MPRI 2.34.2: Quantum Information and Cryptography **2024 - 2025**

Lecture 1: Quantum walk search

Lecturer: Simon Apers (apers@irif.fr)

1 Random walks: mixing time and hitting time

We consider a simple (undirected, unweighted) and d-regular graph $G = (V, E)$ with $|V| = n$ vertices. A random walk on G starts from some initial vertex (sampled from a distribution p_0 over V), and at every timestep hops uniformly at random to one of its d neighboring vertices. We can describe the probability distribution after t steps using a stochastic transition matrix P where $P_{x,y} = 1/d$ if $(x, y) \in E$ and $P_{x,y} = 0$ otherwise. After t steps the random walk distribution is

$$p_t = P^t p_0.$$

If the graph G is connected then P has a unique stationary distribution π such that $P\pi = \pi$, and moreover this is the unique eigenvalue-1 eigenvector of P.

Exercise 1. *Using that G is regular, argue that π must be the uniform distribution.*

If in addition G is not bipartite, then p_t converges to π as $t \to \infty$, irrespective of the initial distribution p_0. The time it takes to get close to π is quantified by the *mixing time*.

Definition 1 (Mixing time)**.** *The ϵ-mixing time of a random walk with transition matrix P is*

$$\mathrm{MT}(\epsilon) = \min\{t \mid \|P^t p_0 - \pi\|_1 \leq \epsilon, \forall p_0\}.$$

On its turn, the mixing time can be related to the *spectral gap* δ of the transition matrix P. If we order the (real) eigenvalues of P as $1 = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq -1$, then the spectral gap is defined as

$$\delta = 1 - \max\{|\lambda_2|, |\lambda_n|\}.$$

The graph is connected and nonbipartite (i.e., has a finite mixing time) if and only if $\delta > 0$. In the exercises you will prove that

$$\mathrm{MT}(\epsilon) \in O\left(\frac{1}{\delta} \log \frac{n}{\epsilon}\right).$$

A different quantity of interest is the random walk *hitting time* $\mathrm{HT}(M)$, defined with respect to some subset of "marked" elements $M \subseteq V$ (e.g., solutions to some search problem). We define it as the expected number of steps of a random walk, starting from the stationary distribution $p_0 = \pi$, until it hits an element of M. The hitting time can also be bounded in terms of the spectral gap:

$$\mathrm{HT}(M) \in O\left(\frac{1}{\delta} \frac{1}{\pi(M)}\right).$$

You can prove this in the exercises (up to a logarithmic factor).

2 Quantum walks

It is clear from the bounds on the random walk mixing time and hitting times that critical roles are played by (i) the stationary distribution of the random walk, which corresponds to the unique eigenvalue-1 eigenvector of P, and (ii) the spectral gap surrounding this eigenvalue. In the following, we show how to construct a *quantum walk* operator $W(P)$ whose stationary state and surrounding gap are closely related to those of P.

2.1 Quantum walk operator

While a random walk is defined over the vertices of a graph, a quantum walk is defined over its edges. Specifically, the state space of a quantum walk is spanned by states of the form $|x, y\rangle$ for $(x, y) \in E$. You can think about the first register as containing the "current" state x, while the second register contains the "next" state y. In that sense, we could implement a "step" of the quantum walk through the shift operator S defined by

$$S\,|x, y\rangle = |y, x\rangle\,.$$

Instead of trivially repeating this, we alternate a step with a "coin toss" that mixes up the next state. We define it using so-called *star states* $|\psi_x\rangle$ for $x \in V$, defined as

$$|\psi_x\rangle = \frac{1}{\sqrt{d}} \sum_{(x,y)\in E} |x, y\rangle\,.$$

Notice that if we measure this state, then the second register contains a uniformly random neighbor of x. We can define a unitary coin toss operator $C(P)$ based on these star states. Specifically, the coin toss implements a reflection around the star states:

$$C(P) = 2\left(\sum_{x\in V} |\psi_x\rangle\,\langle\psi_x|\right) - I.$$

The quantum walk operator $W(P)$ is now described as

$$W(P) = S \cdot C(P).$$

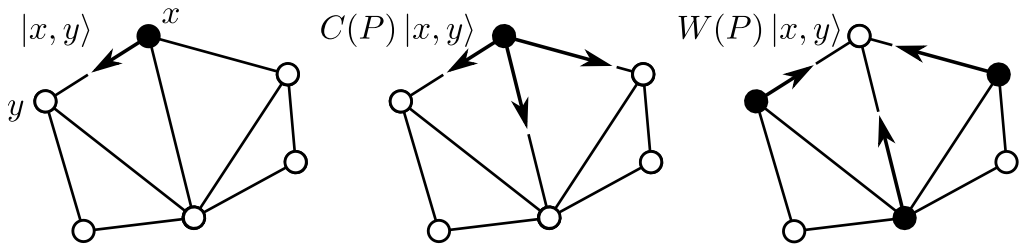


Figure 1: Figure demonstrating a single quantum walk step. (l) A basis state $|x, y\rangle$ is identified with the (directed) edge (x, y). (m) The coin toss $C(P)$ maps an initial state $|x, y\rangle$ to a superposition of outgoing edges. (r) The shift S maps a state $|x, y\rangle$, localized on node x, to a state $|y, x\rangle$, localized on node y.

Exercise 2. *Show that the following quantum state is a stationary state of $W(P)$:*

$$|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{x \in V} |\psi_x\rangle = \frac{1}{\sqrt{nd}} \sum_{(x,y) \in E} |x, y\rangle \,.$$

This shows that the QW operator has an invariant eigenstate $|\pi\rangle$ that is a quantum version of the RW stationary distribution π. Similarly to the RW spectral gap δ, we can define the gap $\Delta > 0$ of the QW operator as the smallest nonzero phase such that $e^{i2\pi\Delta}$ is an eigenvalue of W. The following lemma shows that the quantum gap is quadratically larger than the random walk gap.

Lemma 1 ([Sze04])**.** *If the Markov chain P has spectral gap δ, then the quantum walk operator $W(P)$ has gap*

$$\Delta \in \Omega(\sqrt{\delta}).$$

3 Quantum walk search

Consider again a graph $G = (V, E)$ with $|V| = n$ nodes and spectral gap δ. Let $M \subseteq V$ denote a subset of marked nodes of size $|M| = m$. An implementation of Grover search corresponds to the following:

1. Set up the stationary state
$$|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{x \in V} |\psi_x\rangle \,.$$
2. Repeat $O(\sqrt{n/m})$ times:
   (a) Reflect around marked subspace $\mathrm{span}_{x \in M}\{|\psi_x\rangle\}$ (i.e., apply $2 \sum_{x \in M} |\psi_x\rangle \langle\psi_x| - I$).
   (b) Reflect around stationary state $|\pi\rangle$ (i.e., apply $2 |\pi\rangle \langle\pi| - I$).

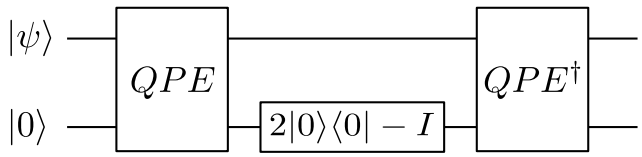
The resulting state will have a constant overlap with the marked state $|\pi_M\rangle = \frac{1}{\sqrt{m}} \sum_{x \in M} |\psi_x\rangle$, so that measuring the state returns a marked element with constant probability.

The idea of quantum walk search is to implement the reflection around $|\pi\rangle$ using a quantum walk. The resulting algorithm is called the "MNRS algorithm", after Magniez-Nayak-Roland-Santha [MNRS07].

Exercise 3 (Reflecting around $|\pi\rangle$)**.** *We can use a quantum walk $W(P)$ to reflect around the quantum state $|\pi\rangle$, i.e., implement the map*

$$|\psi\rangle = \alpha |\pi\rangle + \beta |\pi^\perp\rangle \longrightarrow (2 |\pi\rangle \langle\pi| - I) |\psi\rangle = \alpha |\pi\rangle - \beta |\pi^\perp\rangle \,.$$

Assume that $|\psi\rangle = \alpha |\pi\rangle + \sum_j \beta_j |v_j\rangle$ such that $W(P) |\pi\rangle = |\pi\rangle$ and $W(P) |v_j\rangle = e^{i2\pi\theta_j} |v_j\rangle$ with $1/2 > |\theta_j| > \Delta > 0$. We call Δ the spectral gap of the quantum walk*. Argue that the following circuit implements a reflection around $|\pi\rangle$ (QPE represents quantum phase estimation with respect to $W(P)$ to precision $\Delta/2$).*



How many calls does the circuit make to the quantum walk operator? Conclude that quantum walk search finds a marked element using a number of quantum walk steps in

$$O\left(\frac{1}{\sqrt{\delta}}\sqrt{\frac{n}{m}}\right).$$

References

[MNRS07] Frédéric Magniez, Ashwin Nayak, Jérémie Roland, and Miklos Santha. Search via quantum walk. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 575–584, 2007.

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