Promised and Distributed Quantum Search*

Shengyu Zhang

Computer Science Department, Princeton University, NJ 08544, USA
szhang@cs.princeton.edu

Abstract. This paper gives a quantum algorithm to search in an set S for a k-tuple satisfying some predefined relation, with the promise that some components of a desired k-tuple are in some subsets of S. In particular when $k = 2$, we show a tight bound of the quantum query complexity for the Claw Finding problem, improving previous upper and lower bounds by Buhrman, Durr, Heiligman, Hoyer, Magniez, Santha and de Wolf [7].

We also consider the distributed scenario, where two parties each holds an n-element set, and they want to decide whether the two sets share a common element. We show a family of protocols *s.t.* $q(P)^{3/2} \cdot c(P) = O(n^2 \log n)$, where $q(P)$ and $c(P)$ are the number of quantum queries and the number of communication qubits that the protocol P makes, respectively. This implies that we can pay more for quantum queries to save on quantum communication, and vice versa. To our knowledge, it is the first result about the tradeoff between the two resources.

1 Introduction

Recently Ambainis [5] proposed a novel algorithm for k-Element Distinctness, which is to decide whether there are k equal elements in a given set A of size N. As later pointed out by Magniez, Santha and Szegedy in [13] and by Childs and Eisenberg in [9], Ambainis's algorithm actually gives an $O(N^{k/k+1})$ algorithm for the general k-Subset Finding problem, defined as follows.

k-Subset Finding: Given N elements $x_1, ...x_N \in [M]$, and a k-ary relation $R \subseteq [M]^k$, decide whether there is a k-size set $\{i_1, ..., i_k\}$ *s.t.* $(x_{i_1}, ..., x_{i_k}) \in R$. If yes, output a solution; otherwise reject.

This generalizes Grover's search [11], which can be viewed as the special case of $k = 1$. We can also define the Unique k-Subset Finding problem, which is the same as k-Subset Finding except that it is promised that there is at most one solution set $\{i_1, ..., i_k\}$. As pointed out in [13], by a standard random reduction, we can solve k-Subset Finding with the same complexity as the Unique k-Subset Finding. Therefore, in what follows we mostly study the unique version of the problems.

A lot of recent research in quantum computing is focused on the query models, where the input is accessed by querying an oracle, and the goal is to minimize

* This research was supported in part by NSF grant CCR-0310466.

L. Wang (Ed.): COCOON 2005, LNCS 3595, pp. 430–439, 2005.

the number of the queries made to compute the function. There are mainly two variants of query models. A commonly used one, sometimes called function-evaluation query model, is as follows. A query for the input $x = x_1...x_N$ is represented as

$$|i, b, z\rangle \rightarrow |i, (b + x_i) \ mod \ M, z\rangle \tag{1}$$

where i is the index of the variable that we are currently interested in, b is the value (before the query) in the place where the answer is held, and z is a work state not involved in the current query processing. The other query model is the comparison model, where a query is

$$|i, j, b, z\rangle \rightarrow |i, j, b \oplus \lambda_{x_i \leq x_j}, z\rangle \tag{2}$$

with $b \in \{0, 1\}$ and λ_ϕ being the truth-value of the formula ϕ (throughout the paper). A quantum query computation is a series of operations $U_1, O, U_2, O, ..., U_T$, where each U_i is a unitary operator independent of the input x and O is a query as specified above. We use $Q_2^F(f)$ and $Q_2^C(f)$ to denote the double side bounded error quantum query complexity of f in the function-evaluation model and the comparison model, respectively. For further details on quantum query model, we refer readers to [4, 8] as two surveys.

Ambainis [5] showed that $Q_2^F(f) = O(N^{k/k+1})$ and $Q_2^C(f) = O(N^{k/k+1} \log N)$ for k-Subset Finding. In this paper, we consider two related problems. The first one is to consider what if we know some information about the solution in advance. For example, when $k = 2$, suppose that the unique solution is (i_1, i_2) and we know in advance that i_1 is in some subset of $[N]$. Does this information help our search? To be more precise, consider the following problems.

Unique (m, n) 2-Subset Finding: We are given $x_1, ..., x_N \in [M]$, two sets of indices $J_1, J_2 \subseteq [N]$ with $|J_1| = m, |J_2| = n$, and a relation $R \subseteq [M] \times [M]$, with the promise that there exists at most one pair of $(x_{j_1}, x_{j_2}) \in R$ *s.t.* $j_1 \in J_1$, $j_2 \in J_2$ and $j_1 \neq j_2$. Output the unique pair if it exists, and reject otherwise.

Claw Finding: The above problem with the restrictions that R is the Equality relation and $J_1 \cap J_2 = \emptyset$.

The best previous result for the Claw Finding is given by Buhrman, Durr, Heiligman, Hoyer, Magniez, Santha and de Wolf [7]:

$$\Omega(m^{1/2}) \leq Q_2^C(\text{Claw-Finding}) \leq O((n^{1/2}m^{1/4} + m^{1/2}) \log n) \tag{3}$$

where without loss of generality, they assume $m \geq n$. In this paper, we improve it to the following (almost) tight bounds.

Theorem 1. *For both* Unique (m, n) 2-Subset Finding *and* Claw Finding*, we have*

$$Q_2^F(f) = \Theta((mn)^{1/3} + \sqrt{n} + \sqrt{m}) \tag{4}$$

$$\Omega((mn)^{1/3} + \sqrt{n} + \sqrt{m}) \leq Q_2^C(f) \leq O(((mn)^{1/3} + \sqrt{n} + \sqrt{m})(\log m + \log n)) \tag{5}$$

The proof for the upper bound uses a generalization of Ambainis' quantum walk algorithm [5]. The main difference is that we maintain two sets of registers instead of just one set. The lower bound is shown by a reduction to the $\Omega((n/r)^{1/3})$ lower bound for r-Collision by Shi [2].

We also consider the promised version of the k-Subset Finding problem for general k, and a similar upper bound is given.

The second problem we study is another natural scenario for k-Subset Finding: distributed search. Suppose that Alice has input $x_1, ..., x_n$ and Bob has $y_1, ..., y_n$. Alice can access her input $x_1, ..., x_n$ only by quantum queries as in (1), and she cannot access Bob's input $y_1, ..., y_n$. Symmetric rules apply to Bob. They want to search for the unique pair of (x_i, y_j) in some given relation R, by come communications[1]. In other words, the model is the same as the one used to study quantum communication complexity (see [10]) except that the two parties access their respective inputs by quantum queries (1). So there are two natural resources to consider. One is the number of queries, and the other is the number of qubits in the communication. The former is about quantum query complexity as studied above, and the latter is about quantum communication complexity, introduced by Yao[16] and extensively studied since then (see [10] for a survey). As far as we know, all previous work considers one of these two problems[2]. For example, Ambainis [5] and the first part of this paper consider the quantum query complexity; Buhrman, Cleve and Wigderson [6] show an $O(\sqrt{n}\log n)$ upper bound of quantum communication complexity of Disj, later improved by Hoyer and de Wolf to $O(\sqrt{n}c^{\log^* n})$ [12] and finally to $O(\sqrt{n})$ by Aaronson and Ambainis [1], matching the $\Omega(\sqrt{n})$ lower bound shown by Razborov [15]. Since query and communication are both well-studied resources, it is natural to study both of them simultaneously, and see how they interact with each other.

We can use a protocol similar to the one shown by Buhrman, Cleve and Wigderson [6], but it makes $\Theta(n)$ queries, which is higher than the optimal $\Theta(n^{2/3})$ value. We can also have a protocol achieving the optimal quantum query complexity, but the number of communication qubits is asymptotically more than the optimal $\widetilde{\Theta}(\sqrt{n})$ value. So it seems to exist a tradeoff between the quantum query computation and the quantum communication. This paper gives one tradeoff result as follows. For a protocol P computing function f, denote by $q(P)$ the number of quantum queries and by $c(P)$ the number of communication qubits.

Theorem 2. *Let $f =$ Unique 2-Subset Finding. For any given $q_0 \in (n^{2/3}, n)$, there exists a protocol P with $q(P) = q_0$ and $c(P) = O(\frac{n^2 \log n}{q_0^{3/2}})$.*

[1] If the R is the Equality relation, then the problem is related to Disj, a well-studied function. But we should note that Disj is to decide whether two subsets of an n-element set intersect, while here the distributed search problem is to decide whether two n-element sets intersect.

[2] Some papers study yet other resources. For example, paper [14] gives a lower bound of the tradeoff between communication complexity and round complexity.

In other words, we have a family of protocols with $q(P)^{3/2} \cdot c(P) = O(n^2 \log n)$. This implies that we can pay more for quantum queries to save on quantum communication, and vice versa.

2 The Quantum Query Complexity of Promised Subset Finding

2.1 Review of Ambainis' Search and the Generic Algorithm

We first review Ambainis' search algorithm for UNIQUE k-ELEMENT DISTINCTNESS [5]. The working state is a superposition of basis in the form of $|S, x_S, i\rangle$. Here S is a r-size subset of $[N]$, x_S contains the variable values x_j's for all $j \in S$, and i is an index not in S. An basic tool used in the algorithm is a subroutine called **Quantum Walk** as follows.

Algorithm 1: Quantum Walk on S in A
Input: State $|S, x_S, i\rangle$ and A with $S \subseteq A$, and $i \in A - S$. Suppose that $|S| = r, |A| = N$.

1. $|S, x_S, i\rangle \rightarrow |S, x_S\rangle \left((-1 + \frac{2}{N-r})|i\rangle + \frac{2}{N-r} \sum_{j \in A-S-\{i\}} |j\rangle\right)$
2. $|S, x_S, i\rangle \rightarrow |S \cup \{i\}, x_{S\cup\{i\}}, i\rangle$ by one query.
3. $|S, x_S, i\rangle \rightarrow |S, x_S\rangle \left((-1 + \frac{2}{r+1})|i\rangle + \frac{2}{r+1} \sum_{j \in S-\{i\}} |j\rangle\right)$
4. $|S, x_S, i\rangle \rightarrow |S - \{i\}, x_{S-\{i\}}, i\rangle$ by one query.

An key fact shown by Ambainis [5] is the following. Let $I = \{i_1, ..., i_k\}$ where $(i_1, ..., i_k)$ is the unique k-tuple of equal elements. Define a $(2k+1)$-dimentional subspace

$$\tilde{H} = span\{|\psi_{j,l}\rangle : \ j = 0, ..., k; \ l = 0, 1; \ (j, l) \neq (k, 1)\} \tag{6}$$

where $|\psi_{j,l}\rangle$ is the uniform superposition of states $\{|S, x_S, i\rangle : |S| = r, \ i \in A - S, \ j = |S \cap I|, \ l = \lambda_{i \in I}\}$ (with $\lambda_\phi = 1$ if ϕ is true, and 0 otherwise). Then first, one step of **Quantum Walk** maps $\tilde{H}$ to $\tilde{H}$ itself. Second, the operation of **Quantum Walk**, when restricted on $\tilde{H}$, has $2k + 1$ eigenvalues, one of which is 1 and the corresponding eigenvalue is the starting state $|\psi_{start}\rangle$. The other $2k$ eigenvalues are in the form of $e^{\pm\theta_1 i}, ..., e^{\pm\theta_k i}$, where $\theta_j = (2\sqrt{j} + o(1))/\sqrt{r}$. Though the original k is supposed to be at least 2, we observe that the above fact also holds for case $k = 1$. This will be used in our proof of Theorem 1. Using the following key lemma, Ambainis gave **Algorithm 2** for UNIQUE k-ELEMENT DISTINCTNESS.

Lemma 1 (Ambainis [5]). *Let $\mathcal{H}$ be a finite dimensional Hilbert space and $|\psi_1\rangle$, ..., $|\psi_m\rangle$ be an orthonormal basis for $\mathcal{H}$. Let $|\psi_{good}\rangle$, $|\psi_{start}\rangle$ be two states in $\mathcal{H}$ which are superpositions of $|\psi_1\rangle$, ..., $|\psi_m\rangle$ with real amplitudes and $\langle\psi_{good}|\psi_{start}\rangle = \alpha$. Let U_1, U_2 be unitary transformations on $\mathcal{H}$ satisfying:*

1. *U_1 is the transformation that flips the phase on $|\psi_{good}\rangle$ (*i.e. *$U_1|\psi_{good}\rangle = -|\psi_{good}\rangle$) and leaves any state orthogonal to $|\psi_{good}\rangle$ unchanged.*
2. *U_2 is a transformation which is described by a real-valued $m * m$ matrix in the basis $|\psi_1\rangle$, ..., $|\psi_m\rangle$. Moreover, $U_2|\psi_{start}\rangle = |\psi_{start}\rangle$ and, if $|\psi\rangle$ is an eigenvector of U_2 perpendicular to $|\psi_{start}\rangle$, then $U_2|\psi\rangle = e^{i\theta}|\psi\rangle$ for $\theta \in [\epsilon, 2\pi - \epsilon]$.*

Then, there exists $t = O(\frac{1}{\alpha})$ such that $\langle\psi_{good}|(U_2U_1)^t|\psi_{start}\rangle = \Omega(1)$.

Algorithm 2: for Unique k-Element Distinctness
Input: $x_1, ..., x_N \in [M]$, with the promise that there exists at most one k-size set $I = \{i_1, ..., i_k\} \subseteq [N]$ *s.t.* $x_{i_1} = ... = x_{i_k}$.
Output: I and $x_I = \{x_{i_1}, ..., x_{i_k}\}$ if they exist; otherwise reject.

1. Set up the initial state $|\psi_{start}\rangle = \frac{1}{\sqrt{\binom{N}{r}(N-r)}} \sum_{S\subseteq[N],|S|=r,i\in[N]-S} |S, x_S, i\rangle$.
2. Do $\Theta((\frac{N}{r})^{k/2})$ times
   (a) Check whether $I \subseteq S$. If yes, do the phase flip: $|S, x_S, i\rangle \to -|S, x_S, i\rangle$.
   (b) Do **Quantum Walk** on S in $[N]$ for $\Theta(\sqrt{r})$ times.
3. Measure the resulting state and give the corresponding answer.

By **Lemma 1**, if the (unique) k-size subset I exists, then after Step 2, the state is close to $|\psi_{good}\rangle = \frac{1}{\sqrt{\binom{N-k}{r-k}(N-r)}} \sum_{|S|=r,\ I\subseteq S,\ i\in[N]-S} |S, x_S, i\rangle$, thus the algorithm can output $I = \{i_1, ..., i_k\}$ and $x_I = \{x_{i_1}, ..., x_{i_k}\}$ in Step 3 (with high probability). If such I does not exist, the state after Step 2 is still $|\psi_{start}\rangle$, and thus the algorithm rejects in Step 3.

By letting $r = N^{k/k+1}$, we have an algorithm using $O(N^{k/k+1})$ queries in the function-evaluation model. In comparison model, the upper bound can be achieved with a log factor added [5]. Basically, we keep the set $|S\rangle$ sorted during the computation. So both in the set up phase (Step 1) and in the update phase (Step 2(b)), adding a log factor is enough.

2.2 Proof of Theorem 1

We prove Theorem 1 in this section. For the upper bounds, we give **Algorithm 3**, which refines Ambainis' **Algorithm 2** by maintaining two sets of registers instead of one set.

The following theorem actually shows the upper bound of Theorem 1 in the function-evaluation model.

Theorem 3. *Algorithm 3 outputs the desired results correctly in the function-evaluation model, and we can pick r_1, r_2 to make number of queries be*

$$\begin{cases} O((mn)^{1/3}) & if\ \sqrt{n} \le m \le n^2 \quad (by\ letting\ r_1 = r_2 = (mn)^{1/3}) \\ O(\sqrt{n}) & if\ m < \sqrt{n} \quad (by\ letting\ r_1 = m, r_2 \in [m, (mn)^{1/3}]) \\ O(\sqrt{m}) & if\ m > n^2 \quad (by\ letting\ r_1 \in [n, (mn)^{1/3}], r_2 = n) \end{cases}$$

Algorithm 3: for Unique (m,n) 2-Subset Finding
Input: $x_1, ..., x_N \in [M]$. $J_1, J_2 \subseteq [N]$, $|J_1| = m, |J_2| = n$. $R \subseteq [M] \times [M]$ *s.t.* there is at most one $(x_{j_1}, x_{j_2}) \in R$ with $j_1 \in J_1$, $j_2 \in J_2$ and $j_1 \neq j_2$.
Output: The unique pair (j_1, j_2) if it exists; otherwise reject.

1. Set up the initial state
   $|\psi_{start}\rangle = \frac{1}{\sqrt{T}} \sum_{S_b \subseteq J_b, |S_b| = r_b, i_b \in J_b - S_b} |S_1, x_{S_1}, i_1, S_2, x_{S_2}, i_2\rangle$,
   where $T = \binom{m}{r_1}\binom{n}{r_2}(m - r_1)(n - r_2)$ and $b = 1, 2$.
2. Do $\Theta(\sqrt{\frac{mn}{r_1 r_2}})$ times
   (a) Check whether the unique (j_1, j_2) is in $S_1 \times S_2$. If yes, do the following phase flip: $|S_1, x_{S_1}, i_1, S_2, x_{S_2}, i_2\rangle \to -|S_1, x_{S_1}, i_1, S_2, x_{S_2}, i_2\rangle$.
   (b) Do **Quantum Walk** on S_1 in J_1 for $t_1 = \lceil \frac{\pi}{4}\sqrt{r_1} \rceil$ times.
   Do **Quantum Walk** on S_2 in J_2 for $t_2 = \lceil \frac{\pi}{8}\sqrt{r_2} \rceil$ times.
3. Measure the resulting state and give the corresponding answer.

Proof. Correctness: First, if there is no desired pair, then the algorithm actually does nothing, so the state after Step 2 is still $|\psi_{start}\rangle$. Thus in Step 3, we cannot find the desired pair after the measurement, and we will reject.

On the other side, if there is the pair, we shall use **Lemma 1** to show that we can find it. Suppose $(j_1, j_2) \in J_1 \times J_2$ is the desired pair. First, define $\tilde{H}_1$ as in (6), with $|\psi_{j,l}\rangle$ being the uniform superposition of states $\{|S_1, x_{S_1}, i_1\rangle : S_1 \subseteq J_1, |S_1| = r_1,\ i_1 \in J_1 - S_1,\ j = \lambda_{j_1 \in S_1},\ l = \lambda_{i_1 = j_1}\}$. Note that it is exactly the "$k = 1$" case of (6), so W_1, the operator of **Quantum Walk** on S_1 in J_1, when restricted on $\tilde{H}_1$, has 3 eigenvalues. One of the eigenvalues is 1, and the corresponding eigenvector is $|\psi_{start,1}\rangle = \frac{1}{\sqrt{\binom{m}{r_1}(m-r_1)}} \sum_{S_1 \subseteq J_1, |S_1| = r_1, i_1 \in J_1 - S_1} |S_1, x_{S_1}, i_1\rangle$. The other two eigenvalues are $e^{\pm i\theta_1}$, and $\theta_1 = (2 + o(1))/\sqrt{r_1}$. Therefore, $W_1^{t_1}$ has 3 eigenvalues: 1 (with the eigenvector $|\psi_{start,1}\rangle$) and $e^{\pm i\theta_1'}$ where $\theta_1' = \frac{\pi}{2} + o(1)$.

$\tilde{H}_2$ is defined symmetrically, as well as W_2, $|\psi_{start,2}\rangle$ and θ_2. As a result, $W_2^{t_2}$ has 3 eigenvalues: 1 (with the eigenvector $|\psi_{start,2}\rangle$) and $e^{\pm i\theta_2'}$ where $\theta_2' = \frac{\pi}{4} + o(1)$. The whole step 2(b) restricted on $\tilde{H}_1 \otimes \tilde{H}_2$ is the operation $W = (I_1 \otimes W_2)(W_1 \otimes I_2)$. Now note that the eigenvalues of W are given by

$$\{\lambda \cdot \mu : \lambda \text{ is an eigenvalue of } W_1 \text{ on } \tilde{H}_1, \text{ and } \mu \text{ is an eigenvalue of } W_2 \text{ on } \tilde{H}_2\}.$$

Therefore, W has 9 eigenvalues $\{e^{i(b_1\theta_1' + b_2\theta_2')} : b_1, b_2 \in \{-1, 0, 1\}\}$. It is easy to check that one of eigenvalues is 1, and the corresponding eigenvector is $|\psi_{start,1}\rangle \otimes |\psi_{start,2}\rangle$, which is exactly the $|\psi_{start}\rangle$ in Algorithm 3. All the other 8 eigenvalues are in the form of $e^{\pm i\theta}$, for some $\theta \in [\pi/4 - o(1), 2\pi - \pi/4 + o(1)]$. Finally, we calculate $\alpha = \langle\psi_{start}|\psi_{good}\rangle$: $\alpha = \sqrt{\mathbf{Pr}_{|S_1|=r_1, |S_2|=r_2}[(j_1, j_2) \in S_1 \times S_2]} = \Theta(\sqrt{\frac{r_1 r_2}{mn}})$. So the number of iterations in Step 2 is $1/\alpha = \Theta(\sqrt{\frac{mn}{r_1 r_2}})$ and the correctness holds by **Lemma 1**.

It is easy to verify that the number of queries used is $O(r_1 + r_2 + \sqrt{\frac{mn}{r_1 r_2}}(\sqrt{r_1} + \sqrt{r_2})) = O(r_1 + r_2 + \frac{\sqrt{mn}}{\sqrt{r_1}} + \frac{\sqrt{mn}}{\sqrt{r_2}})$. Now we need minimize it, with restrictions

$r_1 \le m$ (because S_1 is a subset of J_1) and $r_2 \le n$. For the $(r_1 + \frac{\sqrt{mn}}{\sqrt{r_1}})$ part, it is not hard to see that if $m \ge \sqrt{n}$ then $\min_{r_1 \le m}(r_1 + \frac{\sqrt{mn}}{\sqrt{r_1}}) = (mn)^{1/3}$ and the minimum is achieved when $r_1 = (mn)^{1/3}$; otherwise $\min_{r_1 \le m}(r_1 + \frac{\sqrt{mn}}{\sqrt{r_1}}) = m + \sqrt{n}$ and the minimum is obtained when $r_1 = m$. Analyze the $r_2 + \sqrt{mn}/\sqrt{r_2}$ part similarly, and we can get the conclusion as in the statement of the theorem. □

Next we prove the lower bound part in Theorem 1. Note that since Claw-Finding is a special case of (m, n) 2-Subset Finding, it is enough to show the lower bound for Q_2(Claw-Finding).

Proof. It is sufficient to prove the lower bound of $\Omega((mn)^{1/3})$. We will show it by a reduction to the 2-Collision problem, which is to distinguish whether a function $f : [N] \to [N]$ is one-to-one or two-to-one. This problem is shown by Aaronson, Shi [2] and Ambainis [3] to have $\Omega(N^{1/3})$ lower bound of quantum query complexity. Assume that we can solve (m, n) 2-Subset Finding with $o((mn)^{1/3})$ queries, then we can have an $o(N^{1/3})$ algorithm for the 2-Collision problem as follows. Let $f : [N] \to [N]$ be a function, where $N = mn$, and we are to decide whether it is one-to-one or two-to-one. First pick a random set $S_1 \subseteq [N]$ of size m and then pick another random set $S_2 \subseteq [N] - S_1$ of size n. If f is one-to-one, then $f(i_1) \ne f(i_2)$ for any $i_1 \in S_1$ and $i_2 \in S_2$, since $S_1 \cap S_2 = \emptyset$. On the other hand, if f is two-to-one, then by a standard probability calculation we know that with constant probability there will be $i_1 \in S_1$ and $i_2 \in S_2$ such that $f(i_1) = f(i_2)$. Therefore, whether f is two-to-one or one-to-one is, up to a constant probability, equivalent to whether there are $i_1 \in S_1$ and $i_2 \in S_2$ such that $f(i_1) = f(i_2)$, which can be decided with $o((mn)^{1/3}) = o(N^{1/3})$ queries, by our assumption. This contradicts to the $\Omega(N^{1/3})$ lower bound of 2-Collision [2, 3], so Q_2^F(Unique (m, n) 2-Subset Finding) $= \Omega((mn)^{1/3})$. □

We make a few remarks about Claw-Finding problem in the comparison model in **Theorem 1** to end the subsection. The upper bound of Q_2^C(Claw-Finding) is got in the same way we described at the end of Section 2.1, with only a $\log n$ factor added. As to the lower bound, since we can use 2 queries in the function-evaluation model to simulate 1 query in comparison model, we have always $Q_2^F(f) \le 2Q_2^C(f)$. So a lower bound for $Q_2^F(f)$ is also a lower bound for $Q_2^C(f)$ up to a factor of 2.

2.3 The General Case

We can use the same technique to give a generic algorithm for a general promised subset finding problem.

Unique $(n_i, k_i)_{i=1,...,l}$ k-Subset Finding: We are given $x_1, ..., x_N \in [M]$, l sets of indices $J_1, ..., J_l \subseteq [N]$ with $|J_i| = n_i$ $(i = 1, ..., l)$, and a relation $R \subseteq [M]^k$, where $k = \sum_{i=1}^{l} k_i$ is constant, with the promise that there is at most one k-size set $\{j_{11}, ..., j_{1k_1}, ..., j_{l1}, ..., j_{lk_l}\}$ *s.t.* $(x_{j_{11}}, ..., x_{j_{1k_1}}, ..., x_{j_{l1}}, ..., x_{j_{lk_l}}) \in R$

and $j_{ip} \in J_i$ $(i = 1, ..., l; p = 1, ..., k_i)$. Output the unique k-set if it exists; otherwise reject.

If R is Equality relation, we call the problem UNIQUE $(n_i, k_i)_{i=1,...,l}$ k-ELEMENT DISTINCTNESS. An generic algorithm for UNIQUE $(n_i, k_i)_{i=1,...,l}$ k-SUBSET FINDING is as follows. As in [13], we use three kinds of registers: set registers S, data registers $D(s)$ and coin register c.

Algorithm 4: for Unique $(n_i, k_i)_{i=1,...,l}$ k-Subset Finding
Input: $x_1, ..., x_N \in [M]$, $J_1, ..., J_l \subseteq [N]$ with $|J_i| = n_i$ $(i = 1, ..., l)$, $R \subseteq [M]^k$, where $k = \sum_{i=1}^{l} k_i$ is constant, with the promise that there is at most one k-size set $J = \{j_{11}, ..., j_{1k_1}, ..., j_{l1}, ..., j_{lk_l}\}$ *s.t.* $(x_{j_{11}}, ..., x_{j_{1k_1}}, ..., x_{j_{l1}}, ..., x_{j_{lk_l}}) \in R$ and $j_{ip} \in J_i$ $(i = 1, ..., l; p = 1, ..., k_i)$.
Output: Output the unique k-set J if it exists; reject otherwise.

1. Create the state $\sum_{S_i \subseteq J_i, |S_i| = r_i, c_i \in J_i - S_i} |S_1, c_1\rangle ... |S_l, c_l\rangle$.
2. Get the data $D(S_i)$ for each S_i. Then the state is
$$\sum_{S_i \subseteq J_i, |S_i| = r_i, c_i \in J_i - S_i} |S_1, D(S_1), c_1\rangle ... |S_l, D(S_l), c_l\rangle.$$
3. Do $\Theta(\frac{\prod_{i=1}^{l} n_i^{k_i/2}}{\prod_{i=1}^{l} r_i^{k_i/2}})$ times
   (a) If $\boldsymbol{j} \in S_1^{k_1} \times ... \times S_l^{k_l}$, then do phase flip; else do nothing.
   (b) For $i = 1, ..., l$: do **Quantum Walk** on S_i in J_i for $\lceil \sqrt{r_i}\pi / 2^{i+1} \rceil$ times .
4. Measure the resulting state and give the corresponding answer.

Suppose the setup step (Step 2) takes $s(r_1, ..., r_l)$ queries, check step (Step 3(a)) takes $c(r_1, ..., r_l)$ queries, and each **Quantum Walk** on $|S_i, D(S_i), c_i\rangle$ in J_i takes $u(r_i)$ to update the data $D(S_i)$. Using the similar analysis as in the proof for Theorem 1, we can show the following upper bound for UNIQUE $(n_i, k_i)_{i=1,...,l}$ k-SUBSET FINDING and UNIQUE $(n_i, k_i)_{i=1,...,l}$ k-ELEMENT DISTINCTNESS. The only thing needed to note is that the operator of Step 3(b) has eigenvalue $\{e^{i\theta} : \theta = b_1 \frac{\pi}{2} + b_2 \frac{\pi}{4} + ... + b_l \frac{\pi}{2^{l+1}} + o(1), b_1, ..., b_l \in \{-1, 0, 1\}\}$. But it is easy to check that for any $b_1, ..., b_l \in \{-1, 0, 1\}$ such that b_i's are not all zeros, it holds that $\frac{\pi}{2^{l+1}} \leq |b_1 \frac{\pi}{2} + b_2 \frac{\pi}{4} + ... + b_l \frac{\pi}{2^{l+1}}| < \pi$, so we can use the Lemma 1 and the proof passes through.

Theorem 4. *Algorithm 4 has quantum query complexity*
$$O(s(r_1, ..., r_l) + \frac{\prod_{i=1}^{l} n_i^{k_i/2}}{\prod_{i=1}^{l} r_i^{k_i/2}} (c(r_1, ..., r_l) + \sqrt{r_1} u(r_1) + ... + \sqrt{r_l} u(r_l)).$$
In particular, if $s(r_1, ..., r_l) = \sum_i r_i$, $c(r_1, ..., r_l) = 0$ *and* $u(r_i) = 1$ *as in* UNIQUE $(n_i, k_i)_{i=1,...,l}$ k-ELEMENT DISTINCTNESS *problem, then the complexity is*
$$O(\sum_i r_i + \frac{\prod_{i=1}^{l} n_i^{k_i/2}}{\prod_{i=1}^{l} r_i^{k_i/2}} (\sum_i \sqrt{r_i})).$$

When $(\prod_{i=1}^{l} n_i^{k_i})^{\frac{1}{k+1}} \leq n_i$ *is satisfied* $(i = 1, ..., l)$*, we can pick* $r_i = (\prod_{i=1}^{l} n_i^{k_i})^{\frac{1}{k+1}}$*, and the query complexity is* $O((\prod_{i=1}^{l} n_i^{k_i})^{\frac{1}{k+1}})$.

3 Tradeoff Between Quantum Query and Communication

In this section we prove **Theorem 3** by giving a family of protocols achieving the tradeoff result. Note that in **Algorithm 3**, both the preparation of the initial state $|\psi_{start}\rangle$ in Step 1 and the Quantum Walks in Step 2(b) can be done distributively. So it naturally induces a communication protocol as follows.

Protocol 1: for distributed Unique 2-Subset Finding
Input: $x_1, ..., x_N \in [M]$. $J_1, J_2 \subseteq [N]$, $|J_1| = m, |J_2| = n$. $R \subseteq [M] \times [M]$ *s.t.* there is at most one $(x_{j_1}, x_{j_2}) \in R$ with $j_1 \in J_1$, $j_2 \in J_2$ and $j_1 \neq j_2$.
Output: The unique pair (j_1, j_2) if it exists; otherwise reject.

1. Alice sets up her initial state
   $|\psi_a\rangle = \frac{1}{\sqrt{\binom{n}{r_1}(n-r_1)}} \sum_{S_1 \subseteq J_1, |S_1|=r_1, i_1 \in J_1 - S_1} |S_1, x_{S_1}, i_1\rangle$ in her register R_a
   Bob sets up his initial state
   $|\psi_b\rangle = \frac{1}{\sqrt{\binom{n}{r_2}(n-r_2)}} \sum_{S_2 \subseteq J_2, |S_2|=r_2, i_2 \in J_2 - S_2} |S_2, x_{S_2}, i_2\rangle$ in his register R_b
2. Do $\Theta(\frac{n}{\sqrt{r_1 r_2}})$ times
   (a) Bob sends R_b (*i.e.* all his qubits) to Alice.
   (b) Alice checks whether $(j_1, j_2) \in S_1 \times S_2$. If yes, do the following phase flip: $|S_1, x_{S_1}, i_1, S_2, x_{S_2}, i_2\rangle \to -|S_1, x_{S_1}, i_1, S_2, x_{S_2}, i_2\rangle$.
   (c) Alice sends R_b back to Bob.
   (d) Alice does $\lceil \frac{\pi}{4}\sqrt{r_1} \rceil$ times **Quantum Walk** on S_1 in J_1.
   Bob does $\lceil \frac{\pi}{8}\sqrt{r_2} \rceil$ times **Quantum Walk** on S_2 in J_2.
3. Bob does the measurement and outputs the corresponding result.

The correctness of the protocol is obvious because it is essentially the same as Algorithm 3. We now analyze the complexity. The number of queries is the same as that of Algorithm 3, *i.e.* $q(P) = \Theta(r_1 + r_2 + \frac{n}{\sqrt{r_1 r_2}}(\sqrt{r_1} + \sqrt{r_2})) = \Theta(r_1 + r_2 + n(1/\sqrt{r_1} + 1/\sqrt{r_2}))$. The number of communication qubits of this protocol is $c(P) = \Theta(\frac{n}{\sqrt{r_1 r_2}} r_2 \log n) = \Theta(\sqrt{\frac{r_2}{r_1}} n \log n)$. If $t = r_1/r_2 \geq 1$, then $q(P) = \Theta(r_1 + n/\sqrt{r_2}) = \Theta(t r_2 + n/\sqrt{r_2}) \geq \Theta(t^{1/3} n^{2/3})$, and the equality is achieved when $r_2 = (n/t)^{2/3}$. So for any given $q_0 \in (n^{2/3}, n)$, let $r_1 = q_0$ and $r_2 = n^2/q_0^2$, then $q(P) = \Theta(q_0)$ and $c(P) = \Theta(\frac{n^2 \log n}{q_0^{3/2}})$.

4 Conclusion

We show a generalization of the recent quantum search algorithms [5, 9, 13] by using more sets of registers. We hope that it can serve as a building block

for other problems. It will be especially interesting if the algorithm can attack problems which are not given as a promised ones. For example, can the ideas of this paper be used to improve the $O(n^{1.3})$ upper bound [13] for Triangle?

References

1. S. Aaronson and A. Ambainis. Quantum search of spatial regions. Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, pp. 200-209, 2003. Earlier version at quant-ph/0303041
2. S. Aaronson, Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. Journal of the ACM, 51(4), pp. 595-605, 2004. Earlier version at STOC 2002 and FOCS 2002, also at quant-ph/0111102 and quant-ph/0112086.
3. A. Ambainis. Quantum lower bounds for collision and element distinctness with small range. Theory of Computing, 1(3), 2005. Earlier version at quant-ph/0305179
4. A. Ambainis. Quantum query algorithms and lower bounds, Proceedings of FOTFS III, to appear
5. A. Ambainis. Quantum walk algorithm for element distinctness. Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, pp. 22-31, 2004. Earlier version at quant-ph/0311001
6. H. Buhrman, R. Cleve, A. Wigderson. Quantum vs. classical communication and computation. Proceedings of the 30th Annual ACM Symposium on Theory of Computing, pp. 63-68, 1998
7. H. Buhrman, C. Durr, M. Heiligman, P. Hoyer, F. Magniez, M. Santha, R. de Wolf. Quantum algorithms for Element Distinctness. Proceedings of Sixteenth IEEE conference on Computational Complexity, pp. 131-137, 2001. Journal version to appear in SIAM Journal of Computing.
8. H. Buhrman, R. de Wolf. Complexity measures and decision tree complexity: a survey. Theoretical Computer Science, 288(1), pp. 21-43, 2002
9. A. Childs and J. Eisenberg. Quantum algorithms for subset finding. quant-ph/0311038
10. R. de Wolf. Quantum communication and complexity. Theoretical Computer Science, 287(1), pp. 337-353, 2002.
11. L. Grover. A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, pp. 212-219, 1996
12. P. Hoyer and R. de Wolf. Improved quantum communication complexity bounds for disjointness and equality. Proceedings of the 19th Symposium on Theoretical Aspects of Computer Science, pp. 299-310, 2002. Earlier version at quant-ph/0109068.
13. F. Magniez, M. Santha, M. Szegedy. Quantum algorithms for the Triangle problem. Proceedings of the 16th ACM-SIAM Symposium on Discrete Algorithms, pp. 1109-1117, 2005. Earlier versions at quant-ph/0310107 and quant-ph/0310134
14. R. Jain. J. Radhakrishnan, P. Sen. A lower bound for bounded round quantum communication complexity of set disjointness. Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, pp. 220 - 229, 2003
15. A. Razborov. Quantum communication complexity of symmetric predicates. Izvestiya: Mathematics, 67(1), pp. 145-159, 2003
16. A. Yao, Quantum circuit complexity, Proceedings of the 34th IEEE Symposium on Foundations of Computer Science, pp. 352-361, 1993