Adversary Lower Bound for Element Distinctness

Aleksandrs Belovs[*]

Abstract

In this note we construct an explicit optimal (negative-weight) adversary matrix for the element distinctness problem, given that the size of the alphabet is sufficiently large.

1 Introduction

Two main techniques for proving lower bounds on quantum query complexity are the polynomial method [6] developed by Beals *et al.* in 1998, and the adversary method [2] developed by Ambainis in 2000. Both techniques are incomparable. There are functions with adversary bound strictly larger than polynomial degree [3], as well as functions with the reverse relation.

Two main examples of the reverse relation are exhibited by the collision and the element distinctness functions. The input to both functions is a string of length n of symbols in an alphabet of size q, i.e., $x = (x_i) \in [q]^n$. We use notation $[q]$ to denote the set $\{1, \ldots, q\}$. The element distinctness function evaluates to 0 if all symbols in the input string are pairwise distinct, and to 1 otherwise. The collision function is defined similarly with the additional promise that in the positive case the input can be divided into pairwise disjoint pairs of equal elements with different values in different pairs, i.e., for each $i \in [n]$ there exists unique $j \in [n] \setminus \{i\}$ such that $x_i = x_j$. Clearly, this problem is non-trivial only if n is even.

The quantum query complexity of the collision and the element distinctness problems are $O(n^{1/3})$ and $O(n^{2/3})$, respectively, with the algorithms given by Brassard *et al.* [7] and Ambainis [5], respectively. The tight lower bounds were given by Aaronson and Shi [1], Kutin [9] and Ambainis [4] using the polynomial method.

The adversary bound, however, fails for these functions. The so-called certificate complexity barrier [12, 13] implies that the best lower bound achievable by the adversary method is mere $\Omega(\sqrt{n})$. Similarly, the so-called property testing barrier [8] shows that an $\omega(1)$ lower bound for collision is out of reach for the adversary method.

In 2006, a stronger version of the adversary bound was developed by Høyer *et al.* [8]. This is the so-called negative-weight adversary lower bound. Later it was proved to be optimal by Reichardt *et al.* [11, 10]. Let us define it.

Assume $f : \mathcal{D} \to \{0, 1\}$ is a function with domain $\mathcal{D} \subseteq [q]^n$. Let $\mathcal{M}$ be the set of non-zero real matrices with rows indexed by the elements of $f^{-1}(1)$, and columns indexed by the elements of $f^{-1}(0)$. For $i \in [n]$, let Δ_i be the matrix from $\mathcal{M}$ with entry (x, y) equal to 1 if $x_i \neq y_i$, and to 0 otherwise. The *negative-weight adversary bound* is defined as

$$\mathrm{Adv}^{\pm}(f) = \max_{\Gamma \in \mathcal{M}} \frac{\|\Gamma\|}{\max_{i \in [n]} \|\Gamma \circ \Delta_i\|}, \tag{1}$$

where $\| \cdot \|$ is the spectral norm, and $\circ$ is the Hadamard (element-wise) product of matrices.

Let $Q(f)$ denote the query complexity of the best quantum algorithm evaluating f with a bounded error. Then we have the following result:

Theorem 1 ([8, 11, 10])**.** *Let f be as above. Then, $Q(f) = \Theta(\mathrm{Adv}^{\pm}(f))$.*

Although the negative-weight adversary lower bound is known to be tight, it has been almost never used to prove lower bounds for explicit functions. Vast majority of lower bounds by the adversary method used the old positive-weight version of this method. But since the only competing polynomial method

---

[*]Faculty of Computing, University of Latvia, stiboh@gmail.com.

is known to be non-tight, a better understanding of the negative-weight adversary method would be very beneficial. In the sequel, we consider the negative-weight adversary bound only, and will omit the adjective "negative-weight".

The aforementioned proof of the lower bound for element distinctness using the polynomial method is circuitous, and consists of three steps:

1. an $\Omega(n^{1/3})$ lower bound on the collision problem (with somewhat large range) using polynomial method [1, 9];

2. a reduction from the the $\Omega(n^{1/3})$ collision lower bound to an $\Omega(n^{2/3})$ element distinctness lower bound with large range;

3. a reduction of the size of the range [4]. Unfortunately, this reduction only works for lower bounds obtained using the polynomial method.

In this note, we construct an explicit adversary matrix that combines the first two steps. In other words, it gives an $\Omega(n^{2/3})$ lower bound for element distinctness, provided that the size of the alphabet $q = \Omega(n^2)$. We hope it will lead to proving adversary lower bounds for quantum query complexity of other functions.

2 Construction

The aim of this section is to prove the following result:

Theorem 2. *If f is the element distinctness function with $q = \Omega(n^2)$, then there exists $\Gamma \in \mathcal{M}$ such that the expression in (1) is $\Omega(n^{2/3})$.*

We may assume the rows of Γ are indexed with the inputs with a unique collision, i.e., for each index $x \in [q]^n$ of a row in $\mathcal{M}$, there exist $a, b \in [n]$ such that $a \neq b$, $x_a = x_b$, and $x_i \neq x_j$ for all $i \neq j$ unless $\{i, j\} = \{a, b\}$. We say $\{a, b\}$ is the position of the collision in x. The columns of Γ are indexed by inputs with all elements distinct.

The idea of our construction is to embed Γ into a slightly larger matrix $\Gamma' \in \mathcal{M}'$, where $\mathcal{M}'$ is $\mathcal{M}$ with additional rows and columns to be defined later. Define Δ_i on $\mathcal{M}'$ in the same way it is defined on $\mathcal{M}$. Then $\Gamma \circ \Delta_i$ is a submatrix of $\Gamma' \circ \Delta_i$, hence, $\|\Gamma \circ \Delta_i\| \leq \|\Gamma' \circ \Delta_i\|$. The thing to prove then is that $\|\Gamma'\|$ is large, and that $\|\Gamma\|$ is not much smaller than $\|\Gamma'\|$.

The matrix Γ' consists of $\binom{n}{2}$ matrices $G_{a,b}$ stacked one on another for all possible choices $\{a, b\} \subset [n]$. That is,

$$\Gamma' = \begin{pmatrix} G_{1,2} \\ G_{1,3} \\ \vdots \\ G_{n-1,n} \end{pmatrix}.$$

In $G_{a,b}$, the columns are labeled by the elements $y \in [q]^n$, and the rows are labeled by the elements $x \in [q]^n$ with the additional requirement $x_a = x_b$ (thus, there are q^{n-1} rows in each $G_{a,b}$).

We say a column with index y is *illegal* if $y_i = y_j$ for some $i \neq j$. Similarly, we say a row in $G_{a,b}$ with index x is illegal if $x_i = x_j$ for some $i \neq j$ such that $\{i, j\} \neq \{a, b\}$. Thus, after removing all illegal rows and columns, $G_{a,b}$ will represent the part of Γ with the rows indexed by the inputs having collision in $\{a, b\}$.

Clearly, since there are elements of $[q]^n$ that are used as labels of both rows and columns in $\mathcal{M}'$, it is easy to design a matrix $\Gamma' \in \mathcal{M}'$ such that the value in (1) is arbitrarily large. But we design Γ' in such way that it still is a good adversary matrix after the illegal rows and columns are removed.

Let J_q be the $q \times q$ all-ones matrix. Assume $e_0, \ldots, e_{q-1}$ is an orthonormal eigenbasis of J_q with $e_0 = 1/\sqrt{q}(1, \ldots, 1)$ being the eigenvalue q eigenvector. Consider the vectors of the following form:

$$v = e_{v_1} \otimes e_{v_2} \otimes \cdots \otimes e_{v_n}, \tag{2}$$

where $v_i \in \{0, \ldots, q-1\}$. These are eigenvectors of the Hamming Association Scheme on $[q]^n$. For a vector v from (2), the *weight* $|v|$ is defined as the number of non-zero entries in $(v_1, \ldots, v_n)$. Let $E_k^{(n)}$,

for $k = 0, \ldots, n$, be the orthogonal projector on the space spanned by the vectors from (2) having weight k. These are the projectors on the eigenspaces of the association scheme. Let us denote $E_i = E_i^{(1)}$ for $i = 0, 1$. These are $q \times q$ matrices. All entries of E_0 are equal to $1/q$, and the entries of E_1 are given by

$$(E_1)_{xy} = \begin{cases} 1 - 1/q, & x = y; \\ -1/q, & x \neq y. \end{cases}$$

Elements a and b in $G_{a,b}$ should be treated differently from the rest of the elements. For them, we define two $q \times q^2$ operators F_0 and F_1. They are defined by taking the $\sqrt{q}$ multiples of $E_0^{(2)}$ and $E_1^{(2)}$ and considering only the rows consisting of two equal elements. The first operator is $F_0 = e_0(e_0 \otimes e_0)^*$. The second one is

$$F_1 = \sum_{i \neq 0} e_i(e_0 \otimes e_i + e_i \otimes e_0)^*.$$

All entries of F_0 are equal to $q^{-3/2}$. The entry of F_1 on the intersection of a row with index (x, x) and a column with index (y_1, y_2) is

$$\frac{1}{\sqrt{q}} \begin{cases} 2 - 2/q, & y_1 = y_2 = x; \\ 1 - 2/q, & y_1 = x, \text{ or } y_2 = x, \text{ but not both}; \\ -2/q, & y_1 \neq x \text{ and } y_2 \neq x. \end{cases}$$

We are going to define $G_{1,2}$ as a linear combination of $F_\ell \otimes E_k^{(n-2)}$ with $\ell \in \{0, 1\}$, $k \in \{0, \ldots, n-2\}$. All other $G_{a,b}$s are obtained from $G_{1,2}$ by permuting the input variables so that $\{1, 2\}$ gets moved to $\{a, b\}$.

We have to understand three things: how the coefficients of $F_\ell \otimes E_k^{(n-2)}$s contribute to the norm of Γ', how Δ_i acts of these elements, and how they affect the norm $\Gamma' \circ \Delta_i$.

Norm of Γ' Let $W(G) = (\Gamma')^*\Gamma'$, where Γ' is obtained from $G_{1,2} = G$ as described above. It is a positive semidefinite matrix with rows and columns labeled by elements of $[q]^n$. We describe it in the basis from (2). At first, we have

$$W(F_0 \otimes E_k^{(n-2)}) = \frac{(n-k)(n-k-1)}{2} E_k^{(n)}. \tag{3}$$

Here the coefficient is equal to the number of variants of picking a pair of components of v from (2) equal to e_0, if v has weight k. Also, we have

$$v^* \, W(F_1 \otimes E_k^{(n-2)}) \, v' = \begin{cases} (k+1)(n-k-1), & v = v' \text{ and } |v| = k+1 \; ; \\ 1, & |v| = |v'| = k+1 \text{ and } v \text{ can be obtained from } v' \text{ by} \\ & \text{exchanging one } e_0 \text{ with one } e_j \text{ with } j \neq 0 \; ; \\ 0, & \text{otherwise}. \end{cases}$$

For each v of weight $k+1$, there are exactly $(k+1)(n-k-1)$ choices for v' such that the second option holds. Thus,

$$\left\| W(F_1 \otimes E_k^{(n-2)}) \right\| = 2(k+1)(n-k-1), \tag{4}$$

and $W(F_1 \otimes E_k^{(n-2)})$ acts as the zero operator on the orthogonal complement of $E_{k+1}^{(n)}$.

Action of Δ_1 Firstly, our construction ensures that Γ' is symmetric with respect to the permutation of variables. Thus, it suffices to estimate the norm of $\Gamma' \circ \Delta_1$. Next, it is known that $\|A \circ \Delta_1\| \leq 2\|A\|$ for any $A \in \mathcal{M}'$ [10]. Using this, and in order to simplify calculations, we consider not the mapping $\Gamma' \mapsto \Gamma' \circ \Delta_1$, but some mapping $\Gamma' \xmapsto{\Delta_1} \Gamma'_1$ such that $\Gamma' \circ \Delta_1 = \Gamma'_1 \circ \Delta_1$. In other words, we are allowed to change arbitrarily entries (x, y) with $x_1 = y_1$.

Since Δ_1 acts trivially on all input variables except the first one, it is enough to consider its action on E_0, E_1, F_0, and F_1. For the first two, we define:

$$E_0 \xmapsto{\Delta_1} E_0 \qquad \text{and} \qquad E_1 \xmapsto{\Delta_1} -E_0. \tag{5}$$

For F_i, we embed it back into $E^{(2)}$, apply the transformation from (5) and remove the unnecessary rows again. In the result:

$$F_0 \xmapsto{\Delta_1} F_0 \qquad \text{and} \qquad F_1 \xmapsto{\Delta_1} -F_0 + \sum_{i \neq 0} e_i (e_0 \otimes e_i)^*.$$

Thus, if we take $F = F_0 + F_1$, we have

$$F \xmapsto{\Delta_1} \sum_{i \neq 0} e_i (e_0 \otimes e_i)^*. \tag{6}$$

We are going to construct $G_{1,2}$ as

$$G_{1,2} = \sum_k \alpha_k F \otimes E_k^{(n-2)} \tag{7}$$

for some non-negative real α_ks.

Norm of Γ_1' The matrix Γ' can be naturally divided into two submatrices: the first one formed by the matrices $G_{1,b}$, and the second one by $G_{a,b}$s with $a, b \neq 1$. Let W_1 and W_2 be defined similarly as W, but after applying Δ_1 and for the first and the second submatrices, respectively.

Let's start with the first submatrix. From (6), we have

$$W_1(F \otimes E_k^{(n-2)}) = (k+1) E_0 \otimes E_{k+1}^{(n-1)}. \tag{8}$$

For W_2, we may assume $\{a, b\} = \{n-1, n\}$, analyze the action of Δ_1 on $E_k^{(n-2)}$s, and then apply element permutation on the last $n-1$ elements like in the construction of Γ' from $G_{1,2}$.

From (5), we have:

$$\sum_k \alpha_k E_k^{(n-2)} \xmapsto{\Delta_1} E_0 \otimes \sum_k (\alpha_k - \alpha_{k+1}) E_k^{(n-3)}.$$

Using this, as well as (3) and (4), modified to the last $n-1$ elements, we get

$$\left\| W_2 \left(F \otimes \sum_k \alpha_k E_k^{(n-2)} \right) \right\| = O(n^2) \max_k (\alpha_k - \alpha_{k+1})^2. \tag{9}$$

Optimizing α_k Now we are able to choose α_k optimally. We assume that the norm of Γ' is maximized for the right singular subspace $E_0^{(n)}$. Thus, from (3), we have

$$\|\Gamma'\|^2 = \Omega(\alpha_0^2 n^2). \tag{10}$$

From (8) and (9), we have the following conditions on $\|\Gamma_1'\| = O(1)$:

$$\alpha_k^2 \leq \frac{1}{k+1} \qquad \text{and} \qquad \alpha_k - \alpha_{k+1} \leq \frac{1}{n}.$$

Thus, the maximal possible value of α_0 equals, up to a constant factor, to the minimal value of $1/\sqrt{r} + r/n$ over r. The minimum is $n^{-1/3}$ that is attained at $r = n^{2/3}$. Thus, by (10), the optimal value of $\|\Gamma'\|$ is $\Omega(n^{2/3})$.

Norm of Γ In order to finish the proof, it remains to show that $\|\Gamma\|$ is not much smaller than $\|\Gamma'\|$, where Γ is obtained from Γ' by striking out the illegal rows and columns. This is the only place where we use the assumption $q = \Omega(n^2)$. We start with the following technical observation.

Lemma 3. *Let $\tilde{E}_1^{(k)}$ be the matrix $E_1^{\otimes k}$ with the rows and the columns having equal elements in their indices are removed. The sum of the elements of $\tilde{E}_1^{(k)}$ is non-negative.*

Proof. Because of the symmetry, it suffices to prove that the sum of the elements of the first row of $\tilde{E}_1^{(k)}$ is non-negative. We prove a slightly more general statement by induction on k. Assume $k \leq \ell \leq q$ and let $g(k, \ell, q)$ denote the sum of the elements of the first row of the matrix $(qI_\ell - J_\ell)^{\otimes k}$ after the rows and the columns with equal elements are removed. Here I_ℓ and J_ℓ are the $\ell \times \ell$ identity and all-ones matrices, respectively. We prove that $g(k, \ell, q) \geq 0$ for all choices of k, ℓ and q. Then the sum of the elements of the first row of $\tilde{E}_1^{(k)}$ equals $q^{-k}g(k, q, q) \geq 0$.

Assume the first row is labeled by the sequence $(1, 2, \ldots, k)$. It is easy to see that $g(0, \ell, q) = 1$ and $g(1, \ell, q) = q - \ell$ both are non-negative. Now assume $k \geq 2$. Then the labels of the columns $(y_1, \ldots, y_k)$ of the matrix can be divided into three parts:

- $y_1 = 1$. The contribution of the entries in these columns is $(q-1)g(k-1, \ell-1, q)$.

- $y_1 \in [\ell] \setminus [k]$. The contribution from these columns is $-(\ell - k)g(k-1, \ell-1, q)$.

- $y_1 \in [k] \setminus \{1\}$. Assume $y_1 = 2$ at first. Considering $\{y_3, \ldots, y_k\}$ only, we get $g(k-2, \ell-1, q)$. There are $\ell - k + 1$ choices of y_2, when all other elements of y are fixed. There are $k - 1$ choices of y_1. Thus, the total contribution of these columns is $(k-1)(\ell - k + 1)g(k-2, \ell-1, q)$.

Altogether:

$$g(k, \ell, q) = (q - \ell + k - 1)g(k-1, \ell-1, q) + (k-1)(\ell - k + 1)g(k-2, \ell-1, q) \geq 0,$$

because all the multiples are non-negative by the inductive assumption. $\qquad\square$

From our construction of Γ', we know that the singular value of the right singular vector $e_0^{\otimes n}$ is $\Omega(n^{2/3})$, and the corresponding left singular vector is the normalized all-ones vector as well. Hence, the singular value equals the sum of the elements of Γ' divided by $\sqrt{\binom{n}{2}q^{2n-1}}$.

It suffices to prove that the sum of the entires of $G_{1,2}$ doesn't drop much after all illegal rows and columns are removed. Let $\widetilde{G}_{1,2}$ be $G_{1,2}$ with these rows and columns removed. Consider expression (7). The contribution from $\alpha_0 F_0 \otimes E_0^{n-k}$ to the sum of all entries drop by at most a constant factor, because an $\Omega(1)$ fraction of the rows and columns of $G_{1,2}$ is legal (here we use that $q = \Omega(n^2)$).

All other terms in (7) contribute 0 to the sum of the elements in $G_{1,2}$. But their contribution to the sum of the elements of $\widetilde{G}_{1,2}$ is non-negative. Indeed, consider the terms

$$\alpha_k F_0 \otimes E_{v_3} \otimes \cdots \otimes E_{v_n}, \qquad \alpha_k \sum_{i \neq 0} e_i (e_i \otimes e_0)^* \otimes E_{v_3} \otimes \cdots \otimes E_{v_n} \quad \text{and} \quad \alpha_k \sum_{i \neq 0} e_i (e_0 \otimes e_i)^* \otimes E_{v_3} \otimes \cdots \otimes E_{v_n} \tag{11}$$

independently. Here, $v_3, \ldots, v_n \in \{0, 1\}$, and exactly k of them are 1.

In each of them, entry (x, y) of $\widetilde{G}_{1,2}$ only depends on x_i and y_i where $v_i = 1$, as well as $i = 1$ and $i = 2$ in the second and the third cases, respectively. The entry of $\widetilde{G}_{1,2}$ is proportional to the corresponding entry of $\tilde{E}_1^{(k)}$ or $\tilde{E}_1^{(k+1)}$, where the irrelevant elements of x and y are removed. Moreover, the number of entries of $\widetilde{G}_{1,2}$ corresponding to an entry of $\tilde{E}_1^{(k)}$ (or $\tilde{E}_1^{(k+1)}$) is the same for all entries. Hence, by Lemma 3, the contribution of the terms in (11) is non-negative. Thus, the norm of Γ still is $\Omega(n^{2/3})$.

Acknowledgments

References

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

[2] A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

[3] A. Ambainis. Polynomial degree vs. quantum query complexity. In *Proceedings of the 44th IEEE FOCS*, pages 230–239, 2003.

[4] A. Ambainis. Quantum lower bounds for collision and element distinctness with small range. *Theory of Computing*, 1:37–46, 2005.

[5] A. Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37:210–239, 2007.

[6] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001.

[7] G. Brassard, P. Høyer, and A. Tapp. Quantum cryptanalysis of hash and claw-free functions. *LATIN'98: Theoretical Informatics*, pages 163–169, 1998.

[8] P. Høyer, T. Lee, and R. Špalek. Negative weights make adversaries stronger. In *Proceedings of the 39th ACM STOC*, pages 526–535. ACM, 2007.

[9] S. Kutin. Quantum lower bound for the collision problem with small range. *Theory of Computing*, 1(1):29–36, 2005.

[10] T. Lee, R. Mittal, B. Reichardt, R. Špalek, and M. Szegedy. Quantum query complexity of the state conversion problem. In *Proceedings of 52nd IEEE FOCS*, 2011.

[11] B. Reichardt. Reflections for quantum query algorithms. In *Proceedings of 22nd ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pages 560–569, 2011.

[12] R. Špalek and M. Szegedy. All quantum adversary methods are equivalent. *Theory OF Computing*, 2:1–18, 2006.

[13] S. Zhang. On the power of ambainis lower bounds. *Theoretical Computer Science*, 339(2):241–256, 2005.