

ON THE ALGEBRAIC COMBINATORICS OF INJECTIONS AND ITS APPLICATIONS TO INJECTION CODES

Peter J. Dukes, Ferdinand Ihringer, and Nathan Lindzey

December 11, 2019

ABSTRACT. We consider the algebraic combinatorics of the set of injections from a k -element set to an n -element set. In particular, we give a new combinatorial formula for the spherical functions of the Gelfand pair $(S_k \times S_n, \text{diag}(S_k) \times S_{n-k})$. We use this combinatorial formula to give new Delsarte linear programming bounds on the size of codes over injections.

1. Introduction

Let S_n denote the symmetric group on n elements and let $S_{k,n}$ denote the set of injections (alternatively, partial permutations) σ from $[k] := \{1, 2, \dots, k\}$ to $[n]$. Note that $S_{n,n} = S_n$, so this is a natural generalization of the symmetric group. The goals of this paper are two-fold. Firstly, we investigate the algebraic combinatorics of injections. In particular, we investigate the *injection scheme* [24, 26], an association scheme naturally associated with injections which is a simultaneous generalization of the Johnson association scheme and the group association scheme of S_n . Secondly, we apply this theory to analyze injections in the coding-theoretic sense. That is, we use the character table of the injection scheme to compute, for a wide range of parameters, upper bounds on the number of partial permutations with prescribed minimum Hamming distance (or, in general, allowed distance sets).

1.1. The Algebraic Combinatorics of Injections. Throughout this work, let $G_{k,n} := S_k \times S_n$ and $K_{k,n} := \text{diag}(S_k) \times S_{n-k}$. We shall investigate the algebraic combinatorics of $S_{k,n}$ via the Gelfand pair $(G_{k,n}, K_{k,n})$. The spherical functions of $(G_{k,n}, K_{k,n})$ have combinatorial significance, as they describe the eigenvalues of a natural family of graphs defined over $S_{k,n}$, i.e., the character table of the injection association scheme. We begin with a brief overview of previous work related to the subject.

Diaconis and Shahshahani [13] observed that $(G_{k,n}, K_{k,n})$ is a Gelfand pair by showing the double coset algebra $\mathbb{C}[K_{k,n} \backslash G_{k,n} / K_{k,n}]$ is commutative. Later, Greenhalgh [21] found a closed expression for the spherical functions of $(G_{k,n}, K_{k,n})$ evaluated at the double coset $K_{k,n} \backslash (k, k+1) / K_{k,n}$, equivalently, the eigenvalues of the graph over $S_{k,n}$ where σ, σ' is an edge if their respective mappings agree on all but one symbol of the domain. Using this expression, he showed that the mixing time of the uniform random walk on this graph is approximately $(n-k) \log n + cn$ for some constant $c > 0$.

In quantum computing, the algebraic combinatorics of $S_{k,n}$ has been used to show adversarial lower bounds on the time-complexity of the COLLISION, SET-EQUALITY, and INDEX-ERASURE problems.

Research of P.J. Dukes is supported by NSERC grant 312595-2017. F. Ihringer is supported by a postdoctoral fellowship of the Research Foundation - Flanders (FWO).

These lower bounds are derived from properties of the dual characters and Krein parameters of the injection scheme [2, 4, 24], and are expressed in terms of the spherical functions of $(G_{k,n}, K_{k,n})$.

Greenhalgh [21] posed the question of investigating the spherical functions of $(G_{k,n}, K_{k,n})$, as spherical functions often correspond to interesting families of orthogonal polynomials (e.g., special functions). For the case $k = n - 1$, the so-called “unbalanced” pair $(S_{n-1} \times S_n, \text{diag}(S_{n-1}))$, Strahov [29] showed that many of the classical results in the theory of symmetric functions have unbalanced analogues. In particular, he gave a Murnaghan-Nakayama type rule and a Jacobi-Trudi identity for evaluating its spherical functions. Note that the “balanced” pair $(S_n \times S_n, \text{diag}(S_n))$ recovers the classical representation theory of S_n (see [25]).

Such expressions for the cases $2 \leq k \leq n - 2$ are not known, and to what extent the classical representation theory of the symmetric group carries over to these cases is an intriguing question. Indeed, the absence of useful combinatorial formulas for the spherical functions of $(G_{k,n}, K_{k,n})$ has been a major obstacle in each of the areas above.

We make some progress in this direction by giving a combinatorial formula for the spherical functions of $(G_{k,n}, K_{k,n})$. The formula is significantly more revealing than the known formulas, and it is much easier to compute. It can be used to estimate the eigenvalues and ranks of matrices in the Bose-Mesner algebra of the injection scheme, in special cases, giving exact closed-form expressions (we do not pursue this direction in this paper), and it also allows us to efficiently compute the character tables of injection schemes for explicit parameters k and n .

1.2. Injection Codes. We now outline the coding-theoretic framework, starting first with the well-studied case of permutations. The Hamming distance between two permutations $\sigma, \tau \in S_n$ is the number of non-fixed points of $\sigma\tau^{-1}$, or, equivalently, the number of disagreements when σ and τ are written as words in single-line notation. For example, 1234 and 3241 are at distance three. This notion naturally generalizes to injections [17].

A *permutation code* $\text{PC}(n, d)$ is a subset Γ of S_n such that the distance between any two distinct elements of Γ is at least d . The language of classical coding theory is often used: elements of Γ are *words*, n is the *length* of the code, and the parameter d is the *minimum distance*, although for our purposes it is not important whether distance d is ever achieved. Permutation codes are also called *permutation arrays* by some authors, where the words are written as rows of an $n \times |\Gamma|$ array.

The investigation of permutation codes essentially began with the articles [15, 19]. After some years of inactivity, permutation codes enjoyed a resurgence, due in part to their applications to error-correction over certain channels and in tandem with the ongoing development of computational discrete optimization.

For positive integers $n \geq d$, we let $M(n, d)$ denote the maximum size of a $\text{PC}(n, d)$. It is easy to see that $M(n, 1) = M(n, 2) = n!$, and that $M(n, n) = n$. The Singleton bound $M(n, d) \leq n!/(d - 1)!$ holds. The alternating group A_n shows that $M(n, 3) = n!/2$. More generally, a sharply k -transitive subgroup of S_n furnishes a permutation code of (maximum possible) size $n!/(n - k)!$. For instance, the Mathieu groups M_{11} and M_{12} are maximum $\text{PC}(11, 7)$ and $\text{PC}(12, 7)$, respectively. On the other hand, determination of $M(n, d)$ absent any algebraic structure appears to be a difficult problem. A table of bounds on $M(n, d)$ can be found in [28].

A relaxation known as an *injection code* was introduced in [17]. As the name suggests, one considers the problem of packing, with respect to Hamming distance, injections (alternatively partial permutations), of a fixed length k using the alphabet $[n] = \{1, \dots, n\}$. Let $M(n, k, d)$ denote the maximum size of a family of such injections with pairwise Hamming distance at least d . For example, we have $M(n, k, k) = n$ from (for the lower bound) the cyclic shifts of, say, $12 \cdots k$ and (for the upper bound) the pigeonhole principle. The problem of determining $M(n, k, d)$ is, like its counterpart for permutations, challenging in general. However, as we illustrate in Section 5 to follow, there are various closely related problems in combinatorics motivating further study of injection codes.

1.3. Outline. The outline of the paper is as follows. In Section 2, we review integer partitions and tableaux, and generalize the Robinson-Schensted-Knuth correspondence to the setting of injections. Then, in Section 3, we set up the algebraic combinatorics for injections. In particular, we introduce the injection scheme, its associated Gelfand pair, and give a formula for its spherical functions in terms of characters of symmetric groups. The main result of Section 4 pushes this to a purely combinatorial description using a canonical basis for $\mathbb{C}[S_{k,n}]$ in terms of tableaux. In Section 5, we state the Delsarte linear programming bound for injection codes in terms of characters for the injection scheme. Our computations for parameters $k \leq n \leq 15$ are reported as tables of new or improved bounds. Additionally, we offer some motivation for these bounds by noting several combinatorial problems closely connected with injection codes. We conclude with a few open problems that naturally follow our work.

2. Tableaux and Injections

We give a brief overview of some tableau terminology, see [27] for a more detailed treatment. Let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell) \vdash n$ denote an (integer) *partition* of $n \in \mathbb{N}$. Let $\ell(\lambda)$ denote the *length* of λ , that is, the number of parts in the partition. To each $\lambda \vdash n$, we may associate a *tableau* t , a left-justified array of cells with ℓ rows and λ_i cells in i th row. Let λ^\top denote the *transpose* partition, that is, the partition obtained by interchanging the rows and columns of λ 's tableau. For any $\mu = (\mu_1, \mu_2, \dots, \mu_k) \vdash m$ such that $\mu_i \leq \lambda_i$ for all $1 \leq i \leq k$, the *skew-tableau* λ/μ is the array of cells obtained by removing the cells corresponding to μ from λ . A skew-tableau is a *horizontal strip* if no two of its cells lie in the same column.

We say a tableau t of shape $\lambda \vdash n$ is a *Young tableau* if its cells are assigned a unique $i \in [n]$. A Young tableau is *standard* if the cells are in ascending order from left to right in each row, and in ascending order from top to bottom in each column. Let f^λ denote the number of standard Young tableau of shape $\lambda \vdash n$. A *tabloid* $\{t\}$ is a Young tableau such that cells in each row are unordered. For any tabloid $\{t\}$ with n cells, let $\text{row}_{\{t\}}(i)$ denote the index of the row of $\{t\}$ that contains $i \in [n]$, and let $\text{col}_t(i)$ denote the index of the column of t that contains $i \in [n]$.

A well-known fact is that the symmetric group S_n on n symbols admits the following representation-theoretic count:

$$(2.1) \quad |S_n| = \sum_{\lambda \vdash n} (f^\lambda)^2.$$

An elegant combinatorial proof of this fact follows from *Robinson-Schensted Correspondence*, a well-known combinatorial procedure that associates to each permutation $\sigma \in S_n$ a unique pair of standard Young tableaux of the same shape, and vice versa (see [27]).

3. Representation Theory and the Injection Scheme

Throughout this work, we assume a general understanding of group representation theory and the theory of association schemes. We refer the reader to [16] and [20] for more detailed discussions.

3.1. Association Schemes and Finite Gelfand Pairs. Let X be a finite set of cardinality v . An *association scheme* is a set of $d + 1$ binary $v \times v$ matrices $\mathcal{A} = \{A_0, A_1, \dots, A_d\}$ over a set X that satisfy the following axioms:

- (1) $A_i \in \mathcal{A} \Rightarrow A_i^\top \in \mathcal{A}$ for all $0 \leq i \leq m$,
- (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) $A_i A_j = A_j A_i = \sum_{k=1}^d p_{i,j}(k) A_k$ and $p_{i,j}(k) \in \mathbb{Z}$ for all $0 \leq i, j \leq d$.

Moreover, if $A_i = A_i^\top$ for all $0 \leq i \leq m$, then we say the association scheme is *symmetric*.

The matrices A_1, \dots, A_d are referred to as *associates*, and the constants $p_{i,j}(k)$ are the so-called *intersection numbers* of the association scheme. Let v_i denote the *valency* (rowsum) of the associate A_i , and let m_i denote the *multiplicity* (dimension) of the i th eigenspace for all $0 \leq i \leq m$. The matrix algebra generated by the identity matrix and its associates is the association scheme's *Bose-Mesner algebra*, and these matrices form a basis for this algebra. The *character table* of an association scheme is a $(d + 1) \times (d + 1)$ matrix P whose rows are indexed by eigenspaces, columns indexed by matrices of \mathcal{A} , and defined such that $P_{i,j}$ is the eigenvalue for the i th eigenspace of A_j . It turns out that P is invertible, and so the *dual character table* Q of the association scheme is defined to be $Q = vP^{-1}$. The dual character table of the injection scheme will be central for obtaining linear programming bounds on injection codes.

In general, one can determine the intersection numbers of an association scheme from its character table by appealing to the following well-known relation; see, for instance, Chris Godsil's notes [20].

Proposition 3.1. *The intersection numbers satisfy*

$$p_{ij}(k) = \frac{1}{vv_k} \sum_{h=0}^d m_h P_{h,i} P_{h,j} P_{h,k}.$$

Conversely, it is possible to find the eigenvalues from the intersection numbers by computing eigenvalues of 'random' linear combinations of intersection matrices $B_k = [p_{ij}(k)]$, which can be shown [12, p. 13] to furnish another basis for the Bose-Mesner algebra.

For association schemes that arise from groups, the entries of P can be determined via group representation theory, i.e., in terms of the spherical functions of a finite *Gelfand pair* [3].

Theorem 3.2. [25] *Let $K \leq G$ be a group. Then the following are equivalent.*

- (1) (G, K) is a Gelfand Pair;
- (2) The induced representation $1 \uparrow_K^G \cong \bigoplus_{i=1}^d V_i$ (equivalently, the permutation representation of G acting on G/K) is multiplicity-free;
- (3) The double-coset algebra $\mathbb{C}[K \backslash G / K]$ is commutative.

Moreover, a Gelfand pair is symmetric if $KgK = Kg^{-1}K$ for all $g \in G$.

Let (G, K) be a Gelfand pair, $X := G/K$, and define χ_i to be the character of V_i as in the second statement of Theorem 3.2, with dimension $d_i := \chi_i(1)$. The functions $\omega^1, \omega^2, \dots, \omega^d \in \mathbb{C}[X]$ defined such that

$$\omega^i(g) = \frac{1}{|K|} \sum_{k \in K} \chi_i(g^{-1}k) \quad \forall g \in G$$

are called the *spherical functions* and form an orthogonal basis for $\mathbb{C}[K \backslash G / K]$. We call the equation above *the projection formula*, as ω^i is the projection of χ_i onto the space of K -invariant functions.

The (left) K -orbits of X partition the cosets into $(K \backslash G / K)$ -double cosets, which correspond to *spheres* $\Omega_0, \Omega_1, \dots, \Omega_d \subseteq G/K$. It is helpful to think of spheres and spherical functions as the spherical analogues of conjugacy classes and irreducible characters respectively. Indeed, the spherical functions are constant on spheres, and it can be shown that the number of distinct spherical functions equals the number of distinct irreducibles of $\mathbb{C}[X]$, equivalently, the number of spheres of X .

We write ω_j^i for the value of the spherical function ω^i corresponding to the i th irreducible on the double coset corresponding to Ω_j .

Proposition 3.3. [3] *Let (G, K) be a finite Gelfand pair and let P be the character table of the corresponding association scheme. Then*

$$P_{i,j} = |\Omega_j| \omega_j^i.$$

3.2. The Injection Scheme. In this section we recall some basic facts about the *injection scheme*, a symmetric association scheme defined over the set of injections. For proofs of the following basic facts and a more detailed discussion of the injection scheme, we refer the reader to [24].¹

The product $G := S_k \times S_n$ of two symmetric groups acts on an injection $\sigma: [k] \rightarrow [n]$ as $(\pi, \rho): \sigma \mapsto \rho * \sigma * \pi^{-1}$, where $(\pi, \rho) \in G$ and $*$ denotes the composition of functions. The stabilizer of the identity injective function with respect to this action is the group $K_{k,n}$, i.e., the cosets $G_{k,n}/K_{k,n}$ are in one-to-one correspondence with injective functions. This action gives a permutation representation $1 \uparrow_K^G$ that is multiplicity-free, i.e., $(G_{k,n}, K_{k,n})$ is a symmetric Gelfand pair. By the Littlewood-Richardson rule, we have

$$(3.1) \quad 1 \uparrow_{K_{k,n}}^{G_{k,n}} \cong \bigoplus_{\substack{\mu \vdash k, \lambda \vdash n \\ \lambda/\mu \text{ is a horiz. strip}}} \mu \otimes \lambda.$$

The orbitals of G acting diagonally on $G/K \times G/K$ are in one-to-one correspondence with double cosets $K \backslash G / K$. If we think of injections graphically as maximum matchings of the complete bipartite graph $K_{k,n}$, then we observe that the double cosets and orbitals are in one-to-one correspondence with graph isomorphism classes that arise from the multiunion of any injection with the identity injection, i.e., a disjoint union of even paths and even cycles. In light of this, we use the notation $(\lambda|\rho)$ to denote the index of the orbital or double coset corresponding to the isomorphism class containing a cycle of length $2\lambda_i$ for all $1 \leq i \leq \ell(\lambda)$, and a path of length $2\rho_i$ for all $1 \leq i \leq \ell(\rho)$. Note that an isolated node is a path of length zero.

Let $C_{(\lambda|\rho)}$ denote the sphere corresponding to the cycle-path type $(\lambda|\rho)$. For example, we have $(1, 2, 3, 4) \in C_{(1^4|0^4)}$, $(2, 1, 3, 5) \in C_{(2,1|0^3,1)}$, and $(5, 6, 7, 8) \in C_{(\emptyset|1^4)}$. The following result gives a

¹In [24], the scheme is called the k -partial permutation association scheme, as one may interpret injections as partial permutations.

simple count for the sizes of the spheres, analogous to the well-known formula for determining the size of a conjugacy class in S_n .

Proposition 3.4. [24] *For any cycle-path type $(\lambda|\rho)$, the size of the $(\lambda|\rho)$ -sphere is*

$$|C_{(\lambda|\rho)}| = \frac{k!(n-k)!}{\prod_{i=0}^k i^{\ell_i} \ell_i! r_i!}$$

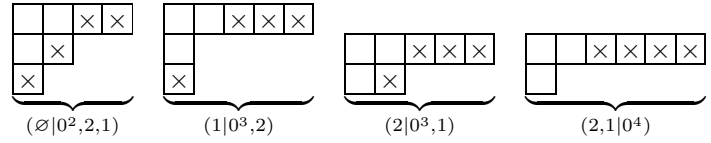
where $\lambda = (0^{\ell_0}, 1^{\ell_1}, \dots, k^{\ell_k})f$, $\rho = (0^{r_0}, 1^{r_1}, \dots, k^{r_k})$, and $\ell(\rho) = r_1 + \dots + r_k$.

Note that the orbitals can be represented as a set $\mathcal{A}_{k,n} := \{A_{(\lambda|\rho)}\}$ of symmetric matrices that sum to the all-ones matrix. In particular, we have

$$A_{(\lambda|\rho)} = \begin{cases} 1 & \text{if } i \cup j \cong (\lambda|\rho), \\ 0 & \text{otherwise,} \end{cases}$$

for all injections i, j and cycle-path types $(\lambda|\rho)$. We call $\mathcal{A}_{k,n}$ *the injection scheme*, or more precisely, *the (k, n) -injection scheme*. Note that the valencies $v_{(\lambda|\rho)}$ are just the sizes of the spheres, and the multiplicity $m_{(\lambda|\rho)}$ is the dimension of the irreducible representation corresponding to $(\lambda|\rho)$. This correspondence between cycle-path types and irreducible representations can be described as follows.

Recall that irreducible representation that appear in the permutation representation of G on injections is of the form $\alpha \otimes \beta$ where β/α is a horizontal strip of size $n - k$. Consider a tableau of β such that the cells of β/α are marked. Every column of α in β with a marked cell below it corresponds to a part in ρ whereas an unmarked column corresponds to a part in λ . For instance, taking $\alpha = (2, 1)$ and $n = 7$, we have the following cycle-path types for varying $\alpha \otimes \beta$:



Note that marked singleton columns correspond to paths of length zero (i.e., isolated nodes).

We are now in a position to give a formula for $\omega_{(\mu|\nu)}^{(\lambda|\rho)}$ for all cycle-path types. Let $\alpha \otimes \beta$ be the irreducible representation of G represented by the cycle-path type $(\lambda|\rho)$. We may pick a double coset representative $(\tau, \sigma) \in G$ of $(\mu|\nu)$ such that $\tau = ()$, as the one-sided action of S_n on injections is transitive. We have

$$\begin{aligned} \omega_{(\mu|\nu)}^{(\lambda|\rho)} &= \omega^{(\lambda|\rho)}(((), \sigma)) = \frac{1}{|K|} \sum_{k \in K} \chi_{\alpha \otimes \beta}(((), \sigma)^{-1}k) \\ &= \frac{1}{|K|} \sum_{(k_1, k_2) \in K} \chi_{\alpha \otimes \beta}((k_1, \sigma^{-1}k_1k_2)) \\ &= \frac{1}{k!(n-k)!} \sum_{k_1 \in S_k} \chi_{\alpha}(k_1) \sum_{k_2 \in S_{n-k}} \chi_{\beta}(\sigma^{-1}k_1k_2). \end{aligned}$$

Note that the entries of the character table of any symmetric association scheme are algebraic integers, and the characters of the symmetric group are integers; therefore, the projection formula above shows that the entries of the character table of the injection scheme are integers. As an aside, this gives a much simpler proof of the integrality of the spectra of so-called (n, k, r) -arrangement graphs, which live in the Bose-Mesner algebra of $\mathcal{A}_{k,n}$ (see [9] for more details).

Although the projection formula gives an explicit way of computing the character table of $\mathcal{A}_{k,n}$, it is difficult to work with from both a computational and analytical point of view. It becomes

prohibitively difficult to compute the character table of $\mathcal{A}_{k,n}$ using this formula for even modest values of k, n , and it seems difficult to derive good expressions for the characters of $\mathcal{A}_{k,n}$ using this formula. Indeed, we are unaware of any result that leverages the projection formula for spherical functions to derive tractable expressions for the character tables of association schemes associated with Gelfand pairs.

4. A Canonical Basis for the Injection Scheme

Let (ρ_1, V_1) and (ρ_2, V_2) be two representations of a group H , and let $\phi : V_1 \rightarrow V_2$ be a linear transformation. We say that ϕ *intertwines* ρ_1 and ρ_2 if $\phi\rho_1(h) = \rho_2(h)\phi$ for all $h \in H$.

Lemma 4.1 (Schur's Lemma). *If (ρ_1, V_1) and (ρ_2, V_2) are irreducible representations of H and ϕ is an intertwining map for ρ_1 and ρ_2 , then either ϕ is the zero map or it is an isomorphism.*

Let $\mathbb{C}[S_{k,n}]$ be space of all complex-valued functions defined over injections $S_{k,n}$. Let $\{e_i\}$ defined such that $e_i(j) = \delta_{i,j}$ for all $i, j \in S_{k,n}$ be the standard basis for this space. For any $\lambda \vdash n$, let M^λ be permutation representation of S_n acting on the set of all λ -tabloids. Let $\{e_{\{t\}}\}$ defined such that $e_{\{t\}}(\{s\}) = \delta_{\{t\}, \{s\}}$ for any two λ -tabloids $\{t\}, \{s\}$ be the standard basis for this space. The product $M^\mu \otimes M^\lambda$ is a $G_{k,n}$ -representation with basis $\{e_{\{s\}} \otimes e_{\{t\}}\}$ where $\{s\}, \{t\}$ range over all μ -tabloids and λ -tabloids respectively.

Let $\{s\}$ be a μ -tabloid and $\{t\}$ be a λ -tabloid such that $\mu \vdash k$ and $\lambda \vdash n$. We say that $\{s\}, \{t\}$ *covers* an injection $\sigma \in S_{k,n}$ if $\text{row}_{\{s\}}(i) = \text{row}_{\{t\}}(\sigma(i))$ for all $1 \leq i \leq k$. For example, the injections $(1, 2, 3, 4, 5)$ in red and $(2, 3, 6, 5, 4)$ in thick blue are covered by the tabloids in normal and bold lettering below, whereas the injection $(4, 3, 6, 5, 2)$ in dashed blue is not:



Let $1_{\{s\}, \{t\}} \in \mathbb{C}[S_{k,n}]$ be the characteristic function of the set of injections covered by $\{s\}, \{t\}$. For any $\mu \vdash k, \lambda \vdash n$ such that λ/μ is a horizontal strip, let $\phi_{\mu, \lambda} : M^\mu \otimes M^\lambda \rightarrow \mathbb{C}[S_{k,n}]$ be the map defined such that

$$\phi_{\mu, \lambda}(e_{\{s\}} \otimes e_{\{t\}}) = 1_{\{s\}, \{t\}} \quad \text{for all } \{s\}, \{t\},$$

then extending linearly. An injection σ is covered by $\{s\}, \{t\}$ if and only if $(\tau, \pi)\sigma$ is covered by $(\{\tau s\}, \{\pi t\})$ for all $(\tau, \pi) \in G_{k,n}$. This implies that

$$\phi_{\mu, \lambda}(\tau e_{\{s\}} \otimes \pi e_{\{t\}}) = (\tau, \pi)\phi_{\mu, \lambda}(e_{\{s\}} \otimes e_{\{t\}}) \quad \text{for all } (\tau, \pi) \in G_{k,n},$$

i.e., the linear map $\phi_{\mu, \lambda}$ intertwines $M^\mu \otimes M^\lambda$ and $\mathbb{C}[S_{k,n}]$.

It is well-known that the λ -isotypic component of M^λ has multiplicity 1, and so the $(\mu \otimes \lambda)$ -isotypic component of $M^\mu \otimes M^\lambda$ has multiplicity 1. Let $(\rho_{\mu, \lambda}, V_\mu \otimes V_\lambda)$ be this $G_{k,n}$ -irreducible. A basis for $\rho_{\mu, \lambda}$ can be obtained by tensoring all pairs of standard μ -polytabloids and standard λ -polytabloids. For each standard Young tableau t , let e_t denote the corresponding standard polytabloid.

We say that an injection σ is *aligned* with respect to $\{s\}, \{t\}$ if $\text{row}_{\{s\}}(i) = \text{row}_{\{t\}}(\sigma(i))$ and $\text{col}_s(i) = \text{col}_t(\sigma(i))$ for all $1 \leq i \leq k$. In the example above, the blue dashed injection $(2, 3, 6, 5, 4)$ is not aligned with the tabloids above, but the red injection $(1, 2, 3, 4, 5)$ is.

Lemma 4.2. *For each irreducible representation $V_\mu \otimes V_\lambda$ of the induced representation $1\uparrow_{K_{k,n}}^{G_{k,n}}$, there exists a $v \in V_\mu \otimes V_\lambda$ such that $\phi_{\mu,\lambda}(v) \neq 0$.*

PROOF. Let e be the identity injection. Consider the pair of standard Young tableaux s, t of shape μ and λ respectively obtained by inserting the numbers $1, 2, \dots, k$ into the rows of s from left to right, top to bottom, then taking t to be the standard Young tableau obtained from s by adding a horizontal strip and labeling the cells $k+1, k+2, \dots, n$ from left to right. For example, if $\mu = (3, 2, 1)$ and $\lambda = (4, 3, 2)$, then s and t are

$$\begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & 5 & \\ \hline 6 & & \\ \hline \end{array} \quad \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 9 \\ \hline 4 & 5 & 8 & \\ \hline 6 & 7 & & \\ \hline \end{array}.$$

Note that e is aligned with respect to $\{s\}, \{t\}$. Let C_s, C_t denote the column-stabilizers of s and t respectively. It is clear that

$$e_s \otimes e_t = \sum_{\pi \in C_s, \pi' \in C_t} \text{sgn}(\pi) \text{sgn}(\pi') e_{\{\pi s\}} \otimes e_{\{\pi' t\}}.$$

Let $v = e_s \otimes e_t$ and $f = \phi_{\mu,\lambda}(v)$. We have

$$f(e) = \sum_{\pi \in C_s, \pi' \in C_t} \text{sgn}(\pi) \text{sgn}(\pi') 1_{\{\pi s\}, \{\pi' t\}}(e).$$

If $\pi \in C_s$ sends i to j such that $1 \leq i, j \leq k$, then $\pi' \in C_t$ must also send i to j , otherwise $\{\pi s\}, \{\pi' t\}$ does not cover e . On the other hand, if $\pi' \in C_t$ sends i to j such that $1 \leq i \leq k$ and $k+1 \leq j \leq n$, then $(\{\pi s\}, \{\pi' t\})$ does not cover e for all $\pi \in C_s$, which implies that the cells of the horizontal strip λ/μ are fixed points of every $\pi' \in C_t$ such that $\{\pi s\}, \{\pi' t\}$ covers e . The foregoing implies that $\text{sgn}(\pi) \text{sgn}(\pi') = 1$ if and only if $\{\pi s\}, \{\pi' t\}$ covers e . In particular, we have

$$f(e) = \sum_{\pi \in C_s, \pi' \in C_t} \text{sgn}(\pi) \text{sgn}(\pi') 1_{\{\pi s\}, \{\pi' t\}}(e) = |C_s|,$$

thus $f = \phi_{\mu,\lambda}(v) \neq 0$, as desired. \square

Now let $f_{s,t} := \phi_{\mu,\lambda}$ where s, t are standard Young tableaux of shape $\mu \vdash k$ and $\lambda \vdash n$ such that λ/μ is a horizontal strip. Let $\mathcal{F} := \{f_{s,t}\}$ where s and t range over all such standard Young tableaux. By Lemma 4.2, $\phi_{\mu,\lambda}$ is not the zero map, so by Schur's Lemma, we have that $\phi_{\mu,\lambda}$ is an isomorphism. The elements of \mathcal{F} are pairwise linearly independent, hence Corollary 2.2 implies that \mathcal{F} is a basis. Moreover, we have the property that basis functions in different isotypic components are orthogonal, thus we arrive at the following theorem.

Theorem 4.3. *The set \mathcal{F} is a basis for $\mathbb{C}[S_{k,n}]$ such that $\langle f_{q,r}, f_{s,t} \rangle = 0$ for all $f_{q,r} \in V_{\mu \otimes \lambda}$ and $f_{s,t} \in V_{\mu' \otimes \lambda'}$ such that $\lambda/\mu \neq \lambda'/\mu'$.*

It would be interesting to refine the result above to a *Fourier basis* for $\mathbb{C}[S_{k,n}]$, that is, further require that basis functions in the same isotypic component are orthogonal. Note that Young's orthogonal form furnishes such a basis for the case $k = n$ (see [16]).

Theorem 4.4 (Frobenius Reciprocity). *Let ρ be an irreducible representation of a group H and let K be a subgroup of H . The multiplicity of the ρ -isotypic component of $1 \uparrow_K^H$ is the dimension of the subspace of K -invariant functions of the ρ -isotypic component.*

Let $Q_{k,n}$ denote the projection onto the space of $K_{k,n}$ -invariant functions. For any $\mu \vdash k$, define $\mu! := \mu_1! \mu_2! \cdots \mu_{\ell(\mu)}!$.

Lemma 4.5. *Let s, t be standard Young tableaux of shape $\mu \vdash k$ and $\lambda \vdash n$ such that λ/μ is a horizontal strip. If $Q_{k,n} f_{s,t} \neq 0$, then $\frac{1}{(\mu^\top)!} Q_{k,n} f_{s,t}$ is the $(\mu \otimes \lambda)$ -spherical function.*

PROOF. By construction, $f_{s,t} \in \mathbb{C}[S_{k,n}]$ lives in the irreducible $W \leq \mathbb{C}[S_{k,n}]$ that is isomorphic to $V_\mu \otimes V_\lambda$. Because $Q_{k,n}$ sends W to W , we have that $Q_{k,n} f_{s,t} \in W$ is a $K_{k,n}$ -invariant function. By Frobenius Reciprocity, the space of $K_{k,n}$ -invariant functions of W has dimension 1; therefore, if $Q_{k,n} f_{s,t} \neq 0$, then it is the $(\mu \otimes \lambda)$ -spherical function up to scaling. To ensure that the (μ, λ) -spherical function is 1 on the $K_{k,n} \backslash () / K_{k,n}$ double coset, we normalize by $|C_s| = (\mu^\top)!$. \square

We are now ready to give a proof of our formula for the spherical functions of $(G_{k,n}, K_{k,n})$. Let s, t be the pair of standard Young tableaux as defined in the proof of Lemma 4.2.

Theorem 4.6. *Let $\omega^{\mu \otimes \lambda}$ be the $(\mu \otimes \lambda)$ -spherical function of the Gelfand pair $(G_{k,n}, K_{k,n})$. Then*

$$\omega_{(\gamma|\rho)}^{\mu \otimes \lambda} = \frac{1}{|C_{(\gamma|\rho)}|} \sum_{\sigma \in C_{(\gamma|\rho)}} \sum_{\pi \in C_t} \text{sgn}(\pi) 1_{\{s\}, \{\pi t\}}(\sigma), \text{ and}$$

$$P_{\mu \otimes \lambda, (\gamma|\rho)} = \sum_{\sigma \in C_{(\gamma|\rho)}} \sum_{\pi \in C_t} \text{sgn}(\pi) 1_{\{s\}, \{\pi t\}}(\sigma)$$

for all cycle-path types $(\gamma|\rho)$. Moreover, .

PROOF. An argument similar to the proof of Lemma 4.2 shows that $Q_{k,n} f_{s,t} \neq 0$, hence $Q_{k,n} f_{s,t} = \omega^{(\mu \otimes \lambda)}$ by the lemma above. In particular, we have

$$\omega_{(\gamma|\rho)}^{\mu \otimes \lambda} = \frac{1}{(\mu^\top)! |C_{(\gamma|\rho)}|} \sum_{\pi \in C_s, \pi' \in C_t} \text{sgn}(\pi) \text{sgn}(\pi') |\{\sigma \in C_{(\gamma|\rho)} : \{\pi s\}, \{\pi' t\} \text{ covers } \sigma\}|.$$

But note that $C_s \leq C_t$, which gives us

$$\omega_{(\gamma|\rho)}^{\mu \otimes \lambda} = \frac{1}{(\mu^\top)! |C_{(\gamma|\rho)}|} \sum_{\pi \in C_s, \tau \pi \in C_t} \text{sgn}(\tau) |\{\sigma \in C_{(\gamma|\rho)} : \{\pi s\}, \{\tau \pi t\} \text{ covers } \sigma\}|.$$

Since $\{\pi s\}, \{\tau \pi t\}$ covers σ if and only if $\{s\}, \{\tau t\}$ covers σ , we may rewrite the above as

$$\omega_{(\gamma|\rho)}^{\mu \otimes \lambda} = \frac{1}{|C_{(\gamma|\rho)}|} \sum_{\pi \in C_t} \text{sgn}(\pi) |\{\sigma \in C_{(\gamma|\rho)} : \{s\}, \{\pi t\} \text{ covers } \sigma\}|.$$

Rearranging completes the proof of the first part, and Proposition 3.3 proves the second part. \square

To give a quick demonstration of the formula's efficacy, let $\bar{\mu} := (\mu_1 + n - k, \mu_2, \dots, \mu_{\ell(\mu)}) \vdash n$ for any $\mu \vdash k$, and consider the spherical function $\omega^{\mu \otimes \bar{\mu}}$. For any $(\gamma|\rho)$ such that ρ has more than μ_1 non-trivial paths, for each $\sigma \in C_{(\gamma|\rho)}$, there exist two cells c_σ, c'_σ in the same column of t that are not in the image of σ . Each of these involutions (c_σ, c'_σ) are sign-reversing, showing that $\omega_{(\gamma|\rho)}^{\mu \otimes \bar{\mu}} = 0$, which is hardly transparent from the projection formula. Indeed, the $(\mu \otimes \bar{\mu})$ -spherical functions play a crucial role in [2, 24], and our formula may allow one to improve the results of [24].

5. Code bounds

5.1. Delsarte's linear programming bound. Consider an association scheme $\mathcal{A} = \{A_0, A_1, \dots, A_d\}$ over X , as defined in Section 3.1.

For a subset $Y \subseteq X$, its characteristic function $\phi = \phi_Y \in \{0, 1\}^X$ is defined in the usual way as

$$\phi(x) = \begin{cases} 1 & \text{if } x \in Y; \\ 0 & \text{otherwise.} \end{cases}$$

Assuming $Y \neq \emptyset$, its *inner distribution vector* $\mathbf{a} = \mathbf{a}_Y = (a_0, a_1, \dots, a_d)$ has entries

$$a_i = \frac{\phi^\top A_i \phi}{\phi^\top \phi},$$

representing the relative frequencies of i th associates among pairs of elements of Y .

The following observation is simple, yet has profound consequences.

Theorem 5.1 (Delsarte, [12]). *For $\emptyset \neq Y \subseteq X$, its inner distribution vector \mathbf{a} satisfies*

$$\mathbf{a}Q \geq \mathbf{0},$$

where Q is the dual eigenmatrix.

A linear programming bound for association schemes is carried by Theorem 5.1 in the following sense. For a set D of associate indices, a D -code is a subset $Y \subseteq X$ such that any two distinct elements of Y are i th associates for some $i \in D$. In other words, in terms of the distribution vector, Y is a D -code if $a_i = 0$ for $i \notin D$. Moreover, distribution vectors are normalized so that $a_0 = 1$. Consider the LP

$$(5.1) \quad \begin{aligned} & \text{maximize} && \sum_i a_i \\ & \text{subject to} && \mathbf{a}Q \geq \mathbf{0}, \ a_0 = 1 \text{ and } a_i = 0 \text{ for } i \in D. \end{aligned}$$

It follows from Theorem 5.1 and the above remarks that the cardinality of a D -code is upper bounded by the solution of (5.1).

Using (5.1), Tarnanen [31] computed LP bounds on permutation codes for $n \leq 10$ and various allowed distance sets. This was extended by Bogaerts [6] to $n \leq 14$. Here, the character table of S_n takes the role of Q , and the set D is built to contain all $\lambda \vdash n$ such that n minus the number of ones in λ belong to the allowed set of Hamming distances. For example, with $n = 5$ and Hamming distances in $\{2, 4, 5\}$, we take D to consist of the associate indices

$$(2, 1, 1, 1), (2, 2, 1), (4, 1), (3, 2), (5).$$

With this in mind, we abuse notation and henceforth let D simply denote our set of allowed Hamming distances.

For the injection scheme $\mathcal{A}_{k,n}$, we implemented (5.1) for $3 \leq k < n \leq 15$, with the exception of a few parameter pairs (k, n) at the larger end of this triangle, which are presently out of reach. Whereas character tables for the symmetric group, and even for $\mathcal{A}_{n-1,n}$ using [29], can be computed recursively for moderately large n , the character table for general k and n is presently more challenging computationally, even with our combinatorial formula from Section 4. On the other hand, the LP itself is comparatively easy to solve (and check numerically), even for parameters near the upper end of our range.

n	k	d	$M \leq$	n	k	d	$M \leq$	n	k	d	$M \leq$
7	6	4	199	11	9	4	256682	13	12	4	123235550
8	6	3	1513			5	47073			5	23347599
	7	4	1462		10	4	936332			6	4687470
9	7	4	2846			5	185560			7	910371
	8	4	12096			6	42068	14	13	4	1621775700
		5	2417	12	8	3	602579			5	309490273
10	7	3	27308		9	4	584327			6	58903464
	8	4	26206		10	4	2699260			7	10510496
		5	5039			5	471981			8	2117618
	9	4	92418		11	4	10241521	15	14	4	23358981663
		5	19158			5	1922527			5	4130012797
		6	4991			6	411090			6	804830167
11	8	4	52646	13	9	4	1185053			7	138132435
										8	24260981

TABLE 1. Upper bounds on $M(n, k, d)$ via linear programming.

In what follows, we let $M(n, k, D)$ denote the maximum size of a D -code in the injection scheme $\mathcal{A}_{k,n}$, where D contains the allowed Hamming distances. We briefly describe a few natural distance sets D and discuss some related combinatorial problems. Tables of LP bounds accompany these different categories of codes.

5.2. Classical minimum distance codes. For the purpose of detecting and correcting errors, the distance sets typically considered in coding theory model a minimum allowed distance; that is, one takes $D = \{d, d+1, \dots\}$ for some integer d . Following the notation used in [11, 17, 31], we write $M(n, k, d)$ in place of $M(n, k, \{d, d+1, \dots\})$ for the maximum size of an injection code with minimum Hamming distance d . Some basic observations and bounds on $M(n, k, d)$ can be found in [17]. A basic recursive upper bound is as follows.

Proposition 5.2 (Singleton bound). $M(n, k, d) \leq n!/(n-k+d-1)! = |S_{k-d+1,n}|$.

For $r > 0$, let b_r be the size of the (any) ball of radius r in $S_{k,n}$. In [17] b_r is determined as

$$\sum_{j=0}^{\lfloor r \rfloor} \binom{k}{j} \sum_{i=0}^j (-1)^i \binom{j}{i} \frac{(n-k+j-i)!}{(n-k)!}.$$

A standard argument then gives the sphere packing bound for injections.

Proposition 5.3 (Sphere packing bound). $M(n, k, d) \leq \frac{|S_{k,n}|}{b_{(d-1)/2}}$.

Additional bounds on $M(n, k, d)$ are motivated by interest in the permutation code case, both for applications to powerline communication [11, 23] and as an extremal problem of independent combinatorial interest. Indeed, equality in the Singleton bound is equivalent to existence of an ordered design; see [10, Section VI.38] and [17] for more information.

The case $d = k - 1$ has special significance for its connection with latin squares. Colbourn, Kløve and Ling [11] showed that the existence of r mutually orthogonal latin squares of order n imply a permutation code of length n and minimum distance $n - 1$ of size rn . Here, the code permutations

correspond to the n level sets occurring among each of the r squares. With this same construction, it is easy to see that the existence of r mutually orthogonal $k \times n$ latin rectangles implies $M(n, k, k-1) \geq rn$. It follows that an upper bound on $M(n, k, k-1)$ induces an upper bound on the number of mutually orthogonal $k \times n$ latin rectangles.

Example 5.4. There exist a set of four mutually orthogonal incomplete 6×6 latin squares missing a common 2×2 subsquare. This implies the existence of four 4×6 latin rectangles which are mutually orthogonal in the sense that superimposing any two produces no repeated pairs. It follows that $M(6, 4, 3) \geq 24$; in fact, $M(6, 4, 3) = 27$ was shown in [17].

Table 1 presents those upper bounds on $M(n, k, d)$ we found which improve the Singleton bound and the sphere packing Bound for $k < n \leq 12$, all $k \leq 10$ with $n \leq 15$, $k = n - 1 < 15$, and $(n, k) \in \{(13, 9), (14, 9)\}$. There is no entry for $(n, k) = (14, 9)$ as the LP bound is never better than one of the two trivial bounds.

While building and verifying our table of code bounds, we noticed that Bogaerts' claim in [6] of there being no improvements via (5.1) to the Singleton bound for permutation codes ($k = n$) with $14 \leq n \leq 16$ is incorrect. The correct values can be found in Table 2.

n	d	$M(n, d) \leq$	n	d	$M(n, d) \leq$
11	4	<i>3326400</i>	14	4	5298680543
	6	158617	5		918752861
	7	36718	6		255869198
12	4	<i>39916800</i>	7		53744475
	5	6141046	8		9901953
	6	1766160	9		2083046
	7	361395	15	4	78702624000
13	4	411555972	5		12053059200
	5	75789397	6		3511921683
	6	21621600	7		773606486
	7	4163390	8		130245681
	8	879527	9		23627561

TABLE 2. LP upper bounds on permutation codes with minimum distance d . Bounds which are obtained in [6], but not due the LP bound, are cursive. Bounds which are correctly the LP bound in [6] are bold.

5.3. Equidistant codes and general distance sets. An *equidistant permutation array*, or $\text{EPA}(n, d)$ is a subset $\Gamma \subseteq S_n$ with the property that any two distinct elements have Hamming distance exactly d . In other words, an $\text{EPA}(n, d)$ is a $\{d\}$ -code in (the conjugacy scheme of) S_n . The problem of determining bounds on these objects dates back to the 1970s, beginning with a question of Bolton in [8]. A concise survey on equidistant permutation arrays can be found in [10, Section VI.44.5]. To our knowledge, the more general problem of equidistant injection codes has not been considered. However, Huczynska [23] has considered equidistant families for the ‘constant composition’ variation in which permutations are replaced by codewords having every element in $[n]$ occurring equally often.

As a particular case, distance $k/2$ for injections of even length k may be especially interesting for possible connections with Hadamard matrices.

n	k	d	$M \leq$	Triv	n	k	d	$M \leq$	Triv	n	k	d	$M \leq$	Triv
5	3	2	5	6	10	8	3	30	33	12	5	2	23	24
	4	3	6	7			6	92	107		6	2	26	27
7	3	2	8	9		9	3	22	23			3	49	50
	4	2	9	10			4	47	58		7	3	60	61
	5	3	14	15			5	92	95			4	104	114
	6	3	13	14			7	75	96			5	92	96
	4		26	30	11	4	3	20	21		8	3	66	67
8	6	3	20	21		6	3	42	43			6	146	156
		4	37	40			4	53	54		9	3	53	57
	7	4	30	32		7	3	49	52			4	115	116
		5	45	52			4	94	100			7	166	191
9	6	3	28	29			5	87	93		10	3	38	43
		4	42	45		8	3	48	52			4	114	119
	7	3	26	30			6	142	143			5	199	201
	8	3	20	21		9	3	33	38			6	212	214
		4	40	44			6	117	119			7	166	168
		6	59	72			7	108	141			8	126	180
10	4	3	18	19			8	60	61			9	76	77
	6	3	35	36		10	4	52	67		11	3	28	29
		4	47	49			5	108	132			4	56	75
	7	3	40	42			6	187	189			5	120	150
		4	77	78			8	93	123			6	393	394
		5	83	87								7	317	324
												9	112	153

TABLE 3. Upper bounds on $M = M(n, k, \{d\})$ for equidistant injection codes. The column with heading ‘Triv’ contains a trivial upper bound given by (5.2); that is, the floor of $|S_{k,n}|$ divided by the LP bound for $M(n, k, \{d\}^c)$.

Table 3 presents various upper bounds on $M(n, k, \{d\})$ for $2 \leq d < k < n \leq 10$, that is, upper bounds on the size of a family of injections in $S_{k,n}$ at pairwise distance exactly d .

Studying various other sets of allowed distances is natural in many situations. Delsarte showed [12] that the solution $M_{LP}(D)$ to (5.1) satisfies a clique-coclique bound

$$(5.2) \quad M_{LP}(D)M_{LP}(D^c) \leq |X|,$$

where D^c denotes the complement of D . In particular, it follows from (5.2) that code bounds in the minimum distance case can be obtained from applying the LP (5.1) to the pairwise *maximal* distance case. As an example, Tarnanen [31] and Dukes and Sawchuk [18] compute LP bounds for some small allowed distances, such as $D = \{2, 3\}$, which hold for general n .

Even dropping the condition that allowed distances form an interval is not without some precedent in other contexts: set systems with intersection conditions modulo a prime, arcs in finite geometries, or the independence number of relation graphs in an association scheme.

We offer a (contrived) example for injections with a distance set which is not an interval. Recall that in ‘eventown’, with population N , there is a family \mathcal{C} of clubs with the property that $|C \cap C'|$ is even for any $C, C' \in \mathcal{C}$. Berlekamp [5] showed that the number of clubs satisfies $|\mathcal{C}| \leq 2^{\lfloor N/2 \rfloor}$.

Problem. The N citizens of eventown are electing a mayor from a selection of n candidates. Each ballot consists of a ranked list of k of the candidates. Is it possible for every two ballots to agree in an even number of places? The answer is yes if $N \leq M(n, k, D)$, where $D = \{2, 4, 6, \dots\}$.

In Table 4, we present a sample of upper bounds found on $M(n, k, D)$ for small n, k and sets of distances $D \subseteq [k]$. We only list entries for which Equation (5.2) is not satisfied with equality, that is

$$M_{\text{LP}}(D)M_{\text{LP}}(D^c) < |X|.$$

Recently, Aljohani, Bamberg, and Cameron defined the concepts of *synchronizing* and *separating* for association schemes [1]. In our language, the injection scheme is non-separating if

$$M(n, k, D)M(n, k, D^c) = |X|$$

for one non-trivial D . Table 4 implies that the injection scheme is non-separating for $(n, k) \in \{(5, 3), (6, 3), (7, 3)\}$ if we limit ourselves to distance-sets and not all possible graphs.

6. Future Work and Open Questions

6.1. Representation Theory. Our main question is to what extent the representation theory of the symmetric group (i.e., the Gelfand pair $(S_n \times S_n, \text{diag}(S_n))$) carries over to the Gelfand pair $(G_{k,n}, K_{k,n})$. Indeed, we believe there are stronger connections to the representation theory of the symmetric group yet to be shown.

For example, following [25, I.7] and letting

$$C' := \bigoplus_{k,n : k \leq n} \mathbb{C}[K_{k,n} \backslash G_{k,n} / K_{k,n}],$$

one can define a natural bilinear multiplication on C' so that it is a commutative and associative graded \mathbb{C} -algebra. Classically, the characteristic map $\text{ch} : C \rightarrow \Lambda$ is an isometric isomorphism between the commutative and associative graded algebra C generated by all irreducible characters of symmetric groups and the ring of symmetric functions Λ . It would be particularly interesting to find an analogous characteristic map $\text{ch}' : C' \rightarrow \Lambda'$ to a suitable polynomial ring Λ' such that its vector space $(\Lambda')^k$ of degree- k polynomials has dimension equal to the number of cycle-types of $S_{k,n}$.

Finally, we suspect there are other Lie and q -analogues of $(G_{k,n}, K_{k,n})$ that might be worth investigating, which would likely require different techniques than the ones presented here.

6.2. Coding Theory. It is of interest to determine when $M(n, k, D)$ can achieve its LP upper bound. For $D = \{d, d+1, \dots, n\}$, a few constructions can be found in [17], but essentially nothing is known for other distance sets D . In another direction, one can also investigate the behavior of the LP bound itself. A look at Table 1 suggests that for fixed k , the LP bound is non-trivial only for a finite number of values of n .

As noted earlier, our data suggests that the injection scheme is usually separating except for maybe a few exceptional cases. It would be interesting to show this formally.

References

- [1] M. Aljohani, J. Bamberg, P. J. Cameron, Synchronization and separation in the Johnson schemes. *Portugaliae Mathematica* 74 (2018), 213–232.

n	k	D	$M \leq$	Triv	n	k	D	$M \leq$	Triv
5	3	$\{1,3\}$	10	12	6	6	$\{1,3\}$	15	18
		$\{1,3\}$	9	10			$\{1,4\}$	37	46
	4	$\{2,4\}$	12	13			$\{1,5\}$	40	42
		$\{1,2,4\}$	17	20			$\{2,4\}$	28	35
		$\{1,3,4\}$	29	30			$\{2,5\}$	41	42
6	3	$\{1,3\}$	16	17			$\{3,4\}$	34	36
		$\{1,4\}$	23	26			$\{3,5\}$	41	43
	5	$\{2,4\}$	17	19			$\{3,6\}$	47	48
		$\{2,5\}$	22	23			$\{4,5\}$	31	34
		$\{3,4\}$	20	21			$\{4,6\}$	64	70
		$\{3,5\}$	25	26			$\{1,2,4\}$	37	46
		$\{1,2,4\}$	27	28			$\{1,3,4\}$	52	60
		$\{1,3,4\}$	31	32			$\{1,2,5\}$	71	78
		$\{1,2,5\}$	34	36			$\{1,3,5\}$	58	60
		$\{1,3,5\}$	37	42			$\{1,4,5\}$	58	61
		$\{1,4,5\}$	56	60			$\{1,2,6\}$	40	41
		$\{2,3,5\}$	27	31			$\{1,3,6\}$	74	75
		$\{2,4,5\}$	52	55			$\{1,4,6\}$	110	120
		$\{1,2,3,5\}$	53	55			$\{2,3,5\}$	42	45
		$\{1,2,4,5\}$	68	72			$\{2,4,5\}$	67	68
7	3	$\{1,3\}$	23	26			$\{2,3,6\}$	82	86
		$\{1,3\}$	22	23			$\{2,4,6\}$	83	86
	4	$\{1,4\}$	24	25			$\{2,5,6\}$	84	96
		$\{2,3\}$	33	35			$\{3,4,5\}$	122	126
		$\{2,4\}$	36	38			$\{3,4,6\}$	64	70
		$\{1,2,4\}$	72	76			$\{3,5,6\}$	108	136
		$\{1,3,4\}$	84	93			$\{1,2,3,5\}$	72	78
		$\{1,4\}$	39	40			$\{1,2,4,5\}$	105	107
	5	$\{1,5\}$	19	20			$\{1,3,4,5\}$	151	152
		$\{2,4\}$	34	36			$\{1,2,3,6\}$	146	162
		$\{2,5\}$	45	47			$\{1,2,4,6\}$	117	122
		$\{3,4\}$	35	36			$\{1,3,4,6\}$	118	122
		$\{3,5\}$	38	40			$\{1,2,5,6\}$	140	148
		$\{1,2,4\}$	62	66			$\{1,3,5,6\}$	141	180
		$\{1,3,4\}$	53	56			$\{2,3,4,6\}$	118	126
		$\{1,2,5\}$	69	72			$\{2,3,5,6\}$	108	136
		$\{1,3,5\}$	69	74			$\{2,4,5,6\}$	280	336
		$\{1,4,5\}$	111	114			$\{1,2,3,4,6\}$	233	240
		$\{2,3,4\}$	125	132			$\{1,2,3,5,6\}$	168	193
		$\{2,3,5\}$	63	64			$\{1,2,4,5,6\}$	360	387
		$\{2,4,5\}$	116	120					
		$\{1,2,3,5\}$	158	168					
		$\{1,2,4,5\}$	168	180					

TABLE 4. Various upper bounds on $M = M(n, k, D)$ for distance sets D . The column with heading ‘Triv’ contains a trivial upper bound given by (5.2); that is, the floor of $|S_{k,n}|$ divided by the LP bound for $M(n, k, D^c)$.

- [2] A. Ambainis, L. Magnin, M. Roetteler, and J. Roland, Symmetry-Assisted Adversaries for Quantum State Generation. *Proceedings of the 2011 IEEE 26th Annual Conference on Computational Complexity* (2011)
- [3] E. Bannai and T. Ito, Algebraic Combinatorics I: Association Schemes. Benjamin & Cummings, Menlo Park, CA, 1984.
- [4] A. Belovs and A. Rosmanis, Adversary lower bounds for the collision and the set equality problems. *Quantum Information & Computation* 18.3&4 (2018), 200–224.
- [5] E.R. Berlekamp, On subsets with intersections of even cardinality. *Canad. Math. Bull.* 4 (1969), 471–477.
- [6] M. Bogaerts, New upper bounds for the size of permutation codes via linear programming. *Electronic Journal of Combinatorics* 17 (2010), #R135.
- [7] M. Bogaerts and P. Dukes, Semidefinite programming for permutation codes. *Discrete Math.* 326 (2014), 34–43.
- [8] D.W. Bolton, Problem, in Combinatorics, D.J.A. Welsh and D. R. Woodall, eds., Instit. Math. Applic., Southend-on-Sea, Essex, England, 1972, 351–352.
- [9] B. Chen, E. Ghorbani and K. Wong, On the eigenvalues of certain Cayley graphs and arrangement graphs. *Linear Algebra and its Applications* 444 (2013), 246–253.
- [10] C.J. Colbourn and J.H. Dinitz, The CRC Handbook of Combinatorial Designs, 2nd Edition, CRC Press, Boca Raton, 2006.
- [11] C.J. Colbourn, T. Kløve, and A.C.H. Ling, Permutation arrays for powerline communication and mutually orthogonal Latin squares. *IEEE Trans. Inform. Theory* 50 (2004), 1289–1291.
- [12] Ph. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* No. 10 (1973).
- [13] P. Diaconis, Finite Fourier Methods: Access to Tools, In *Probabilistic combinatorics, Proc. Symposia Appl. Math.*, B. Bollabos, ed., 44 (1991) Amer. Math. Soc. Providence, R.I., 171–194.
- [14] M. Deza, R. C. Mullin and S. A. Vanstone, Room squares and equidistant permutation arrays. *Ars Combinatoria* 2 (1976), 235–244.
- [15] M. Deza and S.A. Vanstone, Bounds for permutation arrays. *J. Statist. Plann. Inference* 2 (1978), 197–209.
- [16] P. Diaconis, Group Representations in Probability and Statistics, *IMS Lecture Notes Series* 11, Hayward, CA, 1988.
- [17] P.J. Dukes, Coding with injections. *Des. Codes Cryptogr.* 65 (2011), 1–10.
- [18] P. Dukes and N. Sawchuck, Bounds on permutation codes of distance four. *J. Algebraic Combin.* 31 (2010), 143–158
- [19] P. Frankl and M. Deza, On the maximum number of permutations with given maximal or minimal distance. *J. Combin. Theory Ser. A* 22 (1977), 352–360.
- [20] C.D. Godsil, Association schemes, unpublished notes at <https://www.math.uwaterloo.ca/~cgodsil/pdfs/assoc2.pdf>, 2010.
- [21] A. Greenhalgh, Random walks on groups with subgroup invariance properties. Ph.D. Thesis, Dept. of Math., Stanford University, 1987.
- [22] K. Heinrich, G.H.J. van Rees, and W.D. Wallis, A general construction for equidistant permutation arrays, in Graph Theory and Related Topics, J.A. Bondy and U.S.R. Murty, eds., Academic Press, New York, 1979, 247–252.
- [23] S. Huczynska, Equidistant frequency permutation arrays and related constant composition codes. *Des. Codes Cryptogr.* 54 (2010), 109–120.
- [24] N. Lindzey and A. Rosmanis, A tight lower bound for index erasure. Preprint at <https://arxiv.org/abs/1902.07336>.
- [25] I.G. MacDonald, Symmetric Functions and Hall Polynomials. Oxford Mathematical Monographs, 1995.
- [26] A. Munemasa, The injection scheme of permutations. Unpublished manuscript at <http://www.math.is.tohoku.ac.jp/~munemasa/documents/2001-KusatsuReport.pdf>
- [27] B.E. Sagan, The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions. Springer-Verlag, 2000.
- [28] D.H. Smith and R. Montemanni, A new table of permutation codes. *Des. Codes Cryptogr.* 63 (2012), 241–253.
- [29] E. Strahov, Generalized characters of the symmetric group. *Adv. Math.* 212 (2007), 109–142.
- [30] S. Suda, A generalization of the Erdős-Ko-Rado theorem to t -designs in certain semilattices. *Discrete Math.* 312 (2012), 1827–1831.
- [31] H. Tarnanen, Upper bounds on permutation codes via linear programming. *European J. Combin.* 20 (1999), 101–114.

Peter J. Dukes: Mathematics and Statistics, University of Victoria, Victoria, BC

E-mail address: `dukes@uvic.ca`

Ferdinand Ihringer: Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Ghent, Belgium

E-mail address: `Ferdinand.Ihringer@gmail.com`

Nathan Lindzey: Computer Science, University of Colorado Boulder, Boulder, CO

E-mail address: `Nathan.Lindzey@colorado.edu`