin for all nodes, $C_0 \otimes I$, we have a different coin C_1 on the marked state. Numerical data shows that other marked coins exhibit similar properties as $C_1 = -I$, but we will use this coin which simplifies the analysis. Then $C_0 - C_1 = 2|s\rangle\langle s|$, and $U' = U - 2S|s, v\rangle\langle s, v| = U \cdot (I_{dN} - 2|s, v\rangle\langle s, v|)$ using $C_0|s\rangle = |s\rangle$.

The quantum walk U gives rise to a search algorithm on a graph G in the following way:

Quantum Walk Search Algorithm

1. Initialise the quantum system in the uniform superposition $|\Phi_0\rangle$.
2. Do T times: Apply the marked walk U'.
3. Measure the position register.
4. Check if the measured vertex is the marked item.

An item on a vertex of the graph could be marked by setting an auxiliary qubit to $|1\rangle$, whereas the unmarked items could have this qubit set to $|0\rangle$. Then this auxiliary qubit can control the coin to be C for the unmarked items and C' for the marked item.

We will analyse this algorithm to obtain upper bounds on the query complexity of search by random walks.

Complete Graph - Grover's Algorithm: As a first example let us illustrate how we can view Grover's algorithm [Gro96] as a random walk search algorithm on the complete graph. Each vertex has N edges (we will include a self-loop for each vertex). Both vertices and edges are labelled with $1, \ldots, N$; the coin space and the vertex Hilbert space are both N-dimensional and we will write states as $|i\rangle \otimes |j\rangle$, where the first register is the coin-register. The shift operation S is defined as

$$S : |i\rangle \otimes |j\rangle \longrightarrow |j\rangle \otimes |i\rangle.$$

The marked coin in this case is chosen to be $C_1 = -C_0$, which gives $C_1 - C_0 = -2C_0$ and $C' = C_0 \otimes (I - 2|v\rangle\langle v|)$, where $|v\rangle$ is the marked state. Note that $C_0 = 2|s\rangle\langle s| - 1_N$ is the reflection around the mean operator of Grover's ("standard") algorithms and $I - 2|v\rangle\langle v| =: R_v$ the phase flip of the oracle. Recall that Grover's algorithm is of the form $(R_v \cdot C_0)^T |s\rangle$. The initial state for the random walk based algorithm is the uniform superposition $|\Phi_0\rangle = |s\rangle \otimes |s\rangle$. Now $U'|\Phi_0\rangle = S \cdot C'|\Phi_0\rangle = R_v|s\rangle \otimes C_0|s\rangle$, $C' \cdot U'|\Phi_0\rangle = (C_0 \cdot R_v)|s\rangle \otimes (R_v \cdot C_0)|s\rangle$ and $U'^2|\Phi_0\rangle = (R_v \cdot C_0)|s\rangle \otimes (C_0 \cdot R_v)|s\rangle$. So we see that a random walk in this scenario gives exactly Grovers algorithm on both the coin space and the vertex space, at the expense of a factor of 2 in the number of applications.

3 Results in 2 dimensions

We give several upper and lower bounds for the discrete quantum walk on the grid. The N memory locations are arranged in a $\sqrt{N} \times \sqrt{N}$ grid G, labeled by their x and y coordinate as $|x, y\rangle$ for $x, y \in \{0, \ldots, \sqrt{N} - 1\}$. will assume periodic boundary conditions and operate mod $\sqrt{N}$. The natural coin space is 4-dimensional. We will label the edges emanating from each vertex with $\rightarrow, \leftarrow, \uparrow, \downarrow$, indicating the positive and negative x and y directions.

As it turns out, the choice of the coin transformation (or, equivalently, of the permutation π in Eq. (1)) is crucial for the performance of the random walk. We will show that using a "flip-flop" shift, gives a search algorithm that succeeds in $O(\sqrt{N} \log N)$ time. The "flip-flop" shift S_{ff} changes direction after every move, i.e. π flips $\uparrow$ with $\downarrow$ and $\rightarrow$ with $\leftarrow$. Our analysis of the "flip-flop" based walk follows the numerical discovery of its performance by Neil Shenvi [She03]. Another natural shift is the "moving" shift S_m which does not change direction (i.e. in Eq. (1) $\pi = id$ and $|\pi(i)\rangle = |i\rangle$).

$$\begin{array}{rl} S_{ff} : & |\rightarrow\rangle \otimes |x, y\rangle \longrightarrow |\leftarrow\rangle \otimes |x+1, y\rangle \\ & |\leftarrow\rangle \otimes |x, y\rangle \longrightarrow |\rightarrow\rangle \otimes |x-1, y\rangle \\ & |\uparrow\rangle \otimes |x, y\rangle \longrightarrow |\downarrow\rangle \otimes |x, y+1\rangle \\ & |\downarrow\rangle \otimes |x, y\rangle \longrightarrow |\uparrow\rangle \otimes |x, y-1\rangle \end{array} \qquad \begin{array}{rl} S_m : & |\rightarrow\rangle \otimes |x, y\rangle \longrightarrow |\rightarrow\rangle \otimes |x+1, y\rangle \\ & |\leftarrow\rangle \otimes |x, y\rangle \longrightarrow |\leftarrow\rangle \otimes |x-1, y\rangle \\ & |\uparrow\rangle \otimes |x, y\rangle \longrightarrow |\uparrow\rangle \otimes |x, y+1\rangle \\ & |\downarrow\rangle \otimes |x, y\rangle \longrightarrow |\downarrow\rangle \otimes |x, y-1\rangle \end{array} \tag{4}$$

Surprisingly we will show that the "moving" shift gives a walk search algorithm that takes time $\Omega(N)$. So even though it seems this walk "moves faster" than the "flip-flop" walk, the resulting algorithms performs much worse, no better than classical exhaustive search. It is this surprising behavior of S_m which has halted the progress in finding a good discrete quantum walk search algorithm on the grid.

Theorem 1 *For the quantum walk search algorithm associated to the quantum walk $U = S_{ff} \cdot C$, with S_{ff} as in Eq. (4), there is a $T = O(\sqrt{N \log N})$, such that after T steps the probability to determine the marked state is $p_T = O(1/\log N)$.*

Corollary 1 *We can get a local search algorithm based on the quantum walk that finds the marked state with constant probability in time $O(\sqrt{N} \log N)$.*

Proof of Corollary 1: The initial state $|\Phi\rangle$ can be generated with $\sqrt{N}$ local transformations. Since we only have an estimate for T up to a constant factor, we need to repeat the random walk an appropriate (constant) number of times. For the algorithm we will use amplitude amplification [BHMT02] to achieve a time $O(\sqrt{N} \log N)$. We will give more details in the proof of Theorem 1. ■

Theorem 2 *The quantum walk search algorithm associated with S_m as in Eq. (4) takes at least $\Omega(N)$ steps to determine the marked state with constant probability.*

We also consider a two dimensional coin inspired by Dirac's equation in 2+1 dimensions. Let $|\Uparrow\rangle = |0\rangle$ and $|\Downarrow\rangle = |1\rangle$ be the standard basis for one qubit and $|\Leftarrow\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|\Rightarrow\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ be the Hadamard basis. If there is no marked coins, one step of the quantum walk U with the two-dimensional coin consists of:

1. Move up/down:
$$|\Uparrow\rangle \otimes |x\rangle \otimes |y\rangle \rightarrow |\Uparrow\rangle \otimes |x\rangle|y-1\rangle,$$
$$|\Downarrow\rangle \otimes |x\rangle \otimes |y\rangle \rightarrow |\Downarrow\rangle \otimes |x\rangle|y+1\rangle.$$
2. Move left/right:
$$|\Leftarrow\rangle \otimes |x\rangle \otimes |y\rangle \rightarrow |\Leftarrow\rangle \otimes |x-1\rangle|y\rangle,$$
$$|\Rightarrow\rangle \otimes |x\rangle \otimes |y\rangle \rightarrow |\Rightarrow\rangle \otimes |x+1\rangle|y\rangle.$$

If there is a marked coin $|v\rangle$, we define the quantum walk as $U' = U(I - 2|s,v\rangle\langle s,v|)$ where U is the walk with no marked coin and $|s\rangle$ is the state $\frac{1}{\sqrt{2}}|\Uparrow\rangle + \frac{1}{\sqrt{2}}|\Downarrow\rangle$.

Theorem 3 *The associated quantum walk search algorithm takes $O(\sqrt{N \log N})$ steps and the probability to measure the marked state is $\Omega(1/\log N)$. This yields a local search algorithm running in time $O(\sqrt{N} \log N)$.*

4 Results in 3 and more dimensions

In more than 2 dimensions the "flip-flop" based quantum walk search algorithms achieves its optimal performance of $O(\sqrt{N})$. Here G is a grid of N vertices, arranged as $\sqrt[d]{N} \times \ldots \times \sqrt[d]{N}$, with periodic boundary conditions, as before, and states are labelled as $|x_1, \ldots, x_d\rangle$.

Theorem 4 *Let G be the d-dimensional grid with N vertices. Then the associated quantum walk with one marked coin takes $O(\sqrt{N})$ steps and the probability to measure the marked state is constant.*

Theorem 5 *The results of Theorems 1, 2, 3 and 4 hold also for two marked items.*

5 Abstract search algorithm

Before giving the technical details let us give some intuition of the proof. Recall that Grover's algorithm in its standard form is a succession of reflections R_v around the marked state $|v\rangle$ followed by a reflection around the mean $R_{|\Phi\rangle} = 2|\Phi\rangle\langle\Phi| - I_N$, where $|\Phi\rangle$ is the uniform superposition over all items. It can be viewed as a rotation in a two dimensional space, spanned by the marked state $|v\rangle$ and the initial state. In the basis where $|0\rangle = |\Phi\rangle$ and $|v\rangle = \frac{1}{\sqrt{N}}|0\rangle + \sqrt{\frac{N-1}{N}}|1\rangle$, Grover's algorithms corresponds to the transformation (with $\sin\phi = 2\frac{\sqrt{N-1}}{N}$)

$$U = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}. \tag{5}$$

The two eigenvectors of U are $|\pm\omega\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ with eigenvalues $e^{\mp i\phi}$. The initial state is a uniform superposition of the two eigenvectors $|\Phi\rangle = \frac{1}{\sqrt{2}}(|\omega\rangle + |-\omega\rangle)$. After T applications of U, with T chosen such that $T\phi = \frac{\pi}{2}$, we have

$$U^T|\Phi\rangle = U^T\frac{1}{\sqrt{2}}(|\omega\rangle + |-\omega\rangle) = \frac{1}{\sqrt{2}}(-i|\omega\rangle + i|-\omega\rangle) = |1\rangle$$

which has an overlap of $\sqrt{\frac{N-1}{N}}$ with the marked state $|v\rangle$.

In the random walk algorithm the transformation $(I - 2|s,v\rangle\langle s,v|)$ is a counterpart of R_v and the transformation U is an "imperfect" counterpart of $R_{|\Phi\rangle}$. We will first show, that with an appropriate choice of coin (as in Thms. 1, 3, and 4) the resulting transformation is still *approximately* in a 2-dimensional subspace; In this space U' will correspond to a rotation as in Eq. (5). Chosing T appropriately will (approximately) give a state with a "large" overlap with the marked state or its neighbors.

In the case of the "bad" coin, as in Theorem 2, we will show that there is a large eigenspace of eigenvalue 1 of the perturbed walk, and that the initial state has a large overlap with this eigenspace. Hence the state of the system nearly doesn't change by the walk.

More formally, an *abstract search algorithm* consists of two unitary transformations U_1 and U_2 and two states $|\psi_{start}\rangle$ and $|\psi_{good}\rangle$. We require the following properties:

1. $U_1 = I - 2|\psi_{good}\rangle\langle\psi_{good}|$ (in other words, $U|\psi_{good}\rangle = -|\psi_{good}\rangle$ and, if $|\psi\rangle$ is orthogonal to $|\psi_{good}\rangle$, then $|\psi\rangle = |\psi\rangle$);

2. $U_2|\psi_{start}\rangle = |\psi_{start}\rangle$ for some state $|\psi_{start}\rangle$ with real amplitudes and there is no other eigenvector with eigenvalue 1;

3. U_2 is described by a real unitary matrix.

The abstract search algorithm applies the unitary transformation $(U_2U_1)^T$ to the starting state $|\psi_{start}\rangle$. We claim that, under certain constraints, its final state $(U_2U_1)^T|\psi_{start}\rangle$ has a sufficiently large inner product with $|\psi_{good}\rangle$.

The next lemmas, which we will prove in Sec. 7, describe the main properties of an abstract search algorithm that we use. Let $U' = U_2U_1$. Since U_2 is a real unitary matrix, its non-$\pm$1-eigenvalues come in pairs of complex conjugate numbers. Denote them by $e^{\pm i\theta_1}$, ..., $e^{\pm i\theta_m}$. Let $\theta_{min} = \min(\theta_1, \ldots, \theta_m)$.

Lemma 1 *Define the arc $\mathcal{A}$ as the set of $e^{i\theta}$ for all real θ satisfying $-\theta_{min} < \theta < \theta_{min}$. Then U' has at most two eigenvalues*[3] *in $\mathcal{A}$.*

The two eigenvectors with these eigenvalues will be very important to us. We will show that the starting state is close to a linear combination of them. Therefore, we will be able to determine the evolution of the starting state by studying these two eigenvectors.

We start by bounding the two eigenvalues. Let $|\Phi_j^+\rangle$ and $|\Phi_j^-\rangle$ be the eigenvectors with eigenvalues $e^{i\theta_j}$ and $e^{-i\theta_j}$, respectively. We express $|\psi_{good}\rangle$ as a superposition of the eigenvectors of U_2:

$$|\psi_{good}\rangle = a_0|\psi_{start}\rangle + \sum_{j=1}^{m}\left(a_j^+|\Phi_j^+\rangle + a_j^-|\Phi_j^-\rangle\right). \tag{6}$$

Lemma 2 *It is possible to select $|\Phi_j^+\rangle$ and $|\Phi_j^-\rangle$ so that $a_j^+ = a_j^-$ and a_j^+ is a real number.*

In the next lemmas, we assume that this is the case and denote $a_j^+ = a_j^-$ simply as a_j.

Lemma 3 *The eigenvalues of U' in $\mathcal{A}$ are $e^{\pm i\alpha}$ where*

$$\alpha = \Theta\left(\frac{1}{\sqrt{\sum_j \frac{a_j^2}{a_0^2}\frac{1}{1-\cos\theta_j}}}\right). \tag{7}$$

Let $|w_\alpha\rangle$ and $|w_{-\alpha}\rangle$ be the two eigenvectors with eigenvalues $e^{i\alpha}$ and $e^{-i\alpha}$, respectively. Define $|w'_{start}\rangle = \frac{1}{\sqrt{2}}|w_\alpha\rangle - \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle$, $|w_{start}\rangle = \frac{1}{\||w'_{start}\|}|w'_{start}\rangle$. We claim that $|w_{start}\rangle$ is close to the starting state $|\psi_{start}\rangle$. This is quantified by the following lemma.

Lemma 4 *Assume that $\alpha < \frac{1}{2}\theta_{min}$. Then,*

$$\langle\psi_{start}|w_{start}\rangle \geq 1 - \Theta\left(\alpha^4 \sum_j \frac{a_j^2}{a_0^2}\frac{1}{(1-\cos\theta_j)^2}\right).$$

The last lemma shows that, after repeating U_2U_1 a certain number of times, the state has significant overlap with $|\psi_{good}\rangle$. Say we apply $(U_2U_1)^{\lceil\pi/4\alpha\rceil}$ to the state $\frac{1}{\sqrt{2}}|w_\alpha\rangle - \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle$. Then, we get the state which is equal to

$$\frac{1}{\sqrt{2}}e^{i\pi/4}|w_\alpha\rangle - e^{-i\pi/4}\frac{1}{\sqrt{2}}|w_{-\alpha}\rangle = i(\frac{1}{\sqrt{2}}|w_\alpha\rangle + \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle) =: |w_{good}\rangle$$

plus a state of norm $O(\alpha)$ (because $\pi/4$ and $\lceil\pi/4\alpha\rceil\alpha$ differ by an amount which is less than α).

Lemma 5 *Assume that $\alpha < \frac{1}{2}\theta_{min}$. Let $|w_{good}\rangle = \frac{1}{\sqrt{2}}|w_\alpha\rangle + \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle$. Then,*

$$|\langle\psi_{good}|w_{good}\rangle| = \Theta\left(\min\left(\frac{1}{\sqrt{\sum_j a_j^2\cot^2\frac{\theta_j}{4}}}\right), 1\right).$$

[3]The next lemma implies that there are exactly two eigenvalues in $\mathcal{A}$.

Corollary 2 *Assume that* $\alpha < \frac{1}{2}\theta_{min}$.

$$|\langle\psi_{good}|(U_2U_1)^{\lceil\pi/4\alpha\rceil}|w_{good}\rangle = \Theta\left(\min\left(\frac{1}{\sqrt{\sum_j a_j^2 \cot^2\frac{\theta_j}{4}}}\right), 1\right) + O(\alpha).$$

These three lemmas are the basis of our proofs. In each of our positive results, we first find a subspace $\mathcal{H}$ such that the search algorithm restricted to this subspace is a special case of an abstract search algorithm. Then, we apply Lemma 4 to show that the starting state is close to $|w_{start}\rangle$ and Lemma 3 and corollary 2 to show it evolves to a state having significant overlap with $|\psi_{good}\rangle$.

6 Proofs of the main results

6.1 Theorem 1

Let us determine the eigenspectrum of $U = S_{ff} \cdot (C_0 \otimes I_N)$ first.

Claim 6 *[Spectrum of U:] U has eigenvalues* λ_{kl} *with corresponding eigenvectors of the form* $|v_{kl}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$ *for all* $k, l = 0, \ldots, \sqrt{N} - 1$, *where* $|\chi_k\rangle = \frac{1}{\sqrt[4]{N}} \sum_{j=0}^{\sqrt{N}-1} \omega^{kj}|j\rangle$ *with* $\omega = e^{2\pi i/\sqrt{N}}$, *and* λ_{kl} *and* $|v_{kl}\rangle$ *satisfy the equation*

$$C_{kl}|v_{kl}\rangle = \begin{pmatrix} 0 & \omega^{-k} & 0 & 0 \\ \omega^k & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^{-l} \\ 0 & 0 & \omega^l & 0 \end{pmatrix} \cdot C_0|v_{kl}\rangle = \lambda_{kl}|v_{kl}\rangle. \tag{8}$$

The four eigenvalues λ_{kl} *of* C_{kl} *are* $1, -1$ *and* $e^{\pm i\theta_{kl}}$ *where* $\cos\theta_{kl} = \frac{1}{2}(\cos\frac{2\pi k}{\sqrt{N}} + \cos\frac{2\pi l}{\sqrt{N}})$. *Let* $|v_{kl}^1\rangle$, $|v_{kl}^{-1}\rangle$ *and* $|v_{kl}^{\pm}\rangle$ *be the vectors* $|v_{kl}\rangle$ *for the eigenvalues 1, -1 and* $e^{i\pm\theta}$, *respectively. Then,* $|v_{kl}^1\rangle$ *is orthogonal to* $|s\rangle$ *for* $(k,l) \neq (0,0)$ *and* $|v_{kl}^{-1}\rangle$ *is orthogonal to* $|s\rangle$ *for all* (k,l), *including* $(0,0)$.

Proof: Apply U to a vector of the form $|v_{kl}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$ and note that $S_{ff}|\uparrow\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle = \omega^{-k}|\downarrow\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$, and $S_{ff}|\downarrow\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle = \omega^k|\uparrow\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$, and similarly for the y-coordinate, which gives Eq. (8). Solving the equation $|C_{kl} - \lambda I| = 0$ for λ gives the eigenvalues. For $(k,l) \neq (0,0)$ the 1-eigenvector $|v_{kl}^1\rangle$ is proportional to $(\omega^k(\omega^l - 1), 1 - \omega^l, \omega^l(1 - \omega^k), \omega^k - 1)$ and hence orthogonal to $|s\rangle = \frac{1}{2}(1,1,1,1)$. The -1-eigenvector $|v_{kl}^{-1}\rangle$ is proportional to $(\omega^l + 1, \omega^k(\omega^l + 1), -(\omega^k + 1), -\omega^l(\omega^k + 1))$ and hence orthogonal to $|s\rangle = \frac{1}{2}(1,1,1,1)$. For $(k,l) = (0,0)$, $|s\rangle$ is a 1-eigenvector of C_{00}. ∎

For $(k,l) = (0,0)$, the eigenvalue 1 occurs 3 times. Thus, there is a 3-dimensional 1-eigenspace. Since $|s\rangle$ is orthogonal to $|v_{00}^{-1}\rangle$, $|s\rangle$ belongs to this eigenspace. We choose $|v_{00}^1\rangle = |s\rangle$ and $|v_{00}^{\pm}\rangle$ orthogonal to $|s\rangle$.

Let $\mathcal{H}_0'$ be the space spanned by the eigenvectors $|v_{kl}^{\pm}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$, $(k,l) \neq (0,0)$ and $|\Phi_0\rangle = |v_{00}^1\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$. Notice that all other eigenvectors of U are orthogonal to $|s,v\rangle$, by Claim 6. Therefore, $|s,v\rangle$ is in $\mathcal{H}_0'$. Moreover, applying U' keeps the state in $\mathcal{H}_0'$, as shown by

Claim 7 *We have* $U'(\mathcal{H}_0') = \mathcal{H}_0'$. *Furthermore,* U' *has no eigenvector of eigenvalue* 1 *in* $\mathcal{H}_0'$.

Proof: For the first part, notice that $U' = U(I - 2|s,v\rangle\langle s,v|)$. Therefore, it suffices to show $U(\mathcal{H}'_0) = \mathcal{H}'_0$ and $(I - 2|s,v\rangle\langle s,v|)(\mathcal{H}'_0) = \mathcal{H}'_0$. The first equality is true because $\mathcal{H}'_0$ has a basis consisting of eigenvectors of U. Each of those eigenvectors gets mapped to a multiple of itself which is in $\mathcal{H}'_0$. Therefore, $U(\mathcal{H}'_0) = \mathcal{H}'_0$. The second equality follows because $(I - 2|s,v\rangle\langle s,v|)|\psi\rangle = |\psi\rangle - \langle s,v|\psi\rangle|s,v\rangle$. This is a linear combination of $|\psi\rangle$ and $|s,v\rangle$ and, if $|\psi\rangle \in \mathcal{H}'_0$, it is in $\mathcal{H}_0$.

For the second part assume $|\omega_0\rangle$ is an eigenvector of eigenvalue 1 of U' in $\mathcal{H}'_0$. Then

$$0 \neq \langle\Phi_0|\omega_0\rangle = \langle\Phi_0|U'|\omega_0\rangle = \langle\Phi_0|U(I - 2|s,v\rangle\langle s,v|)|\omega_0\rangle = \langle\Phi_0|\omega_0\rangle - 2\langle\Phi_0|s,v\rangle\langle s,v|\omega_0\rangle.$$

This implies $\langle\Phi_0|s,v\rangle\langle s,v|\omega_0\rangle = 0$ and, since $\langle\Phi_0|s,v\rangle = \frac{1}{\sqrt{N}} \neq 0$, that $\langle s,v|\omega_0\rangle = 0$ and $|\omega_0\rangle = U'|\omega_0\rangle = U|\omega_0\rangle$ which in turn implies that $|\omega_0\rangle$ is an eigenvector of eigenvalue 1 of U. Since $|\omega_0\rangle$ has zero overlap with $|s,v\rangle$ and precisely the 1-eigenvectors of U orthogonal to $|\Phi_0\rangle$ have zero overlap with $|s,v\rangle$, it follows that $\langle\Phi_0|\omega_0\rangle = 0$ which contradicts that $|\omega_0\rangle \in \mathcal{H}'_0$. ∎

The above shows that the random walk algorithm starting in $|\Phi_0\rangle$ is restricted to a subspace $\mathcal{H}'_0$ of the Hilbert space. Since $|\Phi_0\rangle$ is the only 1-eigenvector of U in $\mathcal{H}'_0$, we have an instance of the abstract search algorithm on the space $\mathcal{H}'_0$, with $U_1 = I - 2|s,v\rangle\langle s,v|$, $U_2 = U$, $|\psi_{good}\rangle = |s,v\rangle$ and $|\psi_{start}\rangle = |\Phi_0\rangle$.

As described in Section 5, we study the 2-dimensional subspace spanned by $|w_\alpha\rangle$ and $|w_{-\alpha}\rangle$. First, we bound α using Lemma 3. We need to expand $|\psi_{good}\rangle = |s,v\rangle$ in the basis of eigenvectors of U. Define $|\Phi^+_{kl}\rangle = |v^+_{kl}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$. Let $|\Phi^-_{kl}\rangle$ be the vector obtained by replacing every amplitude in $|\Phi^+_{kl}\rangle$ by its conjugate. Then, $|\Phi^-_{kl}\rangle = |v^-_{-k,-l}\rangle \otimes |\chi_{-k}\rangle \otimes |\chi_{-l}\rangle$. (This follows from two observations. First, replacing every amplitude by its conjugate in $|\chi_k\rangle$ gives $|\chi_{-k}\rangle$. Therefore, $|\Phi^-_{kl}\rangle = |v\rangle\otimes|\chi_{-k}\rangle\otimes|\chi_{-l}\rangle$. Second, since $U|\Phi^+_{kl}\rangle = e^{i\theta_{kl}}|\Phi^+_{kl}\rangle$, we have $U|\Phi^-_{kl}\rangle = e^{-i\theta_{kl}}|\Phi^-_{kl}\rangle$, implying that $|v\rangle = |v^-_{-k,-l}\rangle$.) From Lemma 2, we have

$$|s,v\rangle = a_0|\Phi_0\rangle + \sum_{(k,l)\neq(0,0)} a_{kl}(|\Phi^+_{kl}\rangle + |\Phi^-_{kl}\rangle)$$

where $|\Phi^+_{kl}\rangle$ and $|\Phi^-_{kl}\rangle$ appear with the same real coefficient $a_{kl} = \langle s,v|\Phi^+_{kl}\rangle = \langle s,v|\Phi^-_{kl}\rangle$.

Claim 8

$$a_{kl} = \frac{1}{\sqrt{2N}}.$$

Proof: We have $|\langle v|\chi_k\rangle \otimes |\chi_l\rangle| = \frac{1}{\sqrt{N}}$ (since each of the N locations has an equal emplitude in $|\chi_k\rangle \otimes |\chi_l\rangle$). It remains to show that $|\langle s|v^+_{kl}\rangle| = \frac{1}{\sqrt{2}}$. For that, we first notice that $|s\rangle$ is a superposition of $|v^\pm_{kl}\rangle$ (since $|v^1_{kl}\rangle$ and $|v^{-1}_{kl}\rangle$ are orthogonal to $|s\rangle$). By direct calculation $\langle s|C_{kl}|s\rangle = \frac{1}{2}(\cos\frac{2\pi k}{\sqrt{N}} + \cos\frac{2\pi l}{\sqrt{N}})$. We have

$$\langle s|C_{kl}|s\rangle = e^{i\theta_{kl}}\langle s|v^+_{kl}\rangle\langle v^+_{kl}|s\rangle + e^{-i\theta_{kl}}\langle s|v^-_{kl}\rangle\langle v^-_{kl}|s\rangle.$$

This is possible only if $|\langle s|v^+_{kl}\rangle| = |\langle s|v^-_{kl}\rangle| = \frac{1}{\sqrt{2}}$. ∎

Therefore,

$$|s,v\rangle = \frac{1}{\sqrt{N}}|\Phi_0\rangle + \frac{1}{\sqrt{2N}} \sum_{(k,l)\neq(0,0)} (|\Phi^+_{kl}\rangle + |\Phi^-_{kl}\rangle). \tag{9}$$

By Lemma 3, $\alpha = \Theta(\frac{1}{\sqrt{\sum_{kl}\frac{1}{1-\cos\theta_{kl}}}})$. The following claim implies that $\alpha = \Theta(\frac{1}{\sqrt{cN\log N}})$.

Claim 9 $\sum_{(k,l)\neq(0,0)} \frac{1}{1-\cos\theta_{kl}} = \Theta(N \log N)$.

Proof of Claim 9: Recall from Claim 6 that the eigenvalues corresponding to $|v_{kl}^{\pm}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$ are $e^{\pm i\theta_{kl}} = \cos\theta_{kl} \pm i \sin\theta_{kl}$ where $\cos\theta_{kl} = \frac{1}{2}(\cos\frac{2\pi k}{\sqrt{N}} + \cos\frac{2\pi l}{\sqrt{N}})$. For $x \in [0, 2\pi]$, we have

$$1 - \frac{x^2}{2} \leq \cos x \leq 1 - \frac{2x^2}{\pi^2}. \tag{10}$$

Therefore,

$$1 - \frac{1}{4N}(k^2+l^2) \leq \cos\theta_{kl} \leq 1 - \frac{1}{\pi^2 N}(k^2+l^2),$$

$$\frac{1}{\pi^2 N}(k^2+l^2) \leq 1 - \cos\theta_{kl} \leq \frac{1}{4N}(k^2+l^2) \tag{11}$$

This means that it suffices to show

$$N \sum_{k,l} \frac{1}{k^2+l^2} = \Theta(N \log N), \tag{12}$$

where the summation is over all $k, l \in \{0, \ldots, \sqrt{N}-1\}$ such that at least one of k, l is non-zero. This follows because $\sum_{k,l} \frac{1}{k^2+l^2} = \Theta(\log N)$. A simple way to see this is to sum points that lie on m-rectangles with the four corners $(\pm m, \pm m)$. The term $\frac{1}{k^2+l^2}$ for (k, l) on an m-rectangle is bounded as $\frac{1}{2m^2} \leq \frac{1}{k^2+l^2} \leq \frac{1}{m^2}$, and there are $8m$ such points on each m-rectangle. Hence

$$\sum_{m=1}^{\sqrt{N}-1} 8m\frac{1}{2m^2} \leq \sum_{k,l} \frac{1}{k^2+l^2} \leq \sum_{m=1}^{\sqrt{N}-1} 8m\frac{1}{m^2}. \tag{13}$$

The claim now follows from $\sum_{m=1}^{\sqrt{N}-1} \frac{1}{m} = \frac{1}{2}\log N(1+o(1))$. ■

Next, we use Lemma 4 to bound the overlap between $|\Phi_0\rangle$ and $|w_{start}\rangle = \frac{1}{\sqrt{2}}|w_\alpha\rangle - \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle$.

Claim 10 $\sum_{(k,l)\neq(0,0)} \frac{1}{(1-\cos\theta_{kl})^2} = \Theta(N^2)$.

Proof of Claim 10 : Using the proof of Claim 9,

$$\frac{\pi^4 N^2}{(k^2+l^2)^2} \leq \frac{1}{(1-\cos\theta_{kl})^2} \leq \frac{4N^2}{(k^2+l^2)^2}.$$

Therefore, it suffices to bound $N^2 \sum_{(k,l)\neq(0,0)} \frac{1}{(k^2+l^2)^2}$. Again, we sum points (k, l) over rectangles with corners $(\pm m, \pm m)$. Each rectangle has $8m$ points, each of which contributes a term of order $\frac{1}{m^4}$ to the sum. Since $\sum_m 8m\frac{1}{m^4} = \sum_m \frac{8}{m^3}$ is bounded by a constant, the lemma follows. ■

This means that the overlap between the starting state and $|w_{start}\rangle$ is $1 - \Theta(\alpha^4 N^2) = 1 - \Theta(\frac{1}{\log^2 N})$. Equivalently, $|\Phi_0\rangle = |w_{start}\rangle + |\Phi_{rem}\rangle$, with $\||\Phi_{rem}\rangle\| = \Theta(\frac{1}{\log N})$. After $\lceil \frac{\pi}{4\alpha} \rceil$ repetitions, the state becomes $|w_{good}\rangle + |\Phi'_{rem}\rangle$, with $\|\Phi'_{rem}\| = \Theta(\frac{1}{\log N}) + O(\alpha) = \Theta(\frac{1}{\log N})$. Finally, we bound $\langle w_{good}|s, v\rangle$, using Lemma 5. Since all a_{kl} are equal to $\frac{1}{\sqrt{2N}}$ and $\cot x \leq \frac{1}{x}$, we have

$$\frac{1}{\sqrt{\sum_{k,l} a_{kl}^2 \cot^2\frac{\theta_{kl}}{2}}} \geq \frac{1}{\sqrt{\frac{1}{2N}\sum_{k,l} \frac{4}{\theta_{kl}^2}}}. \tag{14}$$

From the proof of Claim 9, we know that $\frac{1}{\theta_{kl}^2}$ is bounded from below and above by $\frac{const}{1-\cos\theta_{kl}}$. Therefore, Claim 9 implies $\sum_{k,l}\frac{1}{\theta_{kl}^2} = \Theta(N\log N)$. Thus, the expression of Eq. (14) is of order $\Omega(\frac{1}{\sqrt{\log N}})$.

To conclude the proof of the theorem, the overlap of the state of the algorithm after $\lceil\frac{\pi}{4\alpha}\rceil$ steps and $|s,v\rangle$ is

$$|\langle w_{good}|s,v\rangle + \langle\Phi'_{rem}|s,v\rangle| \geq |\langle w_{good}|s,v\rangle| - |\langle\Phi'_{rem}|s,v\rangle|.$$

The first term is of order $\Omega(\frac{1}{\sqrt{\log N}})$ and the second term is of lower order ($\Omega(\frac{1}{\log N})$). Therefore, the result is of order $\Omega(\frac{1}{\sqrt{\log N}})$.

Hence a measurement gives the marked location $|v\rangle$ with probability $p \geq \frac{c}{\log N}$. This completes the proof of Theorem 1.

Proof of Corollary 1: First, note that it is possible to generate the initial state $|\Phi_0\rangle$ with $2\sqrt{N}$ local transformations. We start with the state concentrated in one point (say $|0,0,0\rangle$) and first "spread" the amplitude along the x-axis in $\sqrt{N}$ steps. In the first step we rotate the coin register to $\frac{1}{\sqrt[4]{N}}|0\rangle + \sqrt{\frac{\sqrt{N}-1}{\sqrt{N}}}|1\rangle$, followed by a $|1\rangle$-controlled shift in the x-direction, followed by a rotation of the coin register back to $|0\rangle$ in the vertex $(0,0)$. Similarly we repeat this procedure to move $\sqrt{\frac{\sqrt{N}-2}{\sqrt{N}}}$ of amplitude from $(1,0)$ to $(2,0)$ and so on. After $\sqrt{N}$ steps we have a uniform superposition over all vertices with y-coordinate 0. We repeat this process for the y-direction, which gives us the uniform superposition after another $\sqrt{N}$ steps. Note that this procedure also allows us to implement the reflection around the mean, $R_{|\Phi_0\rangle} = I - 2|\Phi_0\rangle\langle\Phi_0|$ in $4\sqrt{N}$ steps: we simply run the procedure in reverse (which maps $|\Phi_0\rangle$ to $|0,0,0\rangle$), then invert the state $|0,0,0\rangle$ (which can be done locally in the vertex $(0,0)$), and run the procedure forward again.

Note that we have determined the run-time T only up to a constant (using Eqs. (11) and (13), (24), (26) we can bound $T_{min} = \frac{\sqrt{N\log N}}{2} \leq T \leq \frac{\pi\sqrt{N\log N}}{2\sqrt{2}} = T_{max}$). To get ε-close to the state $U'^T|\Phi_0\rangle$ we use a standard trick and run the walk for times $T_{min}, (1+\varepsilon)T_{min}, (1+\varepsilon)^2T_{min}, \ldots$ until we reach T_{max}. One of these times is within a factor of $(1\pm\varepsilon)$ of T and hence our state and final measurement probability will be ε-close to the state at time T. We can chose ε to be some small constant. The total time including all repetitions (bounded by $\frac{1}{1-\varepsilon}T_{min}$) is still $O(T) = O(\sqrt{N\log N})$.

Finally, to amplify the success probability we will use amplitude amplification [BHMT02], which is a succession of steps consisting of reflection around the mean $|\Phi_0\rangle$ and a run of the algorithm. The intermediate reflection around the mean can be implemented in $4\sqrt{N}$ steps, the random walk takes $O(\sqrt{N\log N})$ steps, and we need $O(\sqrt{\log N})$ rounds of amplification to obtain a constant probability of success, which gives a total running time of $O(\sqrt{N}\log N)$. ∎

6.2 Theorem 2

Proof: The key difference between this walk using S_m and the walk from Theorem 1 using S_{ff} is that the initial state $|\Phi_0\rangle$ now has very large overlap with the eigenspace of eigenvalue 1 of U and U'. This means that the walk (nearly) does not move at all and the state at any time T has overlap with $|\Phi_0\rangle$ close to 1. The difference becames apparent in the eigenspectrum of U:

Claim 6' *[Spectrum of U:] U has eigenvalues λ_{kl} with corresponding eigenvectors of the form $|v_{kl}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$ for all $k,l = 0,\ldots,\sqrt{N}-1$, where $|\chi_k\rangle = \frac{1}{\sqrt[4]{N}} \sum_{j=0}^{\sqrt{N}-1} \omega^{kj}|j\rangle$ with $\omega = e^{2\pi i/\sqrt{N}}$, and λ_{kl} and $|v_{kl}\rangle$ satisfy the equation*

$$C_{kl}|v_{kl}\rangle = \begin{pmatrix} \omega^k & 0 & 0 & 0 \\ 0 & \omega^{-k} & 0 & 0 \\ 0 & 0 & \omega^l & 0 \\ 0 & 0 & 0 & \omega^{-l} \end{pmatrix} \cdot C_0|v_{kl}\rangle = \lambda_{kl}|v_{kl}\rangle \tag{15}$$

The four eigenvalues λ_{kl} of C_{kl} are $1, -1$ and $e^{\pm i\theta_{kl}}$, where $\cos\theta_{kl} = -\frac{1}{2}(\cos\frac{2\pi k}{\sqrt{N}} + \cos\frac{2\pi l}{\sqrt{N}})$. For the eigenvector $|v^1_{kl}\rangle$ corresponding to eigenvalue 1, we have

$$|\langle v^1_{kl}|s\rangle| \geq \frac{1 + \cos\frac{2\pi k}{\sqrt{N}} + \cos\frac{2\pi l}{\sqrt{N}} + \cos\frac{2\pi(k+l)}{\sqrt{N}}}{4}.$$

Proof: The first part is by straightforward calculation as before (Claim 6). For the second part, the eigenvector corresponding to eigenvalue 1 is $|v^1_{kl}\rangle = \frac{|u^1_{kl}\rangle}{\|u^1_{kl}\|}$ with

$$|u^1_{kl}\rangle = (w^k(1+w^l), 1+w^l, w^l(1+w^k), 1+w^k)$$

We have $\|u^1_{kl}\| \leq 4$ because each of the 4 components of $|u^1_{kl}\rangle$ is at most 2 in absolute value. It remains to bound $\langle u^1_{kl}|s\rangle$. We have

$$\langle v^1_{kl}|s\rangle \geq \frac{\langle u^1_{kl}|s\rangle}{4} = \frac{1}{8}(w^k(1+w^l) + 1 + w^l + w^l(1+w^k) + 1 + w^k) = \frac{1}{4}(1+w^k)(1+w^l).$$

The real part of this expression is $\frac{1}{4}(1 + \cos\frac{2\pi k}{\sqrt{N}} + \cos\frac{2\pi l}{\sqrt{N}} + \cos\frac{2\pi(k+l)}{\sqrt{N}})$. This implies the claim. ■

Let $\mathcal{H}_1$ be the 1-eigenspace of U, spanned by the $|\Phi^1_{kl}\rangle = |v^1_{kl}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$ for $k,l = 0,\ldots,\sqrt{N}-1$, with $|\Phi^1_{00}\rangle = |\Phi_0\rangle$. Write

$$|s,v\rangle = \sum_{k,l} \alpha_{kl}|\Phi^1_{kl}\rangle + |s'\rangle$$

where $|s'\rangle$ has no overlap with the 1-eigenspace $\mathcal{H}_1$. We claim

Claim 11 *U' has a 1-eigenvector $|\Phi^\perp\rangle$ such that $|\langle\Phi_0|\Phi^\perp\rangle|^2 = 1 - \frac{|\alpha_{00}|^2}{\sum_{i,j=1}^{\sqrt{N}} |\alpha_{ij}|^2}$.*

Proof: Let $\beta_{kl} = \frac{\alpha_{kl}}{\sqrt{\sum_{i,j=1}^{\sqrt{N}} |\alpha_{ij}|^2}}$. Let $|\Phi\rangle = \sum_{k,l} \beta_{kl}|\Phi^1_{kl}\rangle$ be the projection of $|s,v\rangle$ on $\mathcal{H}_1$. Since $\langle\Phi_0|\Phi\rangle = \beta_{00}$, we can write

$$|\Phi_0\rangle = \beta_{00}|\Phi\rangle + \sqrt{1-|\beta_{00}|^2}|\Phi^\perp\rangle$$

where $|\Phi^\perp\rangle$ is a vector perpendicular to $|\Phi\rangle$. Since $|\Phi_0\rangle$ and $|\Phi\rangle$ are both in the subspace $\mathcal{H}_1$, $|\Phi^\perp\rangle$ is also in $\mathcal{H}_1$. We claim that $|\Phi^\perp\rangle$ is a 1-eigenvector of U'. The state $|\Phi^\perp\rangle$ is orthogonal to $|s,v\rangle$ because $|\Phi^\perp\rangle$ belongs to $\mathcal{H}_1$ and is orthogonal to $|\Phi\rangle$ which is the projection of $|s,v\rangle$ to that subspace. Therefore, $|\Phi^\perp\rangle$ is a 1-eigenvector of $I - |s,v\rangle\langle s,v|$. $|\Phi^\perp\rangle$ is also a 1-eigenvector of U because it belongs to $\mathcal{H}_1$. This means that it is a 1-eigenvector of $U' = U(I - |s,v\rangle\langle s,v|)$ as well. ■

To complete the proof, we need to bound $|\alpha_{00}|$, $|\alpha_{01}|$, ..., $|\alpha_{\sqrt{N}-1,\sqrt{N}-1}|$. We have $\alpha_{00} = \frac{1}{\sqrt{N}}$. We will show that there are $\Omega(N)$ other α_{kl} of order $\Omega(1/\sqrt{N})$. This would imply that the overlap of $|\Phi_0\rangle$ with a 1-eigenvector of U' is

$$1 - \frac{\alpha_{00}^2}{\sum_{i,j=1}^{\sqrt{N}} |\alpha_{ij}|^2} = 1 - \Omega(\frac{1}{N}).$$

Claim 6' gives the desired a bound on the α_{kl}:

$$|\langle s, v|v_{kl}^1\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle| = |\langle v|\chi_k \otimes \chi_l\rangle| \times |\langle s|v_{kl}^1\rangle| = \frac{|\langle s|v_{kl}^1\rangle|}{\sqrt{N}} \geq \frac{1 + \cos\frac{2\pi k}{\sqrt{N}} + \cos\frac{2\pi l}{\sqrt{N}} + \cos\frac{2\pi(k+l)}{\sqrt{N}}}{4\sqrt{N}}.$$

The range for $\frac{2\pi k}{\sqrt{N}}$ and $\frac{2\pi l}{\sqrt{N}}$ is $[-\frac{\pi}{2}, \frac{\pi}{2}]$. Therefore, for half of all k (resp. half of all l) we have $|k|\frac{2\pi}{\sqrt{N}} \leq \frac{\pi}{4}$ (resp. $|l|\frac{2\pi}{\sqrt{N}} \leq \frac{\pi}{4}$). For the $\frac{N}{4}$ pairs (k, l) that satisfy both of those conditions we have

$$1 + \cos\frac{2\pi k}{\sqrt{N}} + \cos\frac{2\pi l}{\sqrt{N}} + \cos\frac{2\pi(k+l)}{\sqrt{N}} \geq 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \geq 1 + \sqrt{2}.$$

Thus, for at least $\frac{N}{4}$ pairs (k, l)

$$|\alpha_{kl}| = |\langle s, v|v_{kl}^1\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle| \geq \frac{1 + \sqrt{2}}{4\sqrt{N}} > \frac{1}{2\sqrt{N}}.$$

■

6.3 Theorem 3

Proof: The proof for this random walk algorithm with a 2-dimensional coin proceeds in close analogy to the proof of Theorem 1, and we will emphasize and prove the points that differ.

Claim 6" *[Spectrum of U:] U has eigenvalues $\lambda_{kl}^{\pm}$ with corresponding eigenvectors of the form $|v_{kl}^{\pm}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$ for all $k, l = 0, \ldots, \sqrt{N} - 1$, where $|\chi_k\rangle = \frac{1}{\sqrt[4]{N}} \sum_{j=0}^{\sqrt{N}-1} \omega^{kj}|j\rangle$ with $\omega = e^{2\pi i/\sqrt{N}}$, and $\lambda_{kl}^{\pm}$ and $|v_{kl}^{\pm}\rangle$ satisfy the equation*

$$C_{kl}|v_{kl}\rangle = \begin{pmatrix} \omega^l \cos k & i\omega^{-l} \sin k \\ i\omega^l \sin k & \omega^{-l} \cos k \end{pmatrix} |v_{kl}\rangle = \lambda_{kl}|v_{kl}\rangle. \tag{16}$$

The two eigenvalues $\lambda_{kl}^{\pm}$ of C_{kl} are $e^{\pm i\theta_{kl}}$ where $\cos\theta_{kl} = \frac{1}{2}(\cos\frac{2\pi(k+l)}{\sqrt{N}} + \cos\frac{2\pi(k-l)}{\sqrt{N}})$.

As a corollary, we have that there are exactly two eigenvectors with eigenvalue 1, both of them of the form $|v_{00}^{\pm}\rangle \otimes |\chi_0\rangle \otimes |\chi_0\rangle$. Since the coin space is 2-dimensional, the two vectors $|v_{00}\rangle$ span it and, therefore, $|v\rangle \otimes |\chi_0\rangle \otimes |\chi_0\rangle$ is an eigenvector for any $|v\rangle$. In particular, we can take $|v_{00}^+\rangle = |s\rangle$ and $|v_{00}^-\rangle = |s^\perp\rangle$ where $|s^\perp\rangle \perp |s\rangle$. Similarly to Theorem 1, let $\mathcal{H}_0'$ be the space $|v_{00}^+\rangle \otimes |\chi_0\rangle \otimes |\chi_0\rangle$ and $|v_{kl}^{\pm}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$. Similarly to Claim 7, $\mathcal{H}_0'$ is mapped to itself by U'.

Let $|\Phi_{kl}^+\rangle = |v_{kl}^+\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$ and $|\Phi_{kl}^-\rangle = |v_{-k,-l}^-\rangle \otimes |\chi_{-k}\rangle \otimes |\chi_{-l}\rangle$. We can express the state $|s, v\rangle$ as

$$|s, v\rangle = a_0|\Phi_0\rangle + \sum_{(k,l)\neq(0,0)} a_{kl}(|\Phi_{kl}^+\rangle + |\Phi_{kl}^-\rangle). \tag{17}$$

where the equality of the coefficients of $|\Phi^+_{kl}\rangle$ and $|\Phi^-_{kl}\rangle$ follows from the proof of Lemma 2 (and $|\Phi^+_{kl}\rangle$ and $|\Phi^-_{kl}\rangle$ being complex conjugates).

We now have to bound the sum of Eq. (7). We claim that replacing all $\frac{|a_{kl}|^2}{|a_0|^2}$ by $\frac{1}{2}$ does not change the value of the sum. To see that, we first notice that $\theta_{kl} = \theta_{-k,-l}$. Therefore, replacing $|a^2_{kl}|$ and $|a^2_{-k,-l}|$ by $\frac{|a_{kl}|^2+|a_{-k,-l}|^2}{2}$ does not change the sum. Futhermore, $|a_{kl}|^2 + |a_{-k,-l}|^2 = \frac{1}{N}$. (We have $|a_{kl}| = \langle\Phi^+_{kl}|s,v\rangle$, $|a_{-k,-l}| = \langle\Phi^+_{-k,-l}|s,v\rangle = \langle\Phi^-_{-k,-l}|s,v\rangle$. The vectors $|\Phi^+_{kl}\rangle$ and $|\Phi^-_{-k,-l}\rangle$ are the same as $|v^{\pm}_{kl}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$. Therefore, $|a_{kl}|^2 + |a_{-k,-l}|^2$ equals the squared projection of $|s,v\rangle$ to $|v^{\pm}_{kl}\rangle \otimes |\chi_k\rangle \otimes |\chi_l\rangle$ which is equal to $|\langle v|\chi_k\rangle \otimes |\chi_l\rangle|^2 = \frac{1}{N}$.) Also, we still have $a_0 = \frac{1}{\sqrt{N}}$ and $|a_0|^2 = \frac{1}{N}$. Therefore, Eq. (7) simplifies to

$$\alpha = \Theta\left(\frac{1}{\sqrt{\sum_{(k,l)\neq(0,0)} \frac{1}{2(1-\cos\theta_{kl})}}}\right),$$

just as in the proof of Theorem 1. We get $\alpha = \Theta(\sqrt{N \log N})$ as in Lemma 9. The other two parts of Theorem 1 also follow in a similar way. ■

Similarly to Corollary 1 we can get a random walk based search algorith that determines the marked state with constant probability in time $O(\sqrt{N}\log N)$.

6.4 Theorem 4

Proof: Let us call the $2d$ directions on the d-dimensional grid $i_\pm$, where i indicates the dimension and $\pm$ the direction of the walk. Then the "flip-flop" shift operation takes the form

$$S_{ff}|i_\pm\rangle \otimes |x_1 \dots x_i \dots x_d\rangle = |i_\mp\rangle \otimes |x_1 \dots x_i \pm 1 \dots x_d\rangle$$

Let us recapitulate what the key elements in the proof of Theorem 1 are and how they generalize to the d-dimensional case.

Claim 6″ *[Spectrum of U:] U has eigenvalues $\lambda_{k_1k_2\dots k_d}$ with corresponding eigenvectors of the form $|v_{k_1k_2\dots k_d}\rangle \otimes |\chi_{k_1}\rangle \otimes |\chi_{k_2}\rangle \otimes \dots \otimes |\chi_{k_d}\rangle$ ($k_i = 0, \dots, \sqrt[d]{N} - 1$), where $|\chi_i\rangle = \frac{1}{\sqrt[2d]{N}} \sum_{k=0}^{\sqrt[d]{N}-1} \omega^k |k\rangle$ with $\omega = e^{2\pi i/\sqrt[d]{N}}$, and $\lambda_{k_1k_2\dots k_d}$ and $|v_{k_1k_2\dots k_d}\rangle$ satisfy the equation*

$$C_{k_1k_2\dots k_d}|v_{k_1k_2\dots k_d}\rangle = \begin{pmatrix} 0 & \omega^{-k_1} & 0 & 0 & \\ \omega^{k_1} & 0 & 0 & 0 & \\ 0 & 0 & 0 & \omega^{-k_2} & \dots \\ 0 & 0 & \omega^{k_2} & 0 & \\ & & \dots & & \end{pmatrix} \cdot C_0|v_{k_1k_2\dots k_d}\rangle = \lambda_{k_1k_2\dots k_d}|v_{k_1k_2\dots k_d}\rangle. \quad (18)$$

The $2d$ eigenvalues $\lambda_{k_1k_2\dots k_d}$ of $C_{k_1k_2\dots k_d}$ are 1 and -1 with multiplicity $d-1$ each, and $e^{\pm i\theta_{k_1k_2\dots k_d}}$ where $\cos\theta_{k_1k_2\dots k_d} = \frac{1}{d}\sum_{i=1}^{d} \cos\frac{2\pi k_i}{\sqrt[d]{N}}$. All $|v^1_{k_1k_2\dots k_d}\rangle$ corresponding to eigenvalue 1 are orthogonal to $|s\rangle$ for $(k_1k_2\dots k_d) \neq (0,0,\dots,0)$. All $|v^{-1}_{k_1k_2\dots k_d}\rangle$ corresponding to eigenvalue -1 are orthogonal to $|s\rangle$ for all $(k_1k_2\dots k_d)$.

Proof: Eq. (18) is obtained in the same way as in the proof of Claim 6. $C_{k_1k_2\ldots k_d}$ consists of 2 parts, the 2-block-diagonal matrix (call it $D_{k_1k_2\ldots k_d}$) and C_0. Each block in $D_{k_1k_2\ldots k_d}$ has eigenvalues ± 1 and eigenvectors $(\omega^{-\frac{k_i}{2}}, \pm\omega^{\frac{k_i}{2}})$, so the matrix $D_{k_1k_2\ldots k_d}$ itself has eigenspaces of 1 and -1 of dimension d each. In each of these two eigenspaces we can find $d-1$ orthogonal vectors orthogonal to $|s\rangle$. For those vectors $C_0 = 2|s\rangle\langle s| - I$ just flips their sign, so the -1 eigenvectors of $D_{k_1k_2\ldots k_d}$ become $+1$ eigenvectors of $C_{k_1k_2\ldots k_d}$ and vice versa. Call the remaining two eigenvectors of eigenvalue ± 1 $|e_\pm\rangle$ and expand $|s\rangle = \alpha_+|e_+\rangle + \alpha_-|e_-\rangle$. Then $\langle s|C_{k_1k_2\ldots k_d}|s\rangle = \langle s|D_{k_1k_2\ldots k_d}|s\rangle = \frac{1}{d}\sum_{i=1}^{d}\cos 2\pi k_i/\sqrt[d]{N} = \cos\theta_{k_1k_2\ldots k_d}$ implies $|\alpha_+|^2 - |\alpha_-|^2 = \cos\theta_{k_1k_2\ldots k_d}$. Let $|\omega\rangle$ be an eigenvector of $C_{k_1k_2\ldots k_d}$ not orthogonal to $|s\rangle$ and expand $|\omega\rangle = \beta_+|e_+\rangle + \beta_-|e_-\rangle$. Then we obtain (using $|e_+\rangle = \alpha_+^*|s\rangle + \alpha_-|s^\perp\rangle$ and $|e_-\rangle = \alpha_-^*|s\rangle - \alpha_+|s^\perp\rangle$ where $|s^\perp\rangle$ is orthogonal to $|s\rangle$ in the space spanned by $|e_\pm\rangle$) for the eigenvalue $\langle\omega|C_{k_1k_2\ldots k_d}|\omega\rangle = (|\alpha_+|^2 - |\alpha_-|^2) + 4iIm\beta_+^*\beta_-\alpha_+\alpha_-^* = \cos\theta_{k_1k_2\ldots k_d} \pm i\sin\theta_{k_1k_2\ldots k_d}$. ■

For $(k_1k_2\ldots k_d) = (0,0,\ldots,0)$ there are $d+1$ 1-eigenvectors, we set $|v_{0\ldots0}\rangle = |s\rangle$. Then, the other 1-eigenvectors are orthogonal to $|s\rangle$.

Similarly to Theorem 1, we restrict to the subspace $\mathcal{H}_0'$ spanned by $|v^{\pm1}_{k_1k_2\ldots k_d}\rangle \otimes |\chi_{k_1}\rangle \otimes |\chi_{k_2}\rangle \otimes \ldots \otimes |\chi_{k_d}\rangle$ and $|v_{00\ldots0}\rangle \otimes |\chi_0\rangle \otimes |\chi_0\rangle \otimes \ldots \otimes |\chi_0\rangle$. As in Theorem 1, we have $U'(\mathcal{H}_0') = H_0'$. Further

$$|s,v\rangle = \frac{1}{\sqrt{N}}|\Phi_0\rangle + \frac{1}{\sqrt{2N}}\sum_{(k_1,k_2,\ldots,k_d)\neq(0,0,\ldots,0)}(|\Phi^+_{k_1k_2\ldots k_d}\rangle + |\Phi^-_{k_1k_2\ldots k_d}\rangle),$$

where $|\Phi^+_{k_1k_2\ldots k_d}\rangle = |v^{+1}_{k_1k_2\ldots k_d}\rangle \otimes |\chi_{k_1}\rangle \otimes |\chi_{k_2}\rangle \otimes \ldots \otimes |\chi_{k_d}\rangle$ and $|\Phi^-_{k_1k_2\ldots k_d}\rangle = |v^{-1}_{k_1k_2\ldots k_d}\rangle \otimes |\chi_{-k_1}\rangle \otimes |\chi_{-k_2}\rangle \otimes \ldots \otimes |\chi_{-k_d}\rangle$. We use a modified Claim 9:

Claim 9' $\sum_{(k_1,k_2,\ldots k_d)\neq(0,0,\ldots,0)} \frac{1}{1-\cos\theta_{k_1k_2\ldots k_d}} = \Theta(N)$.

Proof: The proof follows along the lines of the proof of Claim 9. By Claim 6‴,

$$\frac{1}{1-\cos\theta_{k_1k_2\ldots k_d}} = \frac{d}{\sum_{j=1}^{d}(1-\cos\frac{2\pi k_j}{N^{1/d}})}$$

Similarly to Lemma 9, this is bounded from above and below by a constant times $N^{2/d}\frac{1}{k_1^2+k_2^2+\ldots+k_d^2}$. Thus, we have to estimate

$$N^{2/d}\sum_{k_1,k_2,\ldots,k_d}\frac{1}{k_1^2+k_2^2+\ldots+k_d^2} \tag{19}$$

where the summation is over all $k_i \in \{0,\ldots,\sqrt[d]{N}-1\}$ such that at least one of the k_i is non-zero. We divide tuples the $(k_1,\ldots,k_d)$ into $N^{1/d}$ "slices", with the m^{th} "slice" containing those tuples where $\max(k_1,k_2,\ldots,k_d) = m$. The m^{th} slice contains $O(m^{d-1})$ tuples. Therefore, the sum $\sum_{k_1,\ldots,k_d}\frac{1}{k_1^2+k_2^2+\ldots+k_d^2}$ over the m^{th} slice is of order $m^{d-1}\frac{1}{m^2} = m^{d-3}$. Since there are $N^{1/d}$ slices and, for each of them, the sum is $m^{d-3} \leq N^{(d-3)/d}$, the sum $\sum_{k_1,\ldots,k_d}\frac{1}{k_1^2+k_2^2+\ldots+k_d^2}$ over all $(k_1,\ldots,k_d) \neq (0,\ldots,0)$ is of order at most $N^{1/d}N^{(d-3)/d} = N^{(d-2)/d}$. This implies that Eq. (19) is of order at most N. It is also of order at least N since each individual term $N^{2/d}\frac{1}{k_1^2+k_2^2+\ldots+k_d^2}$ is at least a constant. ■

Therefore, applying Lemma 3 gives a sharper bound $\alpha = \Theta(\frac{1}{\sqrt{N}})$. Notice that we still fulfill the requirement $\alpha < \frac{1}{2}\theta_{min}$ needed for Lemmas 4 and 5. The reason for that is that all θ_i are at least $\Omega(\frac{1}{N^{1/d}})$.

Similarly to Claim 9', we can show

$$\sum_{(k_1,k_2,\ldots k_d)\neq(0,0,\ldots,0)} \frac{1}{(1-\cos\theta_{k_1k_2\ldots k_d})^2} = \Theta(N)$$

and

$$\sum_{(k_1,k_2,\ldots k_d)\neq(0,0,\ldots,0)} \frac{1}{\cot\theta^2_{k_1k_2\ldots k_d}} = \Theta(N).$$

By combining these two equalities with Lemmas 4 and 5, we get that the overlap between the starting state $|\Phi_0\rangle$ and $|w_{start}\rangle = \frac{1}{\sqrt{2}}|w_\alpha\rangle - \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle$ is $1-\Theta(\frac{1}{\sqrt{N}})$ and the overlap between $|w_{good}\rangle = \frac{1}{\sqrt{2}}|w_\alpha\rangle + \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle$ and $|s,v\rangle$ is $\Omega(1)$. This implies that the search algorithm's final state has a constant overlap with $|s,v\rangle$. ■

6.5 Theorem 5

We first discuss generalizing the positive results (Theorems 1, 4 and 5) to the case with two marked items. The main issue is to state them as instances of the abstract search. Assume there are k marked locations $v_1,\ldots,v_k$. Then, one step of the search algorithm is $U' = (I - 2\sum_{i=1}^{k}|s,v_i\rangle\langle s,v_i|)U$. Currently, we are not able to analyze cases of the abstract search where U_2 flips the sign on more than a 1-dimensional subspace.

For the $k = 2$ case, we can avoid this problem, via a reduction to $k = 1$. Define $|s'\rangle = \frac{1}{\sqrt{2}}|s,v_1\rangle + \frac{1}{\sqrt{2}}|s,v_2\rangle$. We claim that applying $(U')^T$ to the starting state $|\Phi_0\rangle$ gives the same final state as applying $(U'')^T$ where $U'' = (I - 2|s'\rangle\langle s'|)U$.

To show that, let T be a symmetry of the grid such that $T(v_1) = v_2$ and $T(v_2) = v_1$. (For the 2-dimensional grid, if $v_1 = (x_1,y_1)$ and $v_2 = (x_2,y_2)$, then $T(x,y) = (x_1+x_2-x, y_1+y_2-y)$.) We identify T with the unitary mapping $|c,v\rangle$ to $|c,T(v)\rangle$.

Claim 12 *For any $t \geq 0$, $T(U')^t|\Phi_0\rangle = (U')^t|\Phi_0\rangle$.*

Proof: By induction. For the base case, we have to show $T|\Phi_0\rangle = |\Phi_0\rangle$. This follows since $|\Phi_0\rangle$ is a uniform superposition of the states $|s,v\rangle$ and T just permutes locations v.

For the inductive case, notice that T commutes with both $I - 2|s,v_1\rangle\langle s,v_1| - 2|s,v_2\rangle\langle s,v_2|$ and U. Therefore, $TU' = U'T$. If the inductive assumption $T(U')^t|\Phi_0\rangle = (U')^t|\Phi_0\rangle$ is true, then we also have

$$T(U')^{t+1}|\Phi_0\rangle = U'T(U')^t|\Phi_0\rangle = (U')^{t+1}|\Phi_0\rangle,$$

completing the induction step. ■

Let $|s''\rangle = \frac{1}{\sqrt{2}}|s,v_1\rangle - \frac{1}{\sqrt{2}}|s,v_2\rangle$. Then, $(U')^t|\Phi_0\rangle$ is orthogonal to $|s''\rangle$ because $T|s''\rangle = -|s''\rangle$. We have $|s,v_1\rangle\langle s,v_1| + |s,v_2\rangle\langle s,v_2| = |s'\rangle\langle s'| + |s''\rangle\langle s''|$. Together with $(U')^t|\Phi_0\rangle \perp |s''\rangle$, this means

$$(I - 2|s,v_1\rangle\langle s,v_1| - 2|s,v_2\rangle\langle s,v_2|)(U')^t|\Phi_0\rangle = (I - 2|s'\rangle\langle s'|)(U')^t|\Phi_0\rangle.$$

Thus, U' can be replaced by U'' at every step.

The rest of the proofs is now similar to the case of 1 marked location, except that $|s,v\rangle$ is replaced by $|s'\rangle$ everywhere. Theorem 2 also follows similarly to the 1 marked item case, with $|s'\rangle$ instead of $|s,v\rangle$.

7 Proofs of the technical lemmas

In this section, we prove Lemmas 1, 3, 2, 4 and 5. We will repeatedly use the following result which can be found in many linear algebra textbooks.

Fact 1 *The eigenvectors of a real unitary matrix either have eigenvalue* ± 1 *or else they appear in conjugated pairs with eigenvalues* $e^{\pm i\omega}$ *and eigenvector* $|\pm\omega\rangle = \frac{1}{\sqrt{2}}(|R\rangle \pm i|I\rangle)$*, where* $|R\rangle$ *and* $|I\rangle$ *are real normalised vectors and* $\langle R|I\rangle = 0$*.*

Proof of Lemma 1: Let $g = 1 - Re(e^{i\theta_{min}})$. Then, for any $e^{i\theta} \in \mathcal{A}$, $Re(e^{i\theta}) > 1 - g$ and, for every eigenvector $|\omega\rangle$ with an eigenvalue in $\mathcal{A}$, $Re\langle\omega|U'|\omega\rangle > 1 - g$.

If there were more than two eigenvectors of U' in $\mathcal{H}'_0$ with eigenvalues on the arc $\mathcal{A}$, we could construct a linear combination $|a\rangle$ of them such that $|a\rangle \perp |\Phi_0\rangle, |s,v\rangle$. Since $|a\rangle$ is a linear combination of vectors $|\omega\rangle$ with $Re\langle\omega|U'|\omega\rangle > 1 - g$ we have $Re\langle a|U'|a\rangle > 1 - g$. But then $Re\langle a|U'|a\rangle = Re\langle a|U(I - 2|s,v\rangle\langle s,v|)|a\rangle = Re\langle a|U|a\rangle$. Since $|a\rangle$ is orthogonal to $|\Phi_0\rangle$ and all other 1-eigenvectors of U ($|a\rangle \in \mathcal{H}'_0$), $|a\rangle$ is a linear combination of eigenvectors of U at least g away from 1 and hence $Re\langle a|U|a\rangle \leq 1 - g$, which gives a contradiction. ■

Proof of Lemma 2: Let $|\Phi\rangle$ be the vector obtained by replacing every amplitude in $|\Phi_j^+\rangle$ by its complex conjugate. Since U_2 is a real unitary matrix, $U_2|\Phi_j^+\rangle = e^{i\theta_j}|\Phi_j^+\rangle$ implies $U_2|\Phi\rangle = e^{-i\theta_j}|\Phi\rangle$. Therefore, we can assume that $|\Phi_j^-\rangle$ is a complex conjugate of $|\Phi_j^+\rangle$. The coefficients a_j^+ and a_j^- are equal to the inner products $\langle\Phi_j^+|\psi_{start}\rangle$ and $\langle\Phi_j^-|\psi_{start}\rangle$. Since $|\psi_{start}\rangle$ is a real vector, these two inner products are complex conjugates and $a_j^+ = (a_j^-)^*$. By multiplying $|\Phi_j^+\rangle$ and $|\Phi_j^-\rangle$ with appropriate constants, we can achieve $a_j^+ = a_j^-$. ■

Proof of Lemma 3: First, we express $|\psi_{good}\rangle$ in the basis consisting of eigenvectors of U_2:

$$|\psi_{good}\rangle = a_0|\Phi_0\rangle + \sum_{j=1}^{m} a_j(|\Phi_j^+\rangle + |\Phi_j^-\rangle). \tag{20}$$

where $|\Phi_0\rangle = |\psi_{start}\rangle$. We define for real α

$$|w'_\alpha\rangle = a_0 \cot\frac{\alpha}{2}|\Phi_0\rangle + \sum_j a_j\left(\cot\frac{\alpha-\theta_j}{2}|\Phi_j^+\rangle + \cot\frac{\alpha+\theta_j}{2}|\Phi_j^-\rangle\right). \tag{21}$$

Similarly to Claim 2 in [Amb03], we have

Lemma 13 *If* $|w'_\alpha\rangle$ *is orthogonal to* $|\psi_{good}\rangle$*, then* $|\omega_\alpha\rangle = |\psi_{good}\rangle + i|w'_\alpha\rangle$ *is an eigenvector of* U' *with eigenvalue* $e^{i\alpha}$ *and* $|\omega_{-\alpha}\rangle = |\psi_{good}\rangle + i|w'_{-\alpha}\rangle$ *is an eigenvector of* U' *with eigenvalue* $e^{-i\alpha}$*.*

Proof: The proof is similar to [Amb03], but we include it for completeness.

Apply U' to $|\omega_\alpha\rangle$ and expand in the eigenbasis of U:

$$U'|\omega_\alpha\rangle = U(I-2|s,v\rangle\langle s,v|)(|\psi_{good}\rangle + i|w'_\alpha\rangle) = U(-|\psi_{good}\rangle + i|w'_\alpha\rangle) = a_0(-1+i\cot\tfrac{\alpha}{2})|\Phi_0\rangle + \sum_j a_j\left(e^{i\theta_j}(-1+i\cot\tfrac{\alpha-\theta_j}{2})|\Phi_j^+\rangle + e^{-i\theta_j}(-1+i\cot\tfrac{\alpha+\theta_j}{2})|\Phi_j^-\rangle\right).$$

In this equation, every coefficient is equal to the corresponding coefficient in $e^{i\alpha}(|\psi_{good}\rangle + i|w'_\alpha\rangle)$. Namely, for the coefficient of $|\Phi_0\rangle$, we have

$$\left(-1+i\cot\frac{\alpha}{2}\right) = \frac{e^{i(\frac{\pi}{2}+\frac{\alpha}{2})}}{\sin\frac{\alpha}{2}} = e^{i\alpha}\frac{e^{i(\frac{\pi}{2}-\frac{\alpha}{2})}}{\sin\frac{\alpha}{2}} = e^{i\alpha}\left(1+i\cot\frac{\alpha}{2}\right).$$

For the coefficient of $|\Phi_j^+\rangle$, we have

$$e^{i\theta_j}\left(-1+i\cot\frac{-\theta_j+\alpha}{2}\right) = e^{i\theta_j}\frac{e^{i(\frac{\pi}{2}-\frac{\theta_j}{2}+\frac{\alpha}{2})}}{\sin\frac{-\theta_j+\alpha}{2}} = e^{i\alpha}\frac{e^{i(\frac{\pi}{2}+\frac{\theta_j}{2}-\frac{\alpha}{2})}}{\sin\frac{-\theta_j+\alpha}{2}} = e^{i\alpha}\left(1+i\cot\frac{-\theta_j+\alpha}{2}\right)$$

and, similarly, the conditions for the coefficients of $|\Phi_j^-\rangle$ are satisfied. ■

By Eqs. (20) and (21), $\langle s,v|w'_\alpha\rangle = 0$ is equivalent to

$$a_0^2\cot\frac{\alpha}{2} + \sum_{j=1}^{m} a_j^2(\cot\frac{\alpha+\theta_j}{2} + \cot\frac{\alpha-\theta_j}{2}) = 0. \tag{22}$$

Let θ_{min} be the smallest of θ_1, …, θ_m. Then, this equation has exactly one solution in $[0,\theta_{min}]$ and one solution in $[-\theta_{min},0]$. The reason for that is that the cot function is decreasing (except for $x = k\pi$, where it goes to $-\infty$ for $x < k\pi$ and $+\infty$ for $x > k\pi$). Therefore, the whole right hand side is decreasing, except if one of $\frac{\alpha}{2}$, $\frac{\alpha+\theta_j}{2}$, $\frac{\alpha-\theta_j}{2}$ becomes a multiple of π. This happens for $\alpha = 0$ and $\alpha = \pm\theta_{min}$. Since θ_{min} is the smallest of θ_j, $[-\theta_{min},0]$ and $[0,\theta_{min}]$ contain no values of α for which one of the cot becomes infinity. On the interval $[0,\theta_{min}]$ the left-hand side of (22) goes to $+\infty$ if $\alpha\to 0$, $-\infty$ if $\alpha\to\theta_{01}$ and is 0 for exactly one value of α between 0 and θ_{01}. This means that the two eigenvectors of U' in the arc $\mathcal{A}$ are of the form $|s,v\rangle + i|\omega'_\alpha\rangle$ with $|\omega'_\alpha\rangle$ as in Eq. (21).

Next, let us determine this α. Since

$$\cot x + \cot y = \frac{\cos x}{\sin x} + \frac{\cos y}{\sin y} = \frac{\cos x\sin y + \cos y\sin x}{\sin x\sin y} = \frac{\sin(x+y)}{\sin x\sin y} = 2\frac{\sin(x+y)}{\cos(x-y)-\cos(x+y)},$$

Eq. (22) is equivalent to $a_0^2\cot\frac{\alpha}{2} + \sum_j 2a_j^2\frac{\sin\alpha}{\cos\theta_j-\cos\alpha} = 0$ which, in turn, is equivalent to

$$a_0^2\frac{\cot\frac{\alpha}{2}}{\sin\alpha} = \sum_j 2a_j^2\frac{1}{\cos\alpha-\cos\theta_j}.$$

For $\alpha = o(1)$, $\sin\alpha = (1-o(1))\alpha$ and $\cot\alpha = (1+o(1))\frac{1}{\alpha}$. Therefore, we have, with $\cos\alpha\le 1$

$$(1+o(1))\frac{a_0^2}{\alpha^2} = \sum_j a_j^2\cdot\frac{1}{\cos\alpha-\cos\theta_j} \ge \sum_j a_j^2\cdot\frac{1}{1-\cos\theta_j}. \tag{23}$$

This implies

$$\alpha \leq \frac{1}{\sqrt{2}} \frac{1}{\sqrt{\sum_j \frac{a_j^2}{a_0^2} \frac{1}{1-\cos\theta_j}}}. \tag{24}$$

It remains to lower bound α.

Assume that $\alpha < \frac{1}{2}\theta_{min}$. (Otherwise, the lower bound of the lemma is true.) Then, we have

$$\cos\alpha - \cos\theta_j \geq \cos\frac{\theta_j}{2} - \cos\theta_j \geq \frac{1}{2}(1-\cos\theta_j). \tag{25}$$

The first inequality follows from $\alpha < \frac{\theta_{min}}{2} \leq \frac{\theta_j}{2}$ and cos being decreasing on $[0,\pi]$. The second inequality is equivalent to $\cos\frac{\theta_j}{2} \geq \frac{1}{2}(1+\cos\theta_j)$ which follows from $1+\cos\theta_j = 2\cos^2\theta_j \leq 2\cos\theta_j$. Eq. (23) and (25) together imply

$$(1+o(1))\frac{a_0^2}{\alpha^2} \leq \frac{1}{2}\sum_j a_j^2 \frac{1}{1-\cos\theta_j}, \tag{26}$$

which implies the lower bound on α. ■

Proof of Lemma 4: We will show that the starting state is close to the state $|w_{start}\rangle = \frac{1}{\|w'_{start}\|}|w'_{start}\rangle$, $|w'_{start}\rangle = \frac{1}{\sqrt{2}}|w_\alpha\rangle - \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle$. By Eq. (21), we have

$$|w'_{start}\rangle = \sqrt{2}a_0 \cot\frac{\alpha}{2} i|\psi_{start}\rangle + \sum_j \sqrt{2}a_j \left(\cot\frac{\alpha+\theta_j}{2} - \cot\frac{\theta_j-\alpha}{2}\right) i\left(|\Phi_j^+\rangle - |\Phi_j^-\rangle\right).$$

We have $\langle\psi_{start}|w_{start}\rangle = \frac{\langle\psi_{start}|w'_{start}\rangle}{\|w'_{start}\|} = \frac{\sqrt{2}a_0\cot\frac{\alpha}{2}}{\|w'_{start}\|}$. Therefore, we need to bound $\|w'_{start}\|$. We have

$$\|w'_{start}\|^2 = 2a_0^2\cot^2\frac{\alpha}{2} + 4\sum_j a_j^2\left(\cot\frac{\alpha+\theta_j}{2} - \cot\frac{\theta_j-\alpha}{2}\right)^2.$$

Since $\cot x = (1+o(1))\frac{1}{x}$, the first term is $2(1+o(1))a_0^2\frac{4}{\alpha^2} = \Theta(a_0^2/\alpha^2)$. Similarly to the previous lemma, we have

$$\cot\frac{\alpha+\theta_j}{2} - \cot\frac{\theta_j-\alpha}{2} = \frac{\sin\alpha}{\cos\alpha-\cos\theta_j} = \frac{(1+o(1))\alpha}{\cos\alpha-\cos\theta_j}.$$

Since $\alpha < \frac{1}{2}\theta_{min}$, we have $\cos\alpha - \cos\theta_j \geq \frac{1}{2}(1-\cos\theta_j)$ (similarly to Eq. (25)). Therefore,

$$\frac{\|w'\|^2}{a_0^2\cot^2\frac{\alpha}{2}} \leq 1 + \frac{\sum_j a_j^2\left(\frac{(1+o(1))\alpha}{0.5(1-\cos\theta_j)^2}\right)^2}{\Theta(a_0^2/\alpha^2)} = 1 + \Theta\left(\alpha^2\sum_j \frac{a_j^2}{a_0^2}\left(\frac{\alpha}{(-\cos\theta_j}\right)^2\right).$$

This means that

$$\langle\psi_{start}|w\rangle = \frac{\sqrt{2}a_0\cot\frac{\alpha}{2}}{\|w'\|} = 1 - \Theta\left(\alpha^4\sum_j \frac{a_j^2}{a_0^2}\frac{1}{(1-\cos\theta_j)^2}\right).$$

■

Proof of Lemma 5: Let $|w_{good}\rangle = \frac{1}{\sqrt{2}}|w_\alpha\rangle - \frac{1}{\sqrt{2}}|w_{-\alpha}\rangle$. We consider the unnormalized state $|w'_{good}\rangle = |w'_\alpha\rangle - |w'_{-\alpha}\rangle$. Obviously, $|w_{good}\rangle = \frac{|w'_{good}\rangle}{\|w'_{good}\|}$. We have

$$|w'_{good}\rangle = 2a_0|\psi_{start}\rangle +$$

$$\sum_{j=1}^{m} a_j \left((2 + i\cot\frac{\alpha+\theta_j}{2} + i\cot\frac{-\alpha+\theta_j}{2})|\psi_j^+\rangle + (2 + i\cot\frac{\alpha-\theta_j}{2} + i\cot\frac{-\alpha-\theta_j}{2})|\psi_j^-\rangle \right).$$

Also $\langle\psi_{good}|w_{good}\rangle = \frac{\langle\psi_{good}|w'_{good}\rangle}{\|w'_{good}\|}$. Futhermore, $\langle\psi_{good}|w'_{good}\rangle = 2a_0^2 + \sum_{j=1}^m 4a_j^2 = 2\||\psi_{good}\rangle\|^2 = 2$. (The imaginary terms cancel out because $\cot\frac{\pm\alpha+\theta_j}{2} = -\cot\frac{\mp\alpha-\theta_j}{2}$.) It remains to bound $\|w'_{good}\|$. We have

$$\|w'_{good}\|^2 = 2a_0^2 + \sum_{j=1}^{m} 4a_j^2 + \sum_{j=1}^{m} 2a_j^2 \left(\cot\frac{\alpha+\theta_j}{2} + i\cot\frac{-\alpha+\theta_j}{2}\right)^2$$

$$= 2 + \sum_{j=1}^{m} 2a_j^2 \left(\cot\frac{\alpha+\theta_j}{2} + \cot\frac{-\alpha+\theta_j}{2}\right)^2.$$

Since $\alpha < \frac{1}{2}\theta_{min}$, this sum is at most

$$2 + \sum_{j=1}^{m} 2a_j^2 (2\cot\frac{\theta_j/2}{2})^2 \leq 2 + \Theta\left(\sum_{j=1}^{m} a_j^2 \cot^2\frac{\theta_j}{4}\right).$$

Therefore, $\|w'\| = \Theta(\max(\sqrt{\sum_j a_j^2\cot^2\frac{\theta_j}{4}}, 1))$ and $\langle\psi_{good}|w\rangle = \Theta\left(\min\left(\frac{1}{\sqrt{\sum_j a_j^2\cot^2\frac{\theta_j}{4}}}, 1\right)\right)$. ■

8 General graphs

The approach and methods we have presented are amenable to analyze quantum walk algorithms on other graphs G. All we need is the eigenspectrum of the unperturbed walk U, an appropriate subspace H'_0 containing no 1-eigenvectors of U (which is equivalent to proving that all but one 1-eigenvector of U is orthogonal to $|s\rangle$), and the sums in Lemmas 3, 4 and 5 involving the eigenvalues of U (which give the angle α and the overlaps). Then we can apply Lemmas 3-5 to get the desired result.

Hypercube: For instance we can derive the performance of the random walk search algorithm on the hypercube, given in [SKW03] without having to guess the form of the eigenvalues $|\pm\omega_0\rangle$. [SKW03] showed that the random walk search algorithm after time $T = \frac{\pi}{2}\sqrt{N}$ gives a probability of $\approx \frac{1}{2}$ to measure the marked state. For the d-dimensional hypercube (with $N = 2^d$ vertices), the transformation U has $d2^d$ eigenvectors. An argument similar to Claim 7 shows that the quantum walk stays in the 2^d-dimensional subspace spanned by 2^d eigenvectors with eigenvalues $e^{i\theta_k}$ [MR02] with

$$\cos\theta_k = 1 - \frac{2k}{d}$$

for $k = 0 \dots d$, each with degeneracy $\binom{d}{k}$. Among those, $|\Phi_0\rangle$ is the only eigenvector with eigenvalue 1, thus we have an instance of the abstract search. We can now apply Lemmas 3-5. For Lemma 3, we need to compute the sum of inverse gaps of all eigenvalues of U in Lemma 9, which is now of the form

$$\sum_{k=1}^{d} \binom{d}{k} \frac{1}{1-\cos\theta_k} = \frac{d}{2} \sum_{k=1}^{d} \binom{d}{k} \frac{1}{k} = 2^d(1+o(1)) = N(1+o(1)).$$

This gives a time $T = \Theta(\sqrt{N})$ to rotate the state. Evaluating the quantities in Lemmas 4 and 5 shows that measuring the final state gives a marked location with constant probability.

Remarks on general graphs We have seen that crucial to "good" performance of these algorithms are essentially two ingredients:

1. Coin property: The relevant Hilbert space $\mathcal{H}_0'$ of the perturbed walk U' does not contain 1 eigenvectors (i.e. all 1-eigenvectors of U except the starting state $|\Phi_0\rangle$ are orthogonal to the marked state $|s, v\rangle$).

2. Graph property: The gap g between the 1-eigenvalue and the real part of the next closest eigenvalue of U is sufficiently large (determines the overlap of the initial state with the two relevant eigenvectors). Furthermore the sum of inverse gaps of the eigenvalues of U, i.e. of terms $(1-\cos\theta)^{-1}$ where θ is an eigenvalue of U, is sufficiently small, such that the angle between the two eigenvectors of U' with eigenvalue closest to one is sufficiently large (determines the speed of the algorithm).

We call the first item a "Coin" property because, as we have seen, it is the choice of coin that determines this behavior. We call the second property a "Graph" property because the gap and the closeness of the perturbed eigenvalues to 1 depend on the topology of the graph.

To be more precise let us carry our argument through for *Cayley-graphs* of Abelian groups. The eigenvalues of the unperturbed walk U are "split" by the coin to be "around" the eigenvalues of the normalized adjacency matrix of the graph. More precisely, note that the adjacency matrix of a Cayley graph can be written as a sum of commuting shift operations over all d directions $A = \frac{1}{d}\sum_{i=1}^{d} S_i$. The eigenvalues of A are just sums of eigenvalues of shifts (which are the Fourier coefficients). For instance in the case of the grid the eigenvalues of A are of the form $\frac{1}{2}(\cos\frac{2k\pi}{\sqrt{N}} + \cos\frac{2l\pi}{\sqrt{N}}) = \frac{1}{4}(\omega^k + \omega^{-k} + \omega^l + \omega^{-l})$ for $k, l = 0 \dots \sqrt{N} - 1$. From Eq. (8) we see that in general the coin "changes" the eigenvalues to be some linear combination of $\omega^{\pm k,l}$. This is what happens in general, and the resulting eigenspectrum will have gaps of the same order of magnitude as the spectrum of the matrix A (which defines the simple random walk on the graph). Thus, it is likely that the sum $\sum_\theta \frac{1}{1-\cos\theta}$ (θ eigenvalue of U) which determine the speed of the algorithm can be estimated from graph properties alone (given a successful choice of coin).

Related work: Analyzing quantum walks on general graphs has been recently considered by Szegedy [Sze04] who has shown a following general result. If ε fraction of all vertices of a graph is marked and all eigenvalues of a graph differ from 1 by at least δ, then $O(\frac{1}{\sqrt{\varepsilon\delta}})$ steps of quantum walk suffice. This contributes to the same goal as our paper: developing general tools for analyzing quantum walks and using them in quantum algorithms.

The power of two methods (ours and [Sze04]) seems to be incomparable. The strength of our method is that it is able to exploit a finer structure of the graph. For example, consider the 2-dimensional grid with a unique marked item. Applying the theorem of [Sze04] gives a running time of $O(N^{3/4})$, compared to $O(\sqrt{N}\log N)$ for ours. (One marked item is a $1/N$ fraction of all items and the eigenvalue gap δ for the grid is $1/\sqrt{N}$.) The reason for this difference is that *most* eigenvalues are far from 1. The approach of [Sze04] uses worst-case (minimum) difference between 1 and eigenvalues of the graph, which is small ($\frac{1}{\sqrt{N}}$). Our approach uses a quantity ($\sum_\theta \frac{1}{1-\cos\theta}$) that involves all eigenvalues, capturing the fact that most eigenvalues are not close to 1.

The strength of Szegedy's [Sze04] analysis is that it allows to handle multiple marked locations with no extra effort, which we have not been able to achieve with our approach. It might be interesting to combine the methods so that both advantages can be achieved at the same time.

9 Conclusion

We have shown that the discrete quantum walk can search the 2D grid in time $O(\sqrt{N}\log N)$ and higher dimensional grids in time $O(\sqrt{N})$. This improves over previous search algorithm and shows an interesting difference between discrete and continous time quantum walks. More generally, we have opened the route to a general analysis of random walks on graphs by providing the necessary toolbox.

The main open problems are applying this toolbox to other problems and learning to analyze quantum walks if there are multiple (more than 2) marked locations. In the case of our problem, it is possible to reduce the multiple marked location case to the single location case at the cost of increasing the running time by a factor of $\log N$ [AA03]. Still, it would be interesting to be able to analyze the multiple item case directly. A recent paper by Szegedy [Sze04] has shown how to analyze the multiple solution case for a different quantum walk algorithm, element distinctness [Amb03]. It is open whether the methods from [Sze04] can be applied to search on grids.

Acknowledgements Above all we thank Neil Shenvi for providing us with the results of his numerical simulations and stimulating us to search for an analytical proof. JK thanks Frédéric Magniez and Oded Regev for helpful discussions. AA is supported by NSF Grant DMS-0111298. Part of this work was done while AA was at University of Latvia and University of California, Berkeley, supported by Latvia Science Council Grant 01.0354 and DARPA and Air Force Laboratory, Air Force Materiel Command, USAF, under agreement number F30602-01-2-0524, respectively. JK acknowledges support by ACI Sécurité Informatique, 2003-n24, projet "Réseaux Quantiques" and by DARPA and Air Force Laboratory, Air Force Materiel Command, USAF, under agreement number F30602-01-2-0524, and by DARPA and the Office of Naval Research under grant number FDN-00014-01-1-0826. Any opinions, findings, conclusions or recommendations expressed in this paper are those of authors and do not necessarily reflect the views of funding agencies.

References

[AA03] S. Aaronson and A. Ambainis. Quantum search of spatial regions. In *Proc. 44th Annual IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 200–209, 2003.

[AAKV01] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proc. 33th STOC*, pages 50–59, New York, NY, 2001. ACM.

[ABN+01] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous. One-dimensional quantum walks. In *Proc. 33th STOC*, pages 60–69, New York, NY, 2001. ACM.

[Amb03] A. Ambainis. Quantum walk algorithm for element distinctness, 2003. lanl-arXive quant-ph/0311001.

[Ben02] Paul Benioff. Space searches with a quantum robot. In *Quantum computation and information (Washington, DC, 2000)*, volume 305 of *Contemp. Math.*, pages 1–12. Amer. Math. Soc., Providence, RI, 2002.

[BHMT02] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum computation and information (Washington, DC, 2000)*, volume 305 of *Contemp. Math.*, pages 53–74. Amer. Math. Soc., Providence, RI, 2002.

[CCD+03] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proc. 35th STOC*, pages 59–68, 2003. quant-ph/0209131.

[CE03] A.M. Childs and J.M. Eisenberg. Quantum algorithms for subset finding. Technical report, lanl-arXive quant-ph/0311038, 2003.

[CFG02] A. Childs, E. Farhi, and S. Gutmann. An example of the difference between quantum and classical random walks. *Quantum Information Processing*, 1:35, 2002. lanl-report quant-ph/0103020.

[CG03] A.M. Childs and J. Goldstone. Spatial search by quantum walk. Technical report, lanl-arXive quant-ph/0306054, 2003.

[FG98] E. Farhi and S. Gutmann. Quantum computation and decision trees. *Phys. Rev. A*, 58:915–928, 1998.

[Gro96] L. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th STOC*, pages 212–219, Philadelphia, Pennsylvania, 1996. ACM Press.

[Kem03a] J. Kempe. Quantum random walks - an introductory overview. *Contemporary Physics*, 44(4):302–327, 2003. lanl-arXive quant-ph/0303081.

[Kem03b] J. Kempe. Quantum walks hit exponentially faster. In *RANDOM-APPROX 2003*, Lecture Notes in Computer Science, pages 354–369, Heidelberg, 2003. Springer. lanl-arXiv quant-ph/0205083.

[Mey96] D. Meyer. From quantum cellular automata to quantum lattice gases. *J. Stat. Phys.*, 85:551–574, 1996.

[MR95] R. Motwani and P. Raghavan. Randomized Algorithms. Cambridge University Press, 1995.

[MR02] C. Moore and A. Russell. Quantum walks on the hypercube. In J.D.P. Rolim and S. Vadhan, editors, *Proc. RANDOM 2002*, pages 164–178, Cambridge, MA, 2002. Springer.

[MSS03] F. Magniez, M. Santha, and M. Szegedy. Quantum algorithms for the triangle problem. Technical report, 2003. lanl-arXive quant-ph/0310134.

[SKW03] N. Shenvi, J. Kempe, and K.B. Whaley. A quantum random walk search algorithm. *Phys. Rev. A*, 67(5):052307, 2003. lanl-arXive quant-ph/0210064.

[She03] Neil Shenvi. Random Walk Simulations. unpublished.

[Sze04] M. Szegedy. Spectra of quantized walks and a $\sqrt{\delta\varepsilon}$ rule, quant-ph/0401053.