A Tight Lower Bound For Non-Coherent Index Erasure

Nathan Lindzey
Department of Computer Science, University of Colorado at Boulder, USA
nathan.lindzey@colorado.edu

Ansis Rosmanis
Graduate School of Mathematics, Nagoya University, Japan
http://rosmanis.com/research/index.html
ansis.rosmanis@math.nagoya-u.ac.jp

Abstract

The *index erasure problem* is a quantum state generation problem that asks a quantum computer to prepare a uniform superposition over the image of an injective function given by an oracle. We prove a tight $\Omega(\sqrt{n})$ lower bound on the quantum query complexity of the *non-coherent* case of the problem, where, in addition to preparing the required superposition, the algorithm is allowed to leave the ancillary memory in an arbitrary function-dependent state. This resolves an open question of Ambainis, Magnin, Roetteler, and Roland (CCC 2011), who gave a tight bound for the coherent case, the case where the ancillary memory must return to its initial state.

To prove our main result, we first extend the so-called *automorphism principle* (Høyer et al. STOC 2007) to the *general adversary method* for state conversion problems (Lee et al. STOC 2011), which allows one to exploit the symmetries of these problems to lower bound their quantum query complexity. Using this method, we establish a strong connection between the quantum query complexity of non-coherent symmetric state generation problems and the well-known *Krein parameters* of *association schemes*. Krein parameters are usually hard to determine, nevertheless, we give a novel way of computing certain Krein parameters of a commutative association scheme defined over partial permutations. We believe the study of this association scheme may also be of independent interest.

2012 ACM Subject Classification Theory of computation → Quantum query complexity; Mathematics of computing → Combinatorics

Keywords and phrases General Adversary Method, Quantum Query Complexity, Association Schemes, Krein Parameters, Representation Theory

Digital Object Identifier 10.4230/LIPIcs.ITCS.2020.59

Funding *Ansis Rosmanis*: The author is a JSPS International Research Fellow supported by the JSPS KAKENHI Grant Number JP19F19079. Part of this work was done while he was at the Centre for Quantum Technologies at the National University of Singapore supported by the Singapore Ministry of Education and the National Research Foundation under grant R-710-000-012-135.

Acknowledgements AR would like to thank Aleksandrs Belovs and Jérémie Roland for insightful discussions. NL thanks Chris Godsil for useful discussions.

1 Introduction

For proving lower bounds in the *oracle query model*, one assumes access to an oracle O_f that evaluates a black-box function $f\colon [n] \to [m]$ on input queries, where $[n] := \{1, 2, \cdots, n\}$ and $[m] := \{1, 2, \cdots, m\}$, and the goal is to prove that any algorithm for solving the computational problem at hand must make a certain number of oracle queries. This principle for proving lower bounds applies to both classical and quantum computation, and in the latter we let the oracle to be queried in a superposition.

Quantum query algorithms are known to surpass their classical counterparts for many important classical tasks, such as unstructured search, game tree evaluation, random walks, and others (see [17, 1] for recent surveys). Classical tasks aside, one may also be interested in *quantum mechanical tasks*, such as *quantum state generation*. A quantum state generation problem simply asks for a certain quantum state $|\psi_f\rangle$ to be generated on the target register. In this paper, we consider a particular state generation problem known as Index Erasure.

Given an injective function $f\colon [n] \to [m]$ via a black-box oracle O_f, Index Erasure is the task of preparing the quantum state that is the uniform superposition over the image of f, namely,

$$|\psi_f\rangle := \frac{1}{\sqrt{n}} \sum\nolimits_{x=1}^{n} |f(x)\rangle\,.$$

The name of the problem stems from the fact that a quantum computer can prepare the uniform superposition $\frac{1}{\sqrt{n}} \sum_{x=1}^{n} |x\rangle\,|f(x)\rangle$ using a single query to O_f, yet the task of ignoring or *erasing* the first register that records the *index* x is non-trivial. Indeed, if one could solve Index Erasure using a poly-logarithmic number of queries, one would obtain a time-efficient algorithm for Graph Isomorphism (we present more details in Appendix A).

The question of the complexity of Index Erasure was first raised by Shi in [23], where he already observed that the problem can be solved in $\mathrm{O}(\sqrt{n})$ queries by an algorithm based on Grover's search. In the same paper, Shi also introduced the Set Equality problem, which asks to decide whether two injective functions f, f' given via black-box oracles $O_f, O_{f'}$ have the same image or have disjoint images, given a promise that either is the case. Set Equality can be easily reduced to Index Erasure via the swap test, increasing the number of oracle queries by at most a constant factor; therefore, when Midrijānis presented an $\Omega((n/\log n)^{1/5})$ lower bound on the quantum query complexity of Set Equality [16], the same lower bound automatically applied to Index Erasure, ruling out the existence of poly-logarithmic query algorithms for these two problems.

Quantum state generation comes in two forms: the *coherent state generation*, where all memory aside from the target state must return to its initial state, $|\mathbf{0}\rangle := |0 \cdots 0\rangle$, and the *non-coherent state generation*, where there is no such a requirement, namely, where the ancillary memory can remain in some function-dependent state $|t_f\rangle$. Ambainis, Magnin, Roetteler, and Roland devised the *hybrid adversary method* [2], which they used to prove a tight $\Omega(\sqrt{n})$ lower bound for Index Erasure in the *coherent* regime, and left the non-coherent case as an open question. Later, the lower bound for Set Equality was improved to a tight $\Omega(n^{1/3})$ [26, 4], which in turn led to an improved query lower bound for the non-coherent Index Erasure.

In this paper, we close the gap for the non-coherent Index Erasure problem, by proving a tight lower bound on its quantum query complexity under the condition that the range of the black-box function f is sufficiently large. More formally, we show the following.

▶ **Theorem 1** (Main Result). *The bounded-error quantum query complexity of* Index Erasure *is* $\Theta(\sqrt{n})$ *in the non-coherent state generation regime, provided that* $m \geq n^{3\sqrt{n}}$.

To the best of our knowledge, the proof of Theorem 1 is the first application of the general adversary method of Lee, Mittal, Reichardt, Špalek, and Szegedy [15] for a non-coherent state generation problem. We outline the proof below.

1.1 Outline of the Proof of the Main Result

The symmetries of Index Erasure are paramount in our proof. The product $S_n \times S_m$ of two symmetric groups act on a function $f\colon [n] \to [m]$ as $(\pi, \rho)\colon f \mapsto \rho * f * \pi^{-1}$, where $(\pi, \rho) \in S_n \times S_m$ and $*$ denotes the composition of functions. This group action on injective functions defines a representation of $S_n \times S_m$. This representation is multiplicity-free, meaning that it contains no more than one instance of any irrep (irreducible representation) of $S_n \times S_m$. Moreover, it consists of those and only those irreps $\lambda \otimes \lambda'$ where the Young diagram $\lambda \vdash n$ is contained in the Young diagram $\lambda \vdash m$ and the skew shape λ'/λ has no more than one cell per column. Throughout the paper, we often abuse the terminology and we interchangeably use the terms partition λ of n, denoted $\lambda \vdash n$, the Specht module corresponding to λ (which is irreducible and distinct for every λ), and the n-cell Young diagram corresponding to λ.

Two types of irreps are of particular interest to us. Given $\lambda \vdash n$, we call the irrep $\lambda \otimes \bar{\lambda}$ where $\bar{\lambda} \vdash m$ is obtained from λ by adding $m-n$ cells to the first row of λ a *minimal* irrep and the irrep $\lambda \otimes (m-n, \lambda)$ where $(m-n, \lambda) \vdash m$ is obtained from λ by adding one cell to each of the first $m-n$ columns of λ (alternatively, by adding the part $m-n$ to λ) a *maximal* irrep, where we assume $m \geq 2n$. In other words, if $\theta \vdash k$ and $\lambda := (n-k, \theta) \vdash n$, then $(n-k, \theta) \otimes (m-k, \theta)$ is a minimal irrep and $(n-k, \theta) \otimes (m-n, n-k, \theta)$ is a maximal irrep. In particular, to lower bound the quantum query complexity of the non-coherent Index Erasure, we use essentially the same adversary matrix Γ as [2] used for the coherent Index Erasure, which is specified through minimal irreps.

An adversary matrix is a symmetric real matrix whose rows and columns are labeled by all the functions in the domain of the problem, and it is the central object of most adversary methods. In our case, the adversary matrix acts on the same $m^{\underline{n}}$-dimensional space as the representation matrices of $S_n \times S_m$ mentioned above, where $m^{\underline{n}} := m!/(m-n)!$ is the total number of functions. Similarly to [2], we choose

$$\Gamma := \sum\nolimits_{k=0}^{\sqrt{n}} \left(\sqrt{n} - k\right) \sum_{\theta \vdash k} E_{(n-k,\theta)\otimes(m-k,\theta)},$$

where $E_{\lambda\otimes\lambda'}$ is the orthogonal projector on the irrep $\lambda \otimes \lambda'$ (note that we have only used projectors on certain minimal irreps to construct Γ). We also note that the Gram matrices $T_{\lambda\otimes\lambda'} = m^{\underline{n}} E_{\lambda\otimes\lambda'}/d_{\lambda\otimes\lambda'}$, where $d_{\lambda\otimes\lambda'} := \operatorname{tr}[E_{\lambda\otimes\lambda'}]$ is the dimension of $\lambda \otimes \lambda'$, play an important role in our proof.

In order to take advantage of the inherent symmetries of the Index Erasure problem, we first extend the *automorphism principle* of Høyer, Lee, and Špalek [13] to the *general adversary method* for state generation and conversion problems [15] (see Corollary 3 and Theorem 4). This extension leads us to consider the Gram matrix corresponding to the final state $|\psi_f, t_f\rangle$ of an algorithm run with oracle O_f (assuming no error). The Gram matrix corresponding to $|\psi_f\rangle$ is

$$\frac{n}{m} T_{(n)\otimes(m)} + \left(1 - \frac{n}{m}\right) T_{(n)\otimes(m-1,1)} =: T^{\odot},$$

therefore the Gram matrix corresponding to $|\psi_f, t_f\rangle$ is $T^{\odot} \circ T$, where $T_{f,f'} := \langle t_f | t_{f'} \rangle$ and $\circ$ denotes the Schur (i.e., entrywise) matrix product. For the coherent regime lower bound, $\langle \mathbf{0} | \mathbf{0} \rangle = 1$ and $T = J = T_{(n)\otimes(m)}$ is the all-ones matrix. For the non-coherent regime, one of the consequences of the generalization of the automorphism principle is that it suffices to consider T such that $T_{f,f'} = T_{\sigma(f),\sigma(f')}$ for all functions f, f' and all $\sigma \in S_n \times S_m$.

To prove the $\Omega(\sqrt{n})$ lower bound, we must show, for all such Gram matrices T, that

$$\operatorname{tr}\left[\Pi_\Gamma \frac{T^{\odot} \circ T}{m^{\underline{n}}}\right] = o(1), \tag{1.1}$$

where Π_Γ is the orthogonal projector on the image of Γ, and that $\|\Gamma \circ \Delta_x\| = \mathrm{O}(1)$ for all $x \in [n]$, where Δ_x is the binary matrix with $(\Delta_x)_{f,f'} := 1$ if and only if $f(x) \neq f'(x)$.[1] Here we only need to prove the former condition because we use essentially the same adversary matrix as [2], and the latter condition is shown in their work. On the other hand, showing condition (1.1) was a triviality in [2] because $T = J$ in the coherent regime and thus the trace evaluates to n/m.

We now present the three main simplifying steps used to narrow the scope of condition (1.1). First, we use linearity to show that it suffices to prove

$$\operatorname{tr}\left[\Pi_\Gamma \frac{T_{(n)\otimes(m-1,1)} \circ T_{\lambda\otimes\lambda'}}{m^{\underline{n}}}\right] = o(1)$$

for all irreps $\lambda \otimes \lambda'$. That is, we can restrict our attention from a continuum of choices for T to a finite set $\{T_{\lambda\otimes\lambda'}\}_{\lambda\otimes\lambda'}$ of choices, where we have also used that the term $T_{(n)\otimes(m-1,1)}$ "dominates" $T_{(n)\otimes(m)}$ in $T^{\odot}$.

Second, we use the connection between $T_{(n)\otimes(m-1,1)}$ and a specific primitive idempotent of the Johnson (association) scheme to obtain

$$\operatorname{tr}\left[E_{\lambda\otimes\bar{\lambda}} \frac{T_{(n)\otimes(m-1,1)} \circ T_{\lambda\otimes\lambda'}}{m^{\underline{n}}}\right] = o(1)$$

as a sufficient condition, where we have to consider only Young diagrams $\lambda \vdash n$ that have less than $\sqrt{n}$ cells below the first row.

Third, for such λ, we show that the dimension of $\lambda\otimes\bar{\lambda}$ is much smaller than the dimension of any other $\lambda \otimes \lambda'$ (thus the nomenclature "minimal irrep"); therefore, we show it suffices to prove

$$\operatorname{tr}\left[E_{\lambda\otimes\bar{\lambda}} \frac{T_{(n)\otimes(m-1,1)} \circ T_{\lambda\otimes\bar{\lambda}}}{m^{\underline{n}}}\right] = o(1). \tag{1.2}$$

It is convenient to think of (1.1) and its simplifications in terms of the following association scheme. For a pair of functions (f, f'), consider the orbit $\mathcal{O}_\mu := \{(\sigma(f), \sigma(f')) \colon \sigma \in S_n \times S_m\}$, and let A_μ be the binary matrix with $(A_\mu)_{h,h'} = 1$ if and only if $(h, h') \in \mathcal{O}_\mu$. Here we use μ to label distinct orbits and let $\mathcal{C}_n$ be the set of all of them. The set of matrices $\{A_\mu \colon \mu \in \mathcal{C}_n\}$ forms a symmetric association scheme, denoted $\mathcal{A}_{n,m}$, which we call the *partial permutation scheme* due to the bijection $f \leftrightarrow (f(1), f(2), \cdots, f(n))$ between injective functions $f \colon [n] \to [m]$ and n-partial permutations of $[m]$.

In the terminology of (commutative) association schemes, the projectors $E_{\lambda\otimes\lambda'}$ are called the *primitive idempotents*, and their entries corresponding to the orbit $\mathcal{O}_\mu$ multiplied by $m^{\underline{n}}$ are called *dual eigenvalues* of the association scheme, which we denote as $q_{\lambda\otimes\lambda'}(\mu)$. The *valency* $v_\mu^{(m)}$ is the size of $\mathcal{O}_\mu$ divided by $m^{\underline{n}}$, thus, in terms of dual eigenvalues, the left hand side of condition (1.2) can be written as

$$\frac{\sum_{\mu\in\mathcal{C}_n} v_\mu^{(m)} \cdot q_{(n)\otimes(m-1,1)}(\mu) \cdot q^2_{\lambda\otimes\bar{\lambda}}(\mu)}{m^{\underline{n}} d_{(n)\otimes(m-1,1)} d_{\lambda\otimes\bar{\lambda}}}. \tag{1.3}$$

[1] The terms in condition (1.1) and similar expressions are written in such a way to emphasize that $\frac{T^{\odot}\circ T}{m^{\underline{n}}}$ is a density operator.

One of the crucial results of our paper relates the dual eigenvalues corresponding to a minimal irrep $(n-k,\theta)\otimes(m-k,\theta)$ in the $\mathcal{A}_{n,m}$ scheme to the dual eigenvalues corresponding to the maximal irrep $\theta\otimes(n-k,\theta)$ in the $\mathcal{A}_{k,n}$ scheme, where $\theta\vdash k$. This relation allows us to express the terms under the sum in (1.3) as polynomials in m. The condition $m\geq n^{3\sqrt{n}}$ in Theorem 1 ensures that it suffices to restrict the sum to those $\mu\in\mathcal{C}_n$ whose corresponding polynomials are of maximum degree, and for such μ, we relate their valencies $v_\mu^{(m)}$ in the $\mathcal{A}_{n,m}$ scheme to valencies of the $\mathcal{A}_{k,n}$ scheme, which together with certain properties of dual eigenvalues allow us to obtain the desired bound.

1.2 Additional Results on the Partial Permutation Scheme

In the context of quantum query complexity, the partial permutation association scheme was already considered in [21], where a conjecture on its eigenvalues implied tight adversary bounds for the Collision and Set Equality problems. Along these lines, our work shows a connection between quantum query complexity and the *Krein parameters* $q_{i,j}(k)$ of association schemes (see Section 5 for a formal definition). Indeed, condition (1.2) is equivalent to the conditions

$$q_{\lambda\otimes\bar{\lambda},\,\lambda\otimes\bar{\lambda}}((n)\otimes(m-1,1))=o(d_{\lambda\otimes\bar{\lambda}})\quad\text{and}\quad q_{\lambda\otimes\bar{\lambda},\,(n)\otimes(m-1,1)}(\lambda\otimes\bar{\lambda})=o(m)$$

on the Krein parameters of $\mathcal{A}_{n,m}$, and (1.3) gives an expression of these parameters in terms of dual eigenvalues.

The Krein parameters of an association scheme are important because they are the *dual structure constants* of its corresponding *Bose-Mesner algebra*. While the structure constants of Bose-Mesner algebras admit an obvious combinatorial meaning, its dual structure constants do not (e.g., they can be irrational) and are difficult to interpret. Indeed, the question of whether or not there exists a "good" interpretation of these constants has been asked often in algebraic combinatorics, so it seems interesting that we are able to relate these constants to the quantum query complexity of suitably symmetric state generations problems in the non-coherent regime. We are unaware of any previously known connection between quantum computing and the Krein parameters of association schemes.

Aside from computer science, we believe that the partial permutation scheme is of independent interest in combinatorics, as it generalizes both the Johnson scheme and the conjugacy class scheme of S_n. We include other new results on the partial permutation association scheme in the appendix, including a procedure that facilitates the calculation of dual eigenvalues corresponding to maximal irreps when $m\gg n$. We are unaware of any previously known results on the dual eigenvalues or Krein parameters of the partial permutation association scheme.

1.3 Organization of the paper

The paper is organized as follows. In Section 2, we present preliminaries on the quantum query model, with emphasis on state generation problems, including Index Erasure, the general adversary method, and the automorphism principle. In Section 3, we present preliminaries on the representation theory, particularly focusing on the symmetric group and its action on partial permutations. The automorphism principle of the general adversary method requires us to analyze highly symmetric matrices, which are elements of the Bose–Mesner algebra corresponding to the partial permutation scheme. In Section 4, we formally define this association scheme, establishing the labeling of various its parameters and computing some of them, as well as addressing its connection to the Johnson scheme. With this formalism at

our disposal, in Section 5, we show that the proof for $\Omega(\sqrt{n})$ lower bound on the quantum query complexity of the non-coherent INDEX ERASURE can be reduced to upper bounds on certain Krein parameter of the partial permutation scheme. Finally, we place the required bounds on these Krein parameters in Section 6. We defer some proofs and additional results on the partial permutation scheme to the appendix.

2 Quantum state generation

In this paper, we address limitations of quantum query algorithms for solving the INDEX ERASURE problem. We assume that the reader is familiar with foundations of quantum computing (see [18] for an introductory reference), some of which we review here. The basic memory unit of a quantum computer is a qubit, which is a two-dimensional complex Euclidean space $\mathbb{C}[\{0,1\}]$ having *computational* orthonormal basis $\{|0\rangle, |1\rangle\}$. Similarly, a k-qubit system corresponds to Euclidean space $\mathbb{C}[\{0,1\}^k]$ and it has computational basis $\{|b\rangle : b \in \{0,1\}^n\}$. Unit vectors $|\Psi\rangle \in \mathbb{C}[\{0,1\}^k]$ are called (pure) *quantum states* and they represent superpositions over various computations basis states.

Quantum bits are often grouped together in *registers* for the ease of algorithm design and analysis. If $|\psi\rangle, |\phi\rangle$ are states of two registers, then the state of the joint system is $|\psi\rangle \otimes |\phi\rangle$. We often shorten the notation $|\psi\rangle \otimes |\phi\rangle$ to $|\psi\rangle |\phi\rangle$ or $|\psi, \phi\rangle$. Due to *entanglement*, not always the state of the joint system can be written as a tensor product of states of the individual registers.

Quantum information is processed by unitary transformations, which correspond to square matrices U such that $UU^* = U^*U = I$, and they map quantum states to quantum states. This unitary processing of quantum information implies that any (noiseless) quantum computation is reversible.

2.1 Quantum query model

In the oracle model, we are given an access to a black-box oracle O_f that evaluates some unknown function $f\colon [n] \to [m]$. The goal of a query algorithm is to perform some computational task that depends on f, for example, to compute some function of f, such as $\textsc{Parity}(f) := f(1) \oplus f(2) \oplus \cdots \oplus f(n)$ when $m = 2$. In quantum computing, one can query the oracle in superposition. On the other hand, due to the requirement for reversibility, the oracle is typically designed so that it preserves the input query x. Namely, given $|x, y\rangle$ as an input, the oracle O_f outputs $|k, y \oplus f(x)\rangle$ (see Figure 1). Here and below we may assume $x, y, f(x)$ to be represented in binary. Even if f is injective – as it is for INDEX ERASURE – unless one knows how to compute the inverse of f, implementing $|x\rangle \mapsto |f(x)\rangle$ in practice might be much harder than $|x, y\rangle \mapsto |k, y \oplus f(x)\rangle$.

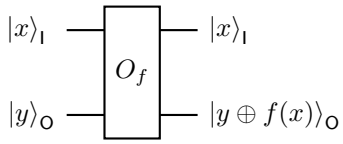


Figure 1 A schematic of a quantum oracle O_f. We assume that y and $f(x)$ are encoded in binary, and thus O_f is its own inverse.

A quantum query algorithm with oracle O_f consists of

- four registers: the input and output registers I and O for accessing the black-box function f, the target register T for storing the result of the computation, and an additional workspace register W;
- an indexed sequence of unitary transformations $U_0, U_1, \cdots, U_Q$ acting on those four registers.

The quantum query algorithm starts its computation in state $|\mathbf{0}\rangle := |00\cdots0\rangle$, and then performs $2Q+1$ unitary operations, alternating between U_i, which acts on all the registers, and O_f, which acts on registers IO. Thus the final state of the computation is

$$|\Psi_f\rangle := U_Q(O_f \otimes I_{\mathsf{TW}})U_{Q-1}(O_f \otimes I_{\mathsf{TW}})\cdots U_1(O_f \otimes I_{\mathsf{TW}})U_0\,|\mathbf{0}\rangle\,,$$

where I_{TW} is the identity operator on registers TW. Figure 2 gives a schematic of a quantum query algorithm. Note that Q is the number of oracle queries performed by the algorithm, and we also refer to it as the *query complexity of the algorithm*.

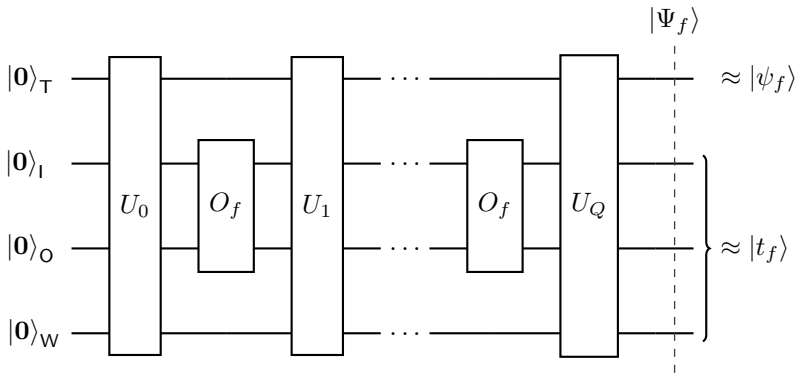


Figure 2 A schematic of a quantum algorithm that uses an oracle O_f. The registers labeled $\mathsf{T}, \mathsf{I}, \mathsf{O}, \mathsf{W}$ are, respectively, the target, input, output, and workspace registers of the algorithm. The target register of the final state $|\Psi_f\rangle$ of the algorithm should be in a state close to the target state $|\psi_f\rangle$.

In this paper we are interested in quantum query algorithms whose goal is to generate a specific f-dependent state $|\psi_f\rangle$ by accessing f via O_f. We note that this generalizes classical function evaluation by a quantum algorithm, where each $|\psi_f\rangle$ is asked to be a computational basis vector. In the next section we describe two distinct regimes of quantum state generation, as well as why they are exactly the same for classical function evaluation.

2.2 Coherent vs. Non-coherent State Generation

When we talk about quantum state generation with oracle O_f, we implicitly assume the domain $[n]$ and the range $[m]$ of f to be fixed. A *quantum state generation* problem is thus specified by a subset $\mathcal{F}$ of functions in form $f\colon [n] \to [m]$, which we call the *domain of the problem*, a complex Euclidean space called the *target space*, and, for every $f \in \mathcal{F}$, a quantum state $|\psi_f\rangle$ in the target space called the *target state*.

One may consider quantum state generation in two regimes: coherent and non-coherent. In the *coherent* state generation regime, all the computational memory other than the target register (i.e., registers IOW) must be returned to its initial state $|\mathbf{0}\rangle$. Therefore, if one was running an algorithm for a superposition of oracles, the final quantum state would be a

superposition of the target states. In contrast, for *non-coherent* state generation, one does not place any requirements on the ancillary memory. More precisely, in the coherent case, for every input $f \in \mathcal{F}$ we require that the final state $|\Psi_f\rangle$ satisfies

$$\Re\langle\psi_f, \mathbf{0}|\Psi_f\rangle \geq \sqrt{1-\epsilon},$$

where $|\mathbf{0}\rangle$ is the initial state of the ancillary registers and a constant $\epsilon \geq 0$ is the desired precision [15] and $\Re$ denotes the real part of the number it precedes. We call the minimum among quantum query complexities among quantum query algorithms that achieve this task the *(ϵ-error) quantum query complexity of the coherent version of the problem*. On the other hand, in the non-coherent case, the final state $|\Psi_f\rangle$ has to satisfy

$$\|(\langle\psi_f| \otimes I)|\Psi_f\rangle\| = \max_{|t_f\rangle} \Re\langle\psi_f, t_f|\Psi_f\rangle \geq \sqrt{1-\epsilon},$$

where the maximum is over unit vectors $|t_f\rangle$ on the system of registers IOW [15], and we analogously define the quantum query complexity of the non-coherent version of the problem.

It is worth noting that evaluation of classical functions can be considered as a special case of quantum state generation, where one is asked to prepare the computational basis state $|\psi_f\rangle$. Since quantum mechanics permits cloning of orthogonal states (computational basis states, in this case), there is no difference between coherent and non-coherent function evaluation, if one is willing to tolerate a two-fold increase in query complexity: at the end of a non-coherent computation, one can copy the target register into an additional register, and then run the whole computation in reverse, restoring all but this additional register to their initial state.

Also, note that an algorithm for the coherent case of a problem solves its non-coherent case as well. Looking on it from the other side: a lower bound on the non-coherent version of the problem is a lower bound on the coherent version as well.

2.3 Index Erasure

The domain of Index Erasure is the set of all injective functions $f\colon [n] \to [m]$. These functions are in one-to-one correspondence with n-partial permutations of $[m]$ and thus $|\mathcal{F}| = m^{\underline{n}} := m!/(m-n)!$. Index Erasure is the task of preparing the quantum state that is the uniform superposition

$$|\psi_f\rangle := \frac{1}{\sqrt{n}} \sum_{x=1}^{n} |f(x)\rangle$$

over the image of f. Note that the state

$$\frac{1}{\sqrt{n}} \sum_{x=1}^{n} |x\rangle|f(x)\rangle$$

can be prepared using a single query to O_f. This would give us the superposition that we seek if we could only ignore or *erase* the first register that records the *index* x, which gives the problem its namesake.

The question of the complexity of Index Erasure was first raised by Shi [23]. As for the upper bound, there is a simple quantum query algorithm for coherent Index Erasure given access to O_f. Thinking of the injective function f as a database with entries in $[m]$, for any $y \in [m]$ we may use Grover's algorithm with O_f to find the unique index x of f such that $f(x) = y$. In other words, there is a circuit that sends the superposition

$$\frac{1}{\sqrt{n}}\sum_{x=1}^{n}|f(x)\rangle \quad \text{to} \quad \frac{1}{\sqrt{n}}\sum_{x=1}^{n}|x\rangle|f(x)\rangle.$$

Inverting this circuit effectively "erases" the index register, which implies that the quantum query complexity of Index Erasure is $\mathrm{O}(\sqrt{n})$.

The first non-trivial lower bounds on the quantum query complexity of Index Erasure were obtained via the Set Equality problem, which asks to decide whether two injective functions f, f' given via black-box oracles $O_f, O_{f'}$ have the same image or have disjoint images, given a promise that either is the case. Set Equality can be easily reduced to non-coherent (and, thus, coherent too) Index Erasure via the swap test, increasing the number of oracle queries by at most a constant factor. Thus, when Midrijānis presented an $\Omega((n/\log n)^{1/5})$ lower bound on the quantum query complexity of Set Equality [16], the same lower bound automatically applied to Index Erasure. Ambainis, Magnin, Roetteler, and Roland devised the *hybrid adversary method* [2], which they used to prove a tight $\Omega(\sqrt{n})$ lower bound for Index Erasure in the *coherent* regime, and left the non-coherent case as an open question. Later, the lower bound for Set Equality was improved to a tight $\Omega(n^{1/3})$ [26, 4], which in turn led to an improved query lower bound for the non-coherent Index Erasure.

The focus of this work is to prove a tight lower bound on the quantum query complexity of Index Erasure in the *non-coherent* case. To show this, we use the so-called *general adversary method* [15] which we review in Section 2.4.

Finally, we note that if one were able to solve Index Erasure using poly-logarithmic number of queries, one would obtain a time-efficient algorithm for Graph Isomorphism. In Appendix A we refer to two similar tests for Graph Isomorphism based on Index Erasure, one on the coherent version, one on the non-coherent version of the problem. However, Midrijānis' lower bound on Set Equality ruled out efficiency of such tests.

2.4 General Adversary Method

The general adversary method places optimal lower bounds on the quantum query complexity of any state conversion problem [15]. State conversion problems generalize state generation problems, yet in this paper it will suffice to introduce the adversary bound only for the latter.

The general adversary bound is stated via the γ_2 and filtered γ_2 norms, which are defined as follows. Let M be any matrix and let $\Delta = \{\Delta_x \colon x \in [n]\}$ be a family of matrices of the same dimensions as M. Define

$$\begin{aligned}\gamma_2(M) &:= \max_{\Gamma'}\{\|M \circ \Gamma'\| \colon \|\Gamma'\| \le 1\},\\ \gamma_2(M|\Delta) &:= \max_{\Gamma}\left\{\|M \circ \Gamma\| \colon \max_{x\in[n]}\|\Delta_x \circ \Gamma\| \le 1\right\},\end{aligned}$$

where $\circ$ denotes the Schur (i.e., entrywise) product of two matrices and, thus, Γ and Γ' are required to have the same dimensions as M. One can show that $\gamma_2(\cdot)$ is a norm over the set of all matrices and $\gamma_2(\cdot|\Delta)$ is a norm over the set of matrices M that has $M_{f,f'} = 0$ whenever $(\Delta_x)_{f,f'} = 0$ for all $x \in [n]$ (see [15] for details). The two norms are called the γ_2 *norm* and the *filtered* γ_2 *norm*, respectively.

The general adversary bound employs various real symmetric matrices whose rows and columns are labeled by black-box functions $f \in \mathcal{F}$ in the same order. The family of *difference matrices* Δ is defined as follows. For each $x \in [n]$, the Δ_x is a binary matrix such that

$(\Delta_x)_{f,f'} := 1$ if and only if $f(x) \neq f'(x)$. A *state matrix* is any positive-semidefinite matrix T such that $T \circ I = I$. In other words, it is a Gram matrix corresponding to some family of unit vectors. Note that $\gamma_2(\cdot|\Delta)$ is a norm on the set of matrices whose diagonals are all-zeros, and a difference of any two state matrices belongs to this set.

Let $\mathcal{T}$ be the set of all state matrices. Note that $\mathcal{T}$ is a compact set and it is closed under the Schur product. Two particular state matrices of our interest are the all ones matrix J, which corresponds to the family $\{|\mathbf{0}\rangle : f \in \mathcal{F}\}$, and the *target matrix* $T^{\odot}$ defined as $(T^{\odot})_{f,f'} := \langle\psi_f|\psi_{f'}\rangle$.

Theorem 2 is a special case of [15, Theorem 4.9].

▶ **Theorem 2.** *The ϵ-error quantum query complexity of a non-coherent state generation problem with the target matrix $T^{\odot}$ and the family of difference matrices Δ is both*

$$\Omega\big(\mathsf{Adv}_{2\sqrt{2\epsilon}}\big) \quad \textit{and} \quad \mathrm{O}\big(\mathsf{Adv}_{\epsilon^4/16}\,\epsilon^{-2}\log\epsilon^{-1}\big),$$

where

$$\mathsf{Adv}_{\delta} := \min_{R,T\in\mathcal{T}}\{\gamma_2(J-R|\Delta)\colon \gamma_2(R-T^{\odot}\circ T)\leq\delta\}. \tag{2.1}$$

In the case of coherent state generation, one imposes $T = J$ in the expression for Adv_{δ}.

In the expression for Adv_{δ}, the state matrix T essentially corresponds to the ancillary states that are prepared in addition to the target states. Thus, assuming there were no error, $T^{\odot} \circ T$ would be the Gram matrix corresponding to the final states of the whole system. However, since one allows some error – determined by the parameter δ – it suffices that the state matrix R corresponding *exactly* to the final states of the algorithm is close to $T^{\odot} \circ T$.

When applying the adversary bound, it is convenient to actually apply it to the zero-error case therefore eliminating the matrix R from the consideration. In particular, this leads to the following corollary of Theorem 2.

A symmetric matrix Γ that satisfies $\|\Delta_x \circ \Gamma\| \leq 1$ for all x is called an *adversary matrix*. Let Π_{Γ} denote the orthogonal projector on the image of Γ.

▶ **Corollary 3.** *Let Γ be an adversary matrix for a non-coherent state generation problem with the target matrix $T^{\odot}$ and the family of difference matrices Δ, let ω be a principal eigenvector of Γ of norm 1, and let*

$$\eta' := \max_{T\in\mathcal{T}} \omega^{\top}(T^{\odot}\circ T\circ\Gamma/\|\Gamma\|)\,\omega.$$

The ϵ-error quantum query complexity of the problem is

$$\Omega\big((1-\eta'-2\sqrt{2\epsilon})\,\|\Gamma\|\,\big).$$

If ω is a uniform superposition over $\mathcal{F}$, then $\eta' \leq \eta$ for

$$\eta := \max_{T\in\mathcal{T}} \mathrm{tr}\left[\Pi_{\Gamma}(T^{\odot}\circ T)/|\mathcal{F}|\right].$$

Proof. For the first part of the corollary, suppose $R, T \in \mathcal{T}$ satisfy $\gamma_2(R - T^{\odot} \circ T) \leq 2\sqrt{2\epsilon}$ and are thus a feasible solution to the minimization in $\mathsf{Adv}_{2\sqrt{2\epsilon}}$. We have

$$\begin{aligned}
\gamma_2(J-R|\Delta) \geq& \|(J-R)\circ\Gamma\| \\
\geq& \|(J-T^{\odot}\circ T)\circ\Gamma\| - \|\Gamma\|\big\|(R-T^{\odot}\circ T)\circ\Gamma/\|\Gamma\|\big\| \\
\geq& \,\omega^{\top}\Gamma\,\omega - \omega^{\top}(T^{\odot}\circ T\circ\Gamma)\,\omega - 2\sqrt{2\epsilon}\|\Gamma\| \\
\geq& (1-\eta'-2\sqrt{2\epsilon})\|\Gamma\|.
\end{aligned}$$

For the second part, note that, if ω is a uniform superposition over $\mathcal{F}$, then, for any two symmetric $|\mathcal{F}| \times |\mathcal{F}|$ matrices M, M', we have $\omega^\top (M \circ M')\, \omega = \operatorname{tr}[MM']/|\mathcal{F}|$. The inequality $\eta' \leq \eta$ results from both $T^\odot \circ T$ and $\Pi_\Gamma - \Gamma/\|\Gamma\|$ being positive-semidefinite. ◀

2.5 Automorphism Principle for State Generation

The *automorphism principle* of [13] addresses the adversary bound for function evaluation problems and states that, without loss of generality, the optimal adversary matrix can be required to respect symmetries of the problem. Here we generalize the automorphism principle to state generation problems.[2]

The wreath product $S_m \wr S_n$ of groups S_m and S_n is the group whose elements are $(\pi, \boldsymbol{\sigma}) \in S_n \times S_m^n$ and whose group operation is

$$\big(\pi', (\sigma'_1, \cdots, \sigma'_n)\big)\big(\pi, (\sigma_1, \cdots, \sigma_n)\big) = \big(\pi'\pi, (\sigma'_1 \sigma_{(\pi')^{-1}(1)}, \cdots, \sigma'_n \sigma_{(\pi')^{-1}(n)})\big)$$

(see [14, Ch. 4]). Similarly to (3.1) below, the action of $S_m \wr S_n$ on $f\colon [n] \to [m]$ is given by

$$\big((\pi, \boldsymbol{\sigma}) f\big)(x) = \sigma_x(f(\pi^{-1}(x)) \qquad \text{for all } x \in [n]. \tag{2.2}$$

The action of a subgroup $G \leq S_m \wr S_n$ on the set of black-box functions $\mathcal{F}$ is *closed* if $g(f) \in \mathcal{F}$ for all $f \in \mathcal{F}$ and $g \in G$.

Suppose M is a symmetric $|\mathcal{F}| \times |\mathcal{F}|$ matrix whose rows and columns are labeled by $f \in \mathcal{F}$ in the same order and suppose the action of a subgroup $G \leq S_m \wr S_n$ on $\mathcal{F}$ is closed. We say that M is *G-invariant* if $M_{g(f),g(f')} = M_{f,f'}$ for all $f, f' \in \mathcal{F}$ and $g \in G$. Similarly, a vector $\omega \in \mathbb{C}[\mathcal{F}]$ is G-invariant if $\omega_{g(f)} = \omega_f$ for all $f \in \mathcal{F}$ and $g \in G$. A subgroup G is an *automorphism group* for a state generation problem with a target matrix $T^\odot$ if G's action on $\mathcal{F}$ is closed and $T^\odot$ is G-invariant.[3]

Note that the free product of two automorphism groups is an automorphism group, so one can consider the maximum automorphism group of a problem. For example, the maximum automorphism group of Parity is the whole wreath product $S_2 \wr S_n$ while the maximum automorphism groups of Or and Index Erasure are, respectively,

$$\{(\pi, (\varepsilon, \cdots, \varepsilon))\colon \pi \in S_n\} \cong S_n,$$
$$\{(\pi, (\sigma, \cdots, \sigma))\colon \pi \in S_n \,\&\, \sigma \in S_m\} \cong S_n \times S_m,$$

where ε is the identity permutation in S_2.

▶ **Theorem 4.** *Let G be an automorphism group for a non-coherent state generation problem. The value of Adv_δ remains the same if one restricts the minimization in the expression defining Adv_δ and the maximization in the expressions defining the γ_2 and filtered γ_2 norms to R, T, Γ, Γ' that are all G-invariant and imposes that $(J - R) \circ \Gamma$ has an G-invariant principal eigenvector.*

The proof of Theorem 4 considers two type of symmetrizations of matrices R, T, Γ, Γ', depending on whether they are arguments in a minimization or a maximization. We defer the proof to Appendix D.

[2] One can easily see that the automorphism principle generalizes even further to state conversion problems.
[3] The G-invariance of $T^\odot$ is equivalent to the existence of a unitary representation U_g of G acting on the target space such that $U_g|\psi_f\rangle = |\psi_{g(f)}\rangle$ for all $f \in \mathcal{F}$ and $g \in G$.

Note that the ability to restrict T and Γ to be G-invariant carries over from Theorem 2 to Corollary 3. The ability to restrict T will be paramount in our proof (see Section 5). On the other hand, the ability to restrict Γ is optional. Namely, Corollary 3 provides an adversary bound regardless of what restrictions one imposes on Γ, yet for too strict restrictions this bound would not be optimal.

For Index Erasure, it is convenient to think of every black-box function $f \in \mathcal{F}$ as a n-partial permutation over the set of symbols $[m]$. As observed in [2], the set of $|\mathcal{F}| \times |\mathcal{F}|$ matrices indexed by $\mathcal{F}$ that are $(S_n \times S_m)$-invariant under the aforementioned action (2.2) afford a *commutative matrix algebra*. In particular, it is the Bose–Mesner algebra of a symmetric association scheme defined over partial permutations, which we formally define in Section 4.

3 Representation Theory Preliminaries

Our main result builds upon finite group representation theory, especially that of the symmetric group. We refer the reader to [6] for a more thorough introduction to group representation theory and [22] for more details on the representation theory of the symmetric group. Throughout this section, let $H, K \leq G$ be subgroups of a finite group G, let $\mathcal{V}$ be a finite-dimensional vector space over $\mathbb{C}$, and for any set X, let $\mathbb{C}[X]$ denote the vector space of dimension $|X|$ of complex-valued functions over X.

3.1 The Representation Theory of the Symmetric Group

A *representation* $(\phi, \mathcal{V})$ of a finite group G is a homomorphism $\phi : G \to GL(\mathcal{V})$ where $GL(\mathcal{V})$ is the *general linear group*, that is, the group of $(\dim \mathcal{V}) \times (\dim \mathcal{V})$ invertible matrices. It is customary to be less formal and denote the representation $(\phi, \mathcal{V})$ simply as ϕ when $\mathcal{V}$ is understood, or as $\mathcal{V}$ when ϕ is understood. For any representation ϕ, we define its *dimension* to be $d_\phi := \dim \phi := \dim \mathcal{V}$. When working concretely with a representation ϕ, we abuse terminology and let $\phi(g)$ refer to a $(\dim \phi) \times (\dim \phi)$ matrix realization of ϕ. Two representations ρ, ϕ are *equivalent* if there exists a matrix P such that $\rho(g) = P^{-1}\phi(g)P$ for all $g \in G$.

Let $(\phi, \mathcal{V})$ be a representation of G, and let $\mathcal{W} \leq \mathcal{V}$ be a *G-invariant* subspace, that is, $\phi(g)w \in \mathcal{W}$ for all $w \in \mathcal{W}$ and for all $g \in G$. We say that $(\phi|_{\mathcal{W}}, \mathcal{W})$ is a *subrepresentation* of ϕ where $\phi|_{\mathcal{W}}$ is the restriction of ϕ to the subspace $\mathcal{W}$. A representation $(\phi, \mathcal{V})$ of G is an *irreducible representation* (or simply, a *G-irrep*) if it has no proper subrepresentations. The *trivial representation* $(1, \mathbb{C})$ defined such that $1 : g \to 1$ for all $g \in G$ is clearly an irrep of dimension one for any group G.

It is well-known that there is a bijection between the set of inequivalent G-irreps and its conjugacy classes $\mathcal{C}$, and that any representation $\mathcal{V}$ of G decomposes uniquely as a direct sum of inequivalent G-irreps

$$\mathcal{V} \cong \bigoplus_{i=1}^{|\mathcal{C}|} m_i \mathcal{V}_i$$

where m_i is the number of occurrences of the G-irrep $\mathcal{V}_i$ in the decomposition. We call the representation $m_i\mathcal{V}_i$ the *ith isotypic component* of $\mathcal{V}$.

A natural way to find representations of groups is to let them act on sets. In particular, for any group G acting on a set X, let $(\phi, \mathbb{C}[X])$ be the *permutation representation* of G on X defined such that

$$(\phi(g)[\zeta])(x) := \zeta(g^{-1}x)$$

for all $g \in G$, $\zeta \in \mathbb{C}[X]$, and $x \in X$. If we let G act on itself, then we obtain the *left regular representation*, which admits the following decomposition into G-irreps

$$\mathbb{C}[G] \cong \bigoplus_{i=1}^{|\mathcal{C}|} d_{\mathcal{V}_i} \mathcal{V}_i.$$

We denote the *Fourier transform* of $\gamma \in \mathbb{C}[G]$ with respect to the representation ϕ as

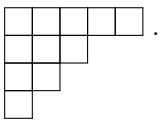
$$\phi(\gamma) := \sum_{g \in G} \gamma(g)\phi(g),$$

which is a linear operator on $\mathcal{V}$.

Let $\mathrm{Sym}(X)$ denote the *symmetric group* on the symbol set X. If $X = [m] := \{1, 2, \cdots, m\}$, then we define $S_m := \mathrm{Sym}(X)$. It is well-known that the conjugacy classes of S_m are given by the cycle-types of permutations of S_m, which in turn are in one-to-one correspondence with *integer partitions* $\lambda \vdash m$, i.e.,

$$\lambda := (\lambda_1, \lambda_2, \cdots, \lambda_k) \vdash m \text{ such that } \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0 \text{ and } \sum_{i=1}^{k} \lambda_i = m.$$

We may visualize λ as a *Young diagram*, a left-justified table of cells that contains λ_i cells in the ith row. When referencing a Young diagram, we alias λ as the *shape*. For example, the Young diagram below has shape $(5, 3, 2, 1) \vdash 11$:



A *standard Young tableau* of shape λ is a Young diagram with unique entries from $[n]$ that are strictly increasing along rows and strictly increasing along columns, e.g.,

1	2	5	8	9
3	6	7		
4	10			
11				

We may write the left regular representation of S_m as

$$\mathbb{C}[S_m] \cong \bigoplus_{\lambda \vdash m} d_\lambda \mathcal{V}_\lambda.$$

where d_λ is the number of standard Young tableau of shape λ, which can be counted elegantly via the *hook rule* (see [22] for a proof).

▶ **Theorem 5** (The Hook Rule). *Let $\lambda \vdash m$, and for any cell $c \in \lambda$ of the Young diagram of λ define the* hook-length $\mathsf{h}_\lambda(c)$ *to be the total number of cells below c in the same column and to the right of c in the same row, plus 1. Then we have*

$$d_\lambda = \frac{m!}{\mathsf{H}(\lambda)} \quad \textit{where} \quad \mathsf{H}(\lambda) := \prod_{c \in \lambda} \mathsf{h}_\lambda(c).$$

Another well-known result is the *branching rule*, which describes how an S_m-irrep decomposes into (S_{m-1})-irreps (see [22] for a proof). We say that a cell of a Young diagram is an *inner corner* if it has no cells to its right and no cells below it.

▶ **Theorem 6** (The Branching Rule). *If $\mathcal{V}_\lambda$ is a S_m-irrep, then*

$$\mathcal{V}_\lambda \cong \bigoplus_{\lambda^-} \mathcal{V}_{\lambda^-}$$

where λ^- ranges over all shapes obtainable by removing an inner corner from λ and $\mathcal{V}_{\lambda^-}$ is the corresponding (S_{m-1})-irrep.

The hook rule and the branching rule can be used to prove the following theorem. We defer its proof to Appendix D.

▶ **Theorem 7.** *Let $\theta \vdash k$ and $\theta^+ \vdash (k+1)$ be any shape obtained by adding an inner corner to θ. For all $m \geq 2(k+1)$, we have*

$$\frac{d_{(m-k-1,\theta^+)}}{d_{(m-k,\theta)}} \geq \frac{m}{k} \cdot \left(1 - \frac{2k+1}{m}\right).$$

Note that the above fraction is greater than 1 when $m > 3k+1$. For any $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell) \vdash n$, henceforth, let $\bar{\lambda} := (\lambda_1 + (m-n), \lambda_2, \cdots, \lambda_\ell) \vdash m$. Theorem 7 has the following corollary.

▶ **Corollary 8.** *Let $\lambda \vdash n$ be a shape such that $\lambda_1 \geq n - \sqrt{n}$ and let $\lambda' \vdash m$ be any shape that covers λ such that λ'/λ is a horizontal strip. Then $d_{\lambda'}/d_{\bar{\lambda}} \in \Omega(m/\sqrt{n})$.*

3.2 The Representation Theory of Partial Permutations

Let $S_{n,m}$ denote the collection of *n-partial permutations of* $[m]$, that is, n-tuples

$$f := (f(1), f(2), \cdots, f(n))$$

with no repeated elements such that $f(x) \in [m]$ for all $x \in [n]$. Injective functions from $[n]$ to $[m]$ are in one-to-one correspondence with $S_{n,m}$, and it is not hard to see that $|S_{n,m}| = m^{\underline{n}}$, and when $m = n$ we recover the symmetric group S_n on n symbols. To understand the representation theory of $S_{n,m}$ we must first broaden our Young tableau vocabulary.

For any $\lambda \vdash m$, let $l(\lambda)$ denote the *length* of λ, that is, the number of parts in the partition. We say that a shape λ *covers* a shape μ if $\mu_i \leq \lambda_i$ for each i. If λ and μ are two shapes such that λ covers μ, then we obtain the *skew shape* λ/μ by removing the cells corresponding to μ from λ. For instance, the shape $(5,3,2,1)$ covers $(2,2,1)$, so we may consider the skew shape $(5,3,2,1)/(2,2,1)$:

A skew shape is a *horizontal strip* if each column has no more than one cell. For example, the skew shape $(5,3,2,1)/(3,3,1)$ is a horizontal strip, but the skew shape above is not.

Henceforth, we let $S_n \times S_m$ act on $S_{n,m}$ as follows:

$$(\tau, \sigma) \cdot (f_1, \cdots, f_n) = (\sigma^{-1}(f_{\tau^{-1}(1)}), \cdots, \sigma^{-1}(f_{\tau^{-1}(n)})) \text{ for all } (\tau, \sigma) \in S_n \times S_m. \tag{3.1}$$

The stabilizer of the *identity n-partial permutaton* $f_{\text{id}} := (1, 2, \cdots, n) \in S_{n,m}$ in $S_n \times S_m$ is isomorphic to the group

$$\text{diag}(S_n) \times S_{m-n} = \{(\tau, \tau, \pi) : \tau \in \text{Sym}([n]), \pi \in \text{Sym}(\{n+1, \cdots, m\}).$$

Using Pieri's rule (see [24]), one can show that the permutation representation of $(S_n \times S_m)$ acting on $S_{n,m} \cong (S_n \times S_m)/(\text{diag}(S_n) \times S_{m-n})$ is *multiplicity-free*, that is, its decomposition has at most one copy of any $(S_n \times S_m)$-irrep, as shown in Theorem 9.

▶ **Theorem 9** ([5]). *The complex-valued functions over n-partial permutations $\mathbb{C}[S_{n,m}]$ admits the following decomposition into $(S_n \times S_m)$-irreps:*

$$\mathbb{C}[S_{n,m}] \cong \bigoplus_{\mu,\lambda} \mathcal{V}_\mu \otimes \mathcal{V}_\lambda$$

where μ, λ ranges over all pairs $\mu \vdash n, \lambda \vdash m$ such that λ/μ is a horizontal strip.

Let $\mathrm{Irr}(S_{n,m})$ denote the set of $(S_n \times S_m)$-irreps that appear in Theorem 9. Every multiplicity-free permutation representation gives rise to a commutative association scheme (see [3]), so a consequence of Theorem 9 is the existence a symmetric association scheme $\mathcal{A}_{n,m}$ over $S_{n,m}$ that we call *the partial permutation association scheme*. In Section 4, we discuss this association scheme in more detail.

A coarser decomposition of $\mathbb{C}[S_{n,m}]$ into irreducibles of S_m can be obtained by identifying $S_{n,m}$ with the set of *tabloids* (i.e., Young tableaux with unordered rows) of shape $(m-n, 1^n)$ and applying Young's rule (see [22]). This representation is known as the $(m-n, 1^n)$-*permutation representation*, which we denote as $\mathcal{M}^{(m-n,1^n)}$. Its isotypic components can be determined combinatorially via the *Kostka numbers* $K_{\lambda,\mu}$ (see [22]).

▶ **Theorem 10.** *The complex-valued functions over n-partial permutations $\mathbb{C}[S_{n,m}]$ admits the following decomposition into S_m-irreps:*

$$\mathbb{C}[S_{n,m}] \cong \mathcal{M}^{(m-n,1^n)} \cong \bigoplus_{\lambda \vdash m} K_{\lambda,(m-n,1^n)}\ \mathcal{V}_\lambda.$$

Note that Theorem 9 gives a multiplicity-free orthogonal decomposition of the λ-isotypic component $K_{\lambda,(m-n,1^n)}\mathcal{V}_\lambda$ of $\mathcal{M}^{(m-n,1^n)}$ into $(S_n \times S_m)$-irreps

$$K_{\lambda,(m-n,1^n)}\mathcal{V}_\lambda \cong \bigoplus_{\mu} \mathcal{V}_\mu \otimes \mathcal{V}_\lambda$$

where the sum ranges over all $\mu \vdash n$ such that λ/μ is a horizontal strip.

The following two types of irreps in $\mathrm{Irr}(S_{n,m})$ will be of particular importance.

▶ **Definition 11** (Minimal and Maximal Irreps). *For any $\lambda \vdash n$, the* minimal irrep *and* maximal irrep *(w.r.t. λ) is $\lambda \otimes \bar{\lambda} \in Irr(S_{n,m})$ and $\lambda \otimes (m-n, \lambda) \in Irr(S_{n,m})$ respectively.*

If $\lambda_1 \geq n - \sqrt{n}$, Theorem 7 implies that the minimal and maximial irreps w.r.t. λ are indeed of the least and largest dimension over all irreps of the form $\lambda \otimes \mu \in \mathrm{Irr}(S_{n,m})$ for sufficiently large m.

For $\lambda \vdash m$, let E_λ be the orthogonal projector onto the λ-isotypic component $K_{\lambda,(m-n,1^n)}\mathcal{V}_\lambda$ of $\mathcal{M}^{(m-n,1^n)}$, which we may write as

$$E_\lambda = \frac{d_\lambda}{m!}\mathcal{M}^{(m-n,1^n)}(\overline{\chi_\lambda})$$

where $\mathcal{M}^{(m-n,1^n)}(\overline{\chi}_\lambda) = \sum_{\sigma \in S_m} \chi_\lambda(\sigma^{-1})\mathcal{M}^{(m-n,1^n)}(\sigma)$ is the Fourier transform of the function $\overline{\chi}_\lambda \in \mathbb{C}[S_m]$ with respect to the permutation representation of S_m acting on $S_{n,m}$. In particular, for any $\zeta \in \mathbb{C}[S_{n,m}]$ and $f \in S_{n,m}$, we have

$$[E_\lambda \zeta](f) = \frac{d_\lambda}{m!} \sum_{\sigma \in S_m} \chi_\lambda(\sigma)\zeta(\sigma^{-1} f)$$

using the well-known fact that $\chi_\lambda(\sigma^{-1}) = \chi_\lambda(\sigma)$ for any $\sigma \in S_m$, $\lambda \vdash m$. From our foregoing discussion, we also have that

$$E_\lambda E_{\mu\otimes\lambda} = E_{\mu\otimes\lambda}$$

where $E_{\mu\otimes\lambda}$ is the orthogonal projector onto $(\mathcal{V}_\mu \otimes \mathcal{V}_\lambda)$ for all $(\mu \otimes \lambda) \in \mathrm{Irr}(S_{n,m})$.

For any integer $k \geq 0$, one may think of the following as a "low-frequency" subspace of $\mathbb{C}[S_{n,m}]$ parameterized by k:

$$\mathcal{U}_k := \bigoplus_{\substack{(\mu\otimes\lambda)\in\mathrm{Irr}(S_{n,m}) \\ m-\lambda_1\leq k}} \mathcal{V}_\mu \otimes \mathcal{V}_\lambda \cong \bigoplus_{\substack{\lambda\vdash m \\ m-\lambda_1\leq k}} K_{\lambda,(m-n,1^n)}\mathcal{V}_\lambda.$$

Equivalently, we have

$$\mathcal{U}_k \cong \{\zeta \in \mathbb{C}[S_{n,m}] : \lambda(\zeta) = 0 \text{ for all } \lambda \vdash m \text{ such that } m - \lambda_1 > k\}$$

where we have identified $\mathbb{C}[S_{n,m}]$ with the space of functions $\zeta \in \mathbb{C}[S_m]$ that are constant on the cosets S_m/S_{m-n}. Let $\alpha = \{(x_1, \alpha(x_1)), (x_2, \alpha(x_2)), \cdots, (x_k, \alpha(x_k))\}$, be an injective function from $[n]$ to $[m]$, which we represent as a set of k ordered pairs, and define

$$S_\alpha := \{f \in S_{n,m} : f(x_j) = \alpha(x_j) \text{ for all } 1 \leq j \leq k\}.$$

Theorem 12 shows that the characteristic functions of S_α have "low Fourier-complexity", namely, they are supported on the "low" Fourier levels of $\mathbb{C}[S_{n,m}]$ (i.e., $\mathrm{Irr}(S_{n,m})$), which are in reverse-lexicographic order on the partitions $\lambda' \vdash m$ corresponding to their S_m-irrep. One can compare these functions to the so-called *k-juntas* in area of Boolean functions, as their output is determined by examining no more than k "coordinates" of its input [19]. Such junta generalizations have been fundamental to some recent developments in extremal combinatorics (see [8, 7] for example). The proof of Theorem 12 resembles [8, Theorem 7], which we defer to Appendix D.

▶ **Theorem 12.** *Let $1_\alpha \in \mathbb{C}[S_{n,m}]$ be the characteristic function of the family S_α. Then $1_\alpha \in \mathcal{U}_k$.*

An immediate corollary of this theorem is the following.

▶ **Corollary 13.** *Let $1_\alpha \in \mathbb{C}[S_{n,m}]$ be the characteristic function of the family S_α. Then $E_{\mu\otimes\lambda}1_\alpha = 0$ for all λ with more than k cells below the first row.*

4 The Partial Permutation Association Scheme

The theory of association schemes will be a convenient language for describing the algebraic and combinatorial components of our work. We refer the reader to Bannai and Ito's reference [3] for a more thorough treatment.

▶ **Definition 14** (Association Schemes). *A* symmetric association scheme *is a collection of $d+1$ binary $|X| \times |X|$ matrices $\mathcal{A} = \{A_0, A_1, \cdots, A_d\}$ over a set X that satisfy the following axioms:*

1. *A_i is symmetric for all $0 \leq i \leq d$,*
2. *$A_0 = I$ where I is the identity matrix,*
3. *$\sum_{i=0}^{d} A_i = J$ where J is the all-ones matrix, and*
4. *$A_iA_j = A_jA_i \in Span\{A_0, A_1, \cdots, A_d\} =: \mathfrak{A}$ for all $0 \leq i, j \leq d$.*

The matrices $A_1, A_2, \cdots, A_d$ are called the associates*, and the algebra $\mathfrak{A}$ is called the* Bose–Mesner *algebra of the association scheme.*

Since the all-ones matrix commutes with every associate, the matrices of an association scheme have constant row sum and constant column sum. Also, since the matrices of a symmetric association scheme are symmetric and commute with each other, they are simultaneously diagonalizable (equivalently, they share a system of orthonormal eigenvectors), which implies that $\mathfrak{A}$ admits a unique basis of *primitive idempotents* $E_0, E_1, \cdots, E_d$, i.e., $E_i^2 = E_i$ for all $0 \leq i \leq d$ and $\sum_{i=0}^{d} E_i = I$.

Since the permutation representation of $S_n \times S_m$ acting on $S_{n,m}$ is multiplicity-free (see Theorem 9), the orbits $A_0, A_1, \cdots, A_d$ (so-called *orbitals*) of the action of $S_n \times S_m$ on ordered pairs $S_{n,m} \times S_{n,m}$ forms a *symmetric association scheme* (see [3] for a proof). We abuse the notation, and also use A_i to denote the binary matrix with entries 1 corresponding to exactly those pairs that are in the orbit A_i. Let $\mathcal{A}_{n,m} := \{I, A_1, \cdots, A_d\}$ denote the *n-partial permutation association scheme of* $[m]$.

Although it is well-known that permutation representation of $S_n \times S_m$ acting on $S_{n,m}$ is multiplicity-free (see [2, 5, 12] for example), the parameters of its corresponding association scheme $\mathcal{A}_{n,m}$ have not been worked out (to the best of our knowledge). We now give a more in-depth treatment of the partial permutation association scheme.

4.1 The Associates

The following is a more combinatorial definition of the associates of $\mathcal{A}_{n,m}$ that gives a combinatorial bijection between the associates of $\mathcal{A}_{n,m}$ and $\mathrm{Irr}(S_{n,m})$, which are the eigenspaces of the association scheme. The bijection is readily observed by thinking of each element of $S_{n,m}$ graphically as a maximum matching of the complete bipartite graph $K_{n,m}$ (see Figure 3).

Let $f_{\mathrm{id}} = (1, 2, \cdots, n)$ denote the *identity n-partial permutation*, which we can view as the maximum matching of $K_{n,m}$ that pairs 1 with 1, 2 with 2, and so on (e.g., the red matching in Figure 3). For any two maximum matchings f, f' of $K_{n,m}$, let $G(f, f')$ be the multigraph whose edge multiset is the multiset union $f \cup f'$. Clearly $G(f, f') = G(f', f)$ and this graph is composed of disjoint even cycles and disjoint even paths. Let c denote the number of disjoint cycles and let $2\lambda_i$ denote the length of an even cycle. Let p denote the number of disjoint paths and let $2\rho_i$ denote the length of an even path. If we order the cycles and paths respectively from longest to shortest and divide each of their lengths by two, assuming $m \geq 2n$, we see that the graphs $G(f, f')$ are in bijection (up to graph isomorphism) with pairs $(\lambda|\rho)$ of integer partitions $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_c), \rho = (\rho_1, \rho_2, \cdots, \rho_p)$ such that $(\lambda_1, \cdots, \lambda_c, \rho_1, \cdots, \rho_p) \vdash n$. Let $\mathrm{d}(f, f') := (\lambda|\rho)$ denote this bijection, which we refer to as the *cycle-path type of f' with respect to f*. Note that $\mathrm{d}(\sigma(f), \sigma(f')) = \mathrm{d}(f, f')$ for all n-partial permutations f, f' and all $\sigma \in S_n \times S_m$. If one of the arguments is the identity matching, then we say $\mathrm{d}(f) := \mathrm{d}(f_{\mathrm{id}}, f)$ is *the cycle-path type of f*. Illustrations of the graphs $G_{(\varnothing|n)}$ and $G_{(n-1|1)}$, and $G_{(\varnothing|1^n)}$ are provided in Figure 3 where $n = 3$ and $m = 6$.

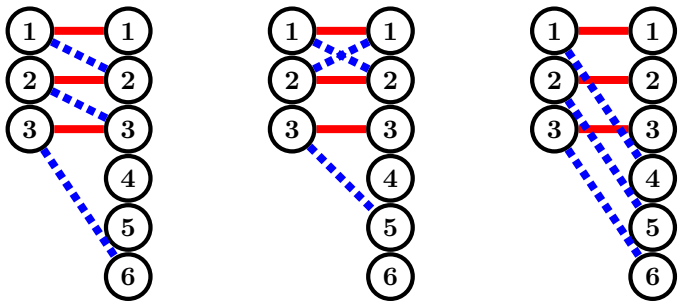
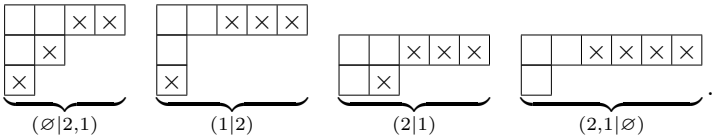


Figure 3 $(2, 3, 6)$ on the left has type $(\varnothing|3)$, $(2, 1, 5)$ has type $(2|1)$, and $(4, 5, 6)$ has type $(\varnothing|1^3)$.

Let $\mathcal{C}_n := \{(\lambda|\rho)\colon |\lambda| + |\rho| = n\}$ where λ and ρ are partitions. When $m \geq 2n$, $\mathcal{C}_n$ is the set of all cycle-path types. Note that $(\varnothing|1^n)$ is not a cycle-path type when $m < 2n$, and for $m = n$, all cycle-path types are of form $(\lambda|\varnothing)$, where $\lambda \vdash n$. We can decompose $\mathcal{C}_n$ as a disjoint union $\mathcal{C}_n = \bigcup_{k=0}^{n} \mathcal{C}_{n,k}$, where $\mathcal{C}_{n,k}$ consists of all $(\lambda|\rho) \in \mathcal{C}_n$ such that $l(\rho) = n - k$.

Recall that any irrep in $\mathrm{Irr}(S_{n,m})$ is of the form $\lambda \otimes \lambda'$ where λ'/λ is a horizontal strip of size $m - n$. To see that cycle-path types $(\tau|\rho)$ have a natural correspondence with these irreducibles, consider a Young diagram of λ' such that the cells of λ'/λ are marked. Every columns of λ in λ' with a marked cell below it corresponds to a part in ρ whereas an unmarked column correspond to a part in τ. For instance, taking $\lambda = (2, 1)$ and $m = 7$, we have



Note that marked singleton columns correspond to paths of length zero (i.e., isolated nodes). For each cycle-path type $(\tau|\rho)$, the $(\tau|\rho)$-*associate* of $\mathcal{A}_{n,m}$ is the following $m^{\underline{n}} \times m^{\underline{n}}$ binary matrix:

$$(A_{(\tau|\rho)})_{i,j} = \begin{cases} 1, & \text{if } \mathrm{d}(i,j) = (\tau|\rho) \\ 0, & \text{otherwise} \end{cases}$$

where $i, j \in S_{m,n}$.

4.2 The Valencies and Multiplicities

For each $0 \leq i \leq d$, let $d_i := \operatorname{tr} E_i$ denote the *multiplicity* of the ith eigenspace of an association scheme, that is, the dimension of its ith eigenspace. For each $0 \leq i \leq d$, define the *valency* v_i to be the row sum of an arbitrary row of A_i (equivalently, the largest eigenvalue of A_i). We now give formulas for the valencies $v^{(m)}_{(\lambda|\rho)}$ and multiplicities $d_{(\lambda|\rho)}$ of $\mathcal{A}_{n,m}$.[4]

For each $(\lambda|\rho)$, define the $(\lambda|\rho)$-*sphere* to be the following set:

$$\Omega_{(\lambda|\rho)} := \{f \in S_{n,m} : \mathrm{d}(f) = (\lambda|\rho)\}.$$

The spheres partition $S_{n,m}$ and it useful to think of them as conjugacy classes. Indeed, when $n = m$, these spheres are the conjugacy classes of S_m. Note that $v^{(m)}_{(\lambda|\rho)} = |\Omega_{(\lambda|\rho)}|$, and basic combinatorial reasoning reveals the following.

▶ **Proposition 15.** *For any cycle-path type $(\lambda|\rho)$, the size of the $(\lambda|\rho)$-sphere is*

$$v^{(m)}_{(\lambda|\rho)} = |\Omega_{(\lambda|\rho)}| = \frac{n!}{\prod_{i=1}^{n} i^{\ell_i} \ell_i! r_i!} (m-n)^{\underline{l(\rho)}}$$

where $\lambda = (1^{\ell_1}, \cdots, n^{\ell_n})$, $\rho = (1^{r_1}, \cdots, n^{r_n})$, and $l(\rho) = r_1 + \cdots + r_n$.

We omit the superscript (m) of the valency when m is clear from the context.

The multiplicities $d_{(\tau|\rho)}$ are easy to deduce due to the fact that each eigenspace of the scheme is isomorphic to an irrep $\mu \otimes \lambda$ of $S_n \times S_m$, and that $\dim \mu \otimes \lambda = \dim \mu \cdot \dim \lambda$. As we have seen, these dimensions are counted by the hook rule. In particular, for a cycle-path type $(\tau|\rho)$, let $\tau \cup \rho$ be the union of the set of parts of the two partitions. Then we have $d_{(\tau|\rho)} = d_{\lambda \otimes \lambda'}$ such that $\lambda = (\tau \cup \rho)^\top \vdash n$, $\lambda' = (\tau \cup (m - n, \rho^\top)^\top)^\top$, and '$\top$' denotes the transpose partition.

[4] The "m" in the superscript (m) of the valency simply indicates the size of the domain of any $f \in S_{n,m}$. It is a notational convenience that will make some of our proofs easier to follow later in the paper.

4.3 The Johnson Ordering of $\mathcal{A}_{n,m}$

The *Johnson scheme* $\mathcal{J}(m,n)$ is a symmetric association scheme defined over the n-subsets of $[m]$. The ith associate $A_i \in \mathcal{J}(m,n)$ of the Johnson scheme is defined such that $(A_i)_{X,Y} = 1$ if $n - |X \cap Y| = i$, and is 0 otherwise for any two n-subsets X, Y. It is well-known that the ith eigenspace of $\mathcal{J}(m,n)$ is isomorphic to the S_m-irrep associated to the partition $(m-i,i) \vdash m$. For proofs of these facts and more, see [10]. Henceforth, let E_i be the primitive idempotent of the Johnson scheme that projects onto $\mathcal{V}_{(m-i,i)}$.

There exists a natural ordering of the $S_{n,m}$ that we call *the Johnson ordering* that shows the Johnson scheme is a "quotient" of $\mathcal{A}_{n,m}$. First, we order $S_{n,m}$ first by the corresponding n-subsets (the particular order does not matter). Next, we lexicographically order all $n!$ n-partial permutations that correspond to the same n-subset (i.e., share the same image). For example, for $n = 3$, we could have:

$$(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1),$$
$$(1,2,4),(1,4,2),(2,1,4),(2,4,1),(4,1,2),(4,2,1),$$
$$(1,3,4),(1,4,3),\cdots$$

Both S_n and S_m act on the indices and entries of an n-partial permutation respectively, and so each of their actions correspond to some collection of $m^{\underline{n}} \times m^{\underline{n}}$ permutation matrices (i.e., their corresponding permutation representations). The action of S_m on $S_{m,n}$ is transitive, but S_n's action has $\binom{m}{n}$ orbits, one for each n-subset. Note that on all $n!$ permutations of S_n corresponding to any given n-subset, the action of S_n corresponds to the regular representation of S_n.

Given $\lambda \vdash n$ and $\lambda' \vdash m$, let E_λ and $E_{\lambda'}$ be the orthogonal projectors on the λ-isotypic and λ'-isotypic subspaces, respectively. Since the actions of S_n and S_m on $S_{n,m}$ commute, E_λ and $E_{\lambda'}$ also commute, and we have $E_{\lambda \otimes \lambda'} = E_\lambda E_{\lambda'}$. From the specific way we ordered $S_{n,m}$ in the previous paragraph, for any $\lambda \vdash n$ we have

$$E_\lambda = I_{\binom{m}{n}} \otimes F_\lambda = \underbrace{F_\lambda \oplus F_\lambda \oplus \cdots \oplus F_\lambda}_{\binom{m}{n} \text{ times}},$$

where F_λ is the $n! \times n!$ orthogonal projector on the λ-isotypic subspace of the regular representation of S_n. Hence, we can write $E_{\lambda \otimes \lambda'}$ as a product of two block matrices:

$$E_{\lambda \otimes \lambda'} = \begin{pmatrix} B^{\lambda'}_{1,1} & B^{\lambda'}_{1,2} & \cdots \\ B^{\lambda'}_{2,1} & B^{\lambda'}_{2,2} & \\ \vdots & & \ddots \end{pmatrix} \begin{pmatrix} F_\lambda & 0 & \cdots \\ 0 & F_\lambda & \\ \vdots & & \ddots \end{pmatrix} = \begin{pmatrix} B^{\lambda'}_{1,1} F_\lambda & B^{\lambda'}_{1,2} F_\lambda & \cdots \\ B^{\lambda'}_{2,1} F_\lambda & B^{\lambda'}_{2,2} F_\lambda & \\ \vdots & & \ddots \end{pmatrix},$$

where the first matrix is $E_{\lambda'}$, in which each block $B^{\lambda'}_{i,j}$ is some $n! \times n!$ matrix.

Note that $F_{(n)} = J/n!$, where J is the $n! \times n!$ all-ones matrix. Thus, from the expression above, we have

$$E_{(n)\otimes(m-1,1)} = J/n! \otimes E_1 = \begin{pmatrix} b_{1,1} J & b_{1,2} J & \cdots \\ b_{2,1} J & b_{2,2} J & \\ \vdots & & \ddots \end{pmatrix},$$

where $b_{i,j}$ are scalars, $1/m^{\underline{n}}$ times the dual eigenvalues described above. Thus we have

$$E_{(n)\otimes(m-1,1)} \circ E_{\lambda\otimes\lambda'} = \begin{pmatrix} b_{1,1}B^{\lambda'}_{1,1}F_\lambda & b_{1,2}B^{\lambda'}_{1,2}F_\lambda & \cdots \\ b_{2,1}B^{\lambda'}_{2,1}F_\lambda & b_{2,2}B^{\lambda'}_{2,2}F_\lambda & \\ \vdots & & \ddots \end{pmatrix}, \tag{4.1}$$

which is orthogonal to E_μ (and thus $E_{\mu\otimes\mu'}$) for all $\mu \vdash n$ such that $\mu \neq \lambda$.

4.4 The Dual Eigenvalues of $\mathcal{A}_{n,m}$

A classic result in the theory of association schemes is that the primitive idempotents can be written as a linear combination of associates weighted by the dual eigenvalues of the scheme (see [9, Ch. 2.1]). In our case, we have

$$E_{\lambda\otimes\lambda'} = \frac{1}{m^{\underline{n}}} \sum_{(\mu|\rho)\in\mathcal{C}_n} q_{\lambda\otimes\lambda'}(\mu|\rho) A_{(\mu|\rho)},$$

and these coefficients $q_{\lambda\otimes\lambda'}(\mu|\rho)$ are the *dual eigenvalues* of $\mathcal{A}_{m,n}$.

The dual eigenvalues corresponding to minimal and maximal irreps play a central role in the proof of our main result. Let us consider matrices in the Bose–Mesner algebra $\mathfrak{A}_{n,m}$ of the partial permutation association scheme. By symmetry, every such matrix can be specified by a row or column corresponding to a single n-partial permutation of $[m]$.

Note that

$$(E_{\lambda\otimes\lambda'})_{f,h} = \frac{q_{\lambda\otimes\lambda'}(\mathrm{d}(f,h))}{m^{\underline{n}}}$$

and that

$$\sum_{f\in S_{n,m}} q_{\lambda\otimes\lambda'}(\mathrm{d}(f,h))\ 1_f = m^{\underline{n}}\,(E_{\lambda\otimes\lambda'})_h \in \lambda\otimes\lambda'$$

for all $\lambda\otimes\lambda'$ and $f,h \in S_{n,m}$, where $1_f \in \mathbb{C}[S_{n,m}]$ denotes the binary unit vector with the unique 1 in position f. The projector $E_{\lambda'}$ onto the λ'-isotypic component can be written as

$$(E_{\lambda'})_{f,h} = \frac{d_{\lambda'}}{m!} \sum_{\sigma\in S_m} \chi_{\lambda'}(\sigma^{-1})(V_\sigma)_{f,h}.$$

where $V_\sigma : 1_f \mapsto 1_{\sigma * f}$ for all $f,h \in S_{n,m}$. The foregoing, and the fact that $E_{\lambda'}E_{\lambda\otimes\lambda'} = E_{\lambda\otimes\lambda'}$ implies the following proposition.

▶ **Proposition 16.** *For any $f,h \in S_{n,m}$, $\lambda \vdash n$, and $\lambda' \vdash m$, we have*

$$q_{\lambda\otimes\lambda'}\big(\mathrm{d}(f,h)\big) = \frac{d_{\lambda'}}{m!} \sum_{\sigma\in S_m} \chi_{\lambda'}(\sigma)\, q_{\lambda\otimes\lambda'}\big(\mathrm{d}(\sigma^{-1} * f, h)\big).$$

▶ **Lemma 17.** *Let $q_i(j)$ be a dual eigenvalue of the Johnson scheme $\mathcal{J}(m,n)$. Then we have*

$$q_1(j) = \frac{\binom{n}{m}}{\binom{m-2}{n-1}} \left(n - j - \frac{n^2}{m}\right).$$

Moreover, if $m \geq n^2$, then $q_i(j) \geq 0$ for all $j \neq n$.

Proof. Let $p_i(j)$ denote the j-th eigenvalue of the i-th associate of the Johnson scheme $\mathcal{J}(m,n)$. It is well-known (see [10] for example) that

$$p_i(j) = \sum_{r=i}^{n} (-1)^{(r-i+j)} \binom{r}{i} \binom{m-2r}{n-r} \binom{m-r-j}{r-j}.$$

Let P be the $(n+1) \times (n+1)$ matrix defined such that $P_{j,i} = p_i(j)$. As their name suggests, the dual eigenvalues $Q_{j,i} := q_i(j)$ are formally dual to the eigenvalues of the association scheme, that is, $Q = \binom{m}{n} P^{-1}$. Inverting P reveals that

$$Q_{j,1} = q_1(j) = \frac{\binom{m}{n}}{\binom{m-2}{n-1}} \left(n - j - \frac{n^2}{m} \right),$$

which is non-negative for all $m \geq n^2$ and $j \neq n$, which completes the proof. ◀

▶ **Lemma 18.** *For all $\mu \in \mathcal{C}_{n,k}$, we have*

$$q_{(n)\otimes(m-1,1)}(\mu) = \frac{(km - n^2)(m-1)}{n(m-n)}.$$

Proof. Recall that the ith eigenspace of the Johnson scheme $\mathcal{J}(m,n)$ is isomorphic to the S_m-irrep associated to the partition $(m-i,i) \vdash m$, and that E_i denotes the primitive idempotent of the Johnson scheme that projects onto its $(m-i,i)$ eigenspace. Since

$$E_{(n)\otimes(m-1,1)} = \frac{J}{n!} \otimes E_1,$$

Lemma 17 implies that

$$\begin{aligned} E_1 &= \frac{1}{\binom{n}{m}} \sum_{j=0}^{n} \left[\frac{\binom{n}{m}}{\binom{m-2}{n-1}} \left(n - j - \frac{n^2}{m} \right) \right] A_j \\ &= \frac{1}{\binom{m-2}{n-1}} \sum_{j=0}^{n} \left(n - j - \frac{n^2}{m} \right) A_j. \end{aligned}$$

Since $(A_j)_{X,Y} = 1$ only if $|X \cap Y| = n - j$, we have the dual eigenvalue

$$\left(m^n E_{(n)\otimes(m-1,1)}\right)_{f,h} = m^n \frac{|\mathrm{im}\ f \cap \mathrm{im}\ h| - n^2/m}{n!\binom{m-2}{n-1}} = \frac{(m-1)(|\mathrm{im}\ f \cap \mathrm{im}\ h| m - n^2)}{n(m-n)}.$$

It follows that

$$q_{(n)\otimes(m-1,1)}(\mu) = \frac{(km - n^2)(m-1)}{n(m-n)}$$

for all $\mu \in \mathcal{C}_{n,k}$, which completes the proof. ◀

5 A sufficient condition on Krein parameters

Recall that $\circ$ denotes the Schur (entrywise) product of two matrices.

▶ **Definition 19** (Krein Parameters). *Let $\mathcal{A}$ be an association scheme on v vertices with d associates. For any $0 \leq i,j \leq d$, there exist constants $q_{i,j}(k)$ such that*

$$E_i \circ E_j = \frac{1}{v} \sum_{k=0}^{d} q_{i,j}(k) E_k,$$

which are called the Krein parameters *of $\mathcal{A}$. More explicitly, we have*

$$q_{i,j}(k) = v\frac{\operatorname{tr}\left[E_k(E_i \circ E_j)\right]}{d_k}.$$

For more details on the Krein parameters of an association scheme, see [3]. The Krein parameters can alternatively be written as

$$q_{i,j}(k) = \frac{1}{vd_k}\sum_{\ell=0}^{d}\frac{q_i(\ell)q_j(\ell)\overline{q_k(\ell)}}{v_\ell} = \frac{d_i d_j}{v}\sum_{\ell=0}^{d}\frac{\overline{p_i(\ell)p_j(\ell)}p_k(\ell)}{v_\ell^2}, \tag{5.1}$$

where $p_i(j)$ denotes the j-th eigenvalue of A_i and $q_i(j)$ denotes the jth *dual eigenvalue* of E_i (see [9, Chap. 2.4] for a proof).

To prove the lower bound on non-coherent Index Erasure, we use the same adversary matrix Γ as [2] used for the coherent case.[5] For simplifying the equations, without loss of generality let us assume that n is a square. As in [2], we choose

$$\Gamma := \sum_{k=0}^{\sqrt{n}}(\sqrt{n}-k)\sum_{\lambda\vdash k}E_{(n-k,\lambda)\otimes(m-k,\lambda)},$$

and thus the orthogonal projection onto its image is

$$\Pi_\Gamma := \sum_{\lambda\colon|\lambda|<\sqrt{n}}E_{(n-|\lambda|,\lambda)\otimes(m-|\lambda|,\lambda)}.$$

Note that the sole principal eigenvector ω of Γ is the uniform superposition over $\mathcal{F}$ (i.e., $\omega_f = 1/\sqrt{m^{\underline{n}}}$ for all $f\in\mathcal{F}$). Thus, as per Corollary 3, we are interested in the quantity

$$\eta = \max_{T\in\mathcal{T}}\operatorname{tr}\left[\Pi_\Gamma\frac{(T\circ T^{\odot})}{m^{\underline{n}}}\right].$$

For any primitive idempotent $E_{\lambda\otimes\lambda'}$, let

$$T_{\lambda\otimes\lambda'} := \left(\frac{m^{\underline{n}}}{\operatorname{tr}E_{\lambda\otimes\lambda'}}\right)E_{\lambda\otimes\lambda'} = \left(\frac{m^{\underline{n}}}{d_{\lambda\otimes\lambda'}}\right)E_{\lambda\otimes\lambda'}$$

be its corresponding state matrix. In [2] it is shown that the target matrix can be written as

$$T^{\odot} = \frac{n}{m}T_{(n)\otimes(m)} + \left(1-\frac{n}{m}\right)T_{(n)\otimes(m-1,1)}.$$

In the coherent case, recall that $T = J$, and therefore

$$\eta = \operatorname{tr}\left[\Pi_\Gamma\frac{T^{\odot}}{m^{\underline{n}}}\right] = \frac{n}{m}\operatorname{tr}\left[\frac{T_{(n)\otimes(m)}}{m^{\underline{n}}}\right] = \frac{n}{m}.$$

The most technically involved part of the proof of the lower bound by [2] is proving that $\|\Delta_x\circ\Gamma\| = \mathrm{O}(1)$. Since we are using the same adversary matrix Γ, we already have the above bound on $\|\Delta_x\circ\Gamma\|$. Our goal is to show that $\operatorname{tr}\left[\Pi_\Gamma(T\circ T^{\odot})/m^{\underline{n}}\right]$ is small for *all* state matrices T.

[5] Technically, the adversary matrix used here is $\sqrt{n}$ times that of [2] as the adversary method they use places slightly different conditions on the adversary matrix.

By dividing the elements in the set $\mathcal{T}$ by $m^{\underline{n}}$ we obtain the set of all density matrices (positive-semidefinite Hermitian matrices with trace 1) of the Bose–Mesner algebra $\mathfrak{A}_{n,m}$. Note that $(T \circ T')/m^{\underline{n}}$ is a density matrix for all $T, T' \in \mathcal{T}$.

For any $T \in \mathcal{T}$, we have

$$\operatorname{tr}\left[\Pi_\Gamma \frac{\big(T \circ T_{(n)\otimes(m)}\big)}{m^{\underline{n}}}\right] = \operatorname{tr}\left[\Pi_\Gamma \frac{T}{m^{\underline{n}}}\right] \leq 1,$$

therefore

$$\operatorname{tr}\left[\Pi_\Gamma \frac{\big(T \circ T^{\odot}\big)}{m^{\underline{n}}}\right] \leq \frac{n}{m} + \left(1 - \frac{n}{m}\right) \operatorname{tr}\left[\Pi_\Gamma \frac{\big(T \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}}\right].$$

Our goal is to bound the latter term:

$$\left(1 - \frac{n}{m}\right) \operatorname{tr}\left[\Pi_\Gamma \frac{\big(T \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}}\right]. \tag{5.2}$$

First note that

$$\mathcal{T} = \left\{\sum_\chi c_\lambda T_\chi \colon \sum_\chi c_\chi = 1 \text{ and } c_\chi \geq 0\right\},$$

where the sums range over $\chi \in \operatorname{Irr}(S_{n,m})$. Hence,

$$\begin{aligned}\max_{T\in\mathcal{T}} \operatorname{tr}\left[\Pi_\Gamma \frac{\big(T \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}}\right] &= \max_{\substack{\{c_\chi \geq 0\}_\chi \\ \sum_\chi c_\chi = 1}} c_\chi \operatorname{tr}\left[\Pi_\Gamma \frac{\big(T_\chi \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}}\right] \\ &= \max_\chi \operatorname{tr}\left[\Pi_\Gamma \frac{\big(T_\chi \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}}\right].\end{aligned}$$

The following proposition simplifies (5.2).

▶ **Proposition 20.** *For any $\lambda = (n - |\nu|, \nu)$ and $\bar{\lambda} = (m - |\nu|, \nu)$, we have*

$$\operatorname{tr}\left[\Pi_\Gamma \frac{\big(T_{\lambda\otimes\lambda'} \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}}\right] = \operatorname{tr}\left[E_{\lambda\otimes\bar{\lambda}} \frac{\big(T_{\lambda\otimes\lambda'} \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}}\right].$$

Proof. By Equation (4.1), if $|\nu| < \sqrt{n}$, then we have

$$\begin{aligned}\Pi_\Gamma \frac{\big(T_{\lambda\otimes\lambda'} \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}} &= \sum_{\mu\colon |\mu|<\sqrt{n}} E_{(n-|\mu|,\mu)\otimes(m-|\mu|,\mu)} \frac{\big(T_{\lambda\otimes\lambda'} \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}} \\ &= E_{(n-|\nu|,\nu)\otimes(m-|\nu|,\nu)} \frac{\big(T_{\lambda\otimes\lambda'} \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}} \\ &= E_{\lambda\otimes\bar{\lambda}} \frac{\big(T_{\lambda\otimes\lambda'} \circ T_{(n)\otimes(m-1,1)}\big)}{m^{\underline{n}}};\end{aligned}$$

otherwise, the left-hand and right-hand side are both 0, which completes the proof. ◀

The proposition above now allows us to bound (5.2) for all $\lambda \vdash n$ having no more than $\sqrt{n}$ cells under its first row.

▶ **Corollary 21.** *Suppose $\lambda \vdash n$ has no more than $\sqrt{n}$ cells below the first row. Then*

$$\operatorname{tr}\left[E_{\lambda\otimes\bar{\lambda}}\frac{\left(T_{(n)\otimes(m-1,1)}\circ T_{\lambda\otimes\lambda'}\right)}{m^{\underline{n}}}\right] \in \mathrm{O}(\sqrt{n}/m)$$

for all $\lambda' \neq \bar{\lambda}$.

Proof. Let $\operatorname{sum}[\cdot]$ denote the sum of the entries of the matrix. We have

$$\begin{aligned}\operatorname{tr}\left[E_{\lambda\otimes\bar{\lambda}}\frac{\left(T_{(n)\otimes(m-1,1)}\circ T_{\lambda\otimes\lambda'}\right)}{m^{\underline{n}}}\right] &= \frac{1}{d_{\lambda\otimes\lambda'}}\operatorname{sum}\left[E_{\lambda\otimes\bar{\lambda}}\circ T_{(n)\otimes(m-1,1)}\circ E_{\lambda\otimes\lambda'}\right]\\ &= \frac{d_{\lambda\otimes\bar{\lambda}}}{d_{\lambda\otimes\lambda'}}\operatorname{tr}\left[E_{\lambda\otimes\lambda'}\frac{\left(T_{(n)\otimes(m-1,1)}\circ T_{\lambda\otimes\bar{\lambda}}\right)}{m^{\underline{n}}}\right]\end{aligned}$$

Since $\left(T_{(n)\otimes(m-1,1)}\circ T_{\lambda\otimes\bar{\lambda}}\right)/m^{\underline{n}}$ is a density matrix, the trace on the right-hand side is at most 1. We now have

$$\leq \frac{d_{\bar{\lambda}}}{d_{\lambda'}} \in \mathrm{O}(\sqrt{n}/m),$$

where the asymptotic bound follows from Corollary 8, completing the proof. ◀

We therefore have

$$\eta = \mathrm{O}\left(\frac{n}{m} + \operatorname{tr}\left[E_{\lambda\otimes\bar{\lambda}}\frac{\left(T_{\lambda\otimes\bar{\lambda}}\circ T_{(n)\otimes(m-1,1)}\right)}{m^{\underline{n}}}\right]\right),$$

and it remains to bound the value

$$\begin{aligned}\operatorname{tr}\left[E_{\lambda\otimes\bar{\lambda}}\frac{\left(T_{\lambda\otimes\bar{\lambda}}\circ T_{(n)\otimes(m-1,1)}\right)}{m^{\underline{n}}}\right] &= \frac{m^{\underline{n}}}{(m-1)d_{\lambda\otimes\bar{\lambda}}}\operatorname{sum}\left[E_{(n)\otimes(m-1,1)}\circ E_{\lambda\otimes\bar{\lambda}}\circ E_{\lambda\otimes\bar{\lambda}}\right]\\ &= \frac{\sum_{\mu\in\mathcal{C}_n} v_\mu^{(m)}\cdot q_{(n)\otimes(m-1,1)}(\mu)\cdot q^2_{\lambda\otimes\bar{\lambda}}(\mu)}{m^{\underline{n}}(m-1)d_{\lambda\otimes\bar{\lambda}}}. \qquad (5.3)\end{aligned}$$

In the next section we show that, under the assumption that $m \geq n^{3\sqrt{n}}$, the value of (5.3), and thus η, is in $\mathrm{O}(1/\sqrt{n})$.

Note that, according to the expression (5.1) for Krein parameters, (5.3) is equal to

$$\frac{q_{\lambda\otimes\bar{\lambda},\,\lambda\otimes\bar{\lambda}}((n)\otimes(m-1,1))}{d_{\lambda\otimes\bar{\lambda}}} = \frac{q_{\lambda\otimes\bar{\lambda},\,(n)\otimes(m-1,1)}(\lambda\otimes\bar{\lambda})}{m-1},$$

and therefore the task of bounding (5.3) is the task of bounding Krein parameters

$$q_{\lambda\otimes\bar{\lambda},\,\lambda\otimes\bar{\lambda}}((n)\otimes(m-1,1)) \quad\text{and}\quad q_{\lambda\otimes\bar{\lambda},\,(n)\otimes(m-1,1)}(\lambda\otimes\bar{\lambda}).$$

6 Bounding relevant Krein parameters

Let $(\mathfrak{A}_{n,m})_{f_{\mathrm{id}}}$ denote the space of the columns of matrices in the Bose–Mesner algebra $\mathfrak{A}_{n,m}$ corresponding to f_{id}. For brevity, we call such columns *characteristic columns*. Note that, due to symmetry, $\phi \in (\mathfrak{A}_{n,m})_{f_{\mathrm{id}}}$ is the characteristic column of exactly one matrix in

$\mathfrak{A}_{n,m}$, in effect defining one-to-one correspondence between $(\mathfrak{A}_{n,m})_{f_{\mathrm{id}}}$ and $\mathfrak{A}_{n,m}$. Since the characteristic column of any primitive idempotent $E_{\lambda\otimes\lambda'}$ is an eigenvector of the $(\lambda\otimes\lambda')$-eigenspace of $\mathcal{A}_{n,m}$, we have $\dim[(\mathfrak{A}_{n,m})_{f_{\mathrm{id}}} \cap (\lambda\otimes\lambda')] \geq 1$. Since the characteristic columns of $\mathcal{A}_{n,m}$ form an orthogonal basis for $(\mathfrak{A}_{n,m})_{f_{\mathrm{id}}}$, we have that $\dim(\mathfrak{A}_{n,m})_{f_{\mathrm{id}}} = |\mathcal{C}_n|$. These facts imply the following proposition.

▶ **Proposition 22.** *For any $\lambda\otimes\lambda' \in \mathrm{Irr}(S_{n,m})$, we have* $\dim[(\mathfrak{A}_{n,m})_{f_{\mathrm{id}}} \cap (\lambda\otimes\lambda')] = 1$.

We let $1_f \in \mathbb{C}[S_{n,m}]$ denote the binary unit vector with the unique 1 in position f. For $\mu \in \mathcal{C}_n$, let

$$1_\mu := \sum_{f\colon \mathrm{d}(f)=\mu} 1_f.$$

6.1 Assignments

We call an injective function $\alpha\colon D \to [n]$ with $D = \mathrm{dom}(\alpha) \subseteq [n]$ an *assignment*. Let $|\alpha| := |\mathrm{dom}(\alpha)| = |\mathrm{im}(\alpha)|$, which we call the *weight* of α. We say that $f \in S_{n,m}$ *agrees* with α if $f(x) = \alpha(x)$ for all $x \in \mathrm{dom}(\alpha)$, and we write $\alpha \rightsquigarrow f$; in other words, $f \in S_\alpha$ In particular, there are $(m-|\alpha|)^{\underline{n-|\alpha|}}$ partial permutations in $S_{n,m}$ that agree with α. Recall that

$$1_\alpha = \sum_{f\colon \alpha\rightsquigarrow f} 1_f.$$

For any assignment α and any permutation $\pi \in S_n$, define assignments α^{-1} and $\alpha * \pi^{-1}$ with domains $\mathrm{im}(\alpha)$ and $\pi(\mathrm{dom}(\alpha))$ respectively in the natural way. Note that the image of both α and $\alpha*\pi^{-1}$ is the same. Since the action of $\pi \in S_n$ maps $f \in S_{n,m}$ to $f*\pi^{-1}$, we have $\alpha \rightsquigarrow h$ if and only if $\pi(\alpha) \rightsquigarrow \pi(h)$. Hence, $V_\pi 1_\alpha = 1_{\pi(\alpha)}$, where $\pi \mapsto V_\pi$ is the representation of S_n defined as $V_\pi : 1_f \mapsto 1_{f*\pi^{-1}}$.

Consider $X := \{x_1, \cdots, x_k\} \subseteq [n]$ with $x_i < x_{i+1}$ for all i, and define $\alpha_X\colon [k] \to [n]$ such that $i \mapsto x_i$. Note that the set of all $\alpha^{-1} * \alpha_X$ such that $\mathrm{im}(\alpha) = X$ equals $S_{k,n}$, where we think of $S_{k,n}$ as the set of injective functions from $[k]$ to $[n]$. We define the cycle-path type of α to be

$$\mathrm{d}(\alpha) := \mathrm{d}(\alpha^{-1} * \alpha_X, \alpha_X) \in \mathcal{C}_k.$$

See Figure 4 for an illustration.

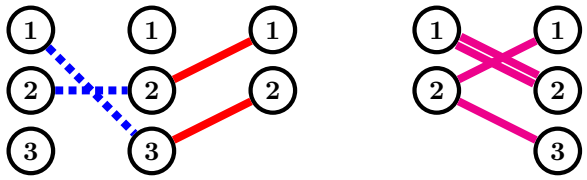


Figure 4 As an example, consider $n = 3$ and an assignment $\alpha\colon D \to [n]$ with $D = \{1,2\}$ defined as $\alpha(1) := 3$ and $\alpha(2) := 2$. The image of α is $X = \{2,3\}$, and thus α_X maps 2 to 1 and 3 to 2. The left picture depicts α with blue dashed lines and α_X^{-1} with red solid lines. The right picture depicts the multigraph resulting from the union of edges corresponding to $\alpha^{-1} * \alpha_X$ and α_X, from which we can see that $\mathrm{d}(\alpha) = (1|1)$.

Corollary 13 immediately implies the following proposition.

▶ **Proposition 23.** *For any assignment α and $\lambda' \vdash m$ such that $m - \lambda'_1 > |\alpha|$, we have $E_{\lambda'} 1_\alpha = 0$.*

6.2 Dual eigenvalues of minimal irreps

Suppose $\theta \vdash k$, and let us analyze the idempotent corresponding to the irrep $(n-k,\theta) \otimes (m-k,\theta)$. For a cycle-path type $\nu \in \mathcal{C}_k$, define

$$\phi_\nu := \sum_{\alpha\colon \mathrm{d}(\alpha)=\nu} 1_\alpha.$$

Note that $\phi_\nu \in (\mathfrak{A}_{n,m})_{f_{\mathrm{id}}}$. Consider the irrep

$$\xi_\theta := \theta \otimes (n-k,\theta) \in \mathrm{Irr}(S_k \times S_n).$$

We will be interested in its dual eigenvalues $q_{\xi_\theta}(\nu)$ for the $\mathcal{A}_{k,n}$ scheme.

▶ **Lemma 24.** *The characteristic column of $m^{\underline{n}} E_{(n-k,\theta)\otimes(m-k,\theta)}$ equals*

$$\phi_{\xi_\theta} := \frac{d_{(m-k,\theta)}}{\binom{n}{k} d_\theta} \sum_{\nu \in \mathcal{C}_k} q_{\xi_\theta}(\nu)\phi_\nu, \tag{6.1}$$

i.e., for any $\mu \in \mathcal{C}_n$ and $f \in S_{n,m}$ with $\mathrm{d}(f) = \mu$, we have $q_{(n-k,\theta)\otimes(m-k,\theta)}(\mu) = (\phi_{\xi_\theta})_f$.

Proof. First, note that $\phi_{\xi_\theta} \in (\mathfrak{A}_{n,m})_{f_{\mathrm{id}}}$ as $\phi_\nu \in (\mathfrak{A}_{n,m})_{f_{\mathrm{id}}}$ for all $\nu \in \mathcal{C}_k$. Recall that Proposition 22 implies that the intersection of $(\mathfrak{A}_{n,m})_{f_{\mathrm{id}}}$ and the $((n-k,\theta)\otimes(m-k,\theta))$-isotypic subspace is one-dimensional. Using this fact and the expression of the primitive idempotents in the $\mathcal{A}_{n,m}$ basis, to prove the first statement of the lemma, it suffices to show that

1. ϕ_{ξ_θ} belongs to the $(n-k,\theta)$-isotypic,
2. ϕ_{ξ_θ} belongs to the $(m-k,\theta)$-isotypic, and
3. that ϕ_{ξ_θ} has the right scaling $d_{(m-k,\theta)}/\binom{n}{k}d_\theta$.

Let us first prove statement (3). Any assignment α with $\mathrm{d}(\alpha) \neq (1^k|\varnothing)$ is incompatible with f_{id}, that is, $\alpha \not\rightsquigarrow f_{\mathrm{id}}$. By linearity, it follows that $(\phi_\nu)_{f_{\mathrm{id}}} = 0$ for $\nu \neq (1^k|\varnothing)$. On the other hand, there are $\binom{n}{k}$ assignments α with $\mathrm{d}(\alpha) = (1^k|\varnothing)$, and they all agree with f_{id}. We deduce that $(\phi_{(1^k|\varnothing)})_{f_{\mathrm{id}}} = \binom{n}{m}$, and

$$\begin{aligned}(\phi_{\xi_\theta})_{f_{\mathrm{id}}} = \frac{d_{(m-k,\theta)}}{d_\theta} q_{\xi_\theta}(1^k|\varnothing) &= d_{(n-k,\theta)} \cdot d_{(m-k,\theta)} \\ &= q_{(n-k,\theta)\otimes(m-k,\theta)}(1^n|\varnothing) \\ &= m^{\underline{n}} \left(E_{(n-k,\theta)\otimes(m-k,\theta)}\right)_{f_{\mathrm{id}},f_{\mathrm{id}}},\end{aligned}$$

where we have used the fact that $q_{\lambda\otimes\lambda'}(1^k|\varnothing)$ is the dimension of $(\lambda \otimes \lambda') \in \mathrm{Irr}(S_{k,n})$. This completes the proof of statement (3).

We now prove statement (1). Equation (6.1) can be written as

$$\phi_{\xi_\theta} = \frac{d_{(m-k,\theta)}}{\binom{n}{k} d_\theta} \sum_{\substack{X\subset[n]\\|X|=k}} \phi_{\xi_\theta,X},$$

where we define

$$\phi_{\xi_\theta,X} := \sum_{\nu\in\mathcal{C}_k} q_{\xi_\theta}(\nu) \sum_{\substack{\alpha\\ \mathrm{d}(\alpha)=\nu\\ \mathrm{im}(\alpha)=X}} 1_\alpha = \sum_{\substack{\alpha\\ \mathrm{im}(\alpha)=X}} q_{\xi_\theta}(\mathrm{d}(\alpha^{-1} * \alpha_X, \alpha_X)) 1_\alpha.$$

Hence,

$$\begin{aligned}
\left[E_{(n-k,\theta)}\right]\phi_{\xi_\theta,X} &= \sum_{\pi\in S_n}\sum_{\substack{\alpha\\ \mathrm{im}(\alpha)=X}} \frac{d_{(n-k,\theta)}\chi_{(n-k,\theta)}(\pi)}{n!} q_{\xi_\theta}(\mathrm{d}(\alpha^{-1}*\alpha_X,\alpha_X))1_{\alpha*\pi^{-1}}\\
&= \sum_{\pi\in S_n}\sum_{\substack{\tilde\alpha*\pi\\ \mathrm{im}(\tilde\alpha*\pi)=X}} \frac{d_{(n-k,\theta)}\chi_{(n-k,\theta)}(\pi)}{n!} q_{\xi_\theta}(\mathrm{d}((\tilde\alpha*\pi)^{-1}*\alpha_X,\alpha_X))1_{\tilde\alpha*\pi*\pi^{-1}}\\
&= \sum_{\substack{\tilde\alpha\\ \mathrm{im}(\tilde\alpha)=X}} \left(\sum_{\pi\in S_n} \frac{d_{(n-k,\theta)}\chi_{(n-k,\theta)}(\pi)}{n!} q_{\xi_\theta}(\mathrm{d}(\pi^{-1}*\tilde\alpha^{-1}*\alpha_X,\alpha_X))\right)1_{\tilde\alpha}\\
&= \sum_{\substack{\tilde\alpha\\ \mathrm{im}(\tilde\alpha)=X}} q_{\xi_\theta}(\mathrm{d}(\tilde\alpha^{-1}*\alpha_X,\alpha_X)1_{\tilde\alpha}\\
&= \phi_{\xi_\theta,X},
\end{aligned}$$

where the second to last equality follows from Proposition 16. By linearity, we deduce that $E_{(n-k,\theta)}\phi_{\xi_\theta} = \phi_{\xi_\theta}$, and thus ϕ_{ξ_θ} belongs to the $(n-k,\theta)$-isotypic subspace, completing the proof of statement (1).

Finally, we prove statement (2). Consider the irreps $\lambda\otimes\lambda' \in \mathrm{Irr}(S_{n,m})$ in the $(n-k,\theta)$-isotypic, which are of the form $(n-k,\theta)\otimes\lambda'$. If $\lambda' \neq (m-k,\theta)$, then λ' has more than k cells below its first row. But then Proposition 23 implies that ϕ_{ξ_θ} is orthogonal to all such $(n-k,\theta)\otimes\lambda'$ irreps, which finishes the proof of the first part of the lemma.

The second part of the lemma is a restatement of the first that is seen by expressing the primitive idempotents in the $\mathcal{A}_{n,m}$ basis, which completes the proof of the lemma. ◀

Recall that, for every $1 \le k \le \sqrt{n}$ and every $\theta \vdash k$, to upper bound

$$\frac{\sum_{\mu\in\mathcal{C}_n} v_\mu^{(m)} \cdot q_{(n)\otimes(m-1,1)}(\mu)\cdot q^2_{(n-k,\theta)\otimes(m-k,\theta)}(\mu)}{m^{\underline{n}}\ (m-1)\ d_{(n-k,\theta)}d_{(m-k,\theta)}} \tag{6.2}$$

$$= \frac{\sum_{\ell=k}^{n}\left((\ell m-n^2)\sum_{\mu\in\mathcal{C}_{n,\ell}} v_\mu^{(m)}\cdot q^2_{(n-k,\theta)\otimes(m-k,\theta)}(\mu)\right)}{m^{\underline{n}}\ n(m-n)\ d_{(n-k,\theta)}d_{(m-k,\theta)}} \tag{6.3}$$

where the second equality follows from Lemma 18. We break the latter sum into two parts, $\ell = k$ and $\ell > k$, then bound these parts individually.

6.3 Case $\ell = k$

Given a partition $\rho = (1^{r_1}, 2^{r_2}, \cdots, n^{r_n})$, define

$$\breve\rho := (1^{r_2}, 2^{r_3}, \cdots, (n-1)^{r_n}) \vdash |\rho| - l(\rho).$$

In terms of Young diagrams, the shape $\breve\rho$ is obtained from ρ by removing the first column. Similarly, for $\mu = (\lambda|\rho) \in \mathcal{C}_n$, define $\breve\mu := (\lambda|\breve\rho)$. In particular, for $\mu \in \mathcal{C}_{n,k}$, we have $\breve\mu \in \mathcal{C}_k$. Also note that, as long as $k \le n/2$, the operation $\rho \mapsto \breve\rho$ defines a one-to-one correspondence between $\mathcal{C}_{n,k}$ and $\mathcal{C}_k$.

Consider $f \in \Omega_\mu$ such that $\mu \in \mathcal{C}_{n,k}$. There exists exactly one assignment α of weight k such that $\alpha \rightsquigarrow f$. Moreover, this assignment satisfies $\mathrm{d}(\alpha) = \breve\mu$. Hence $(\phi_{\breve\mu})_f = 1$ and $(\phi_\nu)_f = 0$ for $\nu \in \mathcal{C}_k \setminus \{\breve\mu\}$. Lemma 24 then implies

$$q_{(n-k,\theta)\otimes(m-k,\theta)}(\mu) = \frac{d_{(m-k,\theta)}}{\binom{n}{k} d_\theta} q_{\xi_\theta}(\breve\mu). \tag{6.4}$$

We also relate the valencies of μ and $\breve\mu$ as follows.

▶ **Proposition 25.** *For $\mu \in \mathcal{C}_{n,k}$, we have $v_\mu^{(m)} = \binom{n}{k}(m-n)^{\underline{n-k}} v_{\breve{\mu}}^{(n)}$.*

Proof. Let $(\lambda|\rho) := \mu$ and $\rho = (1^{r_1}, \cdots, n^{r_n})$, so that $\breve{\mu} = (\lambda|\breve{\rho})$ and $\breve{\rho} = (2^{r_1}, \cdots, (n-1)^{r_n})$. We also have $l(\rho) = n-k$ and $l(\breve{\rho}) = n-k-r_1$. Using Proposition 15, we get

$$\frac{v_{(\lambda|\rho)}^{(m)}}{v_{(\lambda|\breve{\rho})}^{(n)}} = \frac{n!(m-n)^{\underline{n-k}}/r_1!}{k!(n-k)^{\underline{n-k-r_1}}} = \frac{n!(m-n)^{\underline{n-k}}}{k!(n-k)!} = \binom{n}{k}(m-n)^{\underline{n-k}}.$$

Rearranging gives the desired result. ◀

Finally, we need

$$\sum_{\nu \in \mathcal{C}_k} v_\nu^{(n)} q_{\xi_\theta}^2(\nu) = n^{\underline{k}} d_\theta d_{(n-k,\theta)}, \tag{6.5}$$

which holds because, for the primitive idempotent E_{ξ_θ} of $\mathcal{A}_{k,n}$, we have

$$d_{\xi_\theta} = \operatorname{Tr}\big[E_{\xi_\theta}\big] = \operatorname{Tr}\big[E_{\xi_\theta}^2\big] = n^{\underline{k}} \sum_{\nu \in \mathcal{C}_k} v_\nu^{(n)} \left(\frac{q_{\xi_\theta}(\nu)}{n^{\underline{k}}}\right)^2.$$

Putting everything together, we get

$$\begin{aligned}
&\frac{(km-n^2)\sum_{\mu \in \mathcal{C}_{n,k}} v_\mu^{(m)} q^2_{(n-k,\theta)\otimes(m-k,\theta)}(\mu)}{m^{\underline{n}} n(m-n) d_{(n-k,\theta)} d_{(m-k,\theta)}} \\
&= \frac{(km-n^2)\sum_{\nu \in \mathcal{C}_k} \binom{n}{k}(m-n)^{\underline{n-k}} v_\nu^{(n)} \left(\frac{d_{(m-k,\theta)}}{\binom{n}{k} d_\theta} q_{\xi_\theta}(\nu)\right)^2}{m^{\underline{n}} n(m-n) d_{(n-k,\theta)} d_{(m-k,\theta)}} \\
&= \frac{km-n^2}{n(m-n)} \cdot \frac{(m-n)^{\underline{n-k}}}{m^{\underline{n}}} \cdot \frac{d_{(m-k,\theta)} \sum_{\nu \in \mathcal{C}_k} v_\nu^{(n)} q_{\xi_\theta}^2(\nu)}{\binom{n}{k} d_{(n-k,\theta)} (d_\theta)^2} \\
&= \frac{km-n^2}{n(m-n)} \cdot \frac{(m-n)^{\underline{n-k}}}{m^{\underline{n}}} \cdot \frac{k! d_{(m-k,\theta)}}{d_\theta} \\
&\le \frac{km-kn}{n(m-n)} \cdot \frac{(m-n)^{\underline{n-k}}}{m^{\underline{n}}} \cdot \frac{k! m^{\underline{k}}/\mathsf{H}(\theta)}{k!/\mathsf{H}(\theta)} \\
&= \frac{k}{n} \cdot \frac{(m-n)^{\underline{n-k}}}{(m-k)^{\underline{n-k}}} \\
&\le k/n,
\end{aligned}$$

where the first equality is from (6.4) and Proposition 25, the third equality is from (6.5), and for the first inequality we have used

$$d_{(m-k,\theta)} = m!/\mathsf{H}((m-k,\theta)) \le m^{\underline{k}}/\mathsf{H}(\theta).$$

6.4 Case $\ell > k$

Now consider $f \in \Omega_\mu$ such that $\mu \in \mathcal{C}_{n,\ell}$ for $\ell > k$. There are exactly $\binom{\ell}{k}$ assignments α of weight k that agree with f. We therefore have

$$\left|\left(\sum_{\nu \in \mathcal{C}_k} q_{\xi_\theta}(\nu)\phi_\nu\right)_f\right| \le \max_{\nu \in \mathcal{C}_k} |q_{\xi_\theta}(\nu)| \cdot \left(\sum_{\nu \in \mathcal{C}_k} \phi_\nu\right)_f \qquad = q_{\xi_\theta}\big((1^k|\varnothing)\big)\binom{\ell}{k} = d_{\xi_\theta}\binom{\ell}{k},$$

and Lemma 24 implies

$$|q_{(n-k,\theta)\otimes(m-k,\theta)}(\mu)| = |(\phi_{\xi_\theta})_f| \leq d_{(m-k,\theta)} d_{(n-k,\theta)} \ell^{\underline{k}} / n^{\underline{k}}. \tag{6.6}$$

We can also see that

$$\sum_{\mu \in \mathcal{C}_{n,\ell}} v_\mu^{(m)} = \ell! \binom{n}{\ell}^2 (m-n)^{\underline{n-\ell}}, \tag{6.7}$$

as that is the number of elements of $S_{n,m}$ whose image overlaps $[n]$ in ℓ points. Putting everything together, we have

$$\begin{aligned}
&\frac{\sum_{\ell=k+1}^{n} \left((\ell m - n^2) \sum_{\mu \in \mathcal{C}_{n,\ell}} v_\mu^{(m)} \cdot q^2_{(n-k,\theta)\otimes(m-k,\theta)}(\mu) \right)}{m^{\underline{n}} n (m-n) d_{(n-k,\theta)} d_{(m-k,\theta)}} \\
&\leq \frac{\sum_{\ell=k+1}^{n} (\ell m - n^2) \ell! \binom{n}{\ell}^2 (m-n)^{\underline{n-\ell}} \left(d_{(m-k,\theta)} d_{(n-k,\theta)} \ell^{\underline{k}} / n^{\underline{k}} \right)^2}{m^{\underline{n}} n (m-n) d_{(n-k,\theta)} d_{(m-k,\theta)}} \\
&= d_{(m-k,\theta)} d_{(n-k,\theta)} \sum_{\ell=k+1}^{n} \frac{(m-n)^{\underline{n-\ell}}}{m^{\underline{n}}} \frac{\ell m - n^2}{n(m-n)} \binom{n-k}{\ell-k}^2 \ell! \\
&\leq m^k n^k \sum_{\ell=k+1}^{n} \frac{m^{\underline{n-\ell}}}{m^{\underline{n}}} n^{2(\ell-k)} n^\ell \\
&\leq \frac{m^k}{n^k} \sum_{\ell=k+1}^{\infty} \left(\frac{n^3}{m-n} \right)^\ell \\
&= \frac{m^k}{n^k} \cdot \frac{n^{3k+3}}{(m-n)^k} \cdot \frac{1}{m-n-n^3} \\
&\leq 2 \frac{n^{2k+3}}{m},
\end{aligned}$$

where the first inequality follows from (6.6) and (6.7), and the last from $(1-n/m)^k \geq 1 - kn/m$. This completes the proof of the main result.

7 Concluding Remarks and Open Questions

While we have proven a tight $\Omega(\sqrt{n})$ lower bound on the bounded-error quantum query complexity of Index Erasure, the requirement $m \geq n^{3\sqrt{n}}$ on the range of injective functions seems unreasonably strict. We suspect that the same lower bound holds whenever $m \geq c \cdot n$ for any constant $c > \frac{1}{1-\epsilon}$, and we leave proving such a lower bound as an open problem.

When $n = m$, the n-partial permutation association scheme is simply the conjugacy-class association scheme of S_n (see [10]), whose eigenvalues are a normalization of the irreducible characters of S_n. While there is no known closed-formula for computing these normalized characters, they do admit elegant determinantal and combinatorial expressions (i.e., the Jacobi-Trudi and Murnaghan-Nakayama identities). Strahov [25] gave a generalization of the Murnaghan-Nakayama rule for $n = m - 1$, which gives a combinatorial expression for the eigenvalues of $S_{m-1,m}$ association scheme, but for arbitrary $n < m - 1$, there is no known Murnaghan-Nakayama-type rule for expressing the eigenvalues of the $S_{n,m}$ association scheme. Such an expression would give a deeper understanding of the dual eigenvalues of this scheme, and may allow one to extend our lower bound to smaller m.

Finally, our proof suggests a general strategy for deriving lower bounds on the quantum query complexity of sufficiently symmetric state conversion problems in the non-coherent regime. It would be interesting to use our approach to find such lower bounds for other such problems in the non-coherent regime.

References

1. A. Ambainis. Understanding quantum algorithms via query complexity. In *Proceedings of the 2018 International Congress of Mathematicians*, volume 3, pages 3249–3270, 2018.
2. A. Ambainis, L. Magnin, M. Roetteler, and J. Roland. Symmetry-Assisted Adversaries for Quantum State Generation. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 167–177, June 2011. doi:10.1109/CCC.2011.24.
3. E. Bannai and T. Ito. *Algebraic Combinatorics I: Association Schemes*. Mathematics lecture note series. Benjamin/Cummings Pub. Co., 1984.
4. A. Belovs and A. Rosmanis. Adversary lower bounds for the collision and the set equality problems. *Quantum Information & Computation*, 18:200–224, 2018.
5. T. Ceccherini-Silberstein, F. Scarabotti, and F. Tolli. *Harmonic Analysis on Finite Groups: Representation Theory, Gelfand Pairs and Markov Chains*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2008.
6. P. Diaconis. *Group Representations in Probability and Statistics*. Institute of Mathematical Statistics Lecture Notes—Monograph Series, 11. Institute of Mathematical Statistics, Hayward, CA, 1988.
7. D. Ellis, Y. Filmus, and E. Friedgut. LOW-DEGREE BOOLEAN FUNCTIONS ON S_n , WITH AN APPLICATION TO ISOPERIMETRY. *Forum of Mathematics, Sigma*, 5:e23, 2017. doi:10.1017/fms.2017.24.
8. D. Ellis, E. Friedgut, and H. Pilpel. Intersecting families of permutations. *J. Amer. Math. Soc.*, 24:649–682, 2011.
9. C. Godsil. Notes on Association Schemes, June 2010.
10. C. Godsil and K. Meagher. *Erdos-Ko-Rado Theorems: Algebraic Approaches*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2015.
11. C. Godsil and G. Royle. *Algebraic Graph Theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001. doi:10.1007/978-1-4613-0163-9.
12. A.S. Greenhalgh. Random Walks on Groups with Subgroup Invariance Properties. Technical report, Stanford University, Department of Statistics, April 1989.
13. P. Høyer, T. Lee, and R. Špalek. Negative Weights Make Adversaries Stronger. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 526–535, New York, NY, USA, 2007. ACM. doi:10.1145/1250790.1250867.
14. G.D. James and A. Kerber. *The Representation Theory of the Symmetric Group*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1984.
15. T. Lee, R. Mittal, B.W. Reichardt, R. Špalek, and M. Szegedy. Quantum Query Complexity of State Conversion. In *Proceedings of the 2011 IEEE 52Nd Annual Symposium on Foundations of Computer Science*, FOCS '11, pages 344–353, Washington, DC, USA, 2011. IEEE Computer Society. doi:10.1109/FOCS.2011.75.
16. G. Midrijānis. A Polynomial Quantum Query Lower Bound for the Set Equality Problem. In *Automata, Languages and Programming*, pages 996–1005, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.
17. A. Montanaro. Quantum algorithms: An overview. *npj Quantum Information*, 2, November 2015. doi:10.1038/npjqi.2015.23.
18. M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.
19. R. O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.
20. A. Rosmanis. Quantum Adversary Lower Bound for Element Distinctness with Small Range. *Chicago Journal of Theoretical Computer Science*, 2014(4), July 2014.
21. A. Rosmanis and A. Belovs. On Adversary Lower Bounds for the Collision and the Set Equality Problems, 2013. Available at arXiv:1310.5185v1 [quant-ph].
22. B. Sagan. *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*. Graduate Texts in Mathematics. Springer New York, 2001.

23 Y. Shi. Quantum Lower Bounds for the Collision and the Element Distinctness Problems. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS '02, pages 513–519, Washington, DC, USA, 2002. IEEE Computer Society.

24 R.P. Stanley. *Enumerative Combinatorics: Volume 2*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2001.

25 E. Strahov. Generalized characters of the symmetric group. *Advances in Mathematics*, 212(1):109–142, 2007. doi:10.1016/j.aim.2006.09.017.

26 M. Zhandry. A Note on the Quantum Collision and Set Equality Problems. *Quantum Info. Comput.*, 15(7-8):557–567, May 2015.

A Connection to the graph isomorphism

Suppose we are given two rigid graphs G_0 and G_1 on k vertices (e.g., as $k \times k$ adjacency matrices), and we are asked to decide whether there exists a permutation of vertices $\pi \in S_k$ such that $\pi(G_0) = G_1$. Let $S_k(G) := \{\pi(G) \colon \pi \in S_k\}$ and

$$|S_k(G)\rangle := \frac{1}{\sqrt{k!}} \sum_{\pi \in S_k} |\pi(G)\rangle.$$

For a rigid graph G, the function $\pi \mapsto \pi(G)$ is injective and $|S_k(G)\rangle$ is the uniform superposition over the image of this function. Note that $S_k(G_0) = S_k(G_1)$ and $\langle S_k(G_0)|S_k(G_1)\rangle = 1$ if $G_0 \cong G_1$ and $S_k(G_0) \cap S_k(G_1) = \emptyset$ and $\langle S_k(G_0)|S_k(G_1)\rangle = 0$ if $G_0 \ncong G_1$.

Here we present two algorithms for Graph Isomorphism based on ability to generate the state $|S_k(G)\rangle|t_G\rangle$, where $|t_G\rangle$ is the final state of the ancillary memory. Both algorithms always return 0 when the graphs are isomorphic and return 1 with probability 1/2 when the graphs are non-isomorphic.

A.1 Coherent test

Suppose we prepare a quantum state

$$\frac{1}{\sqrt{2}} \sum_{b \in \{0,1\}} |b\rangle|S_k(G_b)\rangle|t_{G_b}\rangle,$$

where the first register specifies whether we create the superposition over permutations of G_0 or G_1 in the second register. Then we apply the Hadamard gate on the first register and measure. This procedure returns 0 with probability

$$\frac{1}{2} + \frac{1}{2}\Re\big[\langle S_k(G_0)|S_k(G_1)\rangle \langle t_{G_0}|t_{G_1}\rangle\big].$$

If $G_0 \ncong G_1$, then $|S_k(G_0)\rangle$ and $|S_k(G_1)\rangle$ are orthogonal states, and the measurement returns 1 with probability 1/2. On the other hand, if $G_0 \cong G_1$, then the probability of outputting 0 completely depends on $\Re[\langle t_{G_0}|t_{G_1}\rangle]$, on which we do not place any restrictions in the non-coherent case. However, in the coherent case, $\Re[\langle t_{G_0}|t_{G_1}\rangle] = 1$ and 0 would be always output whenever $G_0 \cong G_1$.

A.2 Non-coherent test

Now suppose we first prepare a quantum state

$$\frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)|S_k(G_0)\rangle|S_k(G_1)\rangle|t_{G_0}\rangle|t_{G_1}\rangle,$$

and then use the content of the first register to decide whether to swap the next two registers, obtaining

$$\frac{1}{\sqrt{2}}\Big(|0\rangle|S_k(G_0)\rangle|S_k(G_1)\rangle + |1\rangle|S_k(G_1)\rangle|S_k(G_0)\rangle\Big)|t_{G_0}\rangle|t_{G_1}\rangle.$$

Then we apply the Hadamard gate on the first register and measure. This procedure returns 0 with probability

$$\frac{1}{2} + \frac{1}{2}\big\|\langle S_k(G_0)|S_k(G_1)\rangle\big\|^2.$$

Note that the ancillary memory states $|t_{G_0}\rangle$ play no role in this test.

We note that our $\Omega(\sqrt{n})$ lower bound for non-coherent Index Erasure does not apply here because of the condition $m = \Omega(n^{\sqrt{n}})$. In this context, n is the number of vertex permutations, $k!$, and m is the number of rigid graphs, which is of order $2^{\binom{k}{2}}$ [11, Corollary 2.3.3]. Nonetheless, the $\Omega(n^{1/3})$ lower bound (via Set Equality) still applies, which tells us that both Graph Isomorphism tests based on Index Erasure are inefficient. However, this dose not rule out an efficient preparation of $|S_k(G)\rangle$ by exploiting some inner workings of the oracle O_G (that is, by not treating it as a black-box).

B Dual Eigenvalues of Maximal Irreps

In Lemma 24 we essentially expressed dual eigenvalues for irreps of form $(n-k,\theta)\otimes(m-k,\theta)$ via dual eigenvalues for irreps of form $\lambda\otimes(m-n,\lambda)$, where $\theta\vdash k$ and $\lambda\vdash n$. Here we address obtaining the dual eigenvalues for irreps of form $\lambda\otimes(m-n,\lambda)$, in particular, obtaining the column vector $(m^{\underline{n}}E_{\lambda\otimes(m-n,\lambda)})_{f_{\mathrm{id}}}$, whose entries are the dual eigenvalues.

Of course, since we have $E_{\lambda\otimes(m-n,\lambda)} = E_{(m-n,\lambda)}$, we have

$$(m^{\underline{n}}E_{\lambda\otimes(m-n,\lambda)})_{f_{\mathrm{id}}} = m^{\underline{n}}E_{(m-n,\lambda)}1_{f_{\mathrm{id}}},$$

where

$$E_{(m-n,\lambda)} = \frac{d_{(m-n,\lambda)}}{m!}\sum_{\pi\in S_m}\chi_{(m-n,\lambda)}(\pi)V_\pi$$

and $V_\pi\colon 1_f \mapsto 1_{\pi * f}$. Below, however, we present an expression for $(m^{\underline{n}}E_{\lambda\otimes(m-n,\lambda)})_{f_{\mathrm{id}}}$ that might be more usefull when $n \ll m$, especially when n is constant.

Suppose $m \geq 2n$ and consider a $2n$-tuple

$$\boldsymbol{a} := (a_1^{(0)}, a_2^{(0)}, \cdots, a_n^{(0)}, a_1^{(1)}, a_2^{(1)}, \cdots, a_n^{(1)}) \in [m]^{2n}$$

of distinct elements. Consider the idempotent

$$E_{\boldsymbol{a}} := \frac{I - V_{(a_1^{(0)},a_1^{(1)})}}{2}\cdot\frac{I - V_{(a_2^{(0)},a_2^{(1)})}}{2}\cdot\cdots\cdot\frac{I - V_{(a_n^{(0)},a_n^{(1)})}}{2}.$$

The image of $E_{\boldsymbol{a}}$ is orthogonal to all λ'-isotypic subspaces for all $\lambda'\vdash m$ with $\lambda'_1 > m-n$ [4, Lemma 8]. For the $\mathcal{A}_{n,m}$ scheme, this means that the image of $E_{\boldsymbol{a}}$ is orthogonal to all irreps $\lambda\otimes\lambda'$ such that $\lambda' \neq (m-n,\lambda)$. On the other hand, for the vector

$$\phi_{\boldsymbol{a}} := \sum_{b\in\{0,1\}^n}(-1)^{|b|}1_{\boldsymbol{a}^b},$$

where $\boldsymbol{a}^b\colon [n]\to[m]\colon x\mapsto a_x^{(b_x)}$, we have $E_{\boldsymbol{a}}\phi_{\boldsymbol{a}} = \phi_{\boldsymbol{a}}$.

Now consider $a_x^{(0)} = x$ for all $x \in [n]$ and $(m-n)^{\underline{n}}$ choices of distinct $a_1^{(1)}, a_2^{(1)}, \cdots, a_n^{(1)}$ from $\{n+1, n+2, \cdots, m\}$, with their corresponding vectors $\phi_{\boldsymbol{a}}$. By adding all these vectors and then dividing the result by $(m-n)^{\underline{n}}$, we obtain

$$\phi_{\max} := \sum_{\ell=0}^{n} \frac{(-1)^\ell}{(m-n)^{\underline{\ell}}} 1_{(1^{n-\ell}|1^\ell)} \in (\mathfrak{A}_{n,m})_{f_{\mathrm{id}}},$$

where, for $\mu \in \mathcal{C}_n$, 1_μ is the characteristic column of A_μ, namely, $1_\mu = \sum_{f \in \Omega_\mu} 1_f$.

Now consider $\lambda \vdash n$ and the projector

$$E_\lambda = \frac{d_\lambda}{n!} \sum_{\pi \in S_n} \chi_\lambda(\pi) V_\pi$$

on the λ-isotypic subspace. By the above discussion, we have

$$E_\lambda \phi_{\max} = E_{\lambda \otimes (m-n,\lambda)} \phi_{\max},$$

which is proportional to the characteristic column of $E_{\lambda\otimes(m-n,\lambda)} 1_{f_{\mathrm{id}}}$, and the coefficient of proportionality is

$$\frac{1_{f_{\mathrm{id}}}^\top E_\lambda \phi_{\max}}{1_{f_{\mathrm{id}}}^\top E_{\lambda\otimes(m-n,\lambda)} 1_{f_{\mathrm{id}}}} = \frac{(d_\lambda/n!) d_\lambda}{d_\lambda d_{\lambda'}/m^{\underline{n}}} = \frac{d_\lambda m^{\underline{n}}}{d_{\lambda'} n!},$$

where we have used that $1_{f_{\mathrm{id}}}^\top V_\pi 1_{(1^{n-\ell}|1^\ell)} = 0$ whenever π is not the identity permutation ε or $\ell \neq 0$ (or both), $1_{(1^n|\varnothing)} = 1_{f_{\mathrm{id}}}$, and $\chi_\lambda(\varepsilon) = d_\lambda$. Hence,

$$(m^{\underline{n}} E_{\lambda\otimes(m-n,\lambda)})_{f_{\mathrm{id}}} = \frac{d_{\lambda'} n!}{d_\lambda} E_\lambda \phi_{\max} = d_{\lambda'} \sum_{\pi \in S_n} \chi_\lambda(\pi) V_\pi \phi_{\max}.$$

C Partial Permutations and RSK Correspondence

A well-known fact is that S_m admits the following representation-theoretic count

$$|S_m| = \sum_{\lambda \vdash m} (d_\lambda)^2 \tag{C.1}$$

where d_λ is the number of standard Young tableau of shape $\lambda \vdash m$ (see [22]). An elegant combinatorial proof of this fact follows from *Robinson-Schensted Correspondence*, a well-known combinatorial procedure that associates to each permutation $\sigma \in S_m$ a unique pair of standard Young tableaux of the same shape, and vice versa (see [22]).

Knuth generalized this correspondence to a wider class of combinatorial objects called *generalized permutations*, which are $2 \times m$ arrays of integers

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_m \\ j_1 & j_2 & \cdots & j_m \end{pmatrix} \text{ such that } i_1 \leq \cdots \leq i_m \text{ and if } i_r = i_{r+1}, \text{then } j_r \leq j_{r+1}.$$

Robinson-Schensted-Knuth Correspondence (RSK) associates a pair of semistandard Young tableau of the same shape to each generalized permutation, and vice versa (see [22]). We may encode each n-partial permutation $(j_1, j_2, \cdots, j_n) \in S_{n,m}$ as a generalized permutation as follows:

$$(j_1, j_2, \cdots, j_n) \longleftrightarrow \begin{pmatrix} 1 & 2 & \cdots & n & n+1 & \cdots & n+1 \\ j_1 & j_2 & \ldots & j_n & j_{n+1} & \cdots & j_m \end{pmatrix},$$

where $j_{n+1}, \cdots, j_m \in [m] \setminus \{j_1, \cdots, j_n\}$ are ordered from least to greatest. Applying RSK to n-partial permutations associates to each $(j_1, j_2, \cdots, j_n) \in S_{n,m}$ a standard Young tableau P and a semistandard Young tableau Q of the same shape $\lambda \vdash m$. The subtableau of cells labeled $n+1$ in Q form a horizontal strip on $m-n$ cells. Ignoring this horizontal strip results in a standard Young tableau of shape $\mu \vdash n$ such that λ/μ is a horizontal strip, and so we arrive at the following theorem.

▶ **Theorem 26.** *RSK gives an explicit bijection between $S_{n,m}$ and pairs (P, Q) where P is a standard Young tableau of shape $\lambda \vdash m$ and Q is a standard Young tableau of shape $\mu \vdash n$ such that λ/μ is a horizontal strip.*

As a corollary, we get a combinatorial proof of a natural generalization of Equation (C.1).

▶ **Corollary 27.** *The number of n-partial permutations of $[m]$ can be counted as follows:*

$$|S_{n,m}| = \sum_{\mu,\lambda} d_\mu d_\lambda$$

where the sum runs over pairs $\mu \vdash n, \lambda \vdash m$ such that λ/μ is a horizontal strip.

D Proofs

Theorem 7 (restated). *Let $\theta \vdash k$ and $\theta^+ \vdash (k+1)$ be any shape obtained by adding an inner corner to θ. For all $m \geq 2(k+1)$, we have*

$$\frac{d_{(m-k-1,\theta^+)}}{d_{(m-k,\theta)}} \geq \frac{m}{k} \cdot \left(1 - \frac{2k+1}{m}\right).$$

Proof. Recall that, by the hook rule, $\mathsf{H}(\theta) d_\theta = |\theta|!$. First, [20, Claim 6.3] states that

$$\frac{d_{(m-|\theta^+|,\theta)}}{d_{(m-|\theta|,\theta)}} \geq 1 - \frac{2k}{m}.$$

We reprove this claim here for completeness. Note that when we add a cell to the end of the top row of $(m-|\theta^+|, \theta)$ to obtain $(m-|\theta|, \theta)$, this increases the hook-lengths of the cells in the top row by 1, and the rest of the hook-lengths are unchanged. If we just consider the "overhang" and ignore everything else in the first row, then the product of the hook-lengths with respect to $(m-|\theta|, \theta)$ is $(m-2k)!$ whereas it is $(m-2k-1)!$ with respect to $(m-|\theta^+|, \theta)$. This gives us

$$\frac{d_{(m-|\theta^+|,\theta)}}{d_{(m-|\theta|,\theta)}} \geq \frac{m-2k}{m} = 1 - \frac{2k}{m},$$

which proves the claim.

Since $(m-|\theta^+|, \theta)$ is a partition of $(m-1)$, it corresponds to an (S_{m-1})-irrep. When we added one cell to $(m-|\theta^+|, \theta)$ to obtain $(m-|\theta^+|, \theta^+)$, only one hook-length in the first row increased, and before the increment it was at least $m-2k-1$. Thus, in the following derivation, all the other hook-lengths of the first rows of $(m-|\theta^+|, \theta)$ and $(m-|\theta^+|, \theta^+)$ have cancelled out.

$$\begin{aligned}\frac{d_{(m-|\theta^+|,\theta^+)}}{d_{(m-|\theta^+|,\theta)}} &\geq \frac{m!}{(m-1)!} \cdot \frac{m-2k-1}{m-2k} \cdot \frac{\mathsf{H}(\theta)}{\mathsf{H}(\theta^+)} \\ &= m\left(1 - \frac{1}{m-2k}\right) \frac{k! d_{\theta^+}}{(k+1)! d_\theta} \geq \frac{m}{k+1}\left(1 - \frac{1}{m-2k}\right),\end{aligned}$$

where in the middle equality we have used hook-length formula once more, and the last inequality follows from the branching rule (namely, that $d_{\theta^+} \geq d_\theta$). Combining these two inequalities gives the result. ◀

Theorem 12 (restated). *Let $1_\alpha \in \mathbb{C}[S_{n,m}]$ be the characteristic function of the family S_α. Then $1_\alpha \in \mathcal{U}_k$.*

Proof. Let $\mathrm{Stab}_{S_m}(S_\alpha)$ be the stabilizer of S_α, which consists of all the permutations of $[m] \setminus \mathrm{im}(\alpha)$ and, thus, $\mathrm{Stab}_{S_m}(S_\alpha) \cong S_{m-k}$. Let $\lambda \vdash m$ be any irrep of S_m such that $m - \lambda_1 > k$ and let $\lambda(\pi)$ be a matrix that represents $\pi \in S_m$. Finally, let $1_{\mathrm{Stab}(S_\alpha)} \in \mathbb{C}[S_m]$ be the characteristic function of $\mathrm{Stab}_{S_m}(S_\alpha)$, and recall from Section 3.1 that its Fourier transform is

$$\lambda(1_{\mathrm{Stab}(S_\alpha)}) = \sum_{\pi \in S_m} 1_{\mathrm{Stab}(S_\alpha)}(\pi)\, \lambda(\pi) = \sum_{\pi \in S_{m-k}} \left(\lambda \downarrow^{S_m}_{S_{m-k}}\right)(\pi).$$

Since λ has more than k cells below its first row, by the branching rule, no irrep μ of $\lambda \downarrow^{S_m}_{S_{m-k}}$ is isomorphic to the trivial representation $(m-k)$. This, and the fact that $\langle \chi^{(m-k)}, \chi^\mu \rangle = 0$ for any $\mu \vdash m-k$ with $\mu \neq (m-k)$, implies that, for each irrep μ of the multiset of irreps $\lambda \downarrow^{S_m}_{S_{m-k}}$, we have $\sum_{\pi \in S_{m-k}} \mu(\pi) = 0$. This gives us

$$\lambda(1_{\mathrm{Stab}(S_\alpha)}) = \bigoplus_{\mu \in \lambda \downarrow^{S_m}_{S_{m-k}}} \sum_{\pi \in S_{m-k}} \mu(\pi) = 0,$$

which completes the proof. ◀

Theorem 4 (restated). *Let G be an automorphism group for a non-coherent state generation problem. The value of Adv_δ remains the same if one restricts the minimization in the expression defining Adv_δ and the maximization in the expressions defining the γ_2 and filtered γ_2 norms to R, T, Γ, Γ' that are all G-invariant and imposes that $(J - R) \circ \Gamma$ has an G-invariant principal eigenvector.*

Proof. In this proof, let M denote a generic symmetric matrix whose rows and columns are labeled by black-box functions $f \in \mathcal{F}$ in the same order. Let $g(M)$ be obtained by permuting the rows and the columns of M according to the action of $g \in G$ of $\mathcal{F}$ (see (2.2)). Namely, entrywise we define $g(M)$ as

$$(g(M))_{f,f'} := M_{g^{-1}(f), g^{-1}(f')}.$$

Similarly, for a vector $\omega \in \mathbb{C}[\mathcal{F}]$, define $g(\omega)$ entrywise as $(g(\omega))_{f'} := \omega_{g^{-1}(f)}$. For the sake of conciseness, we also occasionally write M^g and ω^g instead of $g(M)$ and $g(\omega)$, respectively. Note that M is G-invariant if $M^g = M$ for all $g \in G$, and $T^\odot, I, J$ are G-invariant. Also note that $(M \circ M')^g = M^g \circ M'^g$.

Let $\Delta = \{\Delta_1, \cdots, \Delta_n\}$ be the family of difference matrices. This family is closed under the action of G is the following sense.

▷ Claim 28. We have $(\pi, \boldsymbol{\sigma})(\Delta_x) = \Delta_{\pi(x)}$ for all $(\pi, \boldsymbol{\sigma}) \in G$.

Proof. Fix $(\pi, \boldsymbol{\sigma}) \in G$ and let $g := (\pi, \boldsymbol{\sigma})^{-1}$. Note that $g = (\pi^{-1}, \boldsymbol{\sigma}')$ for some $\boldsymbol{\sigma}' \in S_m^n$. From (2.2), we have $(g(f))(x) = (g(f'))(x)$ if and only if $f(\pi(x)) = f'(\pi(x))$. As a result, we have

$$((\pi, \boldsymbol{\sigma})(\Delta_x))_{f,f'} = (\Delta_x)_{g(f), g(f')} = 1$$

if and only if $f(\pi(x)) = f'(\pi(x))$. ◀

Note that M^g equals M with its rows and columns permuted. Since permuting rows and columns do not affect the γ_2 norm, we have $\gamma_2(M^g) = \gamma_2(M)$ for all $g \in G$. And, if the diagonal of M is all-zeros, then Claim 28 also implies that $\gamma_2(M^g|\Delta) = \gamma_2(M|\Delta)$ for all $g \in G$.

▶ **Lemma 29.** *Restricting $R, T \in \mathcal{T}$ to be G-invariant does not change the optimal value of the minimization problem defining Adv_δ.*

Proof. Let R, T be an optimal solution of the minimization in (2.1). We define their respective G-symmetrizations as

$$\overline{R} := \frac{1}{|G|}\sum_{g\in G} g(R) \qquad \text{and} \qquad \overline{T} := \frac{1}{|G|}\sum_{g\in G} g(T),$$

which are both clearly in $\mathcal{T}$. Since $g(T^\odot) = T^\odot$ for all $g \in G$, the triangle inequality yields

$$\begin{aligned}\gamma_2(\overline{R} - T^\odot \circ \overline{T}) = \gamma_2\left(\frac{1}{|G|}\sum_{g\in G} g(R - T^\odot \circ T)\right) &\le \frac{1}{|G|}\sum_{g\in G}\gamma_2\big(g(R - T^\odot \circ T)\big)\\ &= \frac{1}{|G|}\sum_{g\in G}\gamma_2(R - T^\odot \circ T) = \gamma_2(R - T^\odot \circ T) \le \delta.\end{aligned}$$

Hence we have show that the pair $\overline{R}, \overline{T}$ is a feasible solution to the minimization in (2.1), and it remains to show that it is also optimal. And, again by the triangle inequality,

$$\begin{aligned}\gamma_2(J - \overline{R}|\Delta) = \gamma_2\left(\frac{1}{|G|}\sum_{g\in G} g(J - R)\middle|\Delta\right) &\le \frac{1}{|G|}\sum_{g\in G}\gamma_2\big(g(J - R)|\Delta\big)\\ &= \frac{1}{|G|}\sum_{g\in G}\gamma_2(J - R|\Delta) = \gamma_2(J - R|\Delta) = \mathsf{Adv}_\delta.\end{aligned}$$

◀

Now, fix G-invariant $R, T \in \mathcal{T}$ and let $M := J - R$, which is also G-invariant. Let us now show that the maximization in

$$\gamma_2(M|\Delta) = \max_{\Gamma}\left\{\|M \circ \Gamma\| \colon \forall x\ \|\Delta_x \circ \Gamma\| \le 1\right\}$$

can be restricted to G-invariant Γ.

The proof is very similar to that of the automorphism principle in [15]. Fix an optimal solution Γ, and without loss of generality assume that the largest eigenvalue of $M \circ \Gamma$ is positive and let it correspond to an eigenvector $\omega \in \mathbb{C}[\mathcal{F}]$ of norm 1. Namely,

$$\|M \circ \Gamma\| = \omega^\top (M \circ \Gamma)\omega.$$

Define the G-symmetrization $\overline{\omega}$ of ω entrywise as

$$\overline{\omega}_f := \sqrt{\frac{1}{|G|}\sum_{g\in G} |(\omega^g)_f|^2},$$

and note that $\overline{\omega}$ also has norm 1. Without loss of generality, all the entries of $\overline{\omega}$ are strictly positive (the rows and columns corresponding to f such that $\overline{\omega}_f = 0$ can be removed from the consideration), and thus we can entrywise define a vector μ as $\mu_f := 1/\overline{\omega}_f$. Let us define

$$\overline{\Gamma} := \mu\mu^\top \circ \frac{1}{|G|} \sum_{g \in G} \Gamma^g \circ \omega^g \omega^{g\top},$$

which is clearly G-invariant.

Let us start by showing that $\|\overline{\Gamma} \circ \Delta_x\| \leq 1$ for all x. Note that $\|\Gamma^g \circ \Delta_x\| \leq 1$ for all x and all $g \in G$ due to Claim 28, $\|\Gamma \circ \Delta_x\| \leq 1$ if and only if $I \pm \Gamma \circ \Delta_x$ is positive-semidefinite, and

$$I \circ \mu\mu^\top \circ \frac{1}{|G|} \sum_{g \in G} \omega^g \omega^{g\top} = I.$$

We thus have that

$$I \pm \overline{\Gamma} \circ \Delta_x = \mu\mu^\top \circ \frac{1}{|G|} \Big(\sum_{g \in G} \omega^g \omega^{g\top} \circ (I \pm \Gamma^g \circ \Delta_x) \Big)$$

is positive-semidefinite as the sum and the entrywise product of positive-semidefinite matrices are positive-semidefinite. Thus, indeed, $\|\overline{\Gamma} \circ \Delta_x\| \leq 1$ for all x.

Now let us use the fact that ω is a principal eigenvector of $M \circ \Gamma$, and, therefore, ω^g is a principal eigenvector of $M \circ \Gamma^g$ for all $g \in G$ (recall that M is G-invariant). We have

$$\begin{aligned} \|M \circ \overline{\Gamma}\| \geq \overline{\omega}\, \overline{\Gamma}\, \overline{\omega}^\top &= \sum_{f,f' \in \mathcal{F}} \Big(\frac{1}{|G|} \sum_{g \in G} (M \circ \Gamma^g \circ \omega^g \omega^{g\top}) \Big)_{f,f'} \\ &= \frac{1}{|G|} \sum_{g \in G} \omega^{g\top} (M \circ \Gamma^g) \omega^g = \|M \circ \Gamma\|. \end{aligned}$$

Thus $\overline{\Gamma}$ is also an optimal solution of the maximization above. Also note that $\overline{\omega}$ is the principal eigenvector of $M \circ \overline{\Gamma}$.

A similar argument shows that, for G-invariant $M' := R - T^{\odot} \circ T$, one can restrict the maximization in

$$\gamma_2(M') = \max_{\Gamma'} \big\{ \|M' \circ \Gamma'\| \colon \|\Gamma'\| \leq 1 \big\}$$

to G-invariant Γ'. ◀