

Quantum Adversary Lower Bound for Element Distinctness with Small Range

Ansis Rosmanis*

Received March 5, 2014; Revised May 12, 2014; Published July 9, 2014

Abstract: The ELEMENT DISTINCTNESS problem is to decide whether each character of an input string is unique. The quantum query complexity of ELEMENT DISTINCTNESS is known to be $\Theta(N^{2/3})$; the polynomial method gives a tight lower bound for any input alphabet, while a tight adversary construction was only known for alphabets of size $\Omega(N^2)$.

We construct a tight $\Omega(N^{2/3})$ adversary lower bound for ELEMENT DISTINCTNESS with minimal non-trivial alphabet size, which equals the length of the input. This result may help to improve lower bounds for other related query problems.

1 Introduction and motivation

Background. In quantum computation, one of the main questions that we are interested in is: What is the quantum circuit complexity of a given computational problem? This question is hard to answer, and so we consider an alternative question: What is the quantum query complexity of the problem? For many problems, it is seemingly easier to (upper and lower) bound the number of times an algorithm requires to access the input rather than to bound the number of elementary quantum operations required by the algorithm. Nonetheless, the study of the quantum query complexity can give us great insights for the quantum circuit complexity. For example, a query-efficient algorithm for SIMON'S PROBLEM [26] helped Shor to develop a time-efficient algorithm for factoring [25]. On the other hand, $\tilde{\Omega}(N^{1/5})$ and $\Omega(N^{1/2})$ lower bounds on the (bounded error) quantum query complexity of the SET EQUALITY [21] and the INDEX ERASURE [6] problems, respectively, ruled out certain approaches for constructing time-efficient quantum algorithms for the GRAPH ISOMORPHISM problem.

*Supported by Mike and Ophelia Lazaridis Fellowship, David R. Cheriton Graduate Scholarship, and the US ARO.

Key words and phrases: quantum query complexity, adversary bound, element distinctness

Currently, two main techniques for proving lower bounds on quantum query complexity are the *polynomial method* developed by Beals, Buhrman, Cleve, Mosca, and de Wolf [7], and the *adversary method* originally developed by Ambainis [2] in what later became known as the positive adversary method. The adversary method was later strengthened by Høyer, Lee, and Špalek [16] by allowing negative weights in the adversary matrix. In recent results [22, 20], Lee, Mittal, Reichardt, Špalek, and Szegedy showed that, unlike the polynomial method [3], the general (i.e., strengthened) adversary method can give tight lower bounds for all problems. This is a strong incentive for the study of the adversary method.

Element Distinctness and Collision. Even though we know that tight adversary (lower) bounds exist for all query problems, for multiple problems we still do not know how to even construct adversary bounds that would match lower bounds obtained by other methods. For about a decade, ELEMENT DISTINCTNESS and COLLISION were prime examples of such problems. Given an input string $z \in \Sigma^N$, the ELEMENT DISTINCTNESS problem is to decide whether each character of z is unique, and the COLLISION problem is its special case given a promise that each character of z is either unique or appears in z exactly twice. As one can think of z as a function that maps $\{1, 2, \dots, N\}$ to Σ , the alphabet Σ is often also called the *range*.

The quantum query complexity of these two problems is known. Brassard, Høyer, and Tapp first gave an $O(N^{1/3})$ quantum query algorithm for COLLISION [13]. Aaronson and Shi then gave a matching $\Omega(N^{1/3})$ lower bound for COLLISION via the polynomial method, requiring that $|\Sigma| \geq 3N/2$ [1]. Due to a particular reduction from COLLISION to ELEMENT DISTINCTNESS, their lower bound also implied an $\Omega(N^{2/3})$ lower bound for ELEMENT DISTINCTNESS, requiring that $|\Sigma| \in \Omega(N^2)$. Subsequently, Kutin (for COLLISION) and Ambainis (for both) removed these requirements on the alphabet size [19, 4]. Finally, Ambainis gave an $O(N^{2/3})$ quantum query algorithm for ELEMENT DISTINCTNESS based on a quantum walk [5], thus improving the best previously known $O(N^{3/4})$ upper bound [14].

Hence, the proof of the $\Omega(N^{2/3})$ lower bound for ELEMENT DISTINCTNESS with minimal non-trivial alphabet size N (and, thus, any alphabet size) consists of three steps: an $\Omega(N^{1/3})$ lower bound for COLLISION, a reduction from an $\Omega(N^{1/3})$ lower bound for COLLISION to an $\Omega(N^{2/3})$ lower bound for ELEMENT DISTINCTNESS with the alphabet size $\Omega(N^2)$, and a reduction of the alphabet size. In this paper we prove the same result directly by providing an $\Omega(N^{2/3})$ general adversary bound for ELEMENT DISTINCTNESS with the alphabet size N .

The problems of SET EQUALITY, k -DISTINCTNESS, and k -SUM are closely related to COLLISION and ELEMENT DISTINCTNESS. SET EQUALITY is a special case of COLLISION given an extra promise that each character of the first half (and, thus, the second half) of the input string is unique. Given a constant k , the k -DISTINCTNESS problem is to decide whether the input string contains some character at least k times. For k -SUM, we assume that Σ is an additive group and the problem is to decide if there exist k numbers among N that sum up to a prescribed number.

Recent adversary bounds. Due to the *certificate complexity barrier* [30, 28], the positive weight adversary method fails to give a better lower bound for ELEMENT DISTINCTNESS than $\Omega(N^{1/2})$. And similarly, due to the *property testing barrier* [16], it fails to give a better lower bound for COLLISION than the trivial $\Omega(1)$. Recently, Belovs gave an $\Omega(N^{2/3})$ general adversary bound for ELEMENT DISTINCTNESS

with a large $\Omega(N^2)$ alphabet size [8]. In a series of works that followed, tight general adversary bounds were given for the k -SUM [12], CERTIFICATE-SUM [10], and COLLISION and SET EQUALITY problems [11], all of them requiring that the alphabet size is large. $\Omega(N^{k/(k+1)})$ and $\Omega(N^{1/3})$ lower bounds for k -SUM and SET EQUALITY, respectively, were improvements over the best previously known lower bounds. (The $\Omega(N^{1/3})$ lower bound for SET EQUALITY was also independently proven by Zhandry [29]; he used a completely different method, which did not require any assumptions on the alphabet size.)

The adversary lower bound for a problem is given via the *adversary matrix* (Section 2.2). The construction of the adversary matrix in all these recent (general) adversary bounds mentioned has one idea in common: the adversary matrix is extracted from a larger matrix that has been constructed using, essentially, the Hamming association scheme [15]. The fact that we initially embed the adversary matrix in this larger matrix is the reason behind the requirement of the large alphabet size. More precisely, due to the birthday paradox, these adversary bounds require the alphabet Σ to be large enough so that a randomly chosen string in Σ^N with constant probability is a negative input of the problem.

Also, for these problems, all the negative inputs are essentially equally hard. However, for k -DISTINCTNESS, for example, the hardest negative inputs seem to be the ones in which each character appears $k - 1$ times, and a randomly chosen negative input for k -DISTINCTNESS is such only with a minuscule probability. This might be a reason why an $\Omega(N^{2/3})$ adversary bound for k -DISTINCTNESS [27] based on the idea of the embedding does not narrow the gap to the best known upper bound, $O(N^{1-2^{k-2}/(2^k-1)})$ [9]. (The $\Omega(N^{2/3})$ lower bound was already known previously via the reduction from ELEMENT DISTINCTNESS attributed to Aaronson in [5].)

Motivation for our work. In this paper we construct an explicit adversary matrix for ELEMENT DISTINCTNESS with the alphabet size $|\Sigma| = N$ (and, thus, any alphabet size) yielding the tight $\Omega(N^{2/3})$ lower bound. We also provide certain “tight” conditions that every optimal adversary matrix for ELEMENT DISTINCTNESS must satisfy,¹ therefore suggesting that every optimal adversary matrix for ELEMENT DISTINCTNESS might have to be, in some sense, close to the adversary matrix that we have constructed.

The tight $\Omega(N^{k/(k+1)})$ adversary bound for k -SUM by Belovs and Špalek [12] is an extension of Belovs’ $\Omega(N^{2/3})$ adversary bound for ELEMENT DISTINCTNESS [8], and it requires $|\Sigma| \in \Omega(N^k)$. We construct the adversary matrix for ELEMENT DISTINCTNESS directly, without the embedding, therefore we do not require the condition $|\Sigma| \in \Omega(N^2)$ as in Belovs’ adversary bound. We hope that this might help to reduce the required alphabet size in the $\Omega(N^{k/(k+1)})$ lower bound for k -SUM.

As we mentioned before, an adversary matrix for k -DISTINCTNESS based on the idea of the embedding might not be able to give tight lower bounds. On the other hand, in our construction we only assume that the adversary matrix is invariant under all index and all alphabet permutations, and that is something we can always do without loss of generality due to the *automorphism principle* [16]—for ELEMENT DISTINCTNESS, k -DISTINCTNESS, and many other problems. Hence, due to the optimality of the general adversary method, we know that one can construct a tight adversary bound for k -DISTINCTNESS that satisfies these symmetries, and we hope that our construction for ELEMENT DISTINCTNESS might give insights in how to do that.

¹Assuming, without loss of generality, that the adversary matrix has the symmetry given by the automorphism principle.

Structure of the paper. This paper is structured as follows. In Section 2 we present the preliminaries of our work, including the adversary method, the automorphism principle, and the basics of the representation theory of the symmetric group. In Section 3 we show that the adversary matrix Γ can be expressed as a linear combination of specific matrices. In this section we also present Claim 3.2, which states what conditions every optimal adversary matrix for ELEMENT DISTINCTNESS must satisfy; we prove this claim in the appendix. In Section 4 we show how to specify the adversary matrix Γ via its submatrix $\Gamma_{1,2}$, which will make the analysis of the adversary matrix simpler. In Section 5 we present tools for estimating the spectral norm of the matrix entrywise product of Γ and the *difference matrix* Δ_i , a quantity that is essential to the adversary method. In Section 6 we use the conditions given by Claim 3.2 to construct an adversary matrix for ELEMENT DISTINCTNESS with the alphabet size N , and we show that this matrix indeed yields the desired $\Omega(N^{2/3})$ lower bound. We conclude in Section 7 with open problems.

2 Preliminaries

2.1 Element distinctness problem

Let N be the length of the input and let Σ be the input alphabet. Let $[i, N] = \{i, i+1, \dots, N\}$ and $[N] = [1, N]$ for short. Given an input string $z \in \Sigma^N$, the ELEMENT DISTINCTNESS problem is to decide whether z contains a collision or not, namely, whether there exist $i, j \in [N]$ such that $i \neq j$ and $z_i = z_j$. We only consider a special case of the problem where we are given a promise that the input contains at most one collision. This promise does not change the complexity of the problem [5].

Let \mathcal{D}_1 and \mathcal{D}_0 be the sets of positive and negative inputs, respectively, that is, inputs with a unique collision and inputs without a collision. If $|\Sigma| < N$, then $\mathcal{D}_0 = \emptyset$, and the problem becomes trivial, therefore we consider the case when $|\Sigma| = N$. We have

$$|\mathcal{D}_1| = \binom{N}{2} \frac{|\Sigma|!}{(|\Sigma| - N + 1)!} = \binom{N}{2} N! \quad \text{and} \quad |\mathcal{D}_0| = \frac{|\Sigma|!}{(|\Sigma| - N)!} = N!.$$

2.2 Adversary method

The general adversary method gives optimal bounds for any quantum query problem. Here we only consider the ELEMENT DISTINCTNESS problem, so it suffices to define the adversary method for decision problems. Let us think of a decision problem p as a Boolean-valued function $p : \mathcal{D} \rightarrow \{0, 1\}$ with domain $\mathcal{D} \subseteq \Sigma^N$, and let $\mathcal{D}_1 = p^{-1}(1)$ and $\mathcal{D}_0 = p^{-1}(0)$.

An adversary matrix for a decision problem p is a real $|\mathcal{D}_1| \times |\mathcal{D}_0|$ matrix Γ whose rows are labeled by the positive inputs \mathcal{D}_1 and columns by the negative inputs \mathcal{D}_0 . Let $\Gamma[[x, y]]$ denote the entry of Γ corresponding to the pair of inputs $(x, y) \in \mathcal{D}_1 \times \mathcal{D}_0$. For $i \in [N]$, the difference matrices Δ_i and $\bar{\Delta}_i$ are the matrices of the same dimensions and the same row and column labeling as Γ that are defined by

$$\Delta_i[[x, y]] = \begin{cases} 0, & \text{if } x_i = y_i, \\ 1, & \text{if } x_i \neq y_i, \end{cases} \quad \text{and} \quad \bar{\Delta}_i[[x, y]] = \begin{cases} 1, & \text{if } x_i = y_i, \\ 0, & \text{if } x_i \neq y_i. \end{cases}$$

Theorem 2.1 (Adversary bound [16, 20]). *The quantum query complexity of the decision problem p is $\Theta(\text{Adv}(p))$, where $\text{Adv}(p)$ is the optimal value of the semi-definite program*

$$\begin{aligned} & \text{maximize} && \|\Gamma\| \\ & \text{subject to} && \|\Delta_i \circ \Gamma\| \leq 1 \text{ for all } i \in [N], \end{aligned} \quad (2.1)$$

where the maximization is over all adversary matrices Γ for p , $\|\cdot\|$ is the spectral norm (i.e., the largest singular value), and \circ is the entrywise matrix product.

Every feasible solution to the semi-definite program (2.1) yields a lower bound on the quantum query complexity of p . Note that we can choose any adversary matrix Γ and scale it so that the condition $\|\Delta_i \circ \Gamma\| \leq 1$ holds. In practice, we use the condition $\|\Delta_i \circ \Gamma\| \in O(1)$ instead of $\|\Delta_i \circ \Gamma\| \leq 1$. Also note that $\Delta_i \circ \Gamma = \Gamma - \bar{\Delta}_i \circ \Gamma$.

2.3 Symmetries of the adversary matrix

It is known that we can restrict the maximization in Theorem 2.1 to adversary matrices Γ satisfying certain symmetries. Let \mathbb{S}_A be the symmetric group of a finite set A , that is, the group whose elements are all the permutations of elements of A and whose group operation is the composition of permutations. The automorphism principle [16] implies that, without loss of generality, we can assume that Γ for ELEMENT DISTINCTNESS is fixed under all index and all alphabet permutations. Namely, index permutations $\pi \in \mathbb{S}_{[N]}$ and alphabet permutations $\tau \in \mathbb{S}_\Sigma$ act on input strings $z \in \Sigma^N$ in the natural way:

$$\begin{aligned} \pi \in \mathbb{S}_{[N]} & : z = (z_1, \dots, z_N) \mapsto z_\pi = (z_{\pi^{-1}(1)}, \dots, z_{\pi^{-1}(N)}), \\ \tau \in \mathbb{S}_\Sigma & : z = (z_1, \dots, z_N) \mapsto z^\tau = (\tau(z_1), \dots, \tau(z_N)). \end{aligned}$$

The actions of π and τ commute: we have $(z_\pi)^\tau = (z^\tau)_\pi$, which we denote by z_π^τ for short. The automorphism principle implies that we can assume

$$\Gamma[[x, y]] = \Gamma[[x_\pi^\tau, y_\pi^\tau]] \quad (2.2)$$

for all $x \in \mathcal{D}_1$, $y \in \mathcal{D}_0$, $\pi \in \mathbb{S}_{[N]}$, and $\tau \in \mathbb{S}_\Sigma$.

Let $\mathcal{X} \cong \mathbb{R}^{|\mathcal{D}_1|}$ and $\mathcal{Y} \cong \mathbb{R}^{|\mathcal{D}_0|}$ be the vector spaces corresponding to the positive and the negative inputs, respectively. (We can view Γ as a linear operator that maps \mathcal{Y} to \mathcal{X} .) Let U_π^τ and V_π^τ be the permutation matrices that respectively act on the spaces \mathcal{X} and \mathcal{Y} and that map every $x \in \mathcal{D}_1$ to x_π^τ and every $y \in \mathcal{D}_0$ to y_π^τ . Then (2.2) is equivalent to

$$U_\pi^\tau \Gamma = \Gamma V_\pi^\tau \quad (2.3)$$

for all $\pi \in \mathbb{S}_{[N]}$, and $\tau \in \mathbb{S}_\Sigma$. Both U and V are representations of $\mathbb{S}_{[N]} \times \mathbb{S}_\Sigma$.

2.4 Representation theory of the symmetric group

Let us present the basics of the representation theory of the symmetric group. (For a detailed study of the representation theory of the symmetric group, refer to [17, 23]; for the fundamentals of the representation theory of finite groups, refer to [24].)

Up to isomorphism, there is one-to-one correspondence between the *irreps* (i.e., irreducible representations) of \mathbb{S}_A and $|A|$ -box *Young diagrams*, and we often use these two terms interchangeably. We use ζ , η , and θ to denote Young diagrams having $o(N)$ boxes, λ , μ , and ν to denote Young diagrams having N , $N - 1$, and $N - 2$ boxes, respectively, and ρ and σ for general statements and other purposes.

Let $\rho \vdash M$ denote that ρ is an M -box Young diagram. For a Young diagram ρ , let $\rho(i)$ and $\rho^\top(j)$ denote the number of boxes in the i -th row and j -th column of ρ , respectively. We write $\rho = (\rho(1), \rho(2), \dots, \rho(r))$, where $r = \rho^\top(1)$ is the number of rows in ρ , and, given $M \geq \rho(1)$, let (M, ρ) be short for $(M, \rho(1), \rho(2), \dots, \rho(r))$.

We say that a box (i, j) is present in ρ and write $(i, j) \in \rho$ if $\rho(i) \geq j$ (equivalently, $\rho^\top(j) \geq i$). The *hook-length* $h_\rho(b)$ of a box b is the sum of the number of boxes on the right from b in the same row (i.e., $\rho(i) - j$) and the number of boxes below b in the same column (i.e., $\rho^\top(j) - i$) plus one (i.e., the box b itself). The dimension of the irrep corresponding to ρ is given by the *hook-length formula*:

$$\dim \rho = |\rho|! / h(\rho), \quad \text{where} \quad h(\rho) = \prod_{(i,j) \in \rho} h_\rho(i, j) \tag{2.4}$$

and $|\rho|$ is the number of boxes in ρ .

Let $\sigma < \rho$ and $\sigma \ll \rho$ denote that a Young diagram σ is obtained from ρ by removing exactly one box and exactly two boxes, respectively. Given $\sigma \ll \rho$, let us write $\sigma \ll_r \rho$ or $\sigma \ll_c \rho$ if the two boxes removed from ρ to obtain σ are, respectively, in different rows or different columns. Let $\sigma \ll_{rc} \rho$ be short for $(\sigma \ll_r \rho) \& (\sigma \ll_c \rho)$. The *distance* between two boxes $b = (i, j)$ and $b' = (i', j')$ is defined as $|i' - i| + |j - j'|$. Given $\sigma \ll_{rc} \rho$, let $d_{\rho, \sigma} \geq 2$ be the distance between the two boxes that we remove from ρ to obtain σ .

The *branching rule* states that the restriction of an irrep ρ of \mathbb{S}_A to $\mathbb{S}_{A \setminus \{a\}}$, where $a \in A$, is

$$\text{Res}_{\mathbb{S}_{A \setminus \{a\}}}^{\mathbb{S}_A} \rho \cong \bigoplus_{\sigma < \rho} \sigma.$$

The more general *Littlewood–Richardson rule* implies that the restriction of an irrep ρ of \mathbb{S}_A to $\mathbb{S}_{\{a,b\}} \times \mathbb{S}_{A \setminus \{a,b\}}$, where $a, b \in A$, is

$$\text{Res}_{\mathbb{S}_{\{a,b\}} \times \mathbb{S}_{A \setminus \{a,b\}}}^{\mathbb{S}_A} \rho \cong \bigoplus_{\sigma \ll_c \rho} (id \times \sigma) \oplus \bigoplus_{\sigma' \ll_r \rho} (sgn \times \sigma'),$$

where $id = (2)$ and $sgn = (1, 1)$ are the trivial and the sign representation of $\mathbb{S}_{\{a,b\}}$, respectively. *Frobenius reciprocity* then tells us that the “opposite” happens when we induce an irrep of $\mathbb{S}_{A \setminus \{a\}}$ or $\mathbb{S}_{\{a,b\}} \times \mathbb{S}_{A \setminus \{a,b\}}$ to \mathbb{S}_A .

Given $\ell \in \{0, 1, 2, 3\}$, a set $A = [N]$ or $A = \Sigma$, its subset $A \setminus \{a_1, \dots, a_\ell\}$, and $\rho \vdash N - \ell$, let us write $\rho_{a_1 \dots a_\ell}$ if we want to stress that we think of ρ as an irrep of $\mathbb{S}_{A \setminus \{a_1, \dots, a_\ell\}}$. We omit the subscript if $\ell = 0$ or when $\{a_1, \dots, a_\ell\}$ is clear from the context. To lighten the notations, given $k \in o(N)$ and $\eta \vdash k$, let $\bar{\eta}_{a_1 \dots a_\ell} = (N - \ell - k, \eta)_{a_1 \dots a_\ell} \vdash N - \ell$; here we omit the subscript if and only if $\ell = 0$.

2.5 Transporters

Suppose we are given a group G , and let ξ_1 and ξ_2 be two isomorphic irreps of G acting on spaces \mathcal{Z}_1 and \mathcal{Z}_2 , respectively. Up to a global phase (i.e., a scalar of absolute value 1), there exists a unique

isomorphism $T_{2\leftarrow 1}$ from ξ_1 to ξ_2 that satisfies $\|T_{2\leftarrow 1}\| = 1$. We call this isomorphism a *transporter* from ξ_1 to ξ_2 (or, from \mathcal{Z}_1 to \mathcal{Z}_2).

In this paper we only consider unitary representations and real vector spaces, therefore all singular values of $T_{2\leftarrow 1}$ are equal to 1 and, for the global phase, we have to choose only between ± 1 . We always choose the global phases so that they respect inversion and composition, namely, so that $T_{1\leftarrow 2}T_{2\leftarrow 1}$ is the identity matrix on \mathcal{Z}_1 and $T_{3\leftarrow 2}T_{2\leftarrow 1} = T_{3\leftarrow 1}$, where ξ_3 is an irrep isomorphic to ξ_1 and ξ_2 .

3 Building blocks of Γ

3.1 Decomposition of U and V into irreps

Without loss of generality, let us assume that the adversary matrix Γ for the ELEMENT DISTINCTNESS problem satisfy the symmetry (2.3) given by the automorphism principle. Both U and V are representations of $\mathbb{S}_{[N]} \times \mathbb{S}_\Sigma$ and, due to Schur's lemma, we want to see what irreps of $\mathbb{S}_{[N]} \times \mathbb{S}_\Sigma$ occur in both U and V . It is also convenient to consider U and V as representations of just $\mathbb{S}_{[N]}$ or just \mathbb{S}_Σ .

Claim 3.1. V decomposes into irreps of $\mathbb{S}_{[N]} \times \mathbb{S}_\Sigma$ as $V \cong \bigoplus_{\lambda \vdash N} \lambda \times \lambda$.

Proof. As a representation of $\mathbb{S}_{[N]}$ and \mathbb{S}_Σ , respectively, V is isomorphic to the regular representation of $\mathbb{S}_{[N]}$ and \mathbb{S}_Σ . For every $y \in \mathcal{D}_0$ and every $\pi \in \mathbb{S}_{[N]}$, there is a unique $\tau \in \mathbb{S}_\Sigma$ such that $y_\pi = y^\tau$, and π and τ belong to isomorphic conjugacy classes. Thus, for every λ , the *isotypical subspace* of \mathcal{Y} corresponding to λ (i.e., the subspace corresponding to all irreps isomorphic to λ) is the same for both $\mathbb{S}_{[N]}$ and \mathbb{S}_Σ [24, Section 2.6]. Since V is isomorphic to the regular representation, the dimension of this subspace is $(\dim \lambda)^2$, which is exactly the dimension of the irrep $\lambda \times \lambda$ of $\mathbb{S}_{[N]} \times \mathbb{S}_\Sigma$. \square

Now let us address U , which acts on the space \mathcal{X} corresponding to the positive inputs $x \in \mathcal{D}_1$. Let us decompose \mathcal{D}_1 as a disjoint union of $\binom{N}{2}$ sets $\mathcal{D}_{i,j}$, where $\{i, j\} \subset [N]$ and $\mathcal{D}_{i,j}$ is the set of all $x \in \mathcal{D}_1$ such that $x_i = x_j$. Let us further decompose $\mathcal{D}_{i,j}$ as a disjoint union of $\binom{N}{2}$ sets $\mathcal{D}_{i,j}^{s,t}$, where $\{s, t\} \subset \Sigma$ and $\mathcal{D}_{i,j}^{s,t}$ is the set of all $x \in \mathcal{D}_{i,j}$ that does not contain s and contains t twice or vice versa. Let $\mathcal{X}_{i,j}$ and $\mathcal{X}_{i,j}^{s,t}$ be the subspaces of \mathcal{X} that correspond to the sets $\mathcal{D}_{i,j}$ and $\mathcal{D}_{i,j}^{s,t}$, respectively. The space $\mathcal{X}_{i,j}^{s,t}$ is invariant under the action of the subgroup $\mathbb{S}_{i,j}^{s,t}$ defined as

$$\mathbb{S}_{i,j}^{s,t} = (\mathbb{S}_{\{i,j\}} \times \mathbb{S}_{[N] \setminus \{i,j\}}) \times (\mathbb{S}_{\{s,t\}} \times \mathbb{S}_{\Sigma \setminus \{s,t\}}),$$

namely, $U_\pi^\tau \mathcal{X}_{i,j}^{s,t} = \mathcal{X}_{i,j}^{s,t}$ for all $(\pi, \tau) \in \mathbb{S}_{i,j}^{s,t}$. Therefore U restricted to the subspace $\mathcal{X}_{i,j}^{s,t}$ is a representation of $\mathbb{S}_{i,j}^{s,t}$, and, similarly to Claim 3.1, it decomposes into irreps as

$$\bigoplus_{\nu \vdash N-2} (id \times \nu) \times ((id \oplus sgn) \times \nu). \quad (3.1)$$

To see how U decomposes into irreps of $\mathbb{S}_{[N]} \times \mathbb{S}_\Sigma$, we induce the representation (3.1) from $\mathbb{S}_{i,j}^{s,t}$ to $\mathbb{S}_{[N]} \times \mathbb{S}_\Sigma$.

The Littlewood–Richardson rule implies that an irrep of $\mathbb{S}_{[N]} \times \mathbb{S}_\Sigma$ isomorphic to $\lambda \times \lambda$ can occur in U due to one of the following scenarios.

- If $\nu \ll_c \lambda$ and $\nu \not\ll_r \lambda$ (i.e., ν is obtained from λ by removing two boxes in the same row), then $\lambda \times \lambda$ occurs once in the induction of $(id \times \nu) \times (id \times \nu)$. Let $\mathcal{X}_{id,\nu}^\lambda$ denote the subspace of \mathcal{X} corresponding to this instance of $\lambda \times \lambda$.
- If $\nu \ll_{rc} \lambda$, then $\lambda \times \lambda$ occurs once in the induction of $(id \times \nu) \times (id \times \nu)$ and once in the induction of $(id \times \nu) \times (sgn \times \nu)$. Let $\mathcal{X}_{id,\nu}^\lambda$ and $\mathcal{X}_{sgn,\nu}^\lambda$ denote the respective subspaces of \mathcal{X} corresponding to these instances of $\lambda \times \lambda$.

Note: the subspaces $\mathcal{X}_{id,\nu}^\lambda$ and $\mathcal{X}_{sgn,\nu}^\lambda$ are independent from the choice of $\{i, j\} \subset [N]$ and $\{s, t\} \subset \Sigma$.

3.2 Γ as a linear combination of transporters

Let $\Xi_{id,\nu}^\lambda$ and $\Xi_{sgn,\nu}^\lambda$ denote the transporters from the unique instance of $\lambda \times \lambda$ in \mathcal{Y} to the subspaces $\mathcal{X}_{id,\nu}^\lambda$ and $\mathcal{X}_{sgn,\nu}^\lambda$, respectively. We will specify the global phases of these transporters in Section 4.3. We consider $\Xi_{id,\nu}^\lambda$ and $\Xi_{sgn,\nu}^\lambda$ as matrices of dimensions $\binom{N}{2}N! \times N!$ and rank $(\dim \lambda)^2$. Schur’s lemma implies that, due to (2.3), we can express Γ as a linear combination of these transporters. Namely,

$$\Gamma = \sum_{\lambda \vdash N} \left(\sum_{\nu \ll_c \lambda} \beta_{id,\nu}^\lambda \Xi_{id,\nu}^\lambda + \sum_{\nu \ll_{rc} \lambda} \beta_{sgn,\nu}^\lambda \Xi_{sgn,\nu}^\lambda \right), \tag{3.2}$$

where the coefficients $\beta_{id,\nu}^\lambda$ and $\beta_{sgn,\nu}^\lambda$ are real.

$\lambda \backslash \nu$	$(N-2)$	$(N-3, 1)$	$(N-4, 2)$	$(N-4, 1, 1)$
(N)	\checkmark_0			
$(N-1, 1)$	\checkmark_1	\checkmark_0		
$(N-2, 2)$	\checkmark_2	\checkmark_1	\checkmark_0	
$(N-2, 1, 1)$		\checkmark_1		\checkmark_0
$(N-3, 3)$		\checkmark_2	\checkmark_1	
$(N-3, 2, 1)$		\checkmark_2	\checkmark_1	\checkmark_1
$(N-3, 1, 1, 1)$				\checkmark_1
$(N-4, 4)$			\checkmark_2	
$(N-4, 3, 1)$			\checkmark_2	\checkmark_2
$(N-4, 2, 2)$			\checkmark_2	
$(N-4, 2, 1, 1)$				\checkmark_2

Table 1: Available operators for the construction of Γ . We distinguish three cases: both λ and ν are the same below the first row (label “ \checkmark_0 ”), λ has one box more below the first row than ν (label “ \checkmark_1 ”), λ has two boxes more below the first row than ν (labels “ \checkmark_2 ” and “ \checkmark_2 ”).

Thus we have reduced the construction of the adversary matrix Γ to choosing the coefficients β of the transporters in (3.2). To illustrate what are the available transporters, let us consider the last four $(N-2)$ -box Young diagrams ν of the *lexicographical order*— $(N-2)$, $(N-3, 1)$, $(N-4, 2)$, and $(N-4, 1, 1)$ —and all λ that are obtained from these ν by adding two boxes in different columns. Table

1 shows pairs of λ and ν for which we have both $\Xi_{id,\nu}^\lambda$ and $\Xi_{sgn,\nu}^\lambda$ available for the construction of Γ (double check mark “✓”) or just $\Xi_{id,\nu}^\lambda$ available (single check mark “√”).

Due to the symmetry, $\|\Delta_i \circ \Gamma\|$ is the same for all $i \in [N]$, so, from now on, let us only consider $\Delta_1 \circ \Gamma$. We want to choose the coefficients β so that $\|\Gamma\| \in \Omega(N^{2/3})$ and $\|\Delta_1 \circ \Gamma\| \in O(1)$. The automorphism principle also implies (see [16]) that we can assume that the principal left and right singular vectors of Γ are the all-ones vectors, which correspond to $\Xi_{id,(N-2)}^{(N)}$. We thus choose $\beta_{id,(N-2)}^{(N)} \in \Theta(N^{2/3})$.

In order to understand how to choose the coefficients β , in Appendix A we prove the following claim, which relates all the coefficients of transporters of Table 1 and more.

Claim 3.2. *Suppose Γ is given as in (3.2) and $\beta_{id,(N-2)}^{(N)} = N^{2/3}$. Consider $\lambda \vdash N$ that has $O(1)$ boxes below the first row and $\nu \ll_c \lambda$. In order for $\|\Delta_1 \circ \Gamma\| \in O(1)$ to hold, we need to have*

1. $\beta_{id,\nu}^\lambda = N^{2/3} + O(1)$ if λ and ν are the same below the first row,
2. $\beta_{id,\nu}^\lambda, \beta_{sgn,\nu}^\lambda = c_\nu^\lambda N^{1/6} + O(1)$ if λ has one box more below the first row than ν , where c_ν^λ is a constant depending only on the part of λ and ν below the first row,²
3. $\beta_{id,\nu}^\lambda, \beta_{sgn,\nu}^\lambda = O(1)$ if λ has two boxes more below the first row than ν .

Note that we always have the freedom of changing (a constant number of) coefficients β up to an additive term of $O(1)$ because of the fact that

$$\gamma_2(\Delta_1) = \max_B \{ \|\Delta_1 \circ B\| : \|B\| \leq 1 \} \leq 2 \quad (3.3)$$

(see [16] for this and other facts about the γ_2 norm). We will use this fact again in Section 6.

4 Specification of Γ via $\Gamma_{1,2}$

Due to the symmetry (2.2), it suffices to specify a single row of the adversary matrix Γ in order to specify the whole matrix. For the convenience, let us instead specify Γ via specifying its $(N! \times N!)$ -dimensional submatrix $\Gamma_{1,2}$ —for $\{i, j\} \subset [N]$, we define $\Gamma_{i,j}$ to be the submatrix of Γ that corresponds to the rows labeled by $x \in \mathcal{D}_{i,j}$, that is, positive inputs x with $x_i = x_j$. We think of $\Gamma_{i,j}$ both as an $N! \times N!$ square matrix and as a matrix of the same dimensions as Γ that is obtained from Γ by setting to zero all the $\binom{N}{2} - 1$ rows that correspond to $x \notin \mathcal{D}_{i,j}$.

4.1 Necessary and sufficient symmetries of $\Gamma_{1,2}$

For all $(\pi, \tau) \in (\mathbb{S}_{\{1,2\}} \times \mathbb{S}_{[3,N]}) \times \mathbb{S}_\Sigma$, we have $U_\pi^\tau \mathcal{X}_{1,2} = \mathcal{X}_{1,2}$ and, therefore, $U_\pi^\tau \Gamma_{1,2} = \Gamma_{1,2} V_\pi^\tau$. This is the necessary and sufficient symmetry that $\Gamma_{1,2}$ must satisfy in order for Γ to be fixed under all index and alphabet permutations. Since $U_{(12)} \Gamma_{1,2} = \Gamma_{1,2}$, we also have $\Gamma_{1,2} V_{(12)} = \Gamma_{1,2}$. We have

$$\Gamma = \sum_{\{i,j\} \subset [N]} \Gamma_{i,j} = \sum_{\pi \in R} U_\pi \Gamma_{1,2} V_{\pi^{-1}} = \binom{N}{2} \frac{1}{N!} \sum_{\pi \in \mathbb{S}_{[M]}} U_\pi \Gamma_{1,2} V_{\pi^{-1}}, \quad (4.1)$$

²Let $\hat{\lambda}$ and $\hat{\nu}$ be the part of λ and ν below the first row, respectively. Then $c_\nu^\lambda = \sqrt{h(\hat{\lambda})/h(\hat{\nu})} = \sqrt{N \dim \nu / \dim \lambda} + O(1/N)$.

where $R = \text{Rep}(\mathbb{S}_{[N]} / (\mathbb{S}_{\{1,2\}} \times \mathbb{S}_{[3,N]}))$ is a transversal of the left cosets of $\mathbb{S}_{\{1,2\}} \times \mathbb{S}_{[3,N]}$ in $\mathbb{S}_{[N]}$.

Let f be a bijection between \mathcal{D}_0 and $\mathcal{D}_{1,2}$ defined as

$$f: \mathcal{D}_0 \rightarrow \mathcal{D}_{1,2}: (y_1, y_2, y_3, \dots, y_N) \mapsto (y_1, y_1, y_3, \dots, y_N),$$

and let F be the corresponding permutation matrix mapping \mathcal{Y} to $\mathcal{X}_{1,2}$. Let us order rows and columns of $\Gamma_{1,2}$ so that they correspond to $f(y)$ and y , respectively, where we take $y \in \mathcal{D}_0$ in the same order for both (see Figure 1). Hence, F becomes the identity matrix on \mathcal{Y} (from this point onward, we essentially think of $\mathcal{X}_{1,2}$ and \mathcal{Y} as the same space). Let us denote this identity matrix by \mathbb{I} .

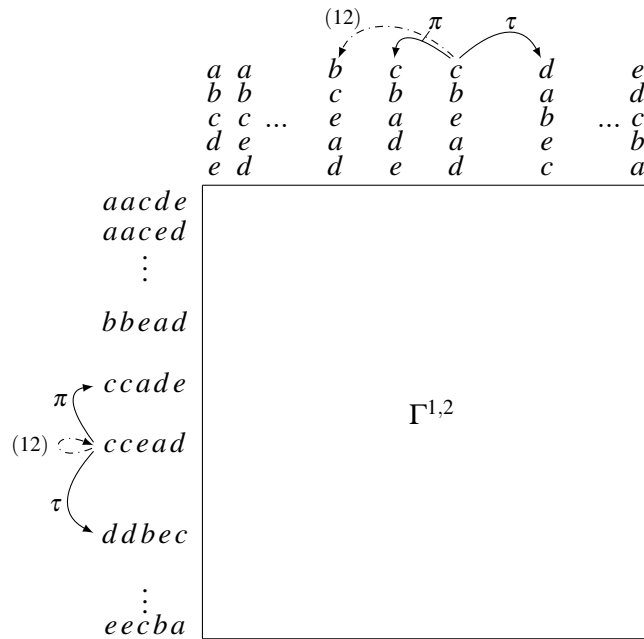


Figure 1: Symmetries of $\Gamma_{1,2}$ for $N = 5$ and $\Sigma = \{a, b, c, d, e\}$. With respect to the bijection f , the order of rows and columns matches. The solid arrows show that U^τ and V^τ act symmetrically on $\Gamma_{1,2}$ (here we use $\tau = (aeb)(cd) \in \mathbb{S}_\Sigma$), and so do U_π and V_π for $\pi \in \mathbb{S}_{[3,N]}$ (here we use $\pi = (354)$). However, as shown by the dash-dotted arrows, $U_{(12)}$ acts as the identity on the rows, while $V_{(12)}$ transposes the columns.

For all $(\pi, \tau) \in \mathbb{S}_{[3,N]} \times \mathbb{S}_\Sigma$ we have $f(y_\pi^\tau) = (f(y))_\pi^\tau$ and, thus, $V_\pi^\tau = FV_\pi^\tau = U_\pi^\tau F = U_\pi^\tau$, where we consider the restriction of U_π^τ to $\mathcal{X}_{1,2}$. Note that $U_{(12)} = \mathbb{I}$ on $\mathcal{X}_{1,2}$, while $V_{(12)} \neq \mathbb{I}$. Hence now the two necessary and sufficient symmetries that $\Gamma_{1,2}$ must satisfy are

$$V_\pi^\tau \Gamma_{1,2} = \Gamma_{1,2} V_\pi^\tau \quad \text{for all } (\pi, \tau) \in \mathbb{S}_{[3,N]} \times \mathbb{S}_\Sigma \quad \text{and} \quad \Gamma_{1,2} V_{(12)} = \Gamma_{1,2}. \quad (4.2)$$

Figure 1 illustrates these symmetries.

4.2 Labeling of projectors and transporters

We use Π , with some subscripts and superscripts, to denote operators acting on \mathcal{Y} ; we use subscripts for irreps of index permutations and superscripts for irreps of alphabet permutations. We also think of each such an operator Π to map \mathcal{Y} to $\mathcal{X}_{1,2}$ and vice versa (technically, $F\Pi$ and ΠF^* , respectively).

Let $\Pi_{id} = (\mathbb{I} + V_{(12)})/2$ and $\Pi_{sgn} = (\mathbb{I} - V_{(12)})/2$ denote the projectors on the isotypical subspaces of \mathcal{Y} corresponding to irreps $id = (2)$ and $sgn = (1, 1)$ of $\mathbb{S}_{\{1,2\}}$, respectively. Let $\Pi_{\rho_{i_1 \dots i_\ell}}$ and $\Pi^{\sigma_{s_1 \dots s_m}}$ denote the projectors on the isotypical subspaces corresponding to an irrep ρ of $\mathbb{S}_{[N] \setminus \{i_1, \dots, i_\ell\}}$ and an irrep σ of $\mathbb{S}_{\Sigma \setminus \{s_1, \dots, s_m\}}$, respectively. Note that $\Pi_{\rho_{i_1 \dots i_\ell}}$ and $\Pi^{\sigma_{s_1 \dots s_m}}$ commute, and let

$$\Pi_{\rho_{i_1 \dots i_\ell}}^{\sigma_{s_1 \dots s_m}} = \Pi_{\rho_{i_1 \dots i_\ell}} \Pi^{\sigma_{s_1 \dots s_m}} = \Pi^{\sigma_{s_1 \dots s_m}} \Pi_{\rho_{i_1 \dots i_\ell}},$$

which is the projector on the isotypical subspace corresponding to the irrep $\rho \times \sigma$ of $\mathbb{S}_{[N] \setminus \{i_1, \dots, i_\ell\}} \times \mathbb{S}_{\Sigma \setminus \{s_1, \dots, s_m\}}$ (note: this subspace may contain multiple instances of the irrep). In general, when multiple such projectors mutually commute, we denote their product with a single Π whose subscript and superscript is, respectively, a concatenation of the subscripts and superscripts of these projectors. For example, $\Pi_{id, v_{12}}^\lambda = \Pi_{id}^\lambda \Pi_{v_{12}}^\lambda$ (note: Π^λ corresponds to an irrep λ of $\mathbb{S}_{\Sigma \setminus \emptyset} = \mathbb{S}_\Sigma$).

Suppose that Π_{sub}^λ and $\Pi_{sub'}^\lambda$ are two projectors each projecting onto a single instance of an irrep $\rho_{i_1 \dots i_\ell} \times \lambda$ of $\mathbb{S}_{[N] \setminus \{i_1, \dots, i_\ell\}} \times \mathbb{S}_\Sigma$, where sub and sub' are subscripts determining these instances. Then let $\Pi_{sub' \leftarrow sub}^\lambda$ denote the transporter from the instance corresponding to Π_{sub}^λ to one corresponding to $\Pi_{sub'}^\lambda$. Let $\Pi_{sub' \leftrightarrow sub}^\lambda = \Pi_{sub' \leftarrow sub}^\lambda + \Pi_{sub \leftarrow sub'}^\lambda$ for short.

4.3 Decomposition of $\Gamma_{1,2}$ into projectors and transporters

Due to (4.2), we can express $\Gamma_{1,2}$ as a linear combination of projectors onto irreps and transporters between isomorphic irreps of $\mathbb{S}_{[3,M]} \times \mathbb{S}_\Sigma$. Due to (4.2) we also have $\Gamma_{1,2} \Pi_{id} = \Gamma_{1,2}$ and $\Gamma_{1,2} \Pi_{sgn} = 0$. Claim 3.1 states that $\mathbb{I} = \sum_{\lambda \vdash N} \Pi_\lambda^\lambda$, and we have $\Pi_\lambda^\lambda = \sum_{v \ll \lambda} \Pi_{v_{12}}^\lambda$. If the two boxes removed from λ to obtain v are in the same row or the same column, then $\Pi_{v_{12}}^\lambda$ projects onto the unique instance of the irrep $v \times \lambda$ in V , and $\Pi_{v_{12}}^\lambda = \Pi_{id, v_{12}}^\lambda$ or $\Pi_{v_{12}}^\lambda = \Pi_{sgn, v_{12}}^\lambda$, respectively. On the other hand, if they are in different rows and columns, then $\Pi_{v_{12}}^\lambda = \Pi_{id, v_{12}}^\lambda + \Pi_{sgn, v_{12}}^\lambda$, where each $\Pi_{id, v_{12}}^\lambda$ and $\Pi_{sgn, v_{12}}^\lambda$ projects onto an instance of the irrep $v \times \lambda$. Hence, similarly to (3.2), we can express $\Gamma_{1,2}$ as a linear combination

$$\Gamma_{1,2} = \sum_{\lambda \vdash N} \left(\sum_{v \ll_c \lambda} \alpha_{id, v}^\lambda \Pi_{id, v_{12}}^\lambda + \sum_{v \ll_{rc} \lambda} \alpha_{sgn, v}^\lambda \Pi_{sgn, v_{12} \leftarrow id, v_{12}}^\lambda \right). \quad (4.3)$$

If $v \ll_{rc} \lambda$, then there exist two distinct $\mu, \mu' \vdash N-1$ such that $v < \mu < \lambda$ and $v < \mu' < \lambda$, and let μ appear in the lexicographic order after μ' . Note that $\Pi_{v_{12}, \mu_1}^\lambda$ projects onto a single instance of $v \times \lambda$. We have

$$\Pi_{sgn, v_{12} \leftarrow id, v_{12}}^\lambda \propto \Pi_{sgn, v_{12}}^\lambda \Pi_{v_{12}, \mu_1}^\lambda \Pi_{id, v_{12}}^\lambda,$$

and we specify the global phase of the transporter $\Pi_{sgn, v_{12} \leftarrow id, v_{12}}^\lambda$ by assuming that the coefficient of this proportionality is positive. We present the value of this coefficient in Section 5.3.

Let us relate (3.2) and (4.3), the two ways in which we can specify the adversary matrix. One can see that the $2(N-2)! \times N!$ submatrix of $\Xi_{id, v_{12}}^\lambda$ and $\Xi_{sgn, v_{12}}^\lambda$ corresponding to $\mathcal{D}_{1,2}^{s,t}$ is proportional,

respectively, to the $2(N-2)! \times N!$ submatrix of $\Pi_{id, v_{12}}^\lambda$ and $\Pi_{sgn, v_{12} \leftarrow id, v_{12}}^\lambda$ corresponding to $\mathcal{D}_{1,2}^{s,t}$. Hence, just like in (4.1), we have

$$\Xi_{id, v}^\lambda = \frac{1}{\gamma_{id, v}^\lambda} \sum_{\pi \in R} U_\pi \Pi_{id, v_{12}}^\lambda V_{\pi^{-1}} \quad \text{and} \quad \Xi_{sgn, v}^\lambda = \frac{1}{\gamma_{sgn, v}^\lambda} \sum_{\pi \in R} U_\pi \Pi_{sgn, v_{12} \leftarrow id, v_{12}}^\lambda V_{\pi^{-1}},$$

and we specify the global phase of the transporters Ξ by assuming that the normalization scalars γ are positive. Note that

$$\begin{aligned} (\gamma_{id, v}^\lambda)^2 \Pi_\lambda^\lambda &= (\gamma_{id, v}^\lambda \Xi_{id, v}^\lambda)^* (\gamma_{id, v}^\lambda \Xi_{id, v}^\lambda) = \left(\sum_{\pi \in R} U_\pi \Pi_{id, v_{12}}^\lambda V_{\pi^{-1}} \right)^* \sum_{\pi \in R} U_\pi \Pi_{id, v_{12}}^\lambda V_{\pi^{-1}} \\ &= \binom{N}{2} \frac{1}{N!} \sum_{\pi \in \mathbb{S}_{[N]}} V_\pi \Pi_{id, v_{12}}^\lambda V_{\pi^{-1}} = \binom{N}{2} \frac{\dim v}{\dim \lambda} \Pi_\lambda^\lambda, \end{aligned}$$

where the last equality holds because V_π and Π^λ commute (thus the sum has to be proportional to Π_λ^λ) and $\text{Tr}[\Pi_{id, v_{12}}^\lambda] / \text{Tr}[\Pi_\lambda^\lambda] = \dim v / \dim \lambda$. The same way we calculate $\gamma_{sgn, v}^\lambda$, and we have

$$\gamma_{id, v}^\lambda = \frac{\beta_{id, v}^\lambda}{\alpha_{id, v}^\lambda} = \gamma_{sgn, v}^\lambda = \frac{\beta_{sgn, v}^\lambda}{\alpha_{sgn, v}^\lambda} = \sqrt{\binom{N}{2} \frac{\dim v}{\dim \lambda}}.$$

5 Tools for estimating $\|\Delta_1 \circ \Gamma\|$

5.1 Division of $\Delta_1 \circ \Gamma$ into two parts

For all $j \in [2, N]$, $\Delta_1 \circ \Gamma_{1,j}$ is essentially the same as $\Delta_1 \circ \Gamma_{1,2}$. And, for all $\{i, j\} \subset [2, N]$, $\Delta_1 \circ \Gamma_{i,j}$ is essentially the same as $\Delta_1 \circ \Gamma_{2,3}$, which, in turn, is essentially the same as $\Delta_3 \circ \Gamma_{1,2}$. Let us distinguish these two cases by dividing Γ into two parts: let Γ' be the $(N-1)N! \times N!$ submatrix of Γ corresponding to $x \in \mathcal{D}_{1,j}$, where $j \in [2, N]$, and let Γ'' be the $\binom{N-1}{2}N! \times N!$ submatrix of Γ corresponding to $x \in \mathcal{D}_{i,j}$, where $\{i, j\} \in [2, N]$.

Claim 5.1. *We have $\|\Delta_1 \circ \Gamma\| \in O(1)$ if and only if both $\|\Delta_1 \circ \Gamma'\| \in O(1)$ and $\|\Delta_1 \circ \Gamma''\| \in O(1)$.*

Let $R' = \text{Rep}(\mathbb{S}_{[2,N]} / \mathbb{S}_{[3,N]})$ and $R'' = \text{Rep}(\mathbb{S}_{[N] \setminus \{3\}} / (\mathbb{S}_{\{1,2\}} \times \mathbb{S}_{[4,N]}))$ be transversals of the left cosets of $\mathbb{S}_{[3,N]}$ in $\mathbb{S}_{[2,N]}$ and of $\mathbb{S}_{\{1,2\}} \times \mathbb{S}_{[4,N]}$ in $\mathbb{S}_{[N] \setminus \{3\}}$, respectively. Similarly to (4.1), we have

$$\Delta_1 \circ \Gamma' = \sum_{\pi \in R'} U_\pi (\Delta_1 \circ \Gamma_{1,2}) V_{\pi^{-1}} \quad \text{and} \quad \Delta_1 \circ \Gamma'' = U_{(13)} \left(\sum_{\pi \in R''} U_\pi (\Delta_3 \circ \Gamma_{1,2}) V_{\pi^{-1}} \right) V_{(13)}, \quad (5.1)$$

which imply

$$\|\Delta_1 \circ \Gamma'\|^2 = \|(\Delta_1 \circ \Gamma')^* (\Delta_1 \circ \Gamma')\| = \left\| \sum_{\pi \in R'} V_\pi (\Delta_1 \circ \Gamma_{1,2})^* (\Delta_1 \circ \Gamma_{1,2}) V_{\pi^{-1}} \right\|, \quad (5.2)$$

$$\|\Delta_1 \circ \Gamma''\|^2 = \|(\Delta_1 \circ \Gamma'')^* (\Delta_1 \circ \Gamma'')\| = \left\| \sum_{\pi \in R''} V_\pi (\Delta_3 \circ \Gamma_{1,2})^* (\Delta_3 \circ \Gamma_{1,2}) V_{\pi^{-1}} \right\|. \quad (5.3)$$

Therefore, we have to consider $\Delta_1 \circ \Gamma_{1,2}$ and $\Delta_3 \circ \Gamma_{1,2}$.

5.2 Commutativity with the action of Δ_i

Instead of Δ_i , let us first consider the action of $\bar{\Delta}_i$. For $i \in [N]$ and $s \in \Sigma$, let $\hat{\Pi}_i^s$ be the projector on all $y \in \mathcal{D}_0$ such that $y_i = s$. Then, due to the particular way we define the bijection f , we have

$$\bar{\Delta}_i \circ \Gamma_{1,2} = \sum_{s \in \Sigma} \hat{\Pi}_i^s \Gamma_{1,2} \hat{\Pi}_i^s \quad \text{whenever } i \neq 2 \quad \text{and} \quad \bar{\Delta}_2 \circ \Gamma_{1,2} = \sum_{s \in \Sigma} \hat{\Pi}_1^s \Gamma_{1,2} \hat{\Pi}_2^s. \quad (5.4)$$

Note that $\hat{\Pi}_i^s$ commutes with every $\Pi_{\rho_{j_1 \dots j_m}}$ whenever $i \in \{j_1, \dots, j_m\}$. Hence, for $i \in \{j_1, \dots, j_m\} \setminus \{2\}$ and every $N! \times N!$ matrix A , we have

$$\Delta_i \circ (\Pi_{\rho_{j_1 \dots j_m}} A) = \Pi_{\rho_{j_1 \dots j_m}} (\Delta_i \circ A) \quad \text{and} \quad \Delta_i \circ (A \Pi_{\rho_{j_1 \dots j_m}}) = (\Delta_i \circ A) \Pi_{\rho_{j_1 \dots j_m}}. \quad (5.5)$$

5.3 Relations among irreps of $\mathbb{S}_{[3,M]} \times \mathbb{S}_\Sigma$ within an isotypical subspace

We are interested to see how Δ_1 acts on $\Gamma_{1,2}$, which requires us to consider how it acts on $\Pi_{id, v_{12}}^\lambda$ and $\Pi_{sgn, v_{12} \leftarrow id, v_{12}}^\lambda$. Unfortunately, this action is hard to calculate directly, therefore we express $\Pi_{id, v_{12}}^\lambda$ and $\Pi_{sgn, v_{12} \leftarrow id, v_{12}}^\lambda$ as linear combinations of certain operators on which the action of Δ_1 is easier to calculate.

Consider $\lambda \vdash N$ and $\mathbf{v} \ll_{rc} \lambda$. The projector $\Pi_{v_{12}}^\lambda$ projects onto the isotypical subspace of \mathcal{Y} corresponding to the irrep $\mathbf{v} \times \lambda$ of $\mathbb{S}_{[3,M]} \times \mathbb{S}_\Sigma$, and this subspace contains two instances of this irrep. There are as many degrees of freedom in splitting this subspace in half so that each half corresponds to a single instance of the irrep as in splitting \mathbb{R}^2 in orthogonal one-dimensional subspaces. We already considered one such split, $\Pi_{v_{12}}^\lambda = \Pi_{id, v_{12}}^\lambda + \Pi_{sgn, v_{12}}^\lambda$, and now let us relate it to another.

Let $\mu, \mu' \vdash N-1$ be such that $\mathbf{v} < \mu < \lambda$, $\mathbf{v} < \mu' < \lambda$, and μ appears after μ' in the lexicographical order. Then $\Pi_{v_{12}, \mu_1}^\lambda$ and $\Pi_{v_{12}, \mu'_1}^\lambda$ project onto two orthogonal instances of the irrep $\mathbf{v} \times \lambda$, and $\Pi_{v_{12}}^\lambda = \Pi_{v_{12}, \mu_1}^\lambda + \Pi_{v_{12}, \mu'_1}^\lambda$. Note that $V_{(12)}$ commutes with $\Pi_{v_{12}}^\lambda$ and that $\Pi^\lambda = \Pi_\lambda$. The *orthogonal form* [17, Section 3.4] of the irrep λ tells us that $V_{(12)}$ restricted to the isotypical subspace corresponding to $\mathbf{v} \times \lambda$ is

$$V_{(12)}|_{v_{12} \times \lambda} = \frac{1}{d_{\lambda, \mathbf{v}}} \left(\Pi_{v_{12}, \mu'_1}^\lambda - \Pi_{v_{12}, \mu_1}^\lambda + \sqrt{d_{\lambda, \mathbf{v}}^2 - 1} \Pi_{v_{12}, \mu'_1 \leftrightarrow v_{12}, \mu_1}^\lambda \right). \quad (5.6)$$

Expression (5.6), in effect, defines the global phase of transporters $\Pi_{v_{12}, \mu'_1 \leftarrow v_{12}, \mu_1}^\lambda$ and $\Pi_{v_{12}, \mu'_1 \leftarrow v_{12}, \mu_1}^\lambda$.

Recall that $\Pi_{id} = (\mathbb{I} + V_{(12)})/2$, and therefore

$$\Pi_{id, v_{12}}^\lambda = \frac{\Pi_{v_{12}}^\lambda + V_{(12)}|_{v_{12} \times \lambda}}{2} = \frac{d_{\lambda, \mathbf{v}} - 1}{2d_{\lambda, \mathbf{v}}} \Pi_{v_{12}, \mu_1}^\lambda + \frac{d_{\lambda, \mathbf{v}} + 1}{2d_{\lambda, \mathbf{v}}} \Pi_{v_{12}, \mu'_1}^\lambda + \frac{\sqrt{d_{\lambda, \mathbf{v}}^2 - 1}}{2d_{\lambda, \mathbf{v}}} \Pi_{v_{12}, \mu'_1 \leftrightarrow v_{12}, \mu_1}^\lambda \quad (5.7)$$

and

$$\begin{aligned} \Pi_{sgn, v_{12} \leftarrow id, v_{12}}^\lambda &= \frac{2d_{\lambda, \mathbf{v}}}{\sqrt{d_{\lambda, \mathbf{v}}^2 - 1}} \Pi_{sgn, v_{12}}^\lambda \Pi_{v_{12}, \mu_1}^\lambda \Pi_{id, v_{12}}^\lambda \\ &= \frac{\sqrt{d_{\lambda, \mathbf{v}}^2 - 1}}{2d_{\lambda, \mathbf{v}}} \Pi_{v_{12}, \mu_1}^\lambda - \frac{\sqrt{d_{\lambda, \mathbf{v}}^2 - 1}}{2d_{\lambda, \mathbf{v}}} \Pi_{v_{12}, \mu'_1}^\lambda + \frac{d_{\lambda, \mathbf{v}} + 1}{2d_{\lambda, \mathbf{v}}} \Pi_{v_{12}, \mu_1 \leftarrow v_{12}, \mu'_1}^\lambda - \frac{d_{\lambda, \mathbf{v}} - 1}{2d_{\lambda, \mathbf{v}}} \Pi_{v_{12}, \mu'_1 \leftarrow v_{12}, \mu_1}^\lambda. \end{aligned} \quad (5.8)$$

5.4 Relations among irreps of $\mathbb{S}_{[4,N]} \times \mathbb{S}_\Sigma$ within an isotypical subspace

We are also interested to see how Δ_3 acts on $\Gamma_{1,2}$, which will require us to consider irreps of $\mathbb{S}_{[4,N]} \times \mathbb{S}_\Sigma$. Let us now consider $k \in o(N)$, $\eta \vdash k$, and $\theta < \eta$. Recall that, according to our notation, $\bar{\eta} = (N - k, \eta) \vdash N$ and $\bar{\theta}_{123} = (N - k - 2, \theta)_{123} \vdash N - 3$ is obtained from $\bar{\eta}$ by removing two boxes in the first row and one box below the first row.

V contains three instances of the irrep $\bar{\theta}_{123} \times \bar{\eta}$ of $\mathbb{S}_{[4,N]} \times \mathbb{S}_\Sigma$: we have

$$\Pi_{\bar{\theta}_{123}}^{\bar{\eta}} = \Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, (\bar{\eta}_1)}^{\bar{\eta}} + \Pi_{\bar{\theta}_{123}, \bar{\theta}_{12}, \bar{\eta}_1}^{\bar{\eta}} + \Pi_{\bar{\theta}_{123}, (\bar{\theta}_{12}, \bar{\theta}_1)}^{\bar{\eta}} = \Pi_{id, \bar{\theta}_{123}, \bar{\eta}_3}^{\bar{\eta}} + \Pi_{sgn, \bar{\theta}_{123}, \bar{\eta}_3}^{\bar{\eta}} + \Pi_{(id), \bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}},$$

where each projector (other than $\Pi_{\bar{\theta}_{123}}^{\bar{\eta}}$) projects on a single instance of the irrep and the subscripts in parenthesis are optional. These two decompositions follow essentially the chain of restrictions $\mathbb{S}_{[N]} \rightarrow \mathbb{S}_{[2,N]} \rightarrow \mathbb{S}_{[3,N]} \rightarrow \mathbb{S}_{[4,N]}$ and $\mathbb{S}_{[N]} \rightarrow \mathbb{S}_{[N] \setminus \{3\}} \rightarrow \mathbb{S}_{\{1,2\}} \times \mathbb{S}_{[4,N]} \rightarrow \mathbb{S}_{[4,N]}$, respectively.

From the orthogonal form of the irrep $\bar{\eta}$, we get that the restriction of $V_{(12)}$ and $V_{(23)}$ to the isotypical subspace corresponding to $\bar{\theta}_{123} \times \bar{\eta}$ is, respectively,

$$V_{(12)}|_{\bar{\theta}_{123} \times \bar{\eta}} = \Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}^{\bar{\eta}} + \frac{1}{d_{\bar{\eta}, \bar{\theta}_{12}}} \left(\Pi_{\bar{\theta}_{123}, \bar{\theta}_{12}, \bar{\eta}_1}^{\bar{\eta}} - \Pi_{\bar{\theta}_{123}, \bar{\theta}_1}^{\bar{\eta}} + \sqrt{d_{\bar{\eta}, \bar{\theta}_{12}}^2 - 1} \Pi_{\bar{\theta}_{123}, \bar{\theta}_{12}, \bar{\eta}_1 \leftrightarrow \bar{\theta}_{123}, \bar{\theta}_1}^{\bar{\eta}} \right),$$

$$V_{(23)}|_{\bar{\theta}_{123} \times \bar{\eta}} = \frac{1}{d_{\bar{\eta}, \bar{\theta}_{12}} - 1} \left(\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}^{\bar{\eta}} - \Pi_{\bar{\theta}_{123}, \bar{\theta}_{12}, \bar{\eta}_1}^{\bar{\eta}} + \sqrt{(d_{\bar{\eta}, \bar{\theta}_{12}} - 1)^2 - 1} \Pi_{\bar{\theta}_{123}, \bar{\eta}_{12} \leftrightarrow \bar{\theta}_{123}, \bar{\theta}_{12}, \bar{\eta}_1}^{\bar{\eta}} \right) + \Pi_{\bar{\theta}_{123}, \bar{\theta}_1}^{\bar{\eta}},$$

where the global phases of the transporters in the expression for $V_{(12)}|_{\bar{\theta}_{123} \times \bar{\eta}}$ are consistent with (5.6).

Therefore we can calculate the ‘‘overlap’’ of $\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}^{\bar{\eta}}$ and

$$\Pi_{id, \bar{\theta}_{123}, \bar{\eta}_3}^{\bar{\eta}} = V_{(13)} (\mathbb{I} + V_{(23)}) \Pi_{\bar{\theta}_{123}, \bar{\eta}_1}^{\bar{\eta}} V_{(13)} / 2 = V_{(23)} V_{(12)} (\mathbb{I} + V_{(23)}) (\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}^{\bar{\eta}} + \Pi_{\bar{\theta}_{123}, \bar{\theta}_{12}, \bar{\eta}_1}^{\bar{\eta}}) V_{(12)} V_{(23)} / 2$$

to be

$$\frac{\text{Tr}[\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}^{\bar{\eta}} \Pi_{id, \bar{\theta}_{123}, \bar{\eta}_3}^{\bar{\eta}}]}{\dim \bar{\theta}_{123} \dim \bar{\eta}} = \frac{2}{d_{\bar{\eta}, \bar{\theta}_{12}} (d_{\bar{\eta}, \bar{\theta}_{12}} - 1)}. \quad (5.9)$$

Since $\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}^{\bar{\eta}} = \Pi_{id} \Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}^{\bar{\eta}}$, we have

$$\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}^{\bar{\eta}} = \Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} + \frac{2}{d_{\bar{\eta}, \bar{\theta}_{12}}^2 - d_{\bar{\eta}, \bar{\theta}_{12}}} \left(\Pi_{id, \bar{\theta}_{123}, \bar{\eta}_3}^{\bar{\eta}} - \Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} \right) + \frac{\sqrt{2(d_{\bar{\eta}, \bar{\theta}_{12}}^2 - d_{\bar{\eta}, \bar{\theta}_{12}} - 2)}}{d_{\bar{\eta}, \bar{\theta}_{12}}^2 - d_{\bar{\eta}, \bar{\theta}_{12}}} \Pi_{\bar{\theta}_{123}, \bar{\theta}_3 \leftrightarrow id, \bar{\theta}_{123}, \bar{\eta}_3}^{\bar{\eta}}. \quad (5.10)$$

5.5 Summing the permutations of $(\Delta_1 \circ \Gamma_{1,2})^* (\Delta_1 \circ \Gamma_{1,2})$

We will express $(\Delta_1 \circ \Gamma_{1,2})^* (\Delta_1 \circ \Gamma_{1,2})$ as a linear combination of projectors $\Pi_{\nu_{12}, \mu_1}^\lambda$ and transporters $\Pi_{\nu_{12}, \mu'_1 \leftarrow \nu_{12}, \mu_1}^\lambda$, where $\lambda \vdash N$, $\nu \ll_c \lambda$, and $\mu, \mu' \vdash N - 1$ are such that $\nu < \mu < \lambda$ and $\nu < \mu' < \lambda$ (we

consider transporters only if $v \ll_{rc} \lambda$, and thus $\mu \neq \mu'$). In order to calculate $\|\Delta_1 \circ \Gamma'\|$ via (5.2), we use

$$\begin{aligned} \frac{1}{N-1} \sum_{\pi \in R'} V_\pi \Pi_{v_{12}, \mu_1}^\lambda V_{\pi^{-1}} &= \frac{1}{(N-1)!} \sum_{\pi \in \mathbb{S}_{[2, N]}} V_\pi \Pi_{v_{12}, \mu_1}^\lambda V_{\pi^{-1}} = \frac{\text{Tr}[V_\pi \Pi_{v_{12}, \mu_1}^\lambda V_{\pi^{-1}}]}{\text{Tr}[\Pi_{\mu_1}^\lambda]} \Pi_{\mu_1}^\lambda = \frac{\dim v}{\dim \mu} \Pi_{\mu_1}^\lambda, \\ \frac{1}{N-1} \sum_{\pi \in R'} V_\pi \Pi_{v_{12}, \mu'_1 \leftarrow v_{12}, \mu_1}^\lambda V_{\pi^{-1}} &= \frac{1}{(N-1)!} \sum_{\pi \in \mathbb{S}_{[2, N]}} V_\pi \Pi_{v_{12}, \mu'_1 \leftarrow v_{12}, \mu_1}^\lambda V_{\pi^{-1}} = 0. \end{aligned} \quad (5.11)$$

The equalities in (5.11) hold because, first of all, $\Pi_{v_{12}, \mu_1}^\lambda$ and $\Pi_{v_{12}, \mu'_1 \leftarrow v_{12}, \mu_1}^\lambda$ are fixed under $\mathbb{S}_{[3, N]} \times \mathbb{S}_\Sigma$. Second, V as a representation of $\mathbb{S}_{[2, N]} \times \mathbb{S}_\Sigma$ is *multiplicity-free* (i.e., it contains each irrep at most once), and thus every operator on \mathcal{Y} that is fixed under $\mathbb{S}_{[2, N]} \times \mathbb{S}_\Sigma$ can be expressed as a linear combination of projectors $\Pi_{\mu''}^{\lambda'}$, where $\lambda' \vdash N$ and $\mu'' < \lambda'$. And third, for $\pi \in \mathbb{S}_{[2, N]}$, V_π commutes with both $\Pi_{\mu_1}^\lambda$ and $\Pi_{\mu'_1}^\lambda$.

6 Construction of the optimal adversary matrix

In Section 4.3 we showed that $\beta_{id, v}^\lambda / \alpha_{id, v}^\lambda = \beta_{sgn, v}^\lambda / \alpha_{sgn, v}^\lambda = \sqrt{\binom{N}{2} \frac{\dim v}{\dim \lambda}}$. We calculate $\dim v$ and $\dim \lambda$ using the hook-length formula, and one can see that, given a fixed $\zeta \vdash k$, $\dim \bar{\zeta}$ can be expressed as a polynomial in N of degree k and having the leading coefficient $1/h(\zeta)$ (see (6.2)). Therefore we get that Claim 3.2 is equivalent to the following claim, which we prove in Appendix A.

Claim 6.1. *Suppose $\Gamma_{1,2}$ is given as in (4.3), $\alpha_{id, (N-2)}^{(N)} = N^{-1/3}$, and Γ is obtained from $\Gamma_{1,2}$ via (4.1). Consider $\lambda \vdash N$ that has $O(1)$ boxes below the first row and $v \ll_c \lambda$. In order for $\|\Delta_1 \circ \Gamma\| \in O(1)$ to hold, we need to have*

1. $\alpha_{id, v}^\lambda = N^{-1/3} + O(1/N)$ if λ and v are the same below the first row,
2. $\alpha_{id, v}^\lambda, \alpha_{sgn, v}^\lambda = N^{-1/3} + O(1/\sqrt{N})$ if λ has one box more below the first row than v ,
3. $\alpha_{id, v}^\lambda, \alpha_{sgn, v}^\lambda = O(1)$ if λ has two boxes more below the first row than v .

(Note that $\alpha_{id, (N-2)}^{(N)} = N^{-1/3}$ implies $\|\Gamma\| \geq \beta_{id, (N-2)}^{(N)} \in \Theta(N^{2/3})$.)

Consider $k \in o(N)$ and $\eta \vdash k$. Claims 3.2 and 6.1 hint that for the optimal adversary matrix we could choose coefficients $\alpha_{id, \bar{\eta}_{12}}^\eta \approx \alpha_{id, \bar{\eta}_{12}}^{\bar{\zeta}} \approx \alpha_{sgn, \bar{\eta}_{12}}^{\bar{\zeta}}$ whenever $\zeta > \eta$ and $\alpha_{id, \bar{\eta}_{12}}^{\bar{\zeta}} = \alpha_{sgn, \bar{\eta}_{12}}^{\bar{\zeta}} = 0$ whenever $\zeta \gg \eta$. Let us do that. For $\zeta > \eta$, note that $\bar{\eta}_{12} < \bar{\eta}_1 < \bar{\zeta}$, $\bar{\eta}_{12} < \bar{\zeta}_1 < \bar{\zeta}$, and $\bar{\eta}_1$ appears after $\bar{\zeta}_1$ is the lexicographic order, and also note that $d_{\bar{\zeta}, \bar{\eta}_{12}} \geq N - 2k - 1$ (the equality is achieved by $\eta = (k)$ and $\zeta = (k+1)$). Therefore, according to (5.7) and (5.8), we have

$$\begin{aligned} \Pi_{id, \bar{\eta}_{12}}^\eta + \sum_{\zeta > \eta} (\Pi_{id, \bar{\eta}_{12}}^{\bar{\zeta}} + \Pi_{sgn, \bar{\eta}_{12} \leftarrow id, \bar{\eta}_{12}}^{\bar{\zeta}}) &= \Pi_{\bar{\eta}_{12}}^\eta + \sum_{\zeta > \eta} (\Pi_{\bar{\eta}_{12}, \bar{\eta}_1}^{\bar{\zeta}} + \Pi_{\bar{\eta}_{12}, \bar{\eta}_1 \leftarrow \bar{\eta}_{12}, \bar{\zeta}_1}^{\bar{\zeta}}) + O(1/N) \\ &= \Pi_{\bar{\eta}_{12}}^\eta + \sum_{\zeta > \eta} 2\Pi_{\bar{\eta}_{12}, \bar{\eta}_1}^{\bar{\zeta}} \Pi_{id} + O(1/N) = 2\Pi_{\bar{\eta}_{12}, \bar{\eta}_1} \Pi_{id} - \Pi_{\bar{\eta}_{12}}^\eta + O(1/N), \end{aligned}$$

where the last equality is due to $\Pi_{\bar{\eta}_{12}}^{\bar{\eta}} = \Pi_{\bar{\eta}_{12}, \bar{\eta}_1}^{\bar{\eta}} = \Pi_{id, \bar{\eta}_{12}}^{\bar{\eta}}$ and $\text{Ind}_{\mathbb{S}_{[2, N]}}^{\mathbb{S}_{[M]}} \bar{\eta}_1 \cong \bar{\eta} \oplus \bigoplus_{\zeta > \eta} \bar{\zeta}$, that is, the branching rule. Thus we choose to construct $\Gamma_{1,2}$ as a linear combination of matrices

$$2\Pi_{\bar{\eta}_{12}, \bar{\eta}_1} \Pi_{id} - \Pi_{\bar{\eta}_{12}}^{\bar{\eta}} = \Pi_{\bar{\eta}_{12}}^{\bar{\eta}} + \sum_{\zeta > \eta} \left(\frac{d_{\bar{\zeta}, \bar{\eta}_{12}} - 1}{d_{\bar{\zeta}, \bar{\eta}_{12}}} \Pi_{id, \bar{\eta}_{12}}^{\bar{\zeta}} + \frac{\sqrt{d_{\bar{\zeta}, \bar{\eta}_{12}}^2 - 1}}{d_{\bar{\zeta}, \bar{\eta}_{12}}} \Pi_{sgn, \bar{\eta}_{12} \leftarrow id, \bar{\eta}_{12}}^{\bar{\zeta}} \right).$$

(At first glance, it may seem that the matrix on the left hand side does not “treat” indices 1 and 2 equally, but that is an illusion due to the way we define the bijection f .)

Theorem 6.2. *Let Γ be constructed via (4.1) from*

$$\Gamma_{1,2} = \sum_{k=0}^{N^{2/3}} \frac{N^{2/3} - k}{N} \sum_{\eta \vdash k} (2\Pi_{\bar{\eta}_{12}, \bar{\eta}_1} \Pi_{id} - \Pi_{\bar{\eta}_{12}}^{\bar{\eta}}).$$

Then $\|\Gamma\| \in \Omega(N^{2/3})$ and $\|\Delta_1 \circ \Gamma\| \in O(1)$, and therefore Γ is an optimal adversary matrix for ELEMENT DISTINCTNESS.

For $\Gamma_{1,2}$ of Theorem 6.2 expressed in the form (4.3), we have $\alpha_{id, (N-2)}^{(N)} = N^{-1/3}$, and therefore $\|\Gamma\| \in \Omega(N^{2/3})$. In the remainder of the paper, let us prove $\|\Delta_1 \circ \Gamma'\| \in O(1)$ and $\|\Delta_1 \circ \Gamma''\| \in O(1)$, which is sufficient due to Claim 5.1.

6.1 Approximate action of Δ_i

The precise calculation of $\Delta_1 \circ \Gamma$ is tedious; we consider it in Appendix A. Here, however, it suffices to upper bound $\|\Delta_1 \circ \Gamma\|$ using the following trick first introduced in [8] and later used in [12, 10, 27, 11].

For any matrix A of the same dimensions as Δ_i , we call a matrix B satisfying $\Delta_i \circ B = \Delta_i \circ A$ an *approximation* of $\Delta_i \circ A$ and we denote it with $\Delta_i \diamond A$. From the fact (3.3) on the γ_2 norm, it follows that $\|\Delta_i \circ A\| \leq 2 \|\Delta_i \diamond A\|$. Hence, to show that $\|\Delta_1 \circ \Gamma'\| \in O(1)$ and $\|\Delta_1 \circ \Gamma''\| \in O(1)$, it suffices to show that $\|\Delta_1 \diamond \Gamma'\| \in O(1)$ and $\|\Delta_1 \diamond \Gamma''\| \in O(1)$ for any $\Delta_1 \diamond \Gamma'$ and $\Delta_1 \diamond \Gamma''$. That is, it suffices to show that we can change entries of Γ' and Γ'' corresponding to (x, y) with $x_1 = y_1$ in a way that the spectral norms of the resulting matrices are constantly bounded.

Note that we can always choose $\Delta_i \diamond A = A$ and $\Delta_i \diamond (A + A') = \Delta_i \diamond A + \Delta_i \diamond A'$. We will express $\Gamma_{1,2}$ as a linear combination of certain $N! \times N!$ matrices and, for every such matrix A , we will choose $\Delta_i \diamond A = A$, except for the following three, for which we calculate the action of Δ_1 or Δ_3 precisely. We have

$$\Delta_1 \circ \Pi_{id} = V_{(12)}/2, \quad \Delta_3 \circ \Pi_{\bar{\theta}_{123}, \bar{\theta}_3} = 0, \quad \text{and} \quad \Delta_3 \circ \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}} = 0$$

due to $\Delta_1 \circ \mathbb{I} = \Delta_3 \circ \mathbb{I} = 0$ and the commutativity relation (5.5).

Due to (5.5), we also have $\Delta_3 \circ (A\Pi_{id}) = (\Delta_3 \circ A)\Pi_{id}$ for every $N! \times N!$ matrix A . One can see that, given any choice of $\Delta_3 \diamond A$, we can choose $\Delta_3 \diamond (A\Pi_{id}) = (\Delta_3 \diamond A)\Pi_{id}$.

6.2 Bounding $\|\Delta_1 \circ \Gamma'\|$

For $k \leq N^{2/3}$ and $\eta \vdash k$, define $N! \times N!$ matrices $(\Gamma_\eta)_{1,2}$ and $(\Gamma_k)_{1,2}$ such that

$$\Gamma_{1,2} = \sum_{k=0}^{N^{2/3}} \frac{N^{2/3} - k}{N} (\Gamma_k)_{1,2}, \quad (\Gamma_k)_{1,2} = \sum_{\eta \vdash k} (\Gamma_\eta)_{1,2}, \quad \text{and} \quad (\Gamma_\eta)_{1,2} = 2\Pi_{\bar{\eta}_{12}, \bar{\eta}_1} \Pi_{id} - \Pi_{\bar{\eta}_{12}}^{\bar{\eta}}.$$

The projector $\Pi_{\bar{\eta}_{12}, \bar{\eta}_1}$ commutes with the action of Δ_1 , therefore we can choose

$$\begin{aligned} \Delta_1 \diamond (\Gamma_\eta)_{1,2} &= 2\Pi_{\bar{\eta}_{12}, \bar{\eta}_1} (\Delta_1 \circ \Pi_{id}) - \Pi_{\bar{\eta}_{12}}^{\bar{\eta}} = \Pi_{\bar{\eta}_{12}, \bar{\eta}_1} V_{(12)} - \Pi_{\bar{\eta}_{12}}^{\bar{\eta}} \\ &= \sum_{\zeta > \eta} \Pi_{\bar{\eta}_{12}, \bar{\eta}_1}^{\bar{\zeta}} V_{(12)} = \sum_{\zeta > \eta} \left(-\frac{1}{d_{\bar{\zeta}, \bar{\eta}_{12}}^{\bar{\zeta}}} \Pi_{\bar{\eta}_{12}, \bar{\eta}_1}^{\bar{\zeta}} + \frac{\sqrt{d_{\bar{\zeta}, \bar{\eta}_{12}}^2 - 1}}{d_{\bar{\zeta}, \bar{\eta}_{12}}^{\bar{\zeta}}} \Pi_{\bar{\eta}_{12}, \bar{\eta}_1 \leftrightarrow \bar{\eta}_{12}, \bar{\zeta}_1}^{\bar{\zeta}} \right), \end{aligned}$$

where the third equality is due to the branching rule and both $\Pi_{\bar{\eta}_{12}}^{\bar{\eta}} = \Pi_{\bar{\eta}_{12}}^{\bar{\eta}} \Pi_{id}$ and $\Pi_{id} V_{(12)} = \Pi_{id}$, and the last equality comes from (5.6). To estimate the norm of $\Delta_1 \diamond \Gamma'$ via (5.2), we have

$$\begin{aligned} &\sum_{\pi \in R'} V_\pi (\Delta_1 \diamond (\Gamma_\eta)_{1,2})^* (\Delta_1 \diamond (\Gamma_\eta)_{1,2}) V_{\pi^{-1}} \\ &\preceq \sum_{\zeta > \eta} \sum_{\pi \in R'} V_\pi \left(\frac{1}{d_{\bar{\zeta}, \bar{\eta}_{12}}^{\bar{\zeta}}} \Pi_{\bar{\eta}_{12}, \bar{\eta}_1}^{\bar{\zeta}} + \Pi_{\bar{\eta}_{12}, \bar{\zeta}_1}^{\bar{\zeta}} - \frac{\sqrt{d_{\bar{\zeta}, \bar{\eta}_{12}}^2 - 1}}{d_{\bar{\zeta}, \bar{\eta}_{12}}^{\bar{\zeta}}} \Pi_{\bar{\eta}_{12}, \bar{\eta}_1 \leftrightarrow \bar{\eta}_{12}, \bar{\zeta}_1}^{\bar{\zeta}} \right) V_{\pi^{-1}} \\ &= (N-1) \sum_{\zeta > \eta} \left(\frac{1}{d_{\bar{\zeta}, \bar{\eta}_{12}}^{\bar{\zeta}}} \frac{\dim \bar{\eta}_{12}}{\dim \bar{\eta}_1} \Pi_{\bar{\eta}_1}^{\bar{\zeta}} + \frac{\dim \bar{\eta}_{12}}{\dim \bar{\zeta}_1} \Pi_{\bar{\zeta}_1}^{\bar{\zeta}} \right) \\ &\preceq \frac{1}{N - o(N)} \sum_{\zeta > \eta} \Pi_{\bar{\eta}_1}^{\bar{\zeta}} + (N-1) \sum_{\zeta > \eta} \frac{\dim \bar{\eta}_{12}}{\dim \bar{\zeta}_1} \Pi_{\bar{\zeta}_1}^{\bar{\zeta}}, \end{aligned} \quad (6.1)$$

where \preceq denotes the *semidefinite ordering*, the equality in the middle comes from (5.11), and the last inequality is due to $\dim \bar{\eta}_{12} \leq \dim \bar{\eta}_1$ and $d_{\bar{\zeta}, \bar{\eta}_{12}}^{\bar{\zeta}} \geq N - 2k - 1$.

Claim 6.3. *Let $\zeta \vdash k$. Then $1 - \dim \bar{\zeta}_1 / \dim \bar{\zeta} \leq 2k/N$.*

Proof. Recall the hook-length formula (2.4). As ζ has $\zeta(1) \leq k$ columns, define $\zeta^\top(j) = 0$ for all $j \in [\zeta(1) + 1, k]$. We have

$$\dim \bar{\zeta} = \frac{N!}{h((N-k, \zeta))} = \frac{N! / (N-2k)!}{h(\zeta) \prod_{j=1}^k (N-k+1-j + \zeta^\top(j))}, \quad (6.2)$$

and therefore

$$1 - \frac{\dim \bar{\zeta}_1}{\dim \bar{\zeta}} = 1 - \frac{(N-1)! / (N-2k-1)!}{N! / (N-2k)!} \prod_{j=1}^k \frac{N-k+1-j + \zeta^\top(j)}{N-k-j + \zeta^\top(j)} < 1 - \frac{N-2k}{N} = \frac{2k}{N}.$$

□

For $\eta' \neq \eta$, we have $(\Delta_1 \diamond (\Gamma_{\eta'})_{1,2})^*(\Delta_1 \diamond (\Gamma_{\eta})_{1,2}) = 0$, therefore, by summing (6.1) over all $\eta \vdash k$, we get

$$\begin{aligned} & \sum_{\pi \in R'} V_{\pi}(\Delta_1 \diamond (\Gamma_k)_{1,2})^*(\Delta_1 \diamond (\Gamma_k)_{1,2})V_{\pi^{-1}} \\ & \asymp \frac{1}{N - o(N)} \sum_{\eta \vdash k} \sum_{\zeta > \eta} \Pi_{\bar{\eta}_1}^{\bar{\zeta}} + (N - 1) \sum_{\zeta \vdash k+1} \sum_{\eta < \zeta} \frac{\dim \bar{\eta}_{12}}{\dim \bar{\zeta}_1} \Pi_{\bar{\zeta}_1}^{\bar{\zeta}} \\ & \leq \frac{1}{N - o(N)} \sum_{\eta \vdash k} \sum_{\zeta > \eta} \Pi_{\bar{\eta}_1}^{\bar{\zeta}} + 2(k + 1) \sum_{\zeta \vdash k+1} \Pi_{\bar{\zeta}_1}^{\bar{\zeta}}, \end{aligned} \tag{6.3}$$

where the first inequality holds because $\sum_{\eta \vdash k} \sum_{\zeta > \eta}$ and $\sum_{\zeta \vdash k+1} \sum_{\eta < \zeta}$ are sums over the same pairs of η and ζ , and the second inequality holds because $\dim \bar{\zeta}_1 = \dim \bar{\zeta}_{12} + \sum_{\eta < \zeta} \dim \bar{\eta}_{12}$ (due to the branching rule) and Claim 6.3.

Finally, by summing (6.3) over k , we get

$$\begin{aligned} (\Delta_1 \diamond \Gamma')^*(\Delta_1 \diamond \Gamma') &= \sum_{\pi \in R'} V_{\pi}(\Delta_1 \diamond \Gamma_{1,2})^*(\Delta_1 \diamond \Gamma_{1,2})V_{\pi^{-1}} \\ &\leq \sum_{k=0}^{N^{2/3}} \frac{(N^{2/3} - k)^2}{N^2} \left(\frac{1}{N - o(N)} \sum_{\eta \vdash k} \sum_{\zeta > \eta} \Pi_{\bar{\eta}_1}^{\bar{\zeta}} + 2(k + 1) \sum_{\zeta \vdash k+1} \Pi_{\bar{\zeta}_1}^{\bar{\zeta}} \right) \leq \mathbb{I}/3. \end{aligned}$$

Hence, $\|\Delta_1 \diamond \Gamma'\| \in O(1)$.

6.3 Bounding $\|\Delta_1 \diamond \Gamma''\|$

Let us decompose the adversary matrix as $\Gamma = 2\Gamma_{\mathcal{A}} - \Gamma_{\mathcal{B}}$, where we define $\Gamma_{\mathcal{A}}$ and $\Gamma_{\mathcal{B}}$ via their restriction to the rows labeled by $x \in \mathcal{D}_{1,2}$:

$$(\Gamma_{\mathcal{A}})_{1,2} = \sum_{k=0}^{N^{2/3}} \frac{N^{2/3} - k}{N} \sum_{\eta \vdash k} \Pi_{\bar{\eta}_{12}, \bar{\eta}_1} \Pi_{id} \quad \text{and} \quad (\Gamma_{\mathcal{B}})_{1,2} = \sum_{k=0}^{N^{2/3}} \frac{N^{2/3} - k}{N} \sum_{\eta \vdash k} \Pi_{\bar{\eta}_{12}}^{\bar{\eta}},$$

respectively. We show that $\|\Delta_1 \diamond \Gamma''_{\mathcal{A}}\| \in O(1)$ and $\|\Delta_1 \diamond \Gamma''_{\mathcal{B}}\| \in O(1)$, which together imply $\|\Delta_1 \diamond \Gamma''\| \in O(1)$. The argument is very similar for both $\Gamma_{\mathcal{A}}$ and $\Gamma_{\mathcal{B}}$, and let us start by showing $\|\Delta_1 \diamond \Gamma''_{\mathcal{A}}\| \in O(1)$.

We are interested to see how Δ_3 acts on $(\Gamma_{\mathcal{A}})_{1,2}$. Let $\theta < \eta$, and we will have to consider $\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1}$. For every $\lambda > \bar{\eta}_1$, note that $V_{(23)}$ and $\Pi_{\bar{\theta}_{123}, \bar{\eta}_1}^{\lambda}$ commute. So, similarly to (5.6), we have

$$V_{(23)} \Pi_{\bar{\theta}_{123}, \bar{\eta}_1} = \frac{1}{d_{\bar{\eta}_1, \bar{\theta}_{123}}} \sum_{\lambda > \bar{\eta}_1} \left(\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1}^{\lambda} - \Pi_{\bar{\theta}_{123}, \bar{\theta}_{12}, \bar{\eta}_1}^{\lambda} + \sqrt{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2 - 1} \Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1 \leftrightarrow \bar{\theta}_{123}, \bar{\theta}_{12}, \bar{\eta}_1}^{\lambda} \right).$$

Hence

$$\frac{\text{Tr}[\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1}^{\lambda} \Pi_{\bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1}^{\lambda}]}{\dim \bar{\theta}_{123} \dim \lambda} = \frac{\text{Tr}[\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1}^{\lambda} V_{(23)} \Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1}^{\lambda} V_{(23)}]}{\dim \bar{\theta}_{123} \dim \lambda} = \frac{1}{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2},$$

and therefore, similarly to (5.10), we have

$$\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1} = \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1} + \frac{1}{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2} (\Pi_{\bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1} - \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1}) + \frac{\sqrt{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2 - 1}}{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2} \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1 \leftrightarrow \bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1}, \quad (6.4)$$

where

$$\Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1 \leftrightarrow \bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1} = \sum_{\lambda > \bar{\eta}_1} \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1 \leftrightarrow \bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1}^\lambda$$

for short.

Without loss of generality, let us assume $N^{2/3}$ to be an integer. Then, by using the branching rule and simple derivations, one can see that

$$\sum_{k=0}^{N^{2/3}-1} \frac{N^{2/3}-k}{N} \sum_{\eta \vdash k} \left(\Pi_{\bar{\eta}_{123}, \bar{\eta}_1} + \sum_{\theta < \eta} \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1} \right) = \sum_{k=0}^{N^{2/3}-1} \left(\frac{1}{N} \sum_{\eta \vdash k} \Pi_{\bar{\eta}_{123}, \bar{\eta}_1} + \frac{N^{2/3}-k}{N} \sum_{\theta \vdash k-1} \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}} \right). \quad (6.5)$$

Therefore we have

$$\begin{aligned} (\Gamma_{\mathcal{A}})_{1,2} &= \sum_{k=0}^{N^{2/3}-1} \frac{N^{2/3}-k}{N} \sum_{\eta \vdash k} \left(\Pi_{\bar{\eta}_{123}, \bar{\eta}_1} + \sum_{\theta < \eta} \Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1} \right) \Pi_{id} \\ &= \sum_{k=0}^{N^{2/3}-1} \left(\frac{1}{N} \sum_{\eta \vdash k} \Pi_{\bar{\eta}_{123}, \bar{\eta}_1} + \frac{N^{2/3}-k}{N} \sum_{\eta \vdash k} \sum_{\theta < \eta} \left(\frac{1}{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2} (\Pi_{\bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1} - \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1}) \right. \right. \\ &\quad \left. \left. + \frac{\sqrt{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2 - 1}}{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2} \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1 \leftrightarrow \bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1} \right) + \frac{N^{2/3}-k}{N} \sum_{\theta \vdash k-1} \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}} \right) \Pi_{id}, \end{aligned}$$

where the first equality comes from the branching rule and the fact that we can ignore $k = N^{2/3}$, and the second equality comes from subsequent applications of (6.4) and (6.5).

Recall that the action of Δ_3 commutes with Π_{id} and $\Delta_3 \circ \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}} = 0$. Therefore we can choose

$$\begin{aligned} \Delta_3 \diamond (\Gamma_{\mathcal{A}})_{1,2} &= \sum_{k=0}^{N^{2/3}-1} \left(\frac{1}{N} \sum_{\eta \vdash k} \Pi_{\bar{\eta}_{123}, \bar{\eta}_1} + \frac{N^{2/3}-k}{N} \sum_{\eta \vdash k} \sum_{\theta < \eta} \left(\frac{1}{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2} (\Pi_{\bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1} - \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1}) \right. \right. \\ &\quad \left. \left. + \frac{\sqrt{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2 - 1}}{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2} \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1 \leftrightarrow \bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1} \right) \right) \Pi_{id}, \end{aligned}$$

and we have

$$\begin{aligned}
 & (\Delta_3 \diamond (\Gamma_{\mathcal{A}})_{1,2})^* (\Delta_3 \diamond (\Gamma_{\mathcal{A}})_{1,2}) \\
 &= \sum_{k=0}^{N^{2/3}-1} \Pi_{id} \left(\frac{1}{N^2} \sum_{\eta \vdash k} \Pi_{\bar{\eta}_{123}, \bar{\eta}_1} + \frac{(N^{2/3}-k)^2}{N^2} \sum_{\eta \vdash k} \sum_{\theta < \eta} \frac{1}{d_{\bar{\eta}_1, \bar{\theta}_{123}}^2} (\Pi_{\bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1} + \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1}) \right) \Pi_{id}, \\
 &\preceq \frac{1}{N^2} \sum_{k=0}^{N^{2/3}-1} \Pi_{id} \left(\sum_{\eta \vdash k} \Pi_{\bar{\eta}_{123}, \bar{\eta}_1} + o(1) \cdot \sum_{\eta \vdash k} \sum_{\theta < \eta} (\Pi_{\bar{\theta}_{123}, \bar{\eta}_{13}, \bar{\eta}_1} + \Pi_{\bar{\theta}_{123}, \bar{\theta}_{13}, \bar{\eta}_1}) \right) \Pi_{id} \preceq \frac{1}{N^2} \mathbb{I}.
 \end{aligned}$$

Finally, (5.3) tells us that

$$\|\Delta_1 \diamond \Gamma''_{\mathcal{A}}\|^2 = \left\| \sum_{\pi \in R''} V_{\pi} (\Delta_3 \diamond (\Gamma_{\mathcal{A}})_{1,2})^* (\Delta_3 \diamond (\Gamma_{\mathcal{A}})_{1,2}) V_{\pi^{-1}} \right\| \leq \left\| \sum_{\pi \in R''} \frac{1}{N^2} \mathbb{I} \right\| \leq 1/2,$$

and, hence, $\|\Delta_1 \diamond \Gamma''_{\mathcal{A}}\| \in O(1)$.

We show that $\|\Delta_1 \diamond \Gamma''_{\mathcal{B}}\| \in O(1)$ in essentially the same way, except now, instead of the decomposition (6.4) of $\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}, \bar{\eta}_1}$ we consider the decomposition (5.10) of $\Pi_{\bar{\theta}_{123}, \bar{\eta}_{12}}$. This concludes the proof that $\|\Delta_1 \diamond \Gamma''\| \in O(1)$, which, in turn, concludes the proof of Theorem 6.2.

7 Open problems

We already mentioned two open problems in the introduction. One is to close the gap between the best known lower bound and upper bound for k -DISTINCTNESS, $\Omega(N^{2/3})$ and $O(N^{1-2^{k-2}/(2^k-1)})$, respectively. We hope that our lower bound for ELEMENT DISTINCTNESS could help to improve the lower bound for k -DISTINCTNESS when $k \geq 3$.

The other is to reduce the required group (i.e., alphabet) size in the $\Omega(N^{k/(k+1)})$ lower bound for k -SUM. As pointed out in [12], the quantum query complexity of k -SUM becomes $O(\sqrt{N})$ for groups of constant size. Therefore it would be interesting to find tradeoffs between the quantum query complexity and the size (and, potentially, the structure) of the group. These tradeoffs might be relatively smooth, unlike the jump in the query complexity of ELEMENT DISTINCTNESS between alphabet sizes $N-1$ and N .

Claims 3.2 and 6.1 suggest that the adversary matrix that we consider in Theorem 6.2 for ELEMENT DISTINCTNESS is a natural choice. While any other optimal adversary matrix probably cannot look too different (in terms of the singular value decomposition), it does not mean that it cannot have a simpler specification. Such a simpler specification might facilitate the construction of adversary bounds for other problems.

In fact, Belovs' construction [8] gives an adversary matrix Γ for ELEMENT DISTINCTNESS for any alphabet size. Unfortunately, his analysis for lower bounding $\|\Gamma\|/\|\Delta_i \circ \Gamma\|$ does not work any more for alphabet sizes $o(N^2)$. Nonetheless, it still might be the case that $\|\Gamma\|/\|\Delta_i \circ \Gamma\| \in \Omega(N^{2/3})$ even when $|\Sigma| = N$, and, if one could show that, it might help to provide tight adversary bounds for COLLISION and SET EQUALITY with minimal non-trivial alphabet size, because the current adversary bounds for them are constructed similarly to Belovs's adversary bound for ELEMENT DISTINCTNESS and require

$|\Sigma| \in \Omega(N^2)$. (We know that such adversary bounds for COLLISION and SET EQUALITY exist due to tight lower bounds via other methods [1, 19, 29] and the optimality of the adversary method [20].)

Jeffery, Magniez, and de Wolf recently studied the model of parallel quantum query algorithms, which can make P queries in parallel in each timestep [18]. They show that such algorithms have to make $\Theta((N/P)^{2/3})$ P -parallel quantum queries to solve ELEMENT DISTINCTNESS. For the lower bound, they generalize the adversary bound given in [10] (which is almost equivalent to one in [8]) and therefore require that the alphabet size is at least $\Omega(N^2)$. The techniques provided in this paper might help to remove this requirement.

Acknowledgments

The author would like to thank Andris Ambainis, Aleksandrs Belovs, Robin Kothari, Hari Krovi, Abel Molina, and John Watrous for fruitful discussions and useful comments. A large portion of the research described in this paper was conducted during author's visit to the University of Latvia.

References

- [1] SCOTT AARONSON AND YAORYUN SHI: Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM*, 51(4):595–605, 2004. [2](#), [21](#)
- [2] ANDRIS AMBAINIS: Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002. [[arXiv:quant-ph/0002066](#)] [2](#)
- [3] ANDRIS AMBAINIS: Polynomial degree vs. quantum query complexity. In *Proc. of 44th IEEE FOCS*, pp. 230–239, 2003. [[arXiv:quant-ph/0305028](#)] [2](#)
- [4] ANDRIS AMBAINIS: Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range. *Theory of Computing*, 1:37–46, 2005. [[arXiv:quant-ph/0305179](#)] [2](#)
- [5] ANDRIS AMBAINIS: Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007. [[arXiv:quant-ph/0311001](#)] [2](#), [3](#), [4](#)
- [6] ANDRIS AMBAINIS, LOÏCK MAGNIN, MARTIN ROETTELER, AND JÉRÉMIE ROLAND: Symmetry-assisted adversaries for quantum state generation. In *Proc. of 26th IEEE Complexity*, pp. 167–177, 2011. [[arXiv:1012.2112](#)] [1](#), [24](#)
- [7] ROBERT BEALS, HARRY BUHRMAN, RICHARD CLEVE, MICHELE MOSCA, AND RONALD DE WOLF: Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. [[arXiv:quant-ph/9802049](#)] [2](#)
- [8] ALEKSANDRS BELOVS: Adversary lower bound for element distinctness. 2012. [[arXiv:1204.5074](#)] [3](#), [16](#), [20](#), [21](#)

- [9] ALEKSANDRS BELOVS: Learning-graph-based quantum algorithm for k -distinctness. In *Proc. of 53rd IEEE FOCS*, pp. 207–216, 2012. [arXiv:1205.1534] 3
- [10] ALEKSANDRS BELOVS AND ANSIS ROSMANIS: On the power of non-adaptive learning graphs. In *Proc. of 28th IEEE Complexity*, pp. 44–55, 2013. [arXiv:1210.3279] 3, 16, 21
- [11] ALEKSANDRS BELOVS AND ANSIS ROSMANIS: Adversary lower bounds for the collision and the set equality problems. 2014. [arXiv:1310.5185] 3, 16
- [12] ALEKSANDRS BELOVS AND ROBERT ŠPALEK: Adversary lower bound for the k -sum problem. In *Proc. of 4th ACM ITCS*, pp. 323–328, 2012. [arXiv:1206.6528] 3, 16, 20
- [13] GILLES BRASSARD, PETER HØYER, AND ALAIN TAPP: Quantum cryptanalysis of hash and claw-free functions. In *Proc. of 3rd LATIN*, volume 1380 of *LNCS*, pp. 163–169. Springer, 1998. [arXiv:quant-ph/9705002] 2
- [14] HARRY BUHRMAN, CHRISTOPH DÜRR, MARK HEILIGMAN, PETER HØYER, FRÉDÉRIC MAGNIEZ, MIKLOS SANTHA, AND RONALD DE WOLF: Quantum algorithms for element distinctness. *SIAM Journal on Computing*, 34(6):1324–1330, 2005. [arXiv:quant-ph/0007016] 2
- [15] CHRIS GODSIL: Association schemes. Lecture Notes, <http://quoll.uwaterloo.ca/pdfs/assoc1.pdf>, 2005. 3
- [16] PETER HØYER, TROY LEE, AND ROBERT ŠPALEK: Negative weights make adversaries stronger. In *Proc. of 39th ACM STOC*, pp. 526–535, 2007. [arXiv:quant-ph/0611054] 2, 3, 5, 9
- [17] GORDON JAMES AND ADALBERT KERBER: *The Representation Theory of the Symmetric Group*. Volume 16 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company, 1981. 5, 13
- [18] STACEY JEFFERY, FRÉDÉRIC MAGNIEZ, AND RONALD DE WOLF: Optimal parallel quantum query algorithms. 2013. [arXiv:1309.6116] 21
- [19] SAMUEL KUTIN: Quantum lower bound for the collision problem with small range. *Theory of Computing*, 1(1):29–36, 2005. [arXiv:quant-ph/0304162] 2, 21
- [20] TROY LEE, RAJAT MITTAL, BEN W. REICHARDT, ROBERT ŠPALEK, AND MARIO SZEGEDY: Quantum query complexity of the state conversion problem. In *Proc. of 52nd IEEE FOCS*, pp. 344–353, 2011. [arXiv:1011.3020] 2, 5, 21
- [21] GATIS MIDRIJĀNIS: A polynomial quantum query lower bound for the set equality problem. In *Proc. of 31th ICALP*, volume 3142 of *LNCS*, pp. 996–1005. Springer, 2004. [arXiv:quant-ph/0401073] 1
- [22] BEN W. REICHARDT: Reflections for quantum query algorithms. In *Proc. of 22nd ACM-SIAM SODA*, pp. 560–569, 2011. [arXiv:1005.1601] 2
- [23] BRUCE E. SAGAN: *The Symmetric Group*. Volume 203 of *Graduate Texts in Mathematics*. Springer, 2001. 5

- [24] JEAN-PIERRE SERRE: *Linear Representations of Finite Groups*. Volume 42 of *Graduate Texts in Mathematics*. Springer, 1977. [5](#), [7](#)
- [25] PETER W. SHOR: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. [[arXiv:quant-ph/9508027](#)] [1](#)
- [26] DANIEL R. SIMON: On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997. [1](#)
- [27] ROBERT ŠPALEK: Adversary lower bound for the orthogonal array problem. 2013. [[arXiv:1304.0845](#)] [3](#), [16](#)
- [28] ROBERT ŠPALEK AND MARIO SZEGEDY: All quantum adversary methods are equivalent. *Theory of Computing*, 2:1–18, 2006. [[arXiv:quant-ph/0409116](#)] [2](#)
- [29] MARK ZHANDRY: A note on the quantum collision and set equality problems. 2013. [[arXiv:1312.1027](#)] [3](#), [21](#)
- [30] SHENGYU ZHANG: On the power of Ambainis lower bounds. *Theoretical Computer Science*, 339(2):241–256, 2005. [[arXiv:quant-ph/0311060](#)] [2](#)

A Necessary conditions for the construction of Γ

A.1 Action of Δ_i on Π_λ^λ and transporters

Let us consider $i \neq 2$. Recall the projectors $\hat{\Pi}_i^s$ from Section 5.2, and note that $V_\pi^\tau \hat{\Pi}_i^s = \hat{\Pi}_i^s V_\pi^\tau$ for all $(\pi, \tau) \in \mathbb{S}_{[N] \setminus \{i\}} \times \mathbb{S}_{\Sigma \setminus \{s\}}$. Analogously to Claim 3.1,

$$\hat{\Pi}_i^s = \sum_{\mu \vdash N-1} \hat{\Pi}_{i, \mu_i}^{s, \mu_s},$$

where $\hat{\Pi}_{i, \mu_i}^{s, \mu_s} = \hat{\Pi}_i^s \Pi_{\mu_i}^{\mu_s} = \Pi_{\mu_i}^{\mu_s} \hat{\Pi}_i^s$ projects on a single instance of the irrep $\mu \times \mu$ of $\mathbb{S}_{[N] \setminus \{i\}} \times \mathbb{S}_{\Sigma \setminus \{s\}}$.

Due to the symmetry, $V_\pi^\tau (\bar{\Delta}_i \circ \Pi_\lambda^\lambda) = (\bar{\Delta}_i \circ \Pi_\lambda^\lambda) V_\pi^\tau$ for all $(\pi, \tau) \in \mathbb{S}_{[N] \setminus \{i\}} \times \mathbb{S}_\Sigma$, therefore we can express

$$\bar{\Delta}_i \circ \Pi_\lambda^\lambda = \sum_{\lambda' \vdash N} \sum_{\mu < \lambda'} \phi_\mu^{\lambda'} \Pi_{\mu_i}^{\lambda'}.$$

We have

$$\begin{aligned} \phi_\mu^{\lambda'} &= \frac{\text{Tr}[(\bar{\Delta}_i \circ \Pi_\lambda^\lambda) \Pi_{\mu_i}^{\lambda'}]}{\text{Tr}[\Pi_{\mu_i}^{\lambda'}]} = \frac{\text{Tr}[\sum_{s \in \Sigma} \hat{\Pi}_i^s \Pi_\lambda^\lambda \hat{\Pi}_i^s \Pi_{\mu_i}^{\lambda'}]}{\dim \lambda' \dim \mu} = N \frac{\text{Tr}[\hat{\Pi}_{i, \mu_i}^{s, \mu_s} \Pi_{\mu_i}^\lambda \hat{\Pi}_{i, \mu_i}^{s, \mu_s} \Pi_{\mu_i}^{\lambda'}]}{\dim \lambda' \dim \mu} \\ &= N \frac{\text{Tr}[\hat{\Pi}_{i, \mu_i}^{s, \mu_s} \Pi_{\mu_i}^\lambda] \cdot \text{Tr}[\hat{\Pi}_{i, \mu_i}^{s, \mu_s} \Pi_{\mu_i}^{\lambda'}]}{\dim \lambda' (\dim \mu)^3} = N \frac{\text{Tr}[\hat{\Pi}_i^s \Pi_{\mu_i}^\lambda] \cdot \text{Tr}[\hat{\Pi}_i^s \Pi_{\mu_i}^{\lambda'}]}{\dim \lambda' (\dim \mu)^3} \\ &= \frac{\text{Tr}[\Pi_{\mu_i}^\lambda] \cdot \text{Tr}[\Pi_{\mu_i}^{\lambda'}]}{N \dim \lambda' (\dim \mu)^3} = \begin{cases} \frac{\dim \lambda}{N \dim \mu}, & \text{if } \mu < \lambda, \\ 0, & \text{if } \mu \not< \lambda \text{ (i.e., } \Pi_{\mu_i}^\lambda = 0), \end{cases} \end{aligned}$$

where the second equality is due to (5.4), the third and sixth equalities are due to the symmetry among all $s \in \Sigma$, and the fourth equality is from [6]. Hence

$$\Delta_i \circ \Pi_\lambda^\lambda = \Pi_\lambda^\lambda - \frac{\dim \lambda}{N} \sum_{\mu < \lambda} \left(\frac{1}{\dim \mu} \sum_{\lambda' > \mu} \Pi_{\mu_i}^{\lambda'} \right) = \Pi_\lambda^\lambda - \frac{\dim \lambda}{N} \sum_{\mu < \lambda} \left(\frac{1}{\dim \mu} \Pi_{\mu_i} \right). \quad (\text{A.1})$$

Now consider $j \neq i$, $\lambda \vdash N$, and $\nu \ll_{rc} \lambda$. Let $\mu, \mu' \vdash N-1$ be such that $\nu < \mu < \lambda$, $\nu < \mu' < \lambda$, and $\mu \neq \mu'$. Let us see how $\bar{\Delta}_i$ acts on the transporter $\Pi_{\nu_{ij}, \mu'_i \leftarrow \nu_{ij}, \mu_i}^\lambda$. We have

$$\hat{\Pi}_i^s \Pi_{\nu_{ij}, \mu'_i \leftarrow \nu_{ij}, \mu_i}^\lambda \hat{\Pi}_i^s = \hat{\Pi}_i^s \Pi_{\mu_i}^{\mu'} \Pi_{\nu_{ij}, \mu'_i \leftarrow \nu_{ij}, \mu_i}^\lambda \Pi_{\mu_i}^{\mu_s} \hat{\Pi}_i^s = 0$$

because $\Pi_{\nu_{ij}, \mu'_i \leftarrow \nu_{ij}, \mu_i}^{\mu_s}$ is a transporter between two instances of the irrep $\nu \times \mu'$ of $\mathbb{S}_{[N] \setminus \{i, j\}} \times \mathbb{S}_{\Sigma \setminus \{s\}}$ and, therefore, orthogonal to $\Pi_{\mu_i}^{\mu_s}$. Hence,

$$\bar{\Delta}_i \circ \Pi_{\nu_{ij}, \mu'_i \leftarrow \nu_{ij}, \mu_i}^\lambda = 0 \quad \text{and} \quad \Delta_i \circ \Pi_{\nu_{ij}, \mu'_i \leftarrow \nu_{ij}, \mu_i}^\lambda = \Pi_{\nu_{ij}, \mu'_i \leftarrow \nu_{ij}, \mu_i}^\lambda. \quad (\text{A.2})$$

A.2 Necessary conditions for $\|\Delta_1 \circ \Gamma\| \in \mathcal{O}(1)$

We will use the following lemmas and corollaries in the proof of Claim 6.1. Let $\Gamma_{1,2}$ be given as in (4.3), and Γ be obtained from $\Gamma_{1,2}$ via (4.1).

Lemma A.1. *Consider $\lambda \vdash N$, $\mu < \lambda$, $\mu' < \lambda$, and $\nu < \mu, \mu'$ (we allow $\mu = \mu'$ here). If $\|\Delta_1 \circ \Gamma'\| \leq 1$, then*

$$\|\Pi_{\nu_{12}, \mu_1}^\lambda (\Delta_1 \circ \Gamma_{1,2}) \Pi_{\nu_{12}, \mu'_1}^\lambda\| \leq \sqrt{\frac{\dim \mu'}{(N-1) \dim \nu}}.$$

Proof. For the proof, let us assume that $\nu \ll_{rc} \lambda$ and $\mu \neq \mu'$. It is easy to see that the proof works in all the other cases too. Let $\Psi_{\nu, \mu}^\lambda = \sum_{\pi \in R'} U_\pi \Pi_{\nu_{12}, \mu_1}^\lambda U_{\pi^{-1}}$, where the transversal R' was defined in Section 5.1. From (5.1), we have

$$\Psi_{\nu, \mu}^\lambda (\Delta_1 \circ \Gamma') = \sum_{\pi \in R'} U_\pi \Pi_{\nu_{12}, \mu_1}^\lambda (\Delta_1 \circ \Gamma_{1,2}) V_{\pi^{-1}}, \quad (\text{A.3})$$

whose norm is at most 1 because $\Psi_{\nu, \mu}^\lambda$ is a projector.

We can express

$$\Pi_{\nu_{12}, \mu_1}^\lambda (\Delta_1 \circ \Gamma_{1,2}) = \psi \Pi_{\nu_{12}, \mu_1}^\lambda + \psi' \Pi_{\nu_{12}, \mu_1 \leftarrow \nu_{12}, \mu'_1}^\lambda,$$

where

$$\psi = \|\Pi_{\nu_{12}, \mu_1}^\lambda (\Delta_1 \circ \Gamma_{1,2}) \Pi_{\nu_{12}, \mu_1}^\lambda\| \quad \text{and} \quad \psi' = \|\Pi_{\nu_{12}, \mu_1}^\lambda (\Delta_1 \circ \Gamma_{1,2}) \Pi_{\nu_{12}, \mu'_1}^\lambda\|.$$

Hence,

$$(\Delta_1 \circ \Gamma_{1,2})^* \Pi_{\nu_{12}, \mu_1}^\lambda (\Delta_1 \circ \Gamma_{1,2}) = \psi^2 \Pi_{\nu_{12}, \mu_1}^\lambda + (\psi')^2 \Pi_{\nu_{12}, \mu'_1}^\lambda + \psi \psi' \Pi_{\nu_{12}, \mu_1 \leftrightarrow \nu_{12}, \mu'_1}^\lambda. \quad (\text{A.4})$$

From (A.3), (A.4), and (5.11), we get

$$(\Delta_1 \circ \Gamma')^* \Psi_{\nu, \mu}^\lambda (\Delta_1 \circ \Gamma') = \psi^2 (N-1) \frac{\dim \nu}{\dim \mu} \Pi_\mu^\lambda + (\psi')^2 (N-1) \frac{\dim \nu}{\dim \mu'} \Pi_{\mu'}^\lambda.$$

The norm of this matrix is at most 1, which completes the proof. \square

Corollary A.2. *Let $\nu \vdash N - 2$, $\mu > \nu$, and $\lambda, \lambda' > \mu$. If $\|\Delta_1 \circ \Gamma'\| \leq 1$, then*

$$\left| \frac{\text{Tr}[\Pi_{\nu_{12}, \mu_1}^\lambda \Gamma_{1,2}]}{\dim \lambda \dim \nu} - \frac{\text{Tr}[\Pi_{\nu_{12}, \mu_1}^{\lambda'} \Gamma_{1,2}]}{\dim \lambda' \dim \nu} \right| \leq 2 \sqrt{\frac{\dim \mu}{(N-1) \dim \nu}}.$$

Proof. From Lemma A.1, we have

$$\begin{aligned} \|\Pi_{\nu_{12}, \mu_1}^\lambda (\Delta_1 \circ \Gamma_{1,2}) \Pi_{\nu_{12}, \mu_1}^\lambda\| &= \frac{|\text{Tr}[\Pi_{\nu_{12}, \mu_1}^\lambda (\Delta_1 \circ \Gamma_{1,2})]|}{\dim \lambda \dim \nu} = \frac{|\text{Tr}[(\Delta_1 \circ \Pi_{\nu_{12}, \mu_1}^\lambda) \Gamma_{1,2}]|}{\dim \lambda \dim \nu} \\ &= \frac{|\text{Tr}[(\Pi_{\nu_{12}, \mu_1}^\lambda - \frac{\dim \lambda}{N \dim \mu} \Pi_{\nu_{12}, \mu_1}) \Gamma_{1,2}]|}{\dim \lambda \dim \nu} = \left| \frac{\text{Tr}[\Pi_{\nu_{12}, \mu_1}^\lambda \Gamma_{1,2}]}{\dim \lambda \dim \nu} - \frac{\text{Tr}[\Pi_{\nu_{12}, \mu_1} \Gamma_{1,2}]}{N \dim \mu \dim \nu} \right| \leq \sqrt{\frac{\dim \mu}{(N-1) \dim \nu}}, \end{aligned}$$

where the second and third equalities are due to (5.4) and (A.1), respectively. We obtain the same inequality with λ' instead of λ , and the result follows from the triangle inequality. \square

Corollary A.3. *Consider $\lambda \vdash N$, $\nu \ll_{rc} \lambda$, and $\mu, \mu' \vdash N - 1$ such that $\nu < \mu < \lambda$, $\nu < \mu' < \lambda$, and μ appears after μ' in the lexicographical order. If $\|\Delta_1 \circ \Gamma'\| \leq 1$, then*

$$\begin{aligned} \left| \alpha_{id, \nu}^\lambda \frac{\sqrt{d_{\lambda, \nu}^2 - 1}}{2d_{\lambda, \nu}} - \alpha_{sgn, \nu}^\lambda \frac{d_{\lambda, \nu} - 1}{2d_{\lambda, \nu}} \right| &\leq \sqrt{\frac{\dim \mu}{(N-1) \dim \nu}}, \\ \left| \alpha_{id, \nu}^\lambda \frac{\sqrt{d_{\lambda, \nu}^2 - 1}}{2d_{\lambda, \nu}} + \alpha_{sgn, \nu}^\lambda \frac{d_{\lambda, \nu} + 1}{2d_{\lambda, \nu}} \right| &\leq \sqrt{\frac{\dim \mu'}{(N-1) \dim \nu}}, \end{aligned}$$

Proof. Since λ is the unique N -box Young diagram that has both μ and μ' as subdiagrams, we have

$$\Pi_{\nu_{12}, \mu'_1} \Gamma_{1,2} \Pi_{\nu_{12}, \mu_1} = \Pi_{\nu_{12}, \mu'_1}^\lambda \Gamma_{1,2} \Pi_{\nu_{12}, \mu_1}^\lambda.$$

Hence, due to (A.2) and the commutativity relations (5.5), we have

$$\Pi_{\nu_{12}, \mu'_1}^\lambda (\Delta_1 \circ \Gamma_{1,2}) \Pi_{\nu_{12}, \mu_1}^\lambda = \Pi^\lambda (\Delta_1 \circ (\Pi_{\nu_{12}, \mu'_1} \Gamma_{1,2} \Pi_{\nu_{12}, \mu_1})) \Pi^\lambda = \Pi_{\nu_{12}, \mu'_1}^\lambda \Gamma_{1,2} \Pi_{\nu_{12}, \mu_1}^\lambda.$$

The same holds with μ and μ' swapped. From (5.7) and (5.8), we get that

$$\begin{aligned} \Pi_{\nu_{12}, \mu'_1}^\lambda \Gamma_{1,2} \Pi_{\nu_{12}, \mu_1}^\lambda &= \left(\alpha_{id, \nu}^\lambda \frac{\sqrt{d_{\lambda, \nu}^2 - 1}}{2d_{\lambda, \nu}} - \alpha_{sgn, \nu}^\lambda \frac{d_{\lambda, \nu} - 1}{2d_{\lambda, \nu}} \right) \Pi_{\nu_{12}, \mu'_1 \leftarrow \nu_{12}, \mu_1}^\lambda, \\ \Pi_{\nu_{12}, \mu_1}^\lambda \Gamma_{1,2} \Pi_{\nu_{12}, \mu'_1}^\lambda &= \left(\alpha_{id, \nu}^\lambda \frac{\sqrt{d_{\lambda, \nu}^2 - 1}}{2d_{\lambda, \nu}} + \alpha_{sgn, \nu}^\lambda \frac{d_{\lambda, \nu} + 1}{2d_{\lambda, \nu}} \right) \Pi_{\nu_{12}, \mu_1 \leftarrow \nu_{12}, \mu'_1}^\lambda, \end{aligned}$$

and we apply Lemma A.1 to complete the proof. \square

Lemma A.4. *Let θ be a Young diagram having at most $N/2 - 2$ boxes and $\eta > \theta$. If $\|\Delta_1 \circ \Gamma''\| \leq 1$, then*

$$\left| \alpha_{id, \bar{\eta}_{12}}^{\bar{\eta}} - \alpha_{id, \bar{\theta}_{12}}^{\bar{\theta}} + \frac{2(\alpha_{id, \bar{\theta}_{12}}^{\bar{\eta}} - \alpha_{id, \bar{\eta}_{12}}^{\bar{\eta}})}{d_{\bar{\eta}, \bar{\theta}_{12}}(d_{\bar{\eta}, \bar{\theta}_{12}} - 1)} \right| \leq 2\sqrt{\frac{\dim \bar{\theta}_3}{\binom{N-1}{2} \dim \bar{\theta}_{123}}}.$$

Proof. Note that $\Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}}(\Delta_3 \circ \Gamma_{1,2})$ can be expressed as a linear combination of $\Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}}$ and $\Pi_{\bar{\theta}_{123}, \bar{\theta}_3 \leftarrow id, \bar{\theta}_{123}, \bar{\eta}_3}^{\bar{\eta}}$, while $\Pi_{\bar{\theta}_{123}}^{\bar{\theta}}(\Delta_3 \circ \Gamma_{1,2})$ is proportional to $\Pi_{\bar{\theta}_{123}}^{\bar{\theta}}$. Similarly to Lemma A.1, we can show that

$$\|\Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}}(\Delta_1 \circ \Gamma_{1,2})\Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}}\| \leq \sqrt{\frac{\dim \bar{\theta}_3}{\binom{N-1}{2} \dim \bar{\theta}_{123}}}, \quad \|\Pi_{\bar{\theta}_{123}}^{\bar{\theta}}(\Delta_1 \circ \Gamma_{1,2})\Pi_{\bar{\theta}_{123}}^{\bar{\theta}}\| \leq \sqrt{\frac{\dim \bar{\theta}_3}{\binom{N-1}{2} \dim \bar{\theta}_{123}}},$$

where, instead of (5.11), we have to use (analogously proven)

$$V_{\pi} \Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} V_{\pi^{-1}} = \binom{N-1}{2} \frac{\dim \bar{\theta}_{123}}{\dim \bar{\theta}_3} \Pi_{\bar{\theta}_3}^{\bar{\eta}} \quad \text{and} \quad \sum_{\pi \in R''} V_{\pi} \Pi_{id, \bar{\theta}_{123}, \bar{\eta}_3 \leftrightarrow \bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} V_{\pi^{-1}} = 0.$$

Then, similarly to Corollary A.2, we get

$$\left| \frac{\text{Tr}[\Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} \Gamma_{1,2}]}{\dim \bar{\eta} \dim \bar{\theta}_{123}} - \frac{\text{Tr}[\Pi_{\bar{\theta}_{123}}^{\bar{\theta}} \Gamma_{1,2}]}{\dim \bar{\theta} \dim \bar{\theta}_{123}} \right| \leq 2\sqrt{\frac{\dim \bar{\theta}_3}{\binom{N-1}{2} \dim \bar{\theta}_{123}}}.$$

We conclude by noticing that

$$\Pi_{\bar{\theta}_{123}}^{\bar{\theta}} \Gamma_{1,2} = \Pi_{\bar{\theta}_{123}}^{\bar{\theta}} (\alpha_{id, \bar{\theta}_{12}}^{\bar{\theta}} \Pi_{\bar{\theta}_{12}}^{\bar{\theta}}) = \alpha_{id, \bar{\theta}_{12}}^{\bar{\theta}} \Pi_{\bar{\theta}_{123}}^{\bar{\theta}}$$

and, due to (5.9),

$$\begin{aligned} \Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} \Gamma_{1,2} \Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} &= \Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} (\alpha_{id, \bar{\eta}_{12}}^{\bar{\eta}} \Pi_{\bar{\eta}_{12}}^{\bar{\eta}} + \alpha_{id, \bar{\theta}_{12}}^{\bar{\eta}} \Pi_{id, \bar{\theta}_{12}}^{\bar{\eta}}) \Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}} \\ &= \left(\left(1 - \frac{2}{d_{\bar{\eta}, \bar{\theta}_{12}}(d_{\bar{\eta}, \bar{\theta}_{12}} - 1)}\right) \alpha_{id, \bar{\eta}_{12}}^{\bar{\eta}} + \frac{2}{d_{\bar{\eta}, \bar{\theta}_{12}}(d_{\bar{\eta}, \bar{\theta}_{12}} - 1)} \alpha_{id, \bar{\theta}_{12}}^{\bar{\eta}} \right) \Pi_{\bar{\theta}_{123}, \bar{\theta}_3}^{\bar{\eta}}. \end{aligned}$$

□

A.3 Proof of Claim 6.1

We can assume that all the coefficients β in the expression (3.2) for Γ are at most N , as N is the trivial upper bound on the quantum query complexity of ELEMENT DISTINCTNESS. That, in turn, means that we can assume that the coefficients α in Point 1, Point 2, and Point 3 of Claim 6.1 are, respectively, at most $O(1)$, $O(\sqrt{N})$, and $O(N)$. Let us prove sequentially every point of the claim.

Point 1. Consider $k \in O(1)$, $\theta \vdash k$, and $\eta > \theta$, so $d_{\bar{\eta}, \bar{\theta}_{12}} = N - O(1)$ and $\dim \bar{\theta}_3 / \dim \bar{\theta}_{123} \in \Theta(1)$. From Lemma A.4, we get that $|\alpha_{id, \bar{\eta}_{12}}^{\bar{\eta}} - \alpha_{id, \bar{\theta}_{12}}^{\bar{\theta}}| \in O(1/N)$, which proves that $\alpha_{id, \bar{\theta}_{12}}^{\bar{\theta}} = N^{-1/3} + O(1/N)$ by the induction over k , where we take $\alpha_{id, (N-2)}^{(N)} = N^{-1/3}$ as the base case.

Point 2. Consider $\theta \vdash O(1)$ and $\eta > \theta$, so $\dim \bar{\theta}_1 / \dim \bar{\theta}_{12} \in \Theta(1)$. From the first inequality of Corollary A.3 (in which we choose $\lambda = \bar{\eta}$ and $\nu = \bar{\theta}_{12}$, forcing $\mu = \bar{\theta}_1$), we get that $|\alpha_{id, \bar{\theta}_{12}}^{\bar{\eta}} - \alpha_{sgn, \bar{\theta}_{12}}^{\bar{\eta}}| \in O(1/\sqrt{N})$. From Corollary A.2 (in which we choose $\nu = \bar{\theta}_{12}$, $\mu = \bar{\theta}_1$, $\lambda = \bar{\theta}$, and $\lambda' = \bar{\eta}$), we get

$$\left| \frac{\text{Tr}[\Pi_{\bar{\theta}_{12}}^{\bar{\theta}} \Gamma_{1,2}]}{\dim \bar{\theta} \dim \bar{\theta}_{12}} - \frac{\text{Tr}[\Pi_{\bar{\theta}_{12}, \bar{\theta}_1}^{\bar{\eta}} \Gamma_{1,2}]}{\dim \bar{\eta} \dim \bar{\theta}_{12}} \right| \in O(1/\sqrt{N}),$$

where we have

$$\Pi_{\bar{\theta}_{12}}^{\bar{\theta}} \Gamma_{1,2} = \alpha_{id, \bar{\theta}_{12}}^{\bar{\theta}} \Pi_{\bar{\theta}_{12}}^{\bar{\theta}} \quad \text{and} \quad \Pi_{\bar{\theta}_{12}, \bar{\theta}_1}^{\bar{\eta}} \Gamma_{1,2} \Pi_{\bar{\theta}_{12}, \bar{\theta}_1}^{\bar{\eta}} = \left(\alpha_{id, \bar{\theta}_{12}}^{\bar{\eta}} \frac{d_{\bar{\eta}, \bar{\theta}_{12}} - 1}{2d_{\bar{\eta}, \bar{\theta}_{12}}} + \alpha_{sgn, \bar{\theta}_{12}}^{\bar{\eta}} \frac{\sqrt{d_{\bar{\eta}, \bar{\theta}_{12}}^2 - 1}}{2d_{\bar{\eta}, \bar{\theta}_{12}}} \right) \Pi_{\bar{\theta}_{12}, \bar{\theta}_1}^{\bar{\eta}}$$

from (5.7) and (5.8). Therefore, $|\alpha_{id, \bar{\theta}_{12}}^{\bar{\theta}} - (\alpha_{id, \bar{\theta}_{12}}^{\bar{\eta}} + \alpha_{sgn, \bar{\theta}_{12}}^{\bar{\eta}})/2| \in O(1/\sqrt{N})$, which together with previously proven $\alpha_{id, \bar{\theta}_{12}}^{\bar{\theta}} = N^{-1/3} + O(1/N)$ and $|\alpha_{id, \bar{\theta}_{12}}^{\bar{\eta}} - \alpha_{sgn, \bar{\theta}_{12}}^{\bar{\eta}}| \in O(1/\sqrt{N})$ imply $\alpha_{id, \bar{\theta}_{12}}^{\bar{\eta}} = N^{-1/3} + O(1/\sqrt{N})$ and $\alpha_{sgn, \bar{\theta}_{12}}^{\bar{\eta}} = N^{-1/3} + O(1/\sqrt{N})$.

Point 3. Consider $\lambda \vdash N$ and $\nu \ll_c \lambda$ that is obtained from λ by removing two boxes in different columns below the first row. Let us consider two cases.

Case 1: $\nu \ll_{rc} \lambda$. Let $\mu, \mu' \vdash N-1$ be such that $\nu < \mu < \lambda$, $\nu < \mu' < \lambda$, and $\mu \neq \mu'$. Since $d_{\lambda, \nu} \geq 2$, $\dim \mu / \dim \nu \in \Theta(N)$, and $\dim \mu' / \dim \nu \in \Theta(N)$, both inequalities of Corollary A.3 together imply $\alpha_{id, \nu}^{\lambda} = O(1)$ and $\alpha_{sgn, \nu}^{\lambda} = O(1)$.

Case 2: $\nu \ll_c \lambda$ and $\nu \not\ll_r \lambda$ (i.e., ν is obtained from λ by removing two boxes in the same, but not the first, row). Let $\mu \vdash N-1$ be the unique Young diagram that satisfies $\nu < \mu < \lambda$, and let λ' be obtained from μ by adding a box in the first row. For Point 2 we already have shown that $\alpha_{id, \nu}^{\lambda'} \in o(1)$ and $\alpha_{sgn, \nu}^{\lambda'} \in o(1)$, so, from Corollary A.2 and $\dim \mu / \dim \nu \in \Theta(N)$, we get that $\alpha_{id, \nu}^{\lambda} \in O(1)$.

AUTHOR

Ansis Rosmanis
 Ph.D. candidate
 David R. Cheriton School of Computer Science and
 Institute for Quantum Computing, University of Waterloo
 ansis.rosmanis@gmail.com