Quantum Lower Bound for a Tripartite Version of the Hidden Shift Problem

Aleksandrs Belovs

Abstract

In this paper, we prove a polynomial lower bound of $\Omega(n^{1/3})$ on the quantum query complexity of the following rather natural generalisation of both the hidden shift and the 3-sum problem. Given an array of $3 \times n$ elements, is it possible to circularly shift its rows so that the sum of the elements in each column becomes zero? It is promised that if this is not the case, then no 3 elements in the table sum up to zero.

The lower bound is proven by a novel application of the dual learning graph framework. Additionally, we state a property testing version of the problem, for which we prove a similar lower bound.

1 Introduction

One of the starting points of this paper is the following problem, posed by Aaronson and Ambainis [1]: construct a partial Boolean function with polylogarithmic quantum query complexity but whose randomised query complexity is $\omega(\sqrt{n})$, where $n$ is the number of input variables. There are relatively many functions known with the required quantum query complexity and randomised query complexity $\Omega(\sqrt{n})$. For instance, one can take the forrelation problem of [1] with quantum query complexity 1, or a more well-known hidden subgroup problem [11]. However, no function with polylogarithmic quantum query complexity and randomised query complexity $\omega(\sqrt{n})$ is known. As shown in [9, 2], such a function would also yield a larger than 5/2-power separation between quantum and randomised query complexities for total Boolean functions.

Aaronson and Ambainis proposed a candidate function, which they call $k$-fold forrelation. It has a very simple quantum $O(1)$-query algorithm, but it seems hard to lower bound its randomised query complexity. However, it is also possible to go in the opposite direction: find a function whose randomised query complexity is $\omega(\sqrt{n})$, and construct an efficient quantum algorithm for it. A potential candidate might be a modification of a function we know is easy quantumly, thus, preserving some hope the modification is also easy quantumly.

One particularly neat starting function, in our opinion, is the following hidden shift problem. Given two strings $x, y \in [q]^n$, the task is to distinguish two cases: in the positive case, $x$ is a circular shift of $y$; in the negative case, all the input variables in $x$ and $y$ are distinct. This problem is equivalent to the hidden subgroup problem in the dihedral group [13], and its quantum query complexity is logarithmic. It is also easy to see that its randomised query complexity is $\Theta(\sqrt{n})$.

In this paper we consider the following modification, which we call the 3-shift-sum problem. We are given an input string $x \in [q]^{3n}$, which we treat as a $3 \times n$ table. In the positive case, it is possible to circularly shifts the rows of the table so that the sum of the elements in each
column becomes divisible by \( q \). In the negative case, no matter how we shift the rows, there is no column with its sum divisible by \( q \). This is a natural amalgamation of the hidden shift and the 3-sum problem, both studied quantumly.

It is easy to see that randomised query complexity of this problem is \( \Theta(n^{2/3}) \). This raises the question of what its quantum query complexity is. The main result of our paper is a simple proof that, unlike the hidden shift problem, the quantum query complexity of the 3-shift-sum problem is polynomial: \( \Omega(n^{1/3}) \).

1.1 Adversary Bound and Dual Learning Graphs

Thus, the 3-shift-sum problem fails to provide the desired separation, but this result is interesting as a novel application of quantum lower bound techniques, namely, the adversary bound and dual learning graphs.

The first version of the adversary method was developed by Ambainis [3]. This version, later known as the positive-weighted adversary, is easy to use, and it has found many applications, but it is subject to some limitations: the certificate complexity [17, 18] and the property testing [12] barriers. The property testing barrier, which is relevant to our problem, states that if any positive input differs from any negative input on at least \( \varepsilon \) fraction of the input variables, the positive-weighted adversary fails to prove a lower bound better than \( \Omega(1/\varepsilon) \). In most cases \( \varepsilon = \Omega(1) \), thus this only gives a trivial lower bound.

The next version of the bound, the negative-weighted adversary [12] is known to be tight [16], but it is harder to apply. An application of the bound to the \( k \)-sum problem was obtained in [8]. This result was later stated in the framework of dual learning graphs in [7], which we are about to describe.

Learning graphs is a model of computation introduced in [4, 5]. They are most naturally stated in terms of certificate structures, which describe where 1-certificates can be located in a positive input. Learning graphs capture quantum query complexity of certificate structures in the following sense. Let \( L \) be the learning graph complexity of a certificate structure \( C \). First, for any function with certificate structure \( C \), there exists a quantum algorithm solving it in \( O(L) \) queries. Second, there exists some function with certificate structure \( C \) and quantum query complexity \( \Omega(L) \). In general, however, these functions are rather contrived. One example when these functions are natural are the following sum problems. A sum problem is parametrised by a family \( S \) of \( O(1) \)-sized subsets of \([n] \). The task, given an input string \( x \in [q]^n \), is to detect whether there exists \( S \in S \) such that \( \sum_{i \in S} x_i \) is divisible by \( q \).

Thus, dual learning graphs give tight lower bounds for all of the above sum problems. In general, of course, dual learning graph do not give lower bounds for all problems with a given certificate structure. For example, the learning graph complexity of the certificate structure corresponding to the hidden shift problem is \( \Omega(n^{1/3}) \), whereas its quantum query complexity is logarithmic. What about the 3-shift-sum problem? It turns out that dual learning graphs are still of help here, but in a slightly different way. The learning graph complexity of the corresponding certificate structure is \( \Theta(\sqrt{n}) \), and we do not know whether it can be converted into a quantum query lower bound. However, a dual learning graph for a different certificate structure can be converted into, albeit not tight, but still a polynomial lower bound. This shows that dual learning graphs are more versatile than it was indicated in [7].

Another interesting feature of our result is that it might be the simplest constructed example of the adversary bound surpassing the property testing barrier. Examples of the negative-weighted adversary breaking the certificate complexity and the property testing barriers were already obtained in [12]. But [12] did not cover the most interesting regime \( \varepsilon = \Omega(1) \) of the property testing barrier. The sum problems of [7] are relatively simple examples of overcoming
the certificate complexity barrier. An example for the $\varepsilon = \Omega(1)$ regime of the property testing barrier was constructed in [6], but the construction is quite technical. Our result gives a similar example by much simple means, comparable to that of [7].

1.2 Property Testing

In the property testing model, one is given some property (a set of positive inputs), and the task is to distinguish whether the input possesses the property, or is $\varepsilon$-far, in relative Hamming distance, from any object having the property.

Overcoming the property testing barrier automatically gives a lower bound for a property testing problem—that of testing whether the input is positive. But it is not always the most natural way to state the problem. We give an example of a lower bound for a problem that is most naturally stated in the property testing settings.

In the 3-shift-sum problem, as we formulated it above, $q$ must be relatively big for the problem to be interesting. For instance, it is easy to see that for $q = 2$ there is almost no negative inputs. In our lower bound, we require that $q = \Omega(n^3)$. But it is possible to formulate a version of the problem that is interesting even when the input alphabet is Boolean. Define the set of positive inputs as before, and define the set of negative inputs as being at relative Hamming distance, say, $1/7$ to it. We prove lower bound of $\Omega(n^{1/3})$ for this version of the problem as well.

Although there is quite a number of quantum algorithm for the property testing problems, there are not so many quantum lower bounds known. (An interested reader might consult a recent survey [15] for more information on the topic.) One of the main reasons, of course, is the property testing barrier for positive-weighted adversary. Up to our knowledge, our result is the first property testing lower bound proven using the adversary method, which answers the problem mentioned in [15]. This shows yet another area of applications of dual learning graphs.

2 Preliminaries

For positive integers $m$ and $\ell \geq m$, let $[m]$ denote the set \{1, 2, ..., $m$\} and $[m, \ell]$ denote the set \{$m, m+1, \ldots, \ell$\}. For $P$ a predicate, we use $1_P$ to denote the variable that is 1 is $P$ is true, and 0 otherwise.

For a $I \times J$-matrix $A$, and $i \in I$ and $j \in J$, we denote by $A[i,j]$ its $(i,j)$-th entry. For $I' \subseteq I$ and $J' \subseteq J$, $A[I',J']$ denotes the corresponding submatrix. We use similar notation also for vectors. Next, $\|\cdot\|$ denotes the spectral norm (the largest singular value), and $\circ$ denotes the Hadamard (entry-wise) product of matrices.

2.1 Adversary Bound

For background on quantum query complexity the reader may refer to [10]. In the paper, we only require the knowledge of the (general) adversary bound that we are about to define.

Let $f: D \to \{0, 1\}$ with $D \subseteq [q]^n$. An adversary matrix for $f$ is a non-zero $f^{-1}(1) \times f^{-1}(0)$-matrix $\Gamma$. For any $i \in [n]$, the $f^{-1}(1) \times f^{-1}(0)$-matrix $\Delta_i$ is defined by

$$\Delta_i[x,y] = \begin{cases} 0, & \text{if } x_i = y_i; \\ 1, & \text{if } x_i \neq y_i. \end{cases}$$

**Theorem 1** (Adversary bound [12, 14, 8]). In the above notation, the quantum query complexity of the function $f$ is $\Theta(\text{ADV}^+(f))$, where $\text{ADV}^+(f)$ is the optimal value of the semi-definite
where the maximization is over all adversary matrices $\Gamma$ for $f$.

We can choose any adversary matrix $\Gamma$ and scale it so that the condition $\|\Delta_i \circ \Gamma\| \leq 1$ holds. Thus, we often use the condition $\|\Delta_i \circ \Gamma\| = O(1)$ instead of $\|\Delta_i \circ \Gamma\| \leq 1$.

Working with the matrix $\Delta_i \circ \Gamma$ might be cumbersome, so we do the following transformation instead. We write $\Gamma \xrightarrow{\Delta} \Gamma'$ if $\Gamma \circ \Delta_i = \Gamma' \circ \Delta_i$. In other words, we modify the entries of $\Gamma$ with $x_i = y_i$. Now, from the fact that $\gamma_2(\Delta_i) = \max_B \{\|\Delta_i \circ B\| : \|B\| \leq 1\} \leq 2$ we conclude that $\|\Delta_i \circ \Gamma\| \leq 2\|\Gamma\|$, hence we can replace $\Delta_i \circ \Gamma$ with $\Gamma'$ in (2b).

2.2 Certificate Structures and Dual Learning Graphs

Let $f : \mathcal{D} \to \{0, 1\}$ be a function with domain $\mathcal{D} \subseteq [q]^n$. For $x \in f^{-1}(1)$, a certificate for $x$ is a subset $S \subseteq [n]$ such that $f(z) = 1$ for all $z \in \mathcal{D}$ satisfying $x_i = y_i$ for all $i \in S$. A certificate structure $\mathcal{C}$ is a collection of non-empty subsets of $2^n$. We say that $f$ has certificate structure $\mathcal{C}$ if, for every $x \in f^{-1}(1)$, there exists $\mathcal{M} \in \mathcal{C}$ such that every $S \in \mathcal{M}$ is a certificate for $x$. It is naturally to assume that all $\mathcal{M} \in \mathcal{C}$ are upward closed.

There are two formulations of the learning graph complexity: primal and dual. For the purposes of this paper, it is enough to state the dual one. A dual learning graph for a certificate structure $\mathcal{C}$ is a feasible solution to the following optimisation problem:

$\max \sqrt{\sum_{\mathcal{M} \in \mathcal{C}} \alpha_{\mathcal{M}}(\emptyset)^2}$
$\text{subject to } \sum_{\mathcal{M} \in \mathcal{C}} (\alpha_{\mathcal{M}}(S) - \alpha_{\mathcal{M}}(S \cup \{j\}))^2 \leq 1 \text{ for all } S \subseteq [n] \text{ and } j \in [n] \setminus S;$
$\alpha_{\mathcal{M}}(S) = 0 \text{ whenever } S \in \mathcal{M};$
$\alpha_{\mathcal{M}}(S) \in \mathbb{R} \text{ for all } S \subseteq [n] \text{ and } \mathcal{M} \in \mathcal{C}.$

The optimal value of this optimisation problem is called the learning graph complexity of $\mathcal{C}$.

3 Formulation of the Problems and Easy Observations

In this section, we formulate the 3-shift-sum problem. Additionally, we define a closely related 3-matching-sum problem. We also sketch proofs of few simple observations about these problems. Strictly speaking, none of these observations is relevant for our main result in the next section.

Both the 3-shift-sum and the 3-matching-sum are partial Boolean functions defined on $[q]^{3n}$, with $q$ and $n$ positive integers. The $3n$ input variables are divided into three groups $A = [1..n]$, $B = [n+1..2n]$ and $C = [2n+1..3n]$. A 3-dimensional matching is a partition $\mu$ of the set $[3n]$ into $n$ triples, $\mu = \{T_1, \ldots, T_n\}$, such that $|T_i \cap A| = |T_i \cap B| = |T_i \cap C| = 1$ for all $i$. This is a natural generalisation of the usual (2-dimensional) matching between sets $A$ and $B$.

We denote the set of 3-dimensional matchings by $M_3$ (we omit $n$, assuming its value is clear from the context). We consider a special type of 3-dimensional matchings, we call 3-shifts. A 3-shift is a matching $\mu = \{T_1, \ldots, T_n\}$ such that there exist two number $b, c \in [n]$ such that $T_i = \{i, n+1+(i+b \mod n), 2n+1+(i+c \mod n)\}$ for all $i$. We denote the set of 3-shifts by $M_3$. 
We define the 3-shift-sum and the 3-matching-sum problems as follows. In a positive input $x \in [q]^{3n}$, there exists $\mu \in M_Q$ such that $x_a + x_b + x_c$ is divisible by $q$ for every triple $\{a, b, c\} \in \mu$. We say that $x$ is of the form $\mu$ in this case. Here, $M_Q$ stands for $M_b$ in 3-shift-sum and for $M_M$ in 3-matching-sum. In a negative input, $y \in [q]^{3n}$, we have $x_a + x_b + x_c \not\equiv 0 \pmod{q}$ for any choice of $a \in A, b \in B$ and $c \in C$. The task is to determine whether the input is positive or negative, provided that one of the two options holds. Since 3-shift-sum is a special case of 3-matching-sum, the latter is a harder problem.

It is easy to describe the certificate structures $C_q$ and $C_M$ of the 3-shift-sum and the 3-matching-sum problems. For each $\mu \in M_q$, there is a corresponding $\mathcal{M} \in C_q$ obtained as follows: a subset $\mu$ is a subset in 3-matching-sum. In a negative input, $y \in [q]^{3n}$, we have $x_a + x_b + x_c \not\equiv 0 \pmod{q}$ for any choice of $a \in A, b \in B$ and $c \in C$. The task is to determine whether the input is positive or negative, provided that one of the two options holds. Since 3-shift-sum is a special case of 3-matching-sum, the latter is a harder problem.

Proposition 2. The quantum query complexity of the 3-shift-sum and the 3-matching-sum problems is $O(\sqrt{n})$.

Proof sketch. Consider a positive input $x$ of the form $\mu \in M_q$. Take random subsets $A' \subseteq A$ and $B' \subseteq B$ of size approximately $\sqrt{n}$, and query all the variables in $A' \cup B'$. With high probability, there exists $T \in \mu$ that intersects both $A'$ and $B'$. Now use Grover’s search to find an element $c \in C$ satisfying $x_a + x_b + x_c \equiv 0 \pmod{q}$ for some $a \in A'$ and $b \in B'$.

Proposition 3. The randomised query complexity of the 3-shift-sum and the 3-matching-sum problems is $\Theta(n^{2/3})$.

Proof sketch. Let us start with the upper bound. Let $x$ be a positive input of the form $\mu = \{T_1, \ldots, T_n\}$. Query random subsets $A' \subseteq A, B' \subseteq B$ and $C' \subseteq C$ of size approximately $n^{2/3}$. With high probability there exists $T \in M_q$ that intersects all three sets $A', B'$ and $C'$.

For the lower bound we assume that $q \gg n^2$, so that almost all inputs are negative. Consider two probability distributions $\mathcal{P}$ and $\mathcal{N}$ on the inputs defined as follows. The distribution $\mathcal{N}$ is uniform over all input strings in $[q]^{3n}$. In the distribution $\mathcal{P}$, a 3-dimensional matching $\mu \in M_q$ is chosen uniformly at random. Then, a string in $[q]^{3n}$ is chosen uniformly at random, and uniquely extended to a positive input of the form $\mu$.

Let $S \subseteq [3n]$. If $|S| \ll n^{2/3}$, the probability $S$ contains a triple from $\mu$ as a subset is negligible. Conditioned on this not happening, the distribution $\mathcal{P}$ is completely indistinguishable from $\mathcal{N}$ given the values of the variables in $S$. Hence, no randomised algorithm using considerably fewer than $n^{2/3}$ queries can distinguish $\mathcal{P}$ and $\mathcal{N}$ with non-negligible probability. Since almost all inputs are negative, any randomised algorithm solving the 3-shift-sum or the 3-matching-sum problem with bounded error uses $\Omega(n^{2/3})$ queries. 

$\Box$

Proposition 4. The learning graph complexity of the certificate structures $C_q$ and $C_M$ is $\Theta(\sqrt{n})$.

Proof. The upper bound is similar to Proposition 2 and we omit the proof. Let us prove the lower bound. Define
\[
\alpha_M(S) = \frac{1}{\sqrt{|M_Q|}} \max\{\sqrt{n} - |S|, 0\} \quad \text{if} \ S \notin \mathcal{M},
\]
and as 0 otherwise. It is easy to see that the objective value (3a) is $\sqrt{n}$, and that (3c) holds.

Fix $S$ and $j$, and let us check (3b). If $|S| \geq \sqrt{n}$, then the left-hand side of (3b) is zero, so assume $|S| \leq \sqrt{n}$. If $S \cup \{j\} \notin \mathcal{M}$, then the value of $\alpha_M(S)$ changes by $1/\sqrt{|M_Q|}$ as the size of $S$ increases by 1. If $\mu \in M_q$ is taken uniformly at random, the probability is $O(\{S\}/n^2) = O(1/n)$ that $S \notin \mathcal{M}$ but $S \cup \{j\} \in \mathcal{M}$. In this case, the value of $\alpha_M(S)$ changes by at most $\sqrt{n}/|M_Q|$. Thus,
\[
\sum_{S \in \mathcal{C}} (\alpha_M(S) - \alpha_M(S \cup \{j\}))^2 \leq |M_Q| \cdot \frac{1}{|M_Q|} + O\left(\frac{|M_Q|}{n}\right) \cdot \frac{n}{|M_Q|} = O(1).
\]
Scaling down $\alpha_M(S)$ by a constant factor, we obtain a feasible solution with objective value $\Omega(\sqrt{n})$. □

4 Lower Bound

In this section, we prove a quantum query lower bound for the 3-shift-sum problem.

Theorem 5. Assume $q \geq 2n^3$. Then the quantum query complexity of the 3-shift-sum problem is $\Omega(n^{1/3})$.

First, we define a different certificate structure, which we denote $C_s'$. For each $\mu \in M_s$, there is a corresponding $M \in C_s'$ obtained as follows: a subset $S \subseteq [3n]$ is in $M$ if and only if there exists a triple $T \in \mu$ satisfying $|T \cap S| \geq 2$.

Note that it is not the certificate structure of the 3-shift-sum problem. This is rather the certificate structure of a problem one might call the 3-shift-equal problem. The input is a $3 \times n$ matrix. In the positive case, there exist circular shifts of rows such that the elements in each column become equal. In the negative case, any two element from two different rows are different.

Proposition 6. The learning graph complexity of the certificate structure $C_s'$ is $\Omega(n^{1/3})$.

Proof. The proof is similar to that of Proposition 12 from [7] for the hidden shift problem. We have $|C_s'| = n^2$. Define

$$\alpha_M(S) = \frac{1}{n} \max \left\{ n^{1/3} - |S|, 0 \right\} \quad \text{if } S \notin M,$$

and as 0 otherwise. It is easy to see that the objective value (3a) is $n^{1/3}$, and that (3c) holds.

Fix $S$ and $j$, and let us check (3b). If $|S| \geq n^{1/3}$, then the left-hand side of (3b) is zero, so assume $|S| \leq n^{1/3}$. There are $n^2$ choices of $M \in C_s$. If $S \cup \{j\} \notin M$, then the value of $\alpha_M(S)$ changes by $1/n$ as the size of $S$ increases by 1. Also, there are at most $|S|n \leq n^{4/3}$ choices of $M$ such that $S \notin M$ but $S \cup \{j\} \in M$. For each of them, the value of $\alpha_M(S)$ changes by at most $n^{-2/3}$. Thus,

$$\sum_{M \in C} \left( \alpha_M(S) - \alpha_M(S \cup \{j\}) \right)^2 \leq n^2 \cdot \frac{1}{n^2} + n^{4/3} \cdot n^{-4/3} = O(1).$$

Scaling down $\alpha_M(S)$ by a constant factor, we obtain a feasible solution with objective value $\Omega(n^{1/3})$. □

Now we transform this dual learning graph into an adversary lower bound. The construction is reminiscent of [7]. We construct a larger matrix $\tilde{\Gamma}$, and obtain $\Gamma$ as a scaled submatrix of $\tilde{\Gamma}$. The rows of $\tilde{\Gamma}$ are labelled by pairs $(\mu, x)$, where $\mu \in M_s$, and $x \in [q]^{3n}$ is an arbitrary string. We denote by $\tilde{G}_\mu$ the submatrix of $\tilde{\Gamma}$ formed by the rows with label $\mu$. Thus, $\tilde{\Gamma}$ is an $n^2 \times 1$ block matrix with blocks $\tilde{G}_\mu$.

Let $X^\mu$ denote the set of positive inputs of form $\mu$. We use $X$ for the set of pairs $(\mu, x)$ with $x \in X^\mu$, $Y$ for the set of negative inputs, and $Z = [q]^{3n}$ is the set of all strings. We obtain $\tilde{\Gamma}$ in two steps: first, we define $\tilde{\Gamma} = q^{n/2} \tilde{\Gamma}[X, Z]$, and then $\Gamma = \tilde{\Gamma}[X, Y]$. Let also $\tilde{G}_\mu = q^{n/2} \tilde{G}_\mu[X^\mu, Z]$. The scaling factor $q^{n/2}$ is chosen to account for the reduction in the number of rows.
Now we turn to the definition of the matrices $\hat{G}^\mu$. They are constructed from the following building blocks. Let $e_0, \ldots, e_{m-1}$ be the Fourier basis of $\mathbb{C}^{Z^r}$. Recall that it is an orthonormal basis given by $e_i[j] = \frac{1}{\sqrt{q}} \omega^{ij}$, where $\omega = e^{2\pi i/q}$. We define two projectors

$$E_0 = e_0 e_0^* \quad \text{and} \quad E_1 = I - E_0 = \sum_{i=1}^{q-1} e_i e_i^*.$$ 

All the entries of $E_0$ are equal to $1/q$. An important relation is

$$E_0 \xrightarrow{\Delta} E_0 \quad \text{and} \quad E_1 \xrightarrow{\Delta} -E_0,$$  

(5)

where $\Delta$ is as in (1) and acts on the only variable. For a positive integer $m$, and a subset $S \subseteq [m]$, we define $E_S^{(m)} = \bigotimes_{j \in [m]} E_{s_j}$ with $s_j = 1_{j \in S}$.

Let $\alpha_M(S)$ be as in the proof of Proposition 6. Identifying $M \in \mathcal{C}_s'$ with the corresponding element $\mu \in M_s$, we define

$$\hat{G}^\mu = \sum_{S \subseteq [3n]} \alpha_\mu(S) E_S^{(3n)}.$$ 

Using (5), we see that $E_S^{(3n)} \xrightarrow{\Delta_j} E_S^{(3n)} \{| j \} \quad \text{if} \quad j \notin S \quad \text{and} \quad E_S^{(3n)} \xrightarrow{\Delta_j} -E_S^{(3n)} \{| j \} \quad \text{if} \quad j \in S$. Thus,

$$\hat{G}^\mu \xrightarrow{\Delta_j} \sum_{S \subseteq [3n]} \sum_{j \notin S \cup \{ j \}} (\alpha_\mu(S) - \alpha_\mu(S \cup \{ j \})) E_S^{(3n)}.$$  

(6)

Denote the right-hand side by $\hat{G}^\mu$. Use these blocks to define the matrix $\tilde{\Gamma}'$ with $\tilde{\Gamma} \xrightarrow{\Delta_j} \tilde{\Gamma}'$. Define $\hat{G}^\mu$, $\tilde{\Gamma}$ and $\Gamma'$ similarly to $\hat{G}^\mu$, $\tilde{\Gamma}$ and $\Gamma$ so that $\Gamma \xrightarrow{\Delta_j} \Gamma'$.

Let us now analyse the matrices $\hat{G}^\mu$. Fix a 3-dimensional matching $\mu = \{T_1, \ldots, T_n\}$. We start with one triple $T_i = \{a_1, a_2, a_3\}$. Let

$$P = \{(a, b, c) \in [3]^3 \mid a + b + c \equiv 0 \pmod{q}\}. $$  

(7)

For $R \subseteq [3]$, let $\Psi_R = \sqrt{q} E_R^{(3)} [P, [q]^3]$. Denote also $T_i^{-1}(S) = \{ j \in [3] \mid a_j \in S \}$. Then, we have the following identity

$$\hat{G}^\mu = \sum_{S \subseteq [3n]} \alpha_\mu(S) \bigotimes_{i \in [n]} \Psi_{T_i^{-1}(S)}.$$  

(8)

By the definition of $\mathcal{C}_s'$, the only $\Psi_R$ that appear in the right-hand side of (8) with non-zero coefficients are $\Psi_\emptyset$, $\Psi_{\{1\}}$, $\Psi_{\{2\}}$ and $\Psi_{\{3\}}$. For these matrices, the following result holds.

**Claim 7.** For $R, R' \in \{\emptyset, \{1\}, \{2\}, \{3\}\}$, we have $\Psi^*_R \Psi_{R'} = \begin{cases} E_R^{(3)}, & \text{if} \ R = R'; \\ 0, & \text{otherwise}. \end{cases}$

**Proof.** These identities will easily follow once we establish singular value decompositions of the matrices $\Psi_R$. We identify the elements in $P$ from (7) with tuples $(b, c) \in [3]^2$ because the value of $a$ is uniquely determined by $b$ and $c$.

First, it easy to see that

$$\Psi_\emptyset = (e_0 \otimes e_0) (e_0 \otimes e_0 \otimes e_0)^*$$  

(9)

Similarly, we get

$$\Psi_{\{1\}} = \sum_{i=1}^{q-1} (e_i \otimes e_0) (e_0 \otimes e_i \otimes e_0)^* \quad \text{and} \quad \Psi_{\{3\}} = \sum_{i=1}^{q-1} (e_0 \otimes e_i) (e_0 \otimes e_0 \otimes e_i)^*.$$  

(10)
Now consider $E_{(1)}^{(3)}$. Its singular value decomposition clearly is

$$E_1 \otimes E_0 \otimes E_0 = \sum_{i=1}^{q-1} (e_i \otimes e_0 \otimes e_0)(e_i \otimes e_0 \otimes e_0)^*.$$  

Now observe that for $t = (a, b, c) \in P$, we have

$$(e_i \otimes e_0 \otimes e_0)[t] = q^{-3/2}\omega^{ia} = q^{-3/2}\omega^{-(b+c)} = (e_0 \otimes e_{q-i} \otimes e_{q-i})[t].$$

Hence,

$$\Psi_{(1)} = \sum_{i=1}^{q-1} (e_{q-i} \otimes e_{q-i})(e_i \otimes e_0 \otimes e_0)^*.$$  

All the left singular vectors appearing in (9)–(11) are pairwise orthogonal, which gives the required identities. □

Using (8) and Claim 7, one readily sees that

$$(\hat{G}^\mu)^* (\hat{G}^\mu) = \sum_{S \subseteq \{3n\}} \alpha_\mu(S)^2 \otimes_{i \in [n]} E_{T_i^{-1}(S)}^{(3)} = \sum_{S \subseteq \{3n\}} \alpha_\mu(S)^2 E_S^{(3n)}. \tag{12}$$

Thus,

$$\hat{\Gamma}^* \hat{\Gamma} = \sum_{\mu \in \mathcal{C}_t} (\hat{G}^\mu)^* (\hat{G}^\mu) = \sum_{S \subseteq \{3n\}} \left[ \sum_{\mu \in \mathcal{C}_t} \alpha_\mu(S)^2 \right] E_S^{(3n)}, \tag{13}$$

hence $\|\hat{\Gamma}\| = \sqrt{\|\hat{\Gamma}^* \hat{\Gamma}\|}$ is at least the objective value (5a), which is $\Omega(n^{1/3})$ by Proposition 6.

Similarly, for $\hat{\Gamma}'$ defined after (6), we get that

$$(\hat{\Gamma}')^* (\hat{\Gamma}') = \sum_{S \subseteq \{3n\} \setminus \{j\}} \left[ \sum_{\mu \in \mathcal{C}_t} (\alpha_\mu(S) - \alpha_\mu(S \cup \{j\}))^2 \right] E_S^{(3n)}.$$

Hence, $\|\hat{\Gamma}'\| = O(1)$ by (33).

The last step is to go from $\hat{\Gamma}$ to $\Gamma$. Recall that $\Gamma$ is obtained by removing all the columns of $\hat{\Gamma}$ that do not correspond to negative inputs. Since $\Gamma'$ is a submatrix of $\hat{\Gamma}'$, we have $\|\Gamma'\| = O(1)$. So, the only thing remaining is to lower bound $\|\Gamma\|$.

For a uniformly random triple $(a, b, c) \in [q]^3$, the probability is $1/q$ that $a+b+c$ is divisible by $q$. There are $n^3$ possible triples having one element in each of $A$, $B$ and $C$. Hence, by the union bound, a uniformly random input in $[q]^{3n}$ is negative with probability at least $1 - n^3 / q \geq 1/2$. That is, $|Y| \geq q^{3n}/2$.

Let $u \in \mathbb{R}^{X^u}$ and $v \in \mathbb{R}^Y$ be uniform unit vectors: $u = e_0^\otimes 2n$ and $v[y] = |Y|^{-1/2}$. To simplify notation, we define $\tilde{v} \in \mathbb{R}^{Z}$ by $\tilde{v}[y] = v[y]$ if $y \in Y$ and $\tilde{v}[y] = 0$ otherwise. The right singular vectors in (10) and (11) are orthogonal to $e_0 \otimes e_0$, hence, using (3),

$$u^* G^\mu v = u^* \hat{G}^\mu \tilde{v} = \sum_{S \subseteq \{3n\}} \alpha_\mu(S) u^* \left( \otimes_{i \in [n]} \Psi_{T_i^{-1}(S)} \right) \tilde{v} = \alpha_\mu(\emptyset) u^* \Psi^0 \tilde{v} \geq n^{-2/3} \cdot \frac{1}{\sqrt{2}}.$$  

using (4) and that $|Y| \geq q^{3n}/2$. Let $\bar{u}$ be the uniform unit vector in $\mathbb{R}^X$. Then, using that $|M_s| = n^2$:

$$\|\Gamma\| \geq \bar{u}^* \Gamma v = \sum_{\mu \in M_s} \frac{1}{n} u^* G^\mu v = n \cdot \frac{n^{-2/3}}{\sqrt{2}} = \frac{n^{1/3}}{\sqrt{2}}.$$  

as required.
5 Property Testing Version

In this section, we prove a quantum lower bound for the property testing version of the 3-shift-sum problem. Unlike the original version of the 3-shift-sum problem, this problem makes sense even for $q = 2$, so, for concreteness, we will define it for Boolean alphabet, however, similar results hold for larger alphabet sizes.

An input is a string in $\{0, 1\}^{3n}$. For a positive input $x$, there exists $\mu \in M_s$ such that $x_a \oplus x_b \oplus x_c = 0$ for every triple $\{a, b, c\} \in \mu$. Here $\oplus$ stands for xor. The negative inputs are defined as being at relative Hamming distance $\varepsilon$ to the set of positive inputs.

**Theorem 8.** For $\varepsilon \leq \frac{1}{7}$, the property testing version of the 3-shift-sum problem requires $\Omega(n^{1/3})$ quantum queries to solve.

The construction and the proof are identical to those in Section 4. One slight difference is in going from $\hat{\Gamma}$ to $\Gamma$ at the end of the proof. The only thing we actually used in this step is that the set of negative inputs $Y$ satisfy $|Y| \geq q^{3n}/2$. If we prove this for this version of the problem, we will be done.

Recall that we treat $x$ as an $3 \times n$ matrix. Fix the last two rows. The input $x$ is negative if its first row is at relative Hamming distance at least $\frac{3}{7}$ from the xor of any of $n^2$ circular shifts of the last two rows. A simple application of the Chernoff and the union bounds shows that this is the case with probability $1 - o(1)$.

6 Open Problems

The quantum query complexity of the two introduced problems is not completely settled down. In this paper we showed an $O(\sqrt{n})$ upper bound and $\Omega(n^{1/3})$ lower bound.

Some other open problems can be formulated. What functions with randomised query complexity $\omega(\sqrt{n})$ could potentially have poly-logarithmic quantum query complexity? Or, can a relatively general result be proven that excludes some of such functions? For what other problems can the dual learning graph framework be useful?

Acknowledgements

This research is partially supported by the ERDF project number 1.1.1.2/I/16/113. Part of this work was done while supported by the ERC Advanced Grant MQC.

References

[1] S. Aaronson and A. Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. In Proc. of 47th ACM STOC, pages 307–316, 2015. arXiv:1411.5729.

[2] S. Aaronson, S. Ben-David, and R. Kothari. Separations in query complexity using cheat sheets. In Proc. of 48th ACM STOC, pages 863–876, 2016. arXiv:1511.01937.

[3] A. Ambainis. Quantum lower bounds by quantum arguments. Journal of Computer and System Sciences, 64(5):750–767, 2002. Earlier: $STOC’00$, arXiv:quant-ph/0002066.

[4] A. Belovs. Span programs for functions with constant-sized 1-certificates. In Proc. of 44th ACM STOC, pages 77–84, 2012. arXiv:1105.4024.
[5] A. Belovs. *Applications of the Adversary Method in Quantum Query Algorithms*. PhD thesis, University of Latvia, 2014. arXiv:1402.3858.

[6] A. Belovs and A. Rosmanis. Adversary lower bounds for the collision and the set equality problems. arXiv:1310.5185 2013.

[7] A. Belovs and A. Rosmanis. On the power of non-adaptive learning graphs. *Computational Complexity*, 23(2):323–354, 2014. Earlier: [CCC’13](arXiv:1210.3279).

[8] A. Belovs and R. Špalek. Adversary lower bound for the $k$-sum problem. In *Proc. of 4th ACM ITCS*, pages 323–328, 2013. arXiv:1206.6528.

[9] S. Ben-David. A super-Grover separation between randomized and quantum query complexities. arXiv:1506.08105 2015.

[10] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(2):21–43, 2002.

[11] M. Ettinger, P. Høyer, and E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1):43–48, 2004. arXiv:quant-ph/0401083.

[12] P. Høyer, T. Lee, and R. Špalek. Negative weights make adversaries stronger. In *Proc. of 39th ACM STOC*, pages 526–535, 2007. arXiv:quant-ph/0611054.

[13] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35:170–188, 2005. arXiv:quant-ph/0302112.

[14] T. Lee, R. Mittal, B. W. Reichardt, R. Špalek, and M. Szegedy. Quantum query complexity of state conversion. In *Proc. of 52nd IEEE FOCS*, pages 344–353, 2011. arXiv:1011.3020.

[15] A. Montanaro and R. de Wolf. A survey of quantum property testing. *Theory of Computing Graduate Surveys*, 7:1–81, 2016. arXiv:1310.2035.

[16] B. W. Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every Boolean function. In *Proc. of 50th IEEE FOCS*, pages 544–551, 2009. arXiv:0904.2759.

[17] R. Špalek and M. Szegedy. All quantum adversary methods are equivalent. *Theory of Computing*, 2:1–18, 2006. Earlier: [ICALP’05](arXiv:quant-ph/0409116).

[18] S. Zhang. On the power of Ambainis lower bounds. *Theoretical Computer Science*, 339(2):241–256, 2005. arXiv:quant-ph/0311060.