MPRI 2.34.2: Quantum Information and Cryptography **2023 - 2024**

Lecture 9: Quantum walk search and collision finding

Lecturer: Simon Apers (apers@irif.fr)

1 Quantum walk search

Consider 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 $|M| = m$. Following the last exercise session, we have the following quantum walk search algorithm:

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 $2 |\pi\rangle \langle \pi| - I$). We can do this using $O(1/\sqrt{\delta})$ QW steps (see exercises).

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.

We can summarize the (query) cost of the QW search algorithm using the following quantities:

- "Setup cost" $\mathcal{S}$: the number of queries needed to create the initial state $|\pi\rangle$ in step 1.
- "Checking cost" $\mathcal{C}$: the number of queries needed to check whether an element is marked in step 2.(a).
- "Update cost" $\mathcal{U}$: the number of queries needed to implement a step of the QW.

The total cost (up to constants) is then

$$\mathcal{S} + \sqrt{\frac{n}{m}} \left(\mathcal{C} + \frac{1}{\sqrt{\delta}} \mathcal{U} \right).$$

This algorithm is called the "MNRS algorithm", after Magniez-Nayak-Roland-Santha [MNRS07].

2 Collision finding with quantum walk search

Assume that we are given an array of integers $x_1, x_2, \ldots, x_N$. A *collision* is a pair of distinct i, j such that $x_i = x_j$. How many elements do we have to query in order to find a collision (or decide that no collision exists)? Classically this essentially requires to query the full array, and so the classical query complexity is $\Omega(N)$. In contrast, using an algorithm based on *quantum walk search* we can find a collision with a *sublinear* number of queries.[1]

[1] While we focus on query complexity for ease of exposition, all algorithms can be implemented with a similar runtime.

The quantum walk algorithm for collision finding was proposed by Ambainis [Amb07]. The algorithm runs quantum walk search over elements or "words" $\mathcal{Y} = (Y, x_Y)$, consisting of (i) a size-k subset $Y \subseteq [N]$, and (ii) the list x_Y of integers x_j with index $j \in Y$. We call an element $\mathcal{Y}$ marked if Y contains both indices of a collision (equivalently, x_Y must contain a collision).

Exercise 1. *Let $n = \binom{N}{k}$ denote the number of elements and m the number of marked elements. Show that $m/n \in \Omega(k^2/N^2)$.*

To use quantum walk search, we consider a graph G with vertex set V indexed by the elements $\mathcal{Y}$. There is an edge between $\mathcal{Y} = (Y, x_Y)$ and $\mathcal{Y}' = (Y', x_{Y'})$ if the subsets Y and Y' differ in exactly one element (i.e., we can obtain Y' from Y by replacing one index). The resulting graph G has $n = \binom{N}{k}$ vertices and is $k(n-k)$-regular. It corresponds to a so-called *Johnson graph*, and one can show that its spectral gap is $\delta \in \Omega(1/k)$ when $k \ll n$.

A star state $|\psi_{\mathcal{Y}}\rangle$ centered on a vertex $\mathcal{Y}$ of G is given by the state

$$|\psi_{\mathcal{Y}}\rangle = \frac{1}{\sqrt{k(n-k)}} \sum_{\mathcal{Y}' \sim \mathcal{Y}} |\mathcal{Y}, \mathcal{Y}'\rangle ,$$

where the sum runs over neighboring elements $\mathcal{Y}'$ of $\mathcal{Y}$. The quantum walk search algorithm then starts from the uniform superposition

$$|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{\mathcal{Y}} |\psi_{\mathcal{Y}}\rangle ,$$

and the algorithm has cost

$$\mathcal{S} + \frac{N}{k}(\sqrt{k}\,\mathcal{U} + \mathcal{C}),$$

where $\mathcal{U}$ is the *update cost* or cost of implementing a single quantum walk step on the Johnson graph G. We now bound the different costs.

For the checking cost $\mathcal{C}$, note that we can check whether a given state $|\psi_{\mathcal{Y}}\rangle$ is marked simply by checking whether the list x_Y contains a collision. Since this list is given explicitly in the description of $|\psi_{\mathcal{Y}}\rangle$, this requires no queries and so $\mathcal{C} = 0$.

The setup cost $\mathcal{S}$ amounts to creating the state $|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{\mathcal{Y}} |\psi_{\mathcal{Y}}\rangle$. We do this in a few steps. First, we prepare the state $\frac{1}{\sqrt{n}} \sum_{\mathcal{Y}} |\mathcal{Y}\rangle |0\rangle$. This takes k queries. Then, we construct the mapping U_ψ defined by $U_\psi |\mathcal{Y}\rangle |0\rangle = |\psi_{\mathcal{Y}}\rangle$. We do this in two steps:

$$\begin{aligned} |\mathcal{Y}\rangle |0\rangle = |Y, x_Y\rangle |0\rangle &\overset{\text{(i)}}{\mapsto} \frac{1}{\sqrt{k(n-k)}} \sum_{\mathcal{Y}' \sim \mathcal{Y}} |Y, x_Y\rangle |Y', 0\rangle \\ &\overset{\text{(ii)}}{\mapsto} \frac{1}{\sqrt{k(n-k)}} \sum_{\mathcal{Y}' \sim \mathcal{Y}} |Y, x_Y\rangle |Y', x_{Y'}\rangle = |\psi_{\mathcal{Y}}\rangle . \end{aligned}$$

Step (i) requires no queries. Step (ii) amounts to gathering the elements $x_{Y'}$ with index in Y'. Since $x_{Y'}$ contains exactly one element not in x_Y, this requires exactly one query. The setup cost $\mathcal{S}$ is hence roughly k.

Finally, we bound the cost $\mathcal{U}$ of a single call to the quantum walk operator W. Recall from last lecture that $W = S \cdot C$ where S is a simple swap (i.e., $S|\mathcal{Y}, \mathcal{Y}'\rangle = |\mathcal{Y}', \mathcal{Y}\rangle$), requiring no queries, and $C = 2\left(\sum_{\mathcal{Y}} |\psi_{\mathcal{Y}}\rangle \langle \psi_{\mathcal{Y}}|\right) - I$ is a reflection around the star subspace. Using a similar trick as before, we can implement the reflection C by making two calls to the preparation operator U_ψ, which requires a single query. This proves that the update cost $\mathcal{U}$ is $O(1)$.

Exercise 2. *Verify that* $C = U_\psi R_0 U_\psi^\dagger$.

Combining these different arguments, we can bound the total cost by

$$\mathcal{S} + \sqrt{\frac{n}{m}}\left(\frac{1}{\sqrt{\delta}}\mathcal{U} + \mathcal{C}\right) \approx k + \frac{N}{\sqrt{k}}.$$

If we set $k = N^{2/3}$ then this yields a quantum algorithm for collision finding with complexity $\widetilde{O}(N^{2/3})$. This is essentially optimal by the $\Omega(N^{2/3})$ lower bound of Aaronson and Shi [AS04].

References

[Amb07] Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.

[AS04] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM (JACM)*, 51(4):595–605, 2004.

[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.