AQAlg: Advanced Quantum Algorithms **2023 - 2024**

Exercises 9: Quantum walk search and collision finding

Lecturer: Simon Apers (apers@irif.fr)

1 Grover search for collision finding

Consider again the problem of finding a collision among an array of integers $x_1, x_2, \ldots, x_N$. Naively we could apply Grover search to the set of all $O(N^2)$ pairs of distinct i, j and mark the pairs that form a collision. However, this would trivially require $\Omega(N)$ queries. Before Ambainis' optimal quantum walk algorithm, a slightly better algorithm was already proposed by Buhrman, Dürr, Heiligman, Høyer, Magniez, Santha and de Wolf [BDH$^+$01] by running Grover search over larger *subsets* of indices rather than just pairs. It is based on the following primitive.

Exercise 1. Let $Y \subseteq [N]$ be a subset of size k. Find a collision with (at least) one index in Y using Grover search with $O(k + \sqrt{N})$ queries.

Hence we can check efficiently whether a small subset contains an index of a collision. The idea in [BDH$^+$01] is to use Grover search to find such a small subset. Specifically, we search over elements $\mathcal{Y} = (Y, x_Y)$, consisting of (i) a size-k subset $Y \subseteq [N]$, and (ii) the list x_Y of integers x_j with index $j \in Y$. With $n = \binom{N}{k}$ the number of elements, the algorithm starts from the superposition

$$\frac{1}{\sqrt{n}} \sum_{Y \subseteq [N]:|Y|=k} |\mathcal{Y} = (Y, x_Y)\rangle .$$

An element $\mathcal{Y}$ is marked if the corresponding subset Y contains at least one index of a collision. We now bound the query complexity of Grover search.

Exercise 2.

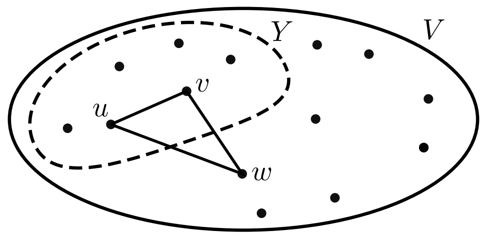
- Let $m > 0$ denote the number of marked elements. Show that $m/n \geq k/N$ if $k \ll N$.
- What is the checking cost $\mathcal{C}$?
- What is the setup cost $\mathcal{S}$?
- What is the final query complexity as a function of k? Find the optimal choice of k.

2 Quantum walk search for triangle finding (extra)

We want to use a quantum algorithm for finding a *triangle* in a graph. More specifically, given a graph $G = (V, E)$ with $|V| = N$, we want to find a triple $x, y, z \in V$ such that $(x, y), (y, z), (x, z) \in E$. We can access the graph by making queries: for any $x, y \in V$, a query returns $f(x, y) = 1$ if $(x, y) \in E$ and $f(x, y) = 0$ otherwise.

Exercise 3. Describe a quantum algorithm based on Grover search for finding a triangle using only $O(N^{3/2})$ queries. This improves on the best classical algorithm which requires $\Omega(N^2)$ queries.

We can use quantum walks to describe a better algorithm. The basis states are indexed by elements $\mathcal{Y} = (Y, x_Y)$, with $Y \subseteq V$ a size-k subset of vertices and x_Y a list of the edges in E with both endpoints in Y, $x_Y = \{(u, v) \in Y \times Y \mid (u, v) \in E\}$. An element $\mathcal{Y}$ is *marked* if x_Y contains at least one edge of a triangle.



Exercise 4. Let $n = \binom{N}{k}$ denote the number of elements and m the number of marked elements. Show that if G contains a triangle then $m/n \in \Omega(k^2/N^2)$.

We again implement a quantum walk algorithm on the Johnson graph with vertices indexed by elements $\mathcal{Y}$, and an edge between $\mathcal{Y}$ and $\mathcal{Y}'$ if Y and Y' differ in exactly one element. We use quantum walk search on the Johnson graph to find a marked element.

Exercise 5. What are the setup cost S and the update cost U (in number of queries)? Assuming that the checking cost $C \in O(\sqrt{N}k^{2/3})$, show that the total query complexity is $O(k^2 + N\sqrt{k} + N^{3/2}/k^{1/3})$. For $k = N^{3/5}$ this is $O(N^{13/10})$.

The checking cost C for an element $\mathcal{Y}$ is the cost of checking whether there exists $w \in V$ and $u, v \in Y$ such that u, v, w forms a triangle. We solve this using a variant of collision finding called "graph collision finding": for a given function f we wish to find $u, v \in Y$ such that $f(u) = f(v)$ and $(u, v) \in E$. A variant of Ambainis' quantum walk algorithm solves this using $O(k^{2/3})$ queries.

Exercise 6.

- For a given $w \in V$, describe (in words) how to use *graph collision finding* to check whether there exists $u, v \in Y$ such that u, v, w forms a triangle using only $O(k^{2/3})$ queries.
- Use Grover search to find a $w \in V$ for which there exists $u, v \in Y$ such that u, v, w forms a triangle. Show that this implies a checking cost $C \in O(\sqrt{N}k^{2/3})$.

References

[BDH+01] Harry Buhrman, Christoph Dürr, Mark Heiligman, Peter Høyer, Frédéric Magniez, Miklos Santha, and Ronald de Wolf. Quantum algorithms for element distinctness. In *Proceedings 16th Annual IEEE Conference on Computational Complexity*, pages 131–137. IEEE, 2001.