QUANTUM INFORMATION AND COMPUTATION: REPORT

Edin Husić
edin.husic@ens-lyon.fr

ENS DE LYON

Discrete quantum random walks

Abstract

In this report, we present the ideas behind the notion of quantum random walks. We further restrict our attention to the paper "Search via quantum walk" by Magniez, Nayak, Roland and Santha and give some general insights and intuition behind their work. The report is intended for the final exam evaluation in the subject "Quantum Information and Computation".

1 General overview

Markov chains are widely used in mathematics and in mathematical modeling for different areas of science such are economics and finance, mathematical biology, genetics, chemistry and computer science in general. In classical computer science Markov chains (random walks) are one of the main algorithmic tool for developing randomized algorithms. As such they are used in many search or sampling algorithms. As an example, one of the best algorithms for solving $3SAT$ is based on the idea of random walk [7]. Nice properties, mathematical foundations and their wide use motivated researchers to investigate how could we use Markov chains on quantum computers. Quantum analogues of random walks emerged gradually in two main directions, discrete time random analogues and a continuous time quantum walk model which can be track back to the work of Feynman [5]. It is worth noticing that continuous random walks can be used as a general model for quantum computation, with any quantum computation represented in some underlying graph. The result was shown by Childs, based on some of the first works on quantum computing by Feynman [3]. Here we give a short overview of discrete time quantum walks and mostly restrict our attention to a one of the latest models proposed, as it is described in the work of Magniez, Nayak, Roland and Santha [6].

Basic ideas and known results: Quantum walk algorithms generally turned out to outperform classical random walks it two ways. First, quantum random walks usually have a faster hitting time, i.e., the expected time of particle moving from a source vertex to a target vertex. Second, they have faster mixing time, that is, the time time taken to spread out over all vertices. It is shown that for the special class of graphs, hitting time of quantum walks can be exponentially faster than in the classical case [4]. In general setting, it has been shown that the separation between quantum and classical mixing time can be quadratic, but no more than this [1].

One of the first discrete time quantum walks introduced, considers an analogue of classical random walk on a line with non-negative transition probabilities only for going left or right on the line. In other words, it consists of a particle ("the walker") jumping at each step either left or right depending on the outcome of the probability system ("the coin"). Quantum analogue of a such random walk consists of three main components: a walker, a coin and evaluation operators. It is based on two quantum systems, one for the walker and one for the coin. The walker is represented by a Hilbert space spanned by the basis states corresponding to the possible positions of the walker. The coin is represented by a 2-dimensional Hilbert space, consider it as a Hilbert space spanned by basis vectors corresponding to outcomes of zero and one of the coin. The total state of the quantum walk is then the tensor product of two states from spaces described above. To simulate the jump of the walker we use an evolution operator to the coin state followed by a conditional shift operator to the total quantum system. Since we are in quantum world now, this allows the walker and the coin to be in a superposition and new possibilities for algorithms. Similarly the quantum random walks on a finite cycle were introduced.

Although simple, this model is used to build more complicated random walks on graphs and to understand important properties of quantum random walks. It can also be used to test the quantumness of a realization of a quantum computer. For more details on quantum walks and their development, we refer the reader to a nice and comprehensive review [9].

All of above shows the importance of random walks in classical computer science as well as in quantum computer science.

We now continue with the review of the main paper considered.

2 Problem statement and previous results

Markov chain preliminaries: For a Markov chain over a finite state set X, the *transition matrix* is $P = (p_{xy})$ where p_{xy} is probability of transition from x to y. A Markov chain is *irreducible* if there is a positive probability for transition from every state to any other state in some number of steps.

An irreducible chain is *ergodic* if it is aperiodic. Every irreducible chain has a unique stationary distribution $\pi = (\pi_x)$, which can be thought as probability of being in state x after infinitely many steps of Markov chain. All eigenvalues of P are not bigger than 1 in the absolute value. If chain is ergodic then eigenvalue 1 is a unique eigenvalue having absolute value 1. The *eigenvalue gap* $\delta(P)$ is $1 - \lambda$ where λ is the maximum absolute value of some eigenvalue not equal to 1. The *time-reversed* Markov chain $P^* = (p^*_{xy})$ of P is determined by equations $\pi_x p_{xy} = \pi_y p^*_{yx}$. The chain is reversible if and only if $P = P^*$. The Markov chain is symmetric if and only if P is equal to its transpose. It is easy to show that stationary distribution of any symmetric Markov chain is the uniform distribution.

Classical problem: We consider an abstract problem of finding a marked element from the set X with n elements. That is, a problem of finding an element of a set of marked elements M, where $M \subseteq X$. The set M is given implicitly with additional data structure that we will formally define later. Using this structure we are able to check if an element x is in M. The most simple solution for the problem would be to uniformly at random sample the elements of X until we find a marked element, but a more efficient solution would include simulating a Markov chain on the state space X to take advantage of a possible structure present in the set X. We will see how this could be done in classical case, and then we state known results for their quantum analogues. Now, we present classical algorithms to better understand their quantum analogues later.

Algorithm 1: Classical search

```
Sample a state $x$ from a probability distribution $s$ on the set $X$;
for $t_2$ steps do
    if state $y$ reached in previous step is marked then
        return $y$ and stop;
    else
        simulate $t_1$ steps of $P$ starting with current state $y$;
    end
end
return no marked elements
```

The values t_1 and t_2 in Algorithm 1 are determined by the properties of P. Intuitively, if we consider some ergodic Markov chain P and high enough value t_1 is the same as sampling the state y from the stationary distribution π of P. Then we sample y for t_2 steps until we find a marked element. In order to find a marked with high probability[1], we take t_2 inversely proportional to the stationary distribution of P. The second algorithm is a more natural version of the first algorithm, where the value t_1 is set to one.

[1] Under the term high probability, we consider a constant positive probability.

Algorithm 2: Classical search

```
Sample a state $x$ from a probability distribution $s$ on the set $X$;
for $t_2$ steps do
    if state $y$ reached in previous step is marked then
        return $y$ and stop;
    else
        simulate one step of $P$ starting with current state $y$;
    end
end
return no marked elements
```

To state complexity of the above algorithms we first consider a model for it that will also nicely translate to the quantum algorithm. We consider three different types of costs. Before that, since these are search algorithms, we need to formalize procedure of determining whether $x \in M$. As said before, we also have a data structure keeping data $d(x)$, for each $x \in X$. From it we can determine if for some state x it holds $x \in M$. Then, the following costs for classical algorithms are considered:

- **Set-up cost** S : The cost of sampling an element x and constructing $d(x)$.
- **Update cost** U : The cost of simulating a step of a Markov chain and updating data structure for the step we made.
- **Checking cost** C : The cost of checking if $x \in M$ using data structure $d(x)$.

The following proposition captures the complexity of the classical algorithms.

Proposition 1 ([6])**.** *Let $\delta > 0$ be the eigenvalue gap of ergodic, symmetric Markov chain P on space X and $|X| = n$. Let $\frac{|M|}{|X|} \geq \epsilon > 0$. For uniform distribution s*

- *Algorithm 1 finds a marked element with high probability if $t_1 \in O(\frac{1}{\delta})$ and $t_2 \in O(\frac{1}{\epsilon})$ are suitably large with the cost of order $S + \frac{1}{\epsilon}\left(\frac{1}{\delta}U + C\right)$.*
- *Algorithm 2 finds a marked element with high probability if $t \in O(\frac{1}{\delta\epsilon})$ is suitably large, with the cost of order $S + \frac{1}{\epsilon\delta}(U + C)$.*

Quantum formalization of the problem: The idea of the quantum random walk used here has already appeared in [2, 8]. The intuition of random walks defined in mentioned works, can be seen as a random walk on the edges of the Markov chain instead of vertices. At each step, one vertex of an edge (x, y), say y, is "mixed" over all possible neighbors of x. The paper of Magniez et al. follows the same idea, while their algorithm and analysis of algorithms are simpler.

To define the problem in quantum setting we consider the problem where a finite set X is given together with a data structure d maintened through the algorithm. To be able to consider data structure in quantum algorithms, we consider the space X_d which represents the set of elements of X together with data structure d, formally $X_d = \{(x, d(x)) : x \in X\}$. Following the intuition behind quantum random walks, we define the quantum analogues of the costs:

- **Quantum Set-up cost** S **:** The cost of constructing the state $\sum_{x\in X} \sqrt{\pi_x} \left|x\right\rangle_d \left|0\right\rangle_d$ from $\left|0\right\rangle_d \left|0\right\rangle_d$.
- **Quantum Update cost** U **:** The cost of realizing one of unitary transformations
$$\left|x\right\rangle_d \left|0\right\rangle_d \to \left|x\right\rangle_d \sum_{y\in X} \sqrt{p_{xy}} \left|y\right\rangle_d$$
$$\left|0\right\rangle_d \left|y\right\rangle_d \to \sum_{x\in X} \sqrt{p^*_{xy}} \left|y\right\rangle_d \left|y\right\rangle_d$$
and their inverses.
- **Quantum Checking cost** C **:** The cost of realizing conditional phase flip
$$\left|x\right\rangle_d \left|y\right\rangle_d \to \begin{cases} -\left|x\right\rangle_d \left|y\right\rangle_d, & \text{if } x \in M \\ \left|x\right\rangle_d \left|y\right\rangle_d, & \text{otherwise.} \end{cases}$$

Observe that the quantum update cost can be used to express the complexity of "mixing" the state over all neighbors of some vertex x.

We state the previous results for the problem of finding a marked elements in the following two theorems. Theorem 2 due to Ambainis, is a quantum analogue of Algorithm 1 and Theorem 3 due to Szegedy is a quantum analogue of Algorithm 2. As we can see, simper approach of Algorithm 2 comes with the additional price in the terms of complexity. The result of Magniez et al. combines the approach of both results and improves them while having the complexity of the faster algorithm. The algorithm due to Magniez et al. is more similar to the quantum analogue of Algorithm 1.

Theorem 2 (Ambainis [2])**.** *Let P be the random walk on the Johnson graph*[2] *on r-subsets of a universe of size m, where $r = o(m)$, and with intersection size $r - 1$ Let M either empty, of the class of all $r-$subsets that contain a fixed subset of size $k \leq r$. Then, there is a quantum algorithm that with high probability, determines if M is empty or finds the k-subset, with cost of order $S + \frac{1}{\sqrt{\delta}}\left(\frac{1}{\sqrt{\epsilon}}U + C\right)$.*

Theorem 3 (Szegedy [8])**.** *Let $\delta > 0$ be the eigenvalue gap of ergodic, symmetric Markov chain P, and let $\frac{|M|}{|X|} \geq \epsilon > 0$. There exists a quantum algorithm that determines, with high probability, if M is non-empty with cost of order $S + \frac{1}{\sqrt{\delta\epsilon}}(U + C)$.*

[2] Johnson graph is a graph having as vertices subsets of size r of a universal set of size m, and edge between two vertices if their intersection is of size $r - 1$.

The algorithm proposed by Magniez et al. expends the scope of the two previously known algorithms in the sense that it *finds* a marked element and is being applicable to all finite ergodic Markov chains without considering special cases.The algorithm combines both of the previously known works, taking the quantum random walks as defined in [8] and the idea that is more similar as in [2].

3 Quantum analogue of Markov chain

Let P be the transition matrix of an irreducible Markov chain on a finite state space X. Denote $|X| = n$. Magniez et al. define the notion of quantum analogue of a classical Markov chain following the approach of Ambainis [2] and later Szegedy [8]. Quantum analogues are defined using two reflection operators.

Let $|\psi\rangle \in \mathcal{H}$. The orthogonal projector onto $\mathrm{Span}(|\psi\rangle)$ is denoted as Π_ψ, where $\Pi_\psi = |\psi\rangle\langle\psi|$. Then the reflection operator through the line generated by $|\psi\rangle$ is $\mathrm{ref}(\psi) = 2\Pi_\psi - Id = 2|\psi\rangle\langle\psi| - Id$. Let $\{|\psi_i\rangle : i \in I\}$ be an orthonormal basis of $\mathcal{K}$ a subspace of $\mathcal{H}$, then orthogonal projector onto $\mathcal{K}$ is $\Pi_\mathcal{K} = \sum_{i\in I} \Pi_{|\psi_i\rangle}$. The reflection through $\mathcal{K}$ is $\mathrm{ref}(\mathcal{K}) = 2\Pi_\mathcal{K} - Id$.[3] Let $x, y \in X$ and vectors $|p_x\rangle, |p_x\rangle$ be

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

Let $\mathcal{A} = \mathrm{Span}\left(|x\rangle|p_x\rangle : x \in X\right)$ and $\mathcal{B} = \mathrm{Span}\left(|p^*_y\rangle|y\rangle : y \in X\right)$ be vector subspaces of $\mathcal{H} = \mathbb{C}^{X\times X}$.

Definition 1 (Quantum walk [6], [8])**.** *The unitary operator $W(P)$ defined on $\mathcal{H}$ as $W(P) = \mathrm{ref}(\mathcal{A})\,\mathrm{ref}(\mathcal{B})$ is called the* quantum walk *based on the classical transition matrix P.*

It is worth mentioning that the above definition is first appeared in the work of Szegedy [8] where it was introduced with bipartite walks and it is consistent with the prior work in the area. It is also not clear what is the real intuition and motivation behind the definition of quantum walk. Szegedy abstracted the approach of Ambianis [2] to define quantum walks with bipartite walks, and Magniez et al. define in the same way but avoiding bipartite walks.

Similarly as the eigenspectrum and eigenvalue gap play a very important roll in the analysis of classical Markov chains the spectral decomposition plays an important roll in quantum setting. These properties are determined through the *discriminant matrix* $D(P) = (\sqrt{p_{xy}p^*_{yx}})$. Since $\sqrt{p_{xy}p^*_{yx}} = \sqrt{\pi_x}p_{xy}\sqrt{\pi_y}$ we can write

$$D(P) = diag(\pi)^{1/2} \cdot P \cdot diag(\pi)^{-1/2}\,.$$

The matrix $diag(\pi)$ is diagonal matrix with the distribution π on the diagonal. Observe that matrices $D(P)$ and P are similar and hence have the same

[3] Id is always the identity operator in a corresponding vector space.

eigenvalues. Hence all singular values of $D(P)$ lie in $[0,1]$ and we can express them as $\cos\theta$ for some $\theta \in \left[0, \frac{\pi}{2}\right]$. The *phase gap* $\Delta(P)$ of $W(P)$ is 2θ where θ is the smallest angle in $\left(0, \frac{\pi}{2}\right)$ such that $\cos\theta$ is singular value of $D(P)$. This is value that plays the similar role in quantum random walks as the eigenvalue gap plays in the classical random walks. The definition is motivated by the fact that angular distance of 1 and any other eigenvalue is at least $\Delta(P)$.

It is pointed out in [9] that a development of a quantum walk operator W based on a classical transition matrix is "remarkable feature" of [8], and that surely adds to the importance of work of Magniez et al. Besides that, it would be also interesting to see if there is a quantum notion that is not just an analogue of a classical Markov chain defined for a given Markov chain, but rather a self contained generalization of the notion of classical Markov chain. Of course this is not so easy question, one could even argue that it is not really possible to do. The main idea of Markov chain is the idea of "forgetting the past" and making the next step based just on the current position of the walker which could be the problem since all allowed operations in quantum computing have to be unitary and hence reversible. The similar problem due to reversibility of unitary operations is pointed out in [5] for the convergence to the stationary distribution of a Markov chain.

4 Quantum search algorithm

We will present the idea of the quantum algorithm for reversible Markov chains. The generalization for non-reversible Markov chains can be found in Section 5 of [6]. Generalization is based on the examining the singular values of $D(P)$ and showing that even when irreducible Markov chain in not necessary reversible, there is a unique singular value of $D(P)$ equal to 1. Also, this does not impact the execution of the algorithm, so from now on we assume that P is a transition matrix of an ergodic, reversible Markov chain.

The main idea here is to use quantum phase estimation to the quantum walk $W(P)$ to be able to implement an approximation of reflection operator about the initial state. Later they used this in a reversible amplitude amplification scheme to get the final algorithm. This is a new idea that turn out to be useful in both its generality an simplicity when compared to previous work. For example Szegedy [8] uses a different approach. He uses the *leaking matrix* P_M, which is obtained from P by deleting rows and columns indexed by M, to find the classical hitting time of M and then also properly define quantum hitting time and bounds it using the classical hitting time.

The algorithm proposed by Magniez et al. can be seen as the quantum analogue of Algorithm 1. The quantum algorithm starts with the initial state

$$|\pi\rangle = \sum_{x \in X} \sqrt{\pi_x}\,|x\rangle\,|p_x\rangle = \sum_{y \in X} \sqrt{\pi_y}\,|p_y^*\rangle\,|y\rangle$$

which corresponds to the stationary distribution π in the classical case. This state can be prepared with cost of $S + U$ as following. We use one set-up operation to prepare $\sum_{x\in X}\sqrt{\pi_x}\,|x\rangle\,|0\rangle$ and then one update operation to go to $\sum_{x\in X}\sqrt{\pi_x}\,|x\rangle\,|p_x\rangle$. Assume that $M \neq \emptyset$, and let $\mathcal{M} = \mathbb{C}^{M\times X}$ be the subspace with marked items in the first register. Then the idea of the algorithm is to transform the initial state $|\pi\rangle$ to the target state $|\mu\rangle$ which is a projection of $|\pi\rangle$ onto the subspace $\mathcal{M}$. The later can be done exactly if we would have a way of computing the reflection operator efficiently, but naive way turns out to be too expensive and the authors propose approximation of the reflection operator. The result regarding the approximation of reflection operator is contained in Theorem 4. The proof relies on k repetitions of quantum phase estimation to get k identical copies of estimates of a phase which increases the precision of phase estimation. Further more, the approximation of reflection operator fixes the unique eigenvector corresponding to the unique eigenvalue 1 of $W(P)$. Such a produced operator is the main concept used in the paper.

Theorem 4. *Let P a transition matrix of an ergodic Markov chain on a state space of size $n \geq 2$, such that the phase gap of the quantum walk $W(P)$ based on P is $\Delta(P)$. Then for any integer k there exists a quantum circuit $R(P)$ that acts on $2\log_2 n + ks$ qubits, where $s \in \log_2\left(\frac{1}{\Delta(P)}\right) + O(1)$, and satisfies the following:*

1. *The circuit $R(P)$ uses $2ks$ Hadamard gates, $O(ks^2)$ controlled phase rotations, and makes at most $k2^{s+1}$ calls to the controlled quantum walk c-$W(P)$ and its inverse c-$W(P)^\dagger$.*

2. *If $|\pi\rangle$ is the unique 1-eigenvector of $W(P)$ as defined above, then $R(P)\,|\pi\rangle\,|0^{ks}\rangle = |\pi\rangle\,|0^{ks}\rangle$.*

3. *If $|\psi\rangle$ lies in the subspace spanned by $\mathcal{A}$ and $\mathcal{B}$ orthogonal to $|\pi\rangle$, then $||\,(R(P) + Id)\,|\psi\rangle\,|0^k s\rangle\,|| \leq 2^{1-k}$.*

Now we are able to state the main algorithm in the paper.

Algorithm 3: Quantum search (P, ϵ)

```
1  for 5 steps do
2      Sample a state $x$ from a probability distribution $\pi$ of $P$;
3      if $x \in M$ then
4          output $x$ and stop ;
5      end
6  end
7  Choose $T$ uniformly a random in $[0, 1/\sqrt{\epsilon}]$, let $k \in \log_2(T) + O(1)$, and
     let $s$ as given by Theorem 4 ;
8  Prepare the initial state $|x\rangle_d |0^{Tks}\rangle$;
9  for T steps do
10     For any basis vector $|x\rangle_d |y\rangle_d |z\rangle$ of $\mathcal{H}$ and the ancillary $(Tks)$-qubit
         space, flip the phase if $x \in M$;
11     Apply circuit $R(P)_d$ of Theorem 4 with $k$, using new set of ancillary
         qubites $|0^{ks}\rangle$ in each iteration;
12 end
13 Observe the first register;
14 return  x if $x \in M$, and "no marked elements" otherwise;
```

The first **for** loop is used to deal with the case when probability of some element being marked p_M is bigger than 1/4, otherwise we $\epsilon \leq p_M \leq 1/4$. Then the step 7 is a version of randomized Grover's search. The next **for** loop is uses the mentioned approximation of reflection operator which as we know is used to model quantum random walk and it is easier to think of it as quantum analogue of Algorithm 1. The following theorem stated proves that the speed up using the quantum computation is quadratic in comparison with classical algorithm.

Theorem 5. *Let δ be the eigenvalue gap of an ergodic, reversible Markov chain P , and let $\epsilon > 0$ be a lower bound on the probability that an element chosen from the stationary distribution of P is marked whenever M is non-empty. Then, with high probability, Algorithm 3 determines if M is empty or finds and element of M, with cost of order $S + \frac{1}{\sqrt{\epsilon}}\left(\frac{1}{\sqrt{\delta}}U + C\right)$.*

The quandartic speed up in quantum case lies in the relation of the phase gap $\Delta(P)$ of $W(P)$ and the eigenvalue gap δ of P. It is shown that $\Delta(P) > 2\sqrt{\delta}$.

5 Comments and questions

Interesting question about random walks and in general quantum computation is whether the computation really uses the quantumness, and is the quantumness necessary?! There have been several arguments for possibility of using classical physics for building experiments that would replicate some interference and statistical properties of quantum walks and model discrete random walks on a line. It has been also argued that quantum properties are necessary for testing the quantumness of a quantum computer realization and for the walks that would include more walkers. It still not known weather more complicated random walks require quantum implementation or they can be implemented using some other classical tools as wave interference of electromagnetic filed [9].

It is highly improbable that the given quantum algorithm does not require quantumness, since it relies on several famous results in quantum computation such are phase estimation, Grover's search and amplitude amplification. On the other side, Algorithm 3 is optimal for the problem in its full generality and the only question would be to try to simplify it even more, or improve it for the special cases of the problem of finding marked element in a finite set.

Regarding the notion of quantum walks, one can ask how could we apply similar definition of quantum walk on Markov chains with infinitely many states. It is not obvious how one could do this since the notion of quantum walks relies on the transition matrix.

References

[1] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 50–59. ACM, 2001.

[2] A. Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.

[3] A. M. Childs. Universal computation by quantum walk. *Physical review letters*, 102(18):180501, 2009.

[4] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 59–68. ACM, 2003.

[5] J. Kempe. Quantum random walks: an introductory overview. *Contemporary Physics*, 44(4):307–327, 2003.

[6] F. Magniez, A. Nayak, J. Roland, and M. Santha. Search via quantum walk. *SIAM Journal on Computing*, 40(1):142–164, 2011.

[7] T. Schoning. A probabilistic algorithm for k-sat and constraint satisfaction problems. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, pages 410–414. IEEE, 1999.

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

[9] S. E. Venegas-Andraca. Quantum walks: a comprehensive review. *Quantum Information Processing*, 11(5):1015–1106, 2012.