XXXX
Draft

Uniqueness for 2-Intersecting Families of Permutations and Perfect Matchings

Gilad Chase, Neta Dafni, Yuval Filmus, & Nathan Lindzey

ABSTRACT. We characterize the largest 2-intersecting families of permutations on n symbols and perfect matchings of the complete $2n$-vertex graph for all n.

1. INTRODUCTION

Erdős–Ko–Rado combinatorics [13] is the study of intersecting families of objects. One of the seminal results of this area is the Ahlswede–Khachatrian theorem [1, 2].

THEOREM 1.1. *Let $\mathcal{F}$ be a subset of $\binom{[n]}{k}$ (the collection of all subsets of $[n] = \{1, \ldots, n\}$ of size k) which is t-*intersecting*: every $A, B \in \mathcal{F}$ satisfy $|A \cap B| \geqslant t$. Then*

$$|\mathcal{F}| \leqslant \max_{r \leqslant (n-t)/2} \left| \left\{ A \subseteq \binom{[n]}{k} : |A \cap [t+2r]| \geqslant t + r \right\} \right|.$$

Furthermore, if $\mathcal{F}$ achieves this bound, then

$$\mathcal{F} = \left\{ A \subseteq \binom{[n]}{k} : |A \cap S| \geqslant t + r \right\}$$

for some $r \leqslant (n-t)/2$ and some $S \subseteq [n]$ of size $t + 2r$.

The theorem consists of two statements: an *upper bound* on the size of a t-intersecting families, and a characterization of the extremal families. The latter part is known as *uniqueness.*

The Ahlswede–Khachatrian theorem is about intersecting families of sets. In this paper, we focus on intersecting families of permutations and perfect matchings.

PERMUTATIONS. Let S_n be the group of all permutations of $[n] := \{1, 2, \cdots, n\}$. Two permutations $\alpha, \beta \in S_n$ are *t-intersecting* if there exist t distinct indices $i_1, \ldots, i_t \in [n]$ such that $\alpha(i_1) = \beta(i_1), \ldots, \alpha(i_t) = \beta(i_t)$. Ellis, Friedgut and Pilpel [12] conjecture that an Ahlswede–Khachatrian result holds for intersecting families of permutations.

XXXX 1st February 2023.

KEYWORDS. Erdős–Ko–Rado Combinatorics, Representation Theory of the Symmetric Group, Analysis of Boolean Functions.

ACKNOWLEDGEMENTS. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 802020-ERC-HARMONIC.

Conjecture 1.2. *Let $\mathcal{F}$ be a subset of S_n which is t-intersecting. Then*

$$|\mathcal{F}| \leqslant \max_{r \leqslant (n-t)/2} |\{\alpha \in S_n : \alpha(i) = i \text{ for at least } t+r \text{ many } i \in [t+2r]\}|.$$

Furthermore, if $\mathcal{F}$ achieves this bound, then

$$\mathcal{F} = \{\alpha \in S_n : \alpha(i_s) = j_s \text{ for at least } t+r \text{ many } s \in [t+2r]\}$$

for some $r \leqslant (n-t)/2$ and distinct $i_1, \ldots, i_{t+2r} \in [n]$ and distinct $j_1, \ldots, j_{t+2r} \in [n]$.

Notice that when $t \leqslant 3$, the maximum is always attained at $r = 0$, in which case the upper bound is $(n-t)!$, and the conjectured extremal families are the so-called *t-cosets* (also known as *canonically t-intersecting families*). These are the families obtained by taking two tuples of t distinct indices $I = (i_1, \ldots, i_t)$ and $J = (j_1, \ldots, i_t)$, then taking all $\sigma \in S_n$ such that $\sigma \cdot I = J$.

Deza and Frankl [17] proved the upper bound part of Conjecture 1.2 for $t = 1$ by noticing that the n cyclic rotations of any fixed permutation are pairwise non-1-intersecting. Showing uniqueness in this case proved to be a lot harder, but eventually many proofs were found [5, 21, 18, 12].

The case $t > 1$ is significantly harder. For every $t > 1$, Ellis, Friedgut and Pilpel [12] proved that the upper bound in Conjecture 1.2 holds for large enough n, and Ellis [10] proved that the uniqueness part of Conjecture 1.2 holds for large enough n. Ellis, Friedgut and Pilpel used a spectral technique based on the so-called Hoffman bound (closely related to the Lovász theta function and to the linear programming bound in coding theory), which has found many other applications in Erdős–Ko–Rado combinatorics [19].

Recently, Meagher and Razafimahatratra [26], refining the techniques of Ellis, Friedgut and Pilpel, proved that 2-intersecting subsets of S_n contain at most $(n-2)!$ permutations, thus verifying the upper bound part of Conjecture 1.2 for $t = 2$ and *all* n. However, they were unable to characterize the extremal families in this case. In this paper, we show that all such families are 2-cosets, thus verifying the uniqueness part of Conjecture 1.2 for $t = 2$ and all n.

Theorem 1.3. *Let $n \geqslant 2$. If $\mathcal{F}$ is a 2-intersecting subset of S_n of size $(n-2)!$, then there exist $i_1 \neq i_2$ and $j_1 \neq j_2$ such that*

$$\mathcal{F} = \{\alpha \in S_n : \alpha(i_1) = j_1 \text{ and } \alpha(i_2) = j_2\}.$$

Perfect matchings. A related area of study is intersecting families of perfect matchings of the complete graph on $2n$ vertices K_{2n}, which can be seen as the non-bipartite analog of S_n, the latter of which is the set of perfect matchings in the complete bipartite graph $K_{n,n}$. Let $\mathcal{M}_{2n}$ be the set of all perfect matchings of K_{2n}. A family of $\mathcal{M}_{2n}$ is *t-intersecting* if each pair of its members have t edges in common. Such a family is *canonically t-intersecting* if there exists a set t edges of K_{2n} such that every member of the family contains those t edges.

While it is easy to prove that a 1-intersecting family of perfect matchings contains at most $(2n-3)!! = (2n-3)(2n-5)\cdots(1)$ perfect matchings, more difficult arguments [20, 22, 25, 9] are needed prove that this is attained uniquely by the canonically 1-intersecting families.

Lindzey [23, 24] extended the arguments of Ellis, Friedgut and Pilpel [12, 10] to the setting of perfect matchings, proving that for all t, the maximum size t-intersecting families are t-cosets, for large enough n.

Recently, Fallat, Meagher and Shirazi showed that the maximum size of a 2-intersecting family is at most $(2n-5)!!$ for all n. However, they were unable to characterize the extremal families in this case. Extending our arguments in the setting of S_n, we prove an analog of Conjecture 1.3 for perfect matchings.

THEOREM 1.4. *Let $n \geqslant 2$. If $\mathcal{F}$ is a 2-intersecting subset of $\mathcal{M}_{2n}$ of size $(2n-5)!!$, then there exist distinct i_1, j_1, i_2, j_2 such that $\mathcal{F}$ consists of all perfect matchings containing the edges $\{i_1, j_1\}, \{i_2, j_2\}$.*

OVERVIEW OF THE PROOFS. The spectral technique used by Ellis, Friedgut and Pilpel shows that for every $t \geqslant 1$, if n is large enough and $\mathcal{F} \subseteq S_n$ is a t-intersecting family of size $(n-t)!$, then the characteristic function of $\mathcal{F}$, denoted as $1_{\mathcal{F}}$, has *degree* at most t. This means that $1_{\mathcal{F}}$ can be expressed as a polynomial of degree at most t in the Boolean variables x_{ij}, where $x_{ij} = 1$ if the input permutation maps i to j. Equivalently, x_{ij} is the (i,j)'th entry of the permutation matrix representing the input permutation.

Similarly, Meagher and Razafimahatratra show that if $n \geqslant 5$ and $\mathcal{F} \subseteq S_n$ is a 2-intersecting family of size $(n-2)!$, then the characteristic function of $\mathcal{F}$ has degree at most 2. This is the starting point of this work.

Ellis, Friedgut and Pilpel used polyhedral techniques (i.e., the Birkhoff–von Neumann theorem on bistochastic matrices) to show that Boolean degree 1 functions are *dictators*, that is, they either depend only on $\alpha(i)$ for some $i \in [n]$ (where α is the input permutation), or they depend only on $\alpha^{-1}(j)$ for some $j \in [n]$. The only 1-intersecting dictators are 1-cosets, and this provides a proof of the uniqueness part of Conjecture 1.2 when $t = 1$.

Similar techniques do not work for larger degree [15]. Instead, we turn to the theory of *complexity measures of Boolean functions* [4], which was recently generalized to S_n and $\mathcal{M}_{2n}$ by Dafni et al. [9]. Using these techniques, Dafni et al. give a simple proof of the uniqueness part of Conjecture 1.2, as well as of its $\mathcal{M}_{2n}$ analogue, for large n. At a high level, these complexity measures allow one to deduce combinatorial structure from algebraic or representation-theoretical properties of Boolean functions. In particular, we use the notion of *certificate complexity* (described below) to distill enough combinatorial information about degree-2 Boolean functions corresponding to 2-intersecting families that we are able to classify the extremal families.

Let $f\colon S_n \to \{0,1\}$ be a Boolean function, and let $\alpha \in S_n$ be such that $f(\alpha) = b$. A *certificate* for α is a subset $\{i_1, \ldots, i_m\} \subseteq [n]$ such that $f(\beta) = b$ whenever $\beta(i_1) = \alpha(i_1), \ldots, \beta(i_m) = \alpha(i_m)$. The idea is that in order to verify that $f(\alpha) = b$, it suffices to check the value of $\alpha(i_1), \ldots, \alpha(i_m)$. The *certificate complexity* of α is the minimum size of a certificate for α, and the certificate complexity of f is the maximum, over all $\alpha \in S_n$, of α's certificate complexity. Let $C(f)$ be the certificate complexity of f.

Suppose that f is the characteristic function of a 2-intersecting subset of S_n. When $C(f) \leqslant n-2$, we give a structure result for f which suffices to bound the size of the family away from $(n-2)!$ unless $C(f) = 2$, in which case f is the characteristic function of a 2-coset. A simple argument (using another complexity measure, *sensitivity*) shows that if $n \geqslant 8$ and $f\colon S_n \to \{0,1\}$ has degree at most 2 then $C(f) \leqslant n-2$, allowing us to apply the preceding argument. Finally, we handle the case $n \leqslant 7$ using exhaustive search, employing an algorithm for enumerating maximum cliques.

Similar techniques work in the case of perfect matchings, with one complication: the proof of our structure result relies on the fact that Boolean degree 1 functions of S_n have certificate complexity 1, but this is not true for $\mathcal{M}_{2n}$ [9]. Using the maximality of maximum-size 2-intersecting families, we are able to overcome this hurdle.

Future research. Conjecture 1.2 is about families of permutations in which any two permutations agree on the images of t points. A related question concerns t-setwise-intersecting families of permutations, in which any two permutations α, β agree on the image of a set of size t: $\{\alpha(i_1), \ldots, \alpha(i_t)\} = \{\beta(i_1), \ldots, \beta(i_t)\}$ for a set of size t. Ellis [11] showed that for every t, if n is large enough then the maximum size of a t-setwise-intersecting subset of S_n is $t!(n-t)!$, and this is achieved uniquely by families of the form

$$\bigl\{\alpha \in S_n : \{\alpha(i_1), \ldots, \alpha(i_t)\} = \{j_1, \ldots, j_t\}\bigr\},$$

which we call *t-setwise-cosets*.

Meagher and Razafimahatrata [26] showed that when $t = 2$, the upper bound holds for all $n \geqslant 2$, and moreover, if $n \geqslant 4$ and f is the characteristic function of a 2-setwise-intersecting family of size $2(n-2)!$, then f has degree at most 2 and additionally satisfies $f^{=(n-2,1,1)} = 0$ (see Section 2.1.1 for an explanation of this notation). In other words, $f^{=\lambda} \neq 0$ only for $\lambda = (n), (n-1,1), (n-2,2)$.

Behajaina, Maleki, Rasoamanana and Razafimahatratra [3] showed that when $t = 3$, the upper bound holds for all $n \geqslant 11$, and moreover, if f is the characteristic function of a 3-setwise-intersecting family of size $6(n-3)!$, then $f^{=\lambda} \neq 0$ only for $\lambda = (n), (n-1,1), (n-2,2), (n-3,3)$.

In both cases, the authors were unable to classify the extremal families. Can we extend our techniques to show that the extremal families are t-setwise-cosets? The first step in this direction was already taken by the second author in her master's thesis [8], who showed that this holds for large n. One of the difficulties in obtaining bounds for small n is taking advantage of the characterization of extremal f, which is stronger than a mere degree bound.

We mention in passing two more challenges. One is to extend the theory of setwise-intersecting families from permutations to perfect matchings. A t-setwise intersecting family of perfect matchings is one in which for any two perfect matchings m_1, m_2 there are two sets A, B of size t such that both m_1, m_2 match the vertices in A to vertices in B. Another possible generalization is to require the existence of a single set C of size $2t$ such that both m_1 and m_2 match vertices in C to vertices in C.

The other is a common generalization of t-intersecting families and t-setwise-intersecting families. Given a partition $\lambda = \lambda_1, \ldots, \lambda_m$, a λ-intersecting family of permutations is one in which for any two permutations α, β there are disjoint sets $A_1, \ldots, A_m$ of sizes $\lambda_1, \ldots, \lambda_m$ such that $\alpha(A_1) = \beta(A_1), \ldots, \alpha(A_m) = \beta(A_m)$. A t-intersecting family corresponds to $\lambda = (1^t)$, and a t-setwise-intersecting family corresponds to $\lambda = (t)$.

Outline of the Paper. We start with a few preliminaries in Section 2. Apart from introducing several key definitions and results, we also prove several results appearing in a more general form in [9], in order to keep the paper self-contained. Theorem 1.3 is then proved in Section 3, and Theorem 1.4 in Section 4.

2. Preliminaries

2.1. Symmetric group. For integer $n \geqslant 1$, the *symmetric group* S_n is the collection of all permutations of $[n]$. We denote the identity permutation by id.

Recall that a *t-coset* of S_n is a set of the form

$$\{\alpha \in S_n : \alpha(i_1) = j_1, \ldots, \alpha(i_t) = j_t\},$$

where $i_1, \ldots, i_t \in [n]$ are distinct and $j_1, \ldots, j_t \in [n]$ are distinct. A t-coset contains $(n-t)!$ permutations. We use the term *coset* for a 1-coset. For $i, j \in [n]$, the coset

$[i \mapsto j]$ consists of all permutations sending i to j:

$$[i \mapsto j] = \{\alpha \in S_n : \alpha(i) = j\}.$$

Recall that two permutations $\alpha, \beta \in S_n$ are *t-intersecting* if there is a t-coset which contains both of them. Equivalently, the two permutations t-intersect if there are distinct indices $i_1, \ldots, i_t \in [n]$ such that $\alpha(i_1) = \beta(i_1), \ldots, \alpha(i_t) = \beta(i_t)$. A subset $\mathcal{F} \subseteq S_n$ is *t-intersecting* if every pair of permutations in $\mathcal{F}$ are t-intersecting.

2.1.1. *Degree.* We can represent permutations $\alpha \in S_n$ using n^2 variables x_{ij} whose semantics are: $x_{ij} = 1$ if $\alpha(i) = j$, and $x_{ij} = 0$ otherwise. The *degree* of a function $f : S_n \to \mathbb{R}$, denoted $\deg f$, is the minimal d such that f can be represented as a degree d polynomial over the variables x_{ij}. For example, the characteristic function of a t-coset has degree at most t as it can be represented by the polynomial $x_{i_1 j_1} \cdots x_{i_t j_t}$.

An equivalent way to define degree is via the representation theory of the symmetric group. Let $\mathbb{R}[S_n]$ be the vector space of all real-valued functions over the symmetric group. Representation theory gives an orthogonal decomposition (with respect to the inner product $\langle f, g \rangle = \sum_{\alpha \in S_n} f(\alpha) g(\alpha)$)

$$\mathbb{R}[S_n] = \bigoplus_{\lambda \vdash n} V^\lambda,$$

where λ goes over all integer partitions of n, and V^λ are certain subspaces known as *isotypic components*, which we define explicitly in Section 2.1.3. Accordingly, every function $f : S_n \to \mathbb{R}$ has a unique decomposition

$$f = \sum_{\lambda \vdash n} f^{=\lambda},$$

where $f^{=\lambda} \in V^\lambda$. Ellis, Friedgut and Pilpel [12, Theorem 7] showed that $\deg f$ is the maximal d such that $f^{=\lambda} \neq 0$ for some λ satisfying $\lambda_1 = n - d$. In particular, every function has degree at most $n - 1$.

We can now formally state the main result of Meagher and Razafimahatratra.

THEOREM 2.1 ([26, Corollary 5.5]). *If $n \geqslant 5$ then any 2-intersecting family $\mathcal{F} \subseteq S_n$ contains at most $(n-2)!$ permutations. Furthermore, if $f : S_n \to \{0, 1\}$ is the characteristic vector of a 2-intersecting family of size $(n-2)!$, then $\deg f \leqslant 2$.*

We also require a result of Ellis, Friedgut and Pilpel [12] that gives a classification of the degree-1 Boolean functions.

THEOREM 2.2 ([12, Corollary 2]). *If $f : S_n \to \{0, 1\}$ has degree at most 1 then either*

$$f = \sum_{j \in J} x_{ij}$$

for some $i \in [n]$ and $J \subseteq [n]$, or

$$f = \sum_{i \in I} x_{ij}$$

for some $I \subseteq [n]$ and $j \in [n]$.

See also [9, Theorem 6.1] for an alternative (but very similar) proof.

2.1.2. *Certificate complexity.* A *certificate* is a set

$$C = \{(i_1, j_1), \ldots, (i_m, j_m)\} \subseteq [n] \times [n].$$

A permutation $\alpha \in S_n$ *satisfies* the certificate C if

$$\alpha(i_1) = j_1, \ldots, \alpha(i_m) = j_m.$$

Notice that the set of permutations that satisfy a certificate C is either empty or a $|C|$-coset. We sometimes think of a permutation $\alpha \in S_n$ as the certificate $\{(1, \alpha(1)), \ldots, (n, \alpha(n))\}$, which we call the *certificate representation* of α.

A *Boolean function* is a function $f \colon S_n \to \{0, 1\}$. Given $\alpha \in S_n$ such that $f(\alpha) = b$, a *certificate for* α (with respect to f) is a certificate C such that:

(i) α satisfies C.
(ii) If β satisfies C then $f(\beta) = b$.

Intuitively, in order to certify that $f(\alpha) = b$, it suffices to verify that α satisfies C.

The *certificate complexity* of α, denoted $C(f, \alpha)$, is the minimum size of a certificate for α. A certificate for α of this size is known as a *minimum certificate*. Since every permutation is determined by its values on the points $1, \ldots, n-1$, the certificate complexity of α is always at most $n - 1$.

The *certificate complexity* of f, denoted $C(f)$, is $\max_{\alpha \in S_n} C(f, \alpha)$. The certificate complexity of f is always at most $n - 1$.

Dafni et al. [9, Theorem 3.1] showed that certificate complexity is polynomially related to the degree, i.e., $C(f) = O((\deg f)^8)$ and $\deg f = O(C(f)^4)$. In the special case of degree 1, we in fact have $C(f) \leqslant 1$ by Theorem 2.2, which we state as a lemma.

Lemma 2.3. *If $f \colon S_n \to \{0, 1\}$ has degree at most 1 then $C(f) \leqslant 1$.*

Proof. By Theorem 2.2, either $f = \sum_{j \in J} x_{ij}$ for some $i \in [n]$ and $J \subseteq [n]$, or $f = \sum_{i \in I} x_{ij}$ for some $I \subseteq [n]$ and $j \in [n]$. In the former, every $\alpha \in S_n$ has the certificate $\{(i, \alpha(i))\}$, and in the latter, every $\alpha \in S_n$ has the certificate $\{(\alpha^{-1}(j), j)\}$. $\square$

The following lemma, which essentially follows from [9, Lemma 7.3], shows that if $\mathcal{F}$ is a 2-intersecting family then minimum certificates of any two permutations in $\mathcal{F}$ must 2-intersect, unless $C(f) = n - 1$.

Lemma 2.4. *Let $f \colon S_n \to \{0, 1\}$ be the characteristic function of a 2-intersecting family, and suppose that $C(f) \leqslant n - 2$. If $f(\alpha) = f(\beta) = 1$ and C_α, C_β are minimum certificates for α, β (respectively), then $|C_\alpha \cap C_\beta| \geqslant 2$.*

Proof. We will show that there exist $\alpha' \in S_n$ satisfying C_α and $\beta' \in S_n$ satisfying C_β such that $\alpha' \cap \beta' = C_\alpha \cap C_\beta$, where we identify α', β' with their certificate representations. Since $f(\alpha') = f(\beta') = 1$ and f is the characteristic function of a 2-intersecting family, we have $|\alpha' \cap \beta'| \geqslant 2$, and so $|C_\alpha \cap C_\beta| \geqslant 2$.

To show this, we start by constructing α' satisfying C_α such that $\alpha' \cap C_\beta = C_\alpha \cap C_\beta$. Let $C_\alpha = \{(i_1, j_1), \ldots, (i_m, j_m)\}$, where $m \leqslant n - 2$, let $i'_1, \ldots, i'_{n-m}$ be the i-indices not involved in C_α, and let $j'_1, \ldots, j'_{n-m}$ be the j-indices not involved in C_α.

For each i'_s, there is at most one j'_t such that $(i'_s, j'_t) \in C_\beta$. We can therefore arrange the indices in such a way that if $(i'_s, j'_t) \in C_\beta$ then $s = t$. We can now define α' explicitly:

$$\alpha'(i_1) = j_1, \ldots, \alpha'(i_m) = j_m, \alpha'(i'_1) = j'_2, \ldots, \alpha'(i'_{n-m-1}) = j'_{n-m}, \alpha'(i'_{n-m}) = j'_1.$$

The same argument (replacing C_α, C_β by C_β, α') shows that we can find β' satisfying C_β such that $\alpha' \cap \beta' = \alpha' \cap C_\beta = C_\alpha \cap C_\beta$, completing the proof. $\square$

When $C(f) = n-1$, the conclusion of Lemma 2.4 indeed fails. For example, consider the family $\mathcal{F} \subseteq S_5$ given by $\mathcal{F} = \{\mathsf{id}, (1\ 2\ 3)\}$, and the minimum certificates $\{(1,1),(2,2),(3,3),(4,4)\}$ and $\{(1,2),(2,3),(3,1),(4,4)\}$.

Using the concept of *sensitivity*, we can rule out the case $C(f) = n-1$ for functions of degree at most 2. The proof is based on a technique used to prove [9, Lemma 3.6].

LEMMA 2.5. *If $n \geqslant 8$ and $f\colon S_n \to \{0,1\}$ has degree at most 2, then $C(f) \leqslant n-2$.*

Proof. The proof is by contradiction. Suppose that $n \geqslant 8$, that $f\colon S_n \to \{0,1\}$ has degree at most 2, and that $C(f) = n-1$. Without loss of generality, $C(f, \mathsf{id}) = n-1$ and $f(\mathsf{id}) = 0$. Then $f((i\ j)) = 1$ for all $i \neq j \in [n]$ (here $(i\ j)$ is the transposition switching i and j), since otherwise $\{(k,k) : \forall k \neq i,j\}$ would be a certificate for id of size $n-2$.

We construct a function $g\colon \{0,1\}^4 \to \{0,1\}$ as follows:

$$g(y_1,y_2,y_3,y_4) = f\big((1\ 2)^{y_1}(3\ 4)^{y_2}(5\ 6)^{y_3}(7\ 8)^{y_4}\big).$$

Here $(i\ j)^0 = \mathsf{id}$, $(i\ j)^1 = (i\ j)$, and f's input is a product of four powers of this kind.

Since f has degree at most 2, it can be written as a polynomial of degree at most 2 in the variables x_{ij}. Given y_1,y_2,y_3,y_4, the value of the variables x_{ij} is:

$$\begin{aligned} x_{11} &= x_{22} = 1 - y_1 & x_{12} &= x_{21} = y_1 \\ x_{33} &= x_{44} = 1 - y_2 & x_{34} &= x_{43} = y_2 \\ x_{55} &= x_{66} = 1 - y_3 & x_{56} &= x_{65} = y_3 \\ x_{77} &= x_{88} = 1 - y_4 & x_{78} &= x_{87} = y_4. \end{aligned}$$

All other variables are assigned zero. This shows that g can be expressed as a polynomial of degree at most 2 in the variables y_1,y_2,y_3,y_4. We say the function g has *degree at most* 2.

By construction, the function g satisfies the following constraints:

$$\begin{aligned} g(0,0,0,0) &= f(\mathsf{id}) = 0 \\ g(1,0,0,0) &= f((1\ 2)) = 1 \\ g(0,1,0,0) &= f((3\ 4)) = 1 \\ g(0,0,1,0) &= f((5\ 6)) = 1 \\ g(0,0,0,1) &= f((7\ 8)) = 1. \end{aligned}$$

We say that g has *sensitivity* 4.

There are only 2^{16} functions from $\{0,1\}^4$ to $\{0,1\}$. For each function, we can check whether it has degree at most 2 by solving linear equations, since each function has a unique representation as a multilinear polynomial in y_1,y_2,y_3,y_4 (a basic fact in Boolean function analysis). Going over all such functions in `SAGE` [30], we discover that none of them has sensitivity 4, a contradiction (see Section Appendix B). $\square$

For experts in Boolean function analysis, we provide an alternative non-computer proof that g cannot have sensitivity 4. Since $\deg g \leqslant 2$, every influential variable has influence at least 1/2 [28, Proposition 3.6]. If g has sensitivity 4, then it depends on 4 variables, and so its total influence is 2. Since g has degree 2, this can only happen if g is homogeneous of degree 2. But in that case, the sensitivity of g at every point is exactly 2 [16, Proposition 3.7].

We note that the bound on the sensitivity cannot be improved: the Boolean function

$$g(y_1,y_2,y_3) = y_1y_2y_3 + (1-y_1)(1-y_2)(1-y_3)$$

has degree 2 and satisfies

$$g(0,0,0)=1, \quad g(1,0,0)=g(0,1,0)=g(0,0,1)=0.$$

2.1.3. *Degree reduction.* Let $\mathcal{F} \subseteq S_n$. We denote the restriction of $\mathcal{F}$ to the coset $[i \mapsto j]$ by $\mathcal{F}|_{[i\mapsto j]}$. We can think of $\mathcal{F}|_{[i\mapsto j]}$ as a subset of S_{n-1}. Formally speaking, we can think of S_n as the set of all bijections from $[n]$ to $[n]$. The restriction of S_n to the coset $[i \mapsto j]$ is isomorphic to the set of all bijections from $[n] \setminus \{i\}$ to $[n] \setminus \{j\}$, which is the same as S_{n-1} up to renumbering.

Let f be the characteristic function of $\mathcal{F}$, i.e., $f(x)=1$ if $x \in \mathcal{F}$, and is 0 otherwise. The definition of degree using polynomials shows that $\deg f|_{[i\mapsto j]} \leqslant \deg f$, where f is the characteristic function of $\mathcal{F}|_{[i\mapsto j]}$. Indeed, given a polynomial representing f, we can obtain a polynomial representing $f|_{[i\mapsto j]}$ by substituting $x_{ij}=1$ and $x_{ij'} = x_{i'j} = 0$ for any $i' \neq i$ and $j' \neq j$.

The following crucial lemma, which forms part of the proof of [9, Lemma 5.7], states that if $\mathcal{F}$ is contained in $[i \mapsto j]$, then the degree of f strictly decreases when restricting to $[i \mapsto j]$.

Lemma 2.6. *Suppose that $f\colon S_n \to \{0,1\}$ is the characteristic function of a family which is a subset of the coset $[i \mapsto j]$. Then $\deg f|_{[i\mapsto j]} \leqslant \max(\deg f - 1, 0)$.*

To prove this lemma, we need a few more combinatorial notions from the representation theory of S_n, but let us first point out that the corresponding result for functions on the Boolean cube $\{0,1\}^n$ is easy to prove. Indeed, suppose that $f\colon \{0,1\}^n \to \{0,1\}$ is such that $f(x)=1$ implies $x_n = 1$. We can write

$$f(x_1,\ldots,x_n) = (1-x_n) f_0(x_1,\ldots,x_{n-1}) + x_n f_1(x_1,\ldots,x_{n-1}).$$

Substituting $x_n = 0$, we get $f_0 = 0$, and so $f = x_n f_1$. The restriction of f to the "coset" $\{x : x_n = 1\}$ is f_1. If $f_1 \neq 0$ then clearly $\deg f = \deg f_1 + 1$, where $\deg f$ is the degree of the unique multilinear polynomial representing f.

The argument proving Lemma 2.6 is more subtle. The starting point is the following explicit description of the subspaces V^λ, which we mentioned in Section 2.1.1. We refer the reader to [29] for a more detailed treatment of the representation theory of S_n.

Let $\lambda = (\lambda_1,\ldots,\lambda_m) \vdash n$ be an *integer partition of* n. A *Young tableau* of *shape* λ is an arrangement of the numbers $1,\ldots,n$ in m rows of lengths $\lambda_1,\ldots,\lambda_m$, left justified. Here are some examples:

$$\begin{array}{|c|c|c|}\hline 3 & 4 & 1 \\ \hline 2 \\ \cline{1-1}\end{array} \qquad \begin{array}{|c|c|}\hline 1 & 4 \\ \hline 2 & 3 \\ \hline\end{array}\ .$$

$$\lambda = (3,1) \quad \lambda = (2,2)$$

Let s,t be a pair of Young tableaux of the same shape $\lambda = (\lambda_1,\ldots,\lambda_m) \vdash n$. The function $e_{s,t}\colon S_n \to \{0,1\}$ is defined as follows: $e_{s,t}(\alpha) = 1$ if for every $k \in [m]$, α sends every number on the k-th row of s to a number on the k-th row of t, and $e_{s,t}(\alpha) = 0$ otherwise. For example, consider

$$s = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2}\end{array} \qquad t = \begin{array}{|c|c|c|}\hline 3 & 1 & 5 \\ \hline 2 & 4 \\ \cline{1-2}\end{array}$$

Then $e_{s,t}(\alpha) = 1$ if $\alpha(1), \alpha(2), \alpha(3) \in \{3,1,5\}$ and $\alpha(4), \alpha(5) \in \{2,4\}$.

For a tableau t with m' columns, we denote by $C(t)$ the *column stabilizer* of t, which is the set of all permutations of the entries of t which only move entries within the same column. Each permutation $\pi \in C(t)$ thus consists of m' permutations $\pi_1,\ldots,\pi_{m'}$, one for each column. The *sign* of π, denote $(-1)^\pi$, is the product of the signs of the permutations $\pi_1, \dots, \pi_{m'}$. We denote the result of applying π to t by t^π.

Let s, t be a pair of Young tableaux of the same shape $\lambda \vdash n$. We define a function $\chi_{s,t} \colon S_n \to \{-1, 0, 1\}$ as follows:

$$\chi_{s,t} = \sum_{\pi \in C(t)} (-1)^\pi e_{s,t^\pi}.$$

Continuing our above example, here is t^π for all elements $\pi \in C(t)$, together with their sign:

$$\left(\begin{array}{|c|c|c|}\hline 3 & 1 & 5 \\ \hline 2 & 4 \\ \cline{1-2}\end{array}, +1\right) \left(\begin{array}{|c|c|c|}\hline 3 & 4 & 5 \\ \hline 2 & 1 \\ \cline{1-2}\end{array}, -1\right) \left(\begin{array}{|c|c|c|}\hline 2 & 1 & 5 \\ \hline 3 & 4 \\ \cline{1-2}\end{array}, -1\right) \left(\begin{array}{|c|c|c|}\hline 2 & 4 & 5 \\ \hline 3 & 1 \\ \cline{1-2}\end{array}, +1\right).$$

We are interested in the functions $\chi_{s,t}$ since they span V^λ.

Theorem 2.7 ([29, Chapter 2]). *Let $\lambda \vdash n$. The subspace V^λ is spanned by the functions $\chi_{s,t}$, where s, t go over all pairs of Young tableaux of shape λ.*

We are now ready to prove Lemma 2.6.

Proof of Lemma 2.6. Assume, for concreteness, that $i = j = n$. If $n = 1$, then $\deg f|_{[n \mapsto n]} = 0$, so there is nothing to prove. If $f|_{[n \mapsto n]} = 0$, then again $\deg f|_{[n \mapsto n]} = 0$, so there is nothing to prove. Thus we assume that $n \geqslant 2$ and that $f|_{[n \mapsto n]} \neq 0$.

Let $d = \deg f|_{[n \mapsto n]}$. According to the spectral definition of degree (see Section 2.1.1), $f|_{[n \mapsto n]}^{=\lambda} \neq 0$ for some $\lambda \vdash (n-1)$ such that $\lambda_1 = (n-1) - d$. Since the decomposition into isotypic components is orthogonal, this implies that

$$\langle f|_{[n \mapsto n]}, f|_{[n \mapsto n]}^{=\lambda} \rangle = \langle f|_{[n \mapsto n]}^{=\lambda}, f|_{[n \mapsto n]}^{=\lambda} \rangle \neq 0.$$

Since $f|_{[n \mapsto n]}^{=\lambda} \in V^\lambda$, Theorem 2.7 implies that $\langle f|_{[n \mapsto n]}, \chi_{s,t} \rangle \neq 0$ for some Young tableaux s, t of shape λ.

Let s', t' be the Young tableaux obtained by adding a new row to s, t (respectively) consisting only of the number n. Here is an example:

$$s = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2}\end{array} \quad t = \begin{array}{|c|c|c|}\hline 3 & 1 & 5 \\ \hline 2 & 4 \\ \cline{1-2}\end{array} \quad \longrightarrow \quad s' = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2} 6 \\ \cline{1-1}\end{array} \quad t' = \begin{array}{|c|c|c|}\hline 3 & 1 & 5 \\ \hline 2 & 4 \\ \cline{1-2} 6 \\ \cline{1-1}\end{array}.$$

The tableaux s', t' have shape $\mu \vdash n$ satisfying $\mu_1 = \lambda_1 = (n-1) - d = n - (d+1)$.

It suffices to show that $\langle f, \chi_{s',t'} \rangle \neq 0$, as the orthogonality of the decomposition into isotypic components would give $f^{=\mu} \neq 0$, and thus $\deg f \geqslant d + 1$ by the spectral definition of degree.

Let $\pi' \in C(t')$ be any permutation such that $\pi'(n) \neq n$. By assumption, $f(\alpha') = 1$ only if $\alpha'(n) = n$, in which case $e_{s',(t')^{\pi'}}(\alpha') = 0$; therefore $\langle f, e_{s',(t')^{\pi'}} \rangle = 0$. This shows that

$$\langle f, \chi_{s',t'} \rangle = \sum_{\substack{\pi' \in C(t') \\ \pi'(n) = n}} (-1)^{\pi'} \langle f, e_{s',(t')^{\pi'}} \rangle.$$

If $\pi'(n) = n$ then $e_{s',(t')^{\pi'}}(\alpha') \neq 0$ only if $\alpha'(n) = n$. Conversely, if $\alpha'(n) = n$, that is, if $\alpha' \in [n \mapsto n]$, then $e_{s',(t')^{\pi'}}(\alpha') = e_{s,t^\pi}(\alpha)$, where α, π are the restrictions of α', π' to $[n-1]$. Moreover, $(-1)^\pi = (-1)^{\pi'}$. Thus

$$\langle f, \chi_{s',t'} \rangle = \sum_{\pi \in C(t)} (-1)^\pi \langle f|_{[n \mapsto n]}, e_{s,t^\pi} \rangle = \langle f|_{[n \mapsto n]}, \chi_{s,t} \rangle \neq 0, \text{ as desired.} \qquad \square$$

2.2. PERFECT MATCHINGS. Recall that $\mathcal{M}_{2n}$ is the collection of all perfect matchings of the complete graph K_{2n}. Since the symmetric group S_n can be viewed as the collection of all perfect matchings of the complete *bipartite* graph $K_{n,n}$, we can think of the perfect matching scheme as the non-bipartite analog of the symmetric group.

It is not difficult to show that $\mathcal{M}_{2n}$ has size $(2n-1)!!$ where

$$(2n-1)!! = (2n-1)(2n-3)(2n-5)\cdots(5)(3)(1) = \frac{(2n)!}{2^n n!}.$$

We sometimes think of a perfect matching in $\mathcal{M}_{2n}$ as a set of n pairs of elements from $[2n]$, which together cover all of $[2n]$ (the *pair representation*). At other times, it will be useful to think of a perfect matching in $\mathcal{M}_{2n}$ as a fixed-point-free involution on $[2n]$, that is, $m(i) \neq i$ is the element that i is matched to, and $m(m(i)) = i$.

Slightly abusing terminology, we define a *t-coset* (canonically t-intersecting family) of $\mathcal{M}_{2n}$ to be a set of the form

$$\{m \in \mathcal{M}_{2n} : m(i_1) = j_1, \ldots, m(i_t) = j_t\},$$

where $i_1, \ldots, i_t, j_1, \ldots, j_t \in [2n]$ are distinct. A t-coset contains $(2(n-t)-1)!!$ perfect matchings. We use the term *coset* for a 1-coset. For $i \neq j \in [2n]$, the coset $[i \leftrightarrow j]$ consists of all perfect matchings in which i, j are matched:

$$[i \leftrightarrow j] = \{m \in \mathcal{M}_{2n} : m(i) = j\}.$$

Note that $[i \leftrightarrow j] = [j \leftrightarrow i]$.

Two perfect matchings $m_1, m_2 \in \mathcal{M}_{2n}$ are *t-intersecting* if there is a t-coset which contains both of them. A subset $\mathcal{F} \subseteq \mathcal{M}_{2n}$ is *t-intersecting* if any two perfect matchings in $\mathcal{F}$ are t-intersecting.

2.2.1. *Degree.* We can represent perfect matchings $m \in \mathcal{M}_{2n}$ using $\binom{2n}{2}$ variables x_{ij} (where the index is an unordered pair of elements) whose semantics are: $x_{ij} = 1$ if $m(i) = j$, and $x_{ij} = 0$ otherwise. The *degree* of a function $f \colon \mathcal{M}_{2n} \to \mathbb{R}$, denoted $\deg f$, is the minimal d such that f can be represented as a degree d polynomial over the variables x_{ij}, e.g., the characteristic function of a t-coset has degree at most t.

An equivalent way to define degree is via the representation theory of the perfect matching scheme. Let $\mathbb{R}[\mathcal{M}_{2n}]$ be the vector space of all real-valued functions over the perfect matching scheme. The representation theory of S_n (see [6, Chapter 11], for example) gives an orthogonal decomposition (with respect to the inner product $\langle f, g\rangle = \sum_{m \in \mathcal{M}_{2n}} f(m)g(m)$)

$$\mathbb{R}[\mathcal{M}_{2n}] = \bigoplus_{\lambda \vdash n} V^{2\lambda},$$

where λ goes over all integer partitions of n, 2λ is the partition of $2n$ obtained by doubling each part, and $V^{2\lambda}$ are the isotypic components, which we define explicitly in Section 2.2.3. Accordingly, every function $f \colon \mathcal{M}_{2n} \to \mathbb{R}$ has a unique decomposition

$$f = \sum_{\lambda \vdash n} f^{=\lambda},$$

where $f^{=\lambda} \in V^{2\lambda}$. Lindzey [24, Theorem 5.1.1] showed that $\deg f$ is the maximal d such that $f^{=\lambda} \neq 0$ for some λ satisfying $\lambda_1 = n - d$. In particular, every function has degree at most $n-1$.

We can now formally state the main result of Fallat, Meagher and Shirazi.

THEOREM 2.8 ([14, Theorem 4.13]). *If $n \geqslant 3$ then any 2-intersecting family $\mathcal{F} \subseteq \mathcal{M}_{2n}$ contains at most $(2n-5)!!$ perfect matchings. Furthermore, if $f \colon \mathcal{M}_{2n} \to \{0,1\}$ is the characteristic vector of a 2-intersecting family of size $(2n-5)!!$, then $\deg f \leqslant 2$.*

We will also need a result of Dafni et al. [9] classifying degree-1 Boolean functions.

THEOREM 2.9 ([9, Theorem 6.2]). *If $f\colon \mathcal{M}_{2n} \to \{0,1\}$ has degree at most 1 then f is either a* dictator*:*

$$f = \sum_{j \in J} x_{ij},$$

for some $i \in [2n]$ and $J \subseteq [2n]$ not containing i; or f is a triangle*:*

$$f = x_{ij} + x_{ik} + x_{jk},$$

for some distinct $i, j, k \in [2n]$; or f is an anti-triangle*:*

$$f = 1 - x_{ij} - x_{ik} - x_{jk},$$

for some distinct $i, j, k \in [2n]$.

2.2.2. *Certificate complexity.* A *certificate* is a set

$$C = \big\{\{i_1, j_1\}, \ldots, \{i_r, j_r\}\big\} \subseteq \binom{[2n]}{2},$$

where $\binom{[2n]}{2}$ is the collection of all subsets of $[2n]$ of size 2. We say $m \in \mathcal{M}_{2n}$ *satisfies* the certificate C if $m(i_1) = j_1, \ldots, m(i_r) = j_r$.

A *Boolean function* is a function $f\colon \mathcal{M}_{2n} \to \{0,1\}$. Just as in Section 2.1.2, for each $m \in \mathcal{M}_{2n}$ we can define the following notions: a certificate for m (with respect to f); the certificate complexity of m, denoted $C(f, m)$; a minimum certificate; and the certificate complexity of f, denoted $C(f)$. As in the case of the symmetric group, $C(f) \leqslant n - 1$, since a perfect matching is determined by any $n - 1$ of its edges. Dafni et al. [9] showed that $C(f)$ is polynomially related to $\deg f$.

In the case of the symmetric group, degree-1 Boolean functions have certificate complexity 1. This is no longer the case for perfect matchings, since triangles and anti-triangles have certificate complexity 2.

LEMMA 2.10. *If $f\colon \mathcal{M}_{2n} \to \{0,1\}$ has degree at most 1 then $C(f) \leqslant 2$.*

Proof. According to Theorem 2.9, f is either a dictator, a triangle, or an anti-triangle. If $f = \sum_{j \in J} x_{ij}$ is a dictator, then every m has a certificate $\big\{\{i, m(i)\}\big\}$. If $f = x_{ij} + x_{ik} + x_{jk}$ is a triangle, then every m such that $f(m) = 1$ has one of the certificates $\big\{\{i,j\}\big\}, \big\{\{i,k\}\big\}, \big\{\{j,k\}\big\}$, and every m such that $f(m) = 0$ has the certificate $\big\{\{i, m(i)\}, \{j, m(j)\}\big\}$. If f is an anti-triangle then $1 - f$ is a triangle, so we can use the same certificates as in the case of a triangle. □

The proof of Lemma 2.4 extends to the perfect matchings with minor changes.

LEMMA 2.11. *Let $f\colon \mathcal{M}_{2n} \to \{0,1\}$ be the characteristic function of a 2-intersecting family, and suppose that $C(f) \leqslant n - 2$. If $f(m_1) = f(m_2) = 1$ and C_{m_1}, C_{m_2} are minimum certificates for m_1, m_2 (respectively), then $|C_{m_1} \cap C_{m_2}| \geqslant 2$.*

Proof. We will show how to construct a perfect matching m_1' satisfying C_{m_1} such that $m_1' \cap C_{m_2} = C_{m_1} \cap C_{m_2}$. The same argument can be used to construct a perfect matching m_2' satisfying C_{m_2} such that $m_1' \cap m_2' = m_1' \cap C_{m_2}$. It follows that $|C_{m_1} \cap C_{m_2}| = |m_1' \cap m_2'| \geqslant 2$, since f is the characteristic function of a 2-intersecting family.

Let $C_{m_1} = \big\{\{i_1, j_1\}, \ldots, \{i_r, j_r\}\big\}$, where $r \leqslant n - 2$, and let $k_1, \ldots, k_{2(n-r)}$ be the indices not mentioned in C_{m_1}. Rearrange the indices so that if $\{k_s, k_t\} \in C_{m_2}$ then $\{s, t\} = \{2\ell - 1, 2\ell\}$ for some $\ell \in [n - r]$. The perfect matching m_1' has the pair representation

$$\{i_1, j_1\}, \ldots, \{i_r, j_r\}, \{k_1, k_{n-r+1}\}, \{k_2, k_{n-r+2}\}, \ldots, \{k_{n-r}, k_{2(n-r)}\}.$$

Since $n - r \geqslant 2$, the new pairs do not intersect C_{m_2}, completing the proof. □

Using sensitivity, we can rule out the case $C(f) = n-1$ for functions of degree at most 2, just as we did for the symmetric group.

LEMMA 2.12. *If* $n \geqslant 8$ *and* $f\colon \mathcal{M}_{2n} \to \{0,1\}$ *has degree at most* 2*, then* $C(f) \leqslant n-2$.

Proof. The proof is by contradiction. Suppose that $n \geqslant 8$, that $f\colon \mathcal{M}_{2n} \to \{0,1\}$ has degree at most 2, and that $C(f) = n-1$, say $C(f,m) = n-1$ for $m = \big\{\{1,2\},\{3,4\},\ldots,\{2n-1,2n\}\big\}$. Since $C(f,m) > n-2$, $m \setminus \big\{\{2i-1,2i\},\{2j-1,2j\}\big\}$ is not a certificate for m for any $i \neq j \in [n]$, and so $f(m^{ij}) \neq f(m)$, where m^{ij} is obtained from m by replacing $\big\{\{2i-1,2i\},\{2j-1,2j\}\big\}$ with $\big\{\{2i-1,2j\},\{2j-1,2i\}\big\}$.

We construct a function $g\colon \{0,1\}^4 \to \{0,1\}$ as follows: $g(y_1,y_2,y_3,y_4)$ is the value of f on the perfect matching obtained from m by applying the subset of the operations ${}^{12}, {}^{34}, {}^{56}, {}^{78}$ specified by the input (for example, if $y_1 = 1$ then we apply ^{12}). As in the proof of Lemma 2.5, this results in a function of degree at most 2 satisfying

$$g(0,0,0,0) \neq g(1,0,0,0) = g(0,1,0,0) = g(0,0,1,0) = g(0,0,0,1),$$

which is impossible. $\square$

2.2.3. *Degree reduction.* Let $\mathcal{F} \subseteq \mathcal{M}_{2n}$. We denote the restriction of $\mathcal{F}$ to the coset $[i \leftrightarrow j]$ by $\mathcal{F}|_{[i\leftrightarrow j]}$, which we can think of as a subset of $\mathcal{M}_{2(n-1)}$.

Let f be the characteristic function of $\mathcal{F}$. The definition of degree using polynomials shows that $\deg f|_{[i\leftrightarrow j]} \leqslant \deg f$. The following analog of Lemma 2.6 shows that if $\mathcal{F}$ is contained in $[i \leftrightarrow j]$, then the degree of f strictly decreases when restricted to $[i \leftrightarrow j]$.

LEMMA 2.13. *Suppose that* $f\colon \mathcal{M}_{2n} \to \{0,1\}$ *is the characteristic function of a family which is a subset of the coset* $[i \leftrightarrow j]$*. Then* $\deg f|_{[i\leftrightarrow j]} \leqslant \max(\deg f - 1, 0)$.

Before we prove this lemma, we need an explicit description of the subspaces $V^{2\lambda}$ mentioned in Section 2.2.1.

Let $\lambda \vdash n$, and let t be a Young tableau of shape 2λ. The function $e_t\colon \mathcal{M}_{2n} \to \{0,1\}$ is defined as follows: $e_t(m) = 1$ if for all $i \in [2n]$, the element $m(i)$ is in the same row of t as i, and $e_t(m) = 0$ otherwise. For example, consider

$$t = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 5 & 6 & 7 & 8 \\ \hline \end{array}$$

Then $e_t(m) = 1$ if $m(1), m(2), m(3), m(4) \in [4]$ and $m(5), m(6), m(7), m(8) \in [8] \setminus [4]$.

Given a Young tableau t of shape 2λ, we define $\chi_t\colon \mathcal{M}_{2n} \to \{-1,0,1\}$ as follows:

$$\chi_t = \sum_{\pi \in C(t)} (-1)^\pi e_{t^\pi}.$$

These functions span $V^{2\lambda}$.

THEOREM 2.14 ([24, Theorem 5.2.6]). *Let* $\lambda \vdash n$*. The subspace* $V^{2\lambda}$ *is spanned by the functions* χ_t*, where* t *goes over all Young tableaux of shape* 2λ.

We can now prove Lemma 2.13. The proof is along the lines of Lemma 2.6.

Proof of Lemma 2.13. Assume, for concreteness, that $i = 2n-1$ and $j = 2n$. If $n = 1$ then $\deg f|_{[2n-1\leftrightarrow 2n]} = 0$, so there is nothing to prove. Similarly, if $f|_{[2n-1\leftrightarrow 2n]} = 0$ then there is nothing to prove. Therefore we can assume that $n \geqslant 2$ and that $f|_{[2n-1\leftrightarrow 2n]} \neq 0$.

Let $d = \deg f|_{[2n-1\leftrightarrow 2n]}$. According to the spectral definition of degree (see Section 2.2.1), $f|^{=\lambda}_{[2n-1\leftrightarrow 2n]} \neq 0$ for some $\lambda \vdash n-1$ such that $\lambda_1 = (n-1)-d$. Since the decomposition into isotypic components is orthogonal, Theorem 2.14 implies that $\langle f|_{[2n-1\leftrightarrow 2n]}, \chi_t \rangle \neq 0$ for some Young tableau t of shape 2λ. Among all tableau t with

$2(n-1-d)$ squares on the first lines satisfying $\langle f|_{[2n-1\leftrightarrow 2n]}, \chi_t\rangle \neq 0$, we choose one which maximizes the number of rows (which is the number of parts in the corresponding partition), say t has R rows.

Let t' be the Young tableau obtained by adding a new row to t consisting only of the numbers $2n-1, 2n$. The tableau t' has shape μ satisfying $\mu_1 = \lambda_1 = n-(d+1)$. We will show that $\langle f, \chi_{t'}\rangle \neq 0$, and so $\deg f \geqslant d+1$ by the spectral definition of degree.

If $\pi' \in C(t')$ is any permutation such that $2n-1, 2n$ do not end up in the same row, then $\langle f, e_{(t')^{\pi'}}\rangle = 0$, since $e_{(t')^{\pi'}}(m) \neq 0$ implies that $m(2n-1) \neq 2n$, and so $f(m) = 0$. Therefore

$$\langle f, \chi_{t'}\rangle = \sum_{r=1}^{R+1} \sum_{\substack{\pi' \in C(t') \\ 2n-1, 2n \text{ are on} \\ \text{row } r \text{ of } (t')^{\pi'}}} (-1)^{\pi'} \langle f, e_{(t')^{\pi'}}\rangle.$$

For $r \leqslant R$, let t^r be the tableau obtained from t by taking the first two elements of row r, moving them to a new row at the very end, removing row r if it is empty, and otherwise sliding the remainder of row r to the left (and then reordering the rows if necessary in order to create a valid tableau). For example,

$$t = \begin{ytableau} 1 & 2 & 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{ytableau} \quad t^1 = \begin{ytableau} 3 & 4 \\ 5 & 6 \\ 7 & 8 \\ 1 & 2 \end{ytableau} \quad t^2 = \begin{ytableau} 1 & 2 & 3 & 4 \\ 7 & 8 \\ 5 & 6 \end{ytableau} \quad t^3 = t, \text{ and}$$

$$t = \begin{ytableau} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{ytableau} \quad t^1 = \begin{ytableau} 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 3 & 4 \\ 1 & 2 \end{ytableau} \quad t^2 = \begin{ytableau} 1 & 2 & 3 & 4 \\ 9 & 10 & 11 & 12 \\ 7 & 8 \\ 5 & 6 \end{ytableau} \quad t^3 = \begin{ytableau} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 11 & 12 \\ 9 & 10 \end{ytableau}.$$

We also define $t^{R+1} := t$. Observe that

$$\langle f, \chi_{t'}\rangle = \sum_{r=1}^{R+1} \sum_{\pi \in C(t^r)} (-1)^{\pi} \langle f|_{[2n-1\leftrightarrow 2n]}, e_{(t^r)^{\pi}}\rangle = \sum_r \langle f|_{[2n-1\leftrightarrow 2n]}, \chi_{t^r}\rangle.$$

If the r-th row of t contains more than two elements, then t^r contains more rows than t, and so by the choice of t, we have $\langle f|_{[2n-1\leftrightarrow 2n]}, \chi_{t^r}\rangle = 0$. Otherwise, χ_{t^r} differs from χ_t by an identical permutation of the first two columns, and so $\langle f|_{[2n-1\leftrightarrow 2n]}, \chi_{t^r}\rangle = \langle f|_{[2n-1\leftrightarrow 2n]}, \chi_t\rangle$. Denoting by ℓ the number of rows of t of length 2, we have

$$\langle f, \chi_{t'}\rangle = (\ell+1)\langle f|_{[2n-1\leftrightarrow 2n]}, \chi_t\rangle \neq 0.$$

The reason we get $\ell+1$ rather than ℓ is the choice $r = R+1$, which gives $t^{R+1} = t$. $\square$

3. Proof of Theorem 1.3

The main result of this section is a proof of Theorem 1.3, i.e., that every largest 2-intersecting family of permutations is a 2-coset for all $n \geqslant 2$. To prove this, we must first prove some lemmas on the structure of 2-intersecting families of permutations, culminating into a key lemma from which the proof of Theorem 1.3 easily follows.

Let us start with a simple observation on 2-intersecting families, whose statement requires a few definitions. We say that two cosets $[i_1 \mapsto j_1], [i_2 \mapsto j_2]$ are *compatible* if their intersection is non-empty. In other words, either the two cosets are equal, or

$i_1 \neq i_2$ and $j_1 \neq j_2$. A family $\mathcal{F} \subseteq S_n$ is *m-covered*, for some integer $m \geqslant 1$, if there are m compatible cosets $[i_1 \mapsto j_1], \ldots, [i_m \mapsto j_m]$ such that $\mathcal{F} \subseteq [i_1 \mapsto j_1] \cup \cdots \cup [i_m \mapsto j_m]$.

LEMMA 3.1. *Let f be the characteristic function of a 2-intersecting family $\mathcal{F} \subseteq S_n$, and suppose that $C(f) \leqslant n-2$. If $\alpha \in \mathcal{F}$, then $\mathcal{F}$ is m-covered for $m = C(f,\alpha) - 1$.*

Proof. Let $C_\alpha = \{(i_1, j_1), \ldots, (i_{m+1}, j_{m+1})\}$ be a minimal certificate for α. Clearly the cosets corresonding to any pair $(i,j), (i',j') \in C_\alpha$ are compatible. We will show that $\mathcal{F} \subseteq [i_1 \mapsto j_1] \cup \cdots \cup [i_m \mapsto j_m]$.

Let $\beta \in \mathcal{F}$, and let C_β be a minimal certificate for β. According to Lemma 2.4, we have $|C_\alpha \cap C_\beta| \geqslant 2$. This implies that $(i_s, j_s) \in C_\beta$ for some $s \in [m]$, hence $\beta \in [i_s \mapsto j_s] \subseteq [i_1 \mapsto j_1] \cup \cdots \cup [i_m \mapsto j_m]$. □

The following structure lemma provides a kind of converse to Lemma 3.1.

LEMMA 3.2. *Let $\mathcal{F} \subseteq S_n$ be an m-covered family, say $\mathcal{F} \subseteq [i_1 \mapsto j_1] \cup \cdots \cup [i_m \mapsto j_m]$. Suppose that its characteristic function f has degree at most 2. Then every α has a certificate of the form $\{(i_1, \alpha(i_1)), \ldots, (i_m, \alpha(i_m)), (i,j)\}$, i.e., $C(f) \leqslant m+1$.*

Proof. It suffices to prove by induction on m that if $\mathcal{F} \subseteq S_n$ is m-covered, i.e., of the form $\mathcal{F} \subseteq [i_1 \mapsto j_1] \cup \cdots \cup [i_m \mapsto j_m]$, and its characteristic function f has degree at most 2, then for every distinct $k_1, \ldots, k_m \in [n]$, the restriction of f to $[i_1 \mapsto k_1] \cap \cdots \cap [i_m \mapsto k_m]$ has degree no greater than 1. Indeed, by Lemma 2.3 this restriction has a certificate $\{(i,j)\}$, and so for any $\alpha \in S_n$, we may simply take $k_1 = \alpha(i_1), \ldots, k_m = \alpha(i_m)$ to obtain a certificate of α of the required form.

We start with the base case $m = 1$. Let $\mathcal{F} \subseteq S_n$ be such that $\mathcal{F} \subseteq [i_1 \mapsto j_1]$, and suppose that its characteristic function f has degree at most 2. Lemma 2.6 directly implies that the restriction of f to $[i_1 \mapsto j_1]$ has degree at most 1, as required.

Suppose now that $m \geqslant 2$. Let $\mathcal{F} \subseteq S_n$ be such that $\mathcal{F} \subseteq [i_1 \mapsto j_1] \cup \cdots \cup [i_m \mapsto j_m]$, and suppose that its characteristic function f has degree at most 2. Consider any distinct $k_1, \ldots, k_m \in [n]$. We show the restriction of f to $[i_1 \mapsto k_1] \cap \cdots \cap [i_m \mapsto k_m]$ has degree at most 1.

Suppose first that $k_s \neq j_s$ for some $s \in [m]$, say $k_m \neq j_m$ without loss of generality. The restriction of $\mathcal{F}$ to $[i_m \mapsto k_m]$ is contained in $[i_1 \mapsto j_1] \cup \cdots \cup [i_{m-1} \mapsto j_{m-1}]$, and its characteristic function has degree at most 2. Therefore the induction hypothesis implies that the restriction of f to $[i_1 \mapsto k_1] \cap \cdots \cap [i_m \mapsto k_m]$ has degree at most 1.

It remains to show that the restriction of f to $[i_1 \mapsto j_1] \cap \cdots \cap [i_m \mapsto j_m]$ has degree at most 1. To see this, consider the function

$$g := x_{i_1 j_1} \cdots x_{i_m j_m} f = f - \sum_{\substack{k_1, \ldots, k_m \\ (k_1, \ldots, k_m) \neq (j_1, \ldots, j_m)}} x_{i_1 k_1} \cdots x_{i_m k_m} f.$$

We showed above that the restriction of f to $[i_1 \mapsto k_1] \cap \cdots \cap [i_m \mapsto k_m]$ has degree at most 1 whenever $(k_1, \ldots, k_m) \neq (j_1, \ldots, j_m)$. Thus every term in the sum on the right-hand side has degree at most $m+1$, as it can be represented as $x_{i_1 k_1} \cdots x_{i_m k_m}$ times the degree-1 function representing the restriction of f to $[i_1 \mapsto k_1] \cap \cdots \cap [i_m \mapsto k_m]$. Consequently, we have $\deg g \leqslant \max(\deg f, m+1) = m+1$.

By construction, g is the characteristic function of a family which is contained in the coset intersection $\mathcal{I} = [i_1 \mapsto j_1] \cap \cdots \cap [i_m \mapsto j_m]$. Applying Lemma 2.6 repeatedly, we conclude that the restriction of g to $\mathcal{I}$ has degree at most $\max(m+1-m, 0) = 1$. Since the restriction of f to $\mathcal{I}$ is the same as the restriction of g to $\mathcal{I}$, this completes the proof of the induction step. □

Lemma 3.3 (Key Lemma). *Let $\mathcal{F} \subseteq S_n$ be a 2-intersecting family whose characteristic function f has degree at most 2, and suppose that $C(f) \leqslant n-2$. Then the family $\mathcal{F}$ is contained in the union of at most T many $C(f)$-cosets, where*

$$T = \frac{2\lfloor C(f)/2 \rfloor (C(f)-1)!}{2^{\lfloor C(f)/2 \rfloor}}.$$

Moreover, $C(f) \geqslant 2$.

Proof. If $\mathcal{F}$ is empty then the lemma is vacuously true. Otherwise, choose an arbitrary $\beta \in \mathcal{F}$. Lemma 2.4, applied to $\alpha = \beta$, shows that $C(f,\beta) \geqslant 2$. Lemma 3.1 shows that $\mathcal{F}$ is m-covered, where $m = C(f,\beta) - 1$. Without loss of generality, we can assume that $\mathcal{F} \subseteq [1 \mapsto 1] \cup \cdots \cup [m \mapsto m]$.

Lemma 3.2 shows that $C(f) \leqslant m+1$, thus $m = C(f) - 1$ and $C(f) = C(f,\beta) \geqslant 2$. Lemma 3.2 also shows that every $\alpha \in \mathcal{F}$ has a certificate C_α of the form

$$\{(1,\alpha(1)), \ldots, (m,\alpha(m)), (i,j)\}.$$

It also implies that $\mathcal{F}$ is not $(m-1)$-covered (otherwise its certificate complexity would be at most $m < C(f)$). Therefore, if X is any set of at most $m-1$ compatible cosets, then there is a $\alpha_X \in \mathcal{F}$ which is not contained in the union of the cosets in X. Fix a certificate C_X for α_X of the form $\{(1,\alpha_X(1)), \ldots, (m,\alpha_X(m)), (i_X, j_X)\}$.

We think of the certificates C_α, C_X as colored using $m+1$ colors: for $k \in [m]$, a pair $(k,*)$ is colored k, and the remaining pair (i,j) is colored $m+1$. We can determine the color of a pair (i',j') given only the pair: if $i' \in [m]$ then the color is i', and otherwise the color is $m+1$.

We will prove the lemma by showing that if $\alpha \in \mathcal{F}$ then C_α is one of at most T possible certificates. Since C_α corresponds to a $C(f)$-coset containing α, the lemma would follow. In the proof, we will freely identify a pair (i,j) with the corresponding coset $[i \mapsto j]$, and from now on we will only ever mention cosets.

The proof is slightly different depending on the parity of $C(f)$. We start with the case in which $C(f) = 2r$ is even. Let $\alpha \in \mathcal{F}$. We define a sequence

$$X_0 \subset \cdots \subset X_r \subseteq C_\alpha,$$

where X_s is a collection of $2s$ compatible cosets, as follows. The starting point is $X_0 = \varnothing$. Now let $s < r$, and suppose that X_s has been defined. Since $|X_s| = 2s \leqslant C(f) - 2 = m-1$, there is a permutation $\alpha_{X_s} \in \mathcal{F}$ which lies outside of the union of the cosets in X_s. According to Lemma 2.4, the certificates C_α and C_{X_s} must have at least two cosets in common q_1, q_2. The choice of α_{X_s} guarantees that $q_1, q_2 \notin X_s$, and we define $X_{s+1} = X_s \cup \{q_1, q_2\}$. By construction, $X_{s+1} \subseteq C_\alpha$, and so the cosets in X_{s+1} are indeed compatible.

Note that $|X_r| = 2r = |C_\alpha|$, and so $X_r = C_\alpha$. For $s < r$, given X_s, the set $X_{s+1} \setminus X_s$ consists of two cosets belonging to C_{X_s}. Moreover, since $X_{s+1} \subseteq C_\alpha$ and C_α contains one coset of each color, the colors of the two cosets in $X_{s+1} \setminus X_s$ are different from the colors of the cosets in X_s. Since C_{X_s} also contains one coset of each color, this means that there are $\binom{|C_{X_s}|-|X_s|}{2} = \binom{C(f)-2s}{2}$ choices for $X_{s+1} \setminus X_s$. In total, the number of possible choices for C_α is

$$\prod_{s=0}^{r-1} \binom{C(f)-2s}{2} = \frac{C(f)!}{2^r},$$

matching the formula for T in the statement of the lemma.

Now suppose that $C(f) = 2r+1$ is odd. Let $\alpha \in \mathcal{F}$. We define a sequence

$$X_0 \subset \cdots \subset X_r \subseteq C_\alpha,$$

where X_s is a collection of $2s+1$ compatible cosets, as follows. We start by defining X_0. According to Lemma 2.4, the certificates C_α and $C_\varnothing$ must contain at least two cosets in common q_1, q_2. At least one of these cosets is of the form $(k, \alpha(k))$ for some $k \in [m]$. We define $X_0 = \{(k, \alpha(k))\}$. Now let $s < r$, and suppose that X_s has been defined. Since $|X_s| = 2s+1 \leqslant C(f) - 2 = m - 1$, we can define X_{s+1} as in the case of even $C(f)$.

Note that $|X_r| = 2r+1 = |C_\alpha|$, and so $X_r = C_\alpha$. The certificate X_0 contains a single coset $(k, \ell) \in C_\varnothing$, where $k \in [m]$, and so there are $m = C(f) - 1$ choices for X_0. For $s < r$, given X_s, there are $\binom{|C_{X_s}|-|X_s|}{2} = \binom{C(f)-2s-1}{2}$ choices for X_{s+1} (this is the same as in the case of even $C(f)$). In total, the number of possible choices for C_α is

$$(C(f)-1)\prod_{s=0}^{r-1}\binom{C(f)-2s-1}{2} = (C(f)-1)\frac{(C(f)-1)!}{2^r},$$

matching the formula for T in the statement of the lemma. □

Proof of Theorem 1.3. Let $\mathcal{F}$ be a 2-intersecting subset of S_n of size $(n-2)!$, where $n \geqslant 2$, and let f be its characteristic function. Our goal is to show that

$$\mathcal{F} = \{\alpha \in S_n : \alpha(i_1) = j_1 \text{ and } \alpha(i_2) = j_2\}$$

for some $i_1 \neq i_2 \in [n]$ and $j_1 \neq j_2 \in [n]$, i.e., we must show that $\mathcal{F}$ is a 2-coset.

Suppose first that $n \geqslant 8$. Since $n \geqslant 5$, Theorem 2.1 shows that $\deg f \leqslant 2$. Lemma 2.5 shows that $C(f) \leqslant n-2$. Lemma 3.3 implies that $C(f) \geqslant 2$ and $|\mathcal{F}| \leqslant T(n - C(f))!$, where $T = \lfloor C(f)/2 \rfloor (C(f)-1)!/2^{\lfloor C(f)/2 \rfloor}$. Therefore

$$\frac{(n-2)!}{(n-C(f))!} \leqslant \frac{2\lfloor C(f)/2\rfloor (C(f)-1)!}{2^{\lfloor C(f)/2\rfloor}}.$$

The left-hand side is clearly increasing in n. Since $n \geqslant C(f) + 2$, it follows that

$$\frac{C(f)!}{2} \leqslant \frac{2\lfloor C(f)/2\rfloor (C(f)-1)!}{2^{\lfloor C(f)/2\rfloor}},$$

and so

$$C(f) \leqslant \frac{2\lfloor C(f)/2\rfloor}{2^{\lfloor C(f)/2\rfloor - 1}}.$$

If $C(f) = 2r$ is even then this reads $2r \leqslant 2r/2^{r-1}$, and so $r = 1$. If $C(f) = 2r+1$ is odd then this reads $2r+1 \leqslant 2r/2^{r-1}$, which never holds. We conclude that $C(f) = 2$.

Let $\alpha \in \mathcal{F}$ be arbitrary. Since $C(f) = 2$, there is a certificate of the form $\{(i_1, j_1), (i_2, j_2)\}$ for α. The number of permutations satisfying this certificate is $(n-2)!$, and we conclude that $\mathcal{F}$ consists of all permutations satisfying the certificate, completing the proof in this case.

In order to complete the proof, we consider the case $n \leqslant 7$. It suffices to show that for $n \in \{2,3,4,5,6,7\}$, any 2-intersecting family of size $(n-2)!$ which contains the identity permutation is of the form

$$\{\alpha \in S_n : \alpha(i_1) = i_1, \alpha(i_2) = i_2\}$$

for some $i_1 \neq i_2$.

If $n = 2$ or $n = 3$ then $(n-2)! = 1$, and the claim can be verified directly. In order to verify the remaining cases $n \in \{4,5,6,7\}$, we formulate the task as a maximum clique problem. Let G_n be the graph whose vertex set consists of all permutations which 2-intersect the identity permutation, and in which two permutations are connected if they 2-intersect. A 2-intersecting family containing the identity permutation is the same as a clique in G_n. Using `SAGE` [30], which internally uses the software library

`Cliquer` [27], we verify that a maximum clique in G_n contains $(n-2)!$ many permutations, and furthermore, there are exactly $\binom{n}{2}$ many maximum cliques, matching the number of 2-cosets containing the identity permutation. The relevant code appears in Appendix C. This completes the proof. $\square$

4. Proof of Theorem 1.4

The proof of Theorem 1.4 is similar to that of Theorem 1.3, but there is an additional complication: Lemma 2.10 only states that degree-1 Boolean functions have certificate complexity 2. This causes the proof strategy that we used for Lemma 3.2 to fail for $\mathcal{M}_{2n}$. To get around this, we show that an analogue of Lemma 3.2 holds for $\mathcal{M}_{2n}$ if we further insist that $\mathcal{F}$ is an *(inclusion-)maximal* 2-intersecting family, i.e., that $\mathcal{F}$ is not contained in a larger 2-intersecting family.

We start by defining *extended certificates* of $\mathcal{M}_{2n}$. An extended certificate of size c is either a standard certificate of size c, or a pair $(C', \{i,j,k\})$, where C' is a certificate of size $c-1$ and $i,j,k \in [2n]$ are distinct elements not appearing in C'. A perfect matching $m \in \mathcal{M}_{2n}$ satisfies a certificate $(C', \{i,j,k\})$ if it satisfies C' and doesn't contain any of the pairs $\{i,j\}, \{i,k\}, \{j,k\}$.

Lemma 4.1. *Let $c \leqslant n-2$, $C_1 = (C_1', \{i,j,k\})$ be an extended certificate of size c, and let C_2 be an extended certificate of size c. If any perfect matching satisfying C_1 and any perfect matching satisfying C_2 are 2-intersecting, then the same holds when C_1 is replaced by C_1'.*

Proof. Suppose that m_1 is a perfect matching satisfying C_1' but not C_1. Without loss of generality, $m_1(i) = j$. We need to show that if m_2 is a perfect matching satisfying C_2 then m_1 and m_2 are 2-intersecting.

Because m_1 satisfies C_1, we have that its pair representation consists of C_1 together with $n-(c-1) \geqslant 3$ more pairs, one of which is $\{i,j\}$. Among the other pairs, at least one $\{a,b\}$ does not involve k. Consider the following two perfect matchings:

$$m_1' = m_1 \setminus \big\{\{i,j\},\{a,b\}\big\} \cup \big\{\{i,a\},\{j,b\}\big\},$$
$$m_1'' = m_1 \setminus \big\{\{i,j\},\{a,b\}\big\} \cup \big\{\{i,b\},\{j,a\}\big\}.$$

Both of these perfect matchings avoid the edges $\{i,j\},\{i,k\},\{j,k\}$. If m_2 contains $\{i,a\}$ then it cannot contain $\{i,b\}$ or $\{j,a\}$, and similarly for $\{j,b\},\{i,b\},\{j,a\}$. Therefore m_2 cannot intersect both $\big\{\{i,a\},\{j,b\}\big\}$ and $\big\{\{i,b\},\{j,a\}\big\}$. Suppose that m_2 does not intersect $\big\{\{i,a\},\{j,b\}\big\}$. Then $m_1' \cap m_2 \subseteq m_1 \cap m_2$. On the other hand, m_1' satisfies C_1, and so $|m_1' \cap m_2| \geqslant 2$. We conclude that $|m_1 \cap m_2| \geqslant 2$, as needed. $\square$

We say that two cosets $[i_1 \leftrightarrow j_1], [i_2 \leftrightarrow j_2]$ are *compatible* if their intersection is non-empty. A family is *r-covered* if it is contained in the union of r compatible cosets.

The proof of the following lemma is identical to that of Lemma 3.1 (with Lemma 2.11 standing for Lemma 2.4) *mutatis mutandis.*

Lemma 4.2. *Let f be the characteristic function of a 2-intersecting family $\mathcal{F} \subseteq \mathcal{M}_{2n}$, and suppose that $C(f) \leqslant n-2$. If $m \in \mathcal{F}$ then $\mathcal{F}$ is r-covered for $r = C(f,m) - 1$.*

The following structure lemma is the analog of Lemma 3.2. There are three differences in the statement. First, we assume that $\mathcal{F}$ is maximal. Second, we assume that $r \leqslant n-2$. Third, we only provide certificates to perfect matchings belonging to $\mathcal{F}$.

Lemma 4.3. *Let $\mathcal{F} \subseteq \mathcal{M}_{2n}$ be an r-covered family, say*

$$\mathcal{F} \subseteq [i_1 \leftrightarrow j_1] \cup \cdots \cup [i_r \leftrightarrow j_r],$$

where $r \leqslant n-3$. Suppose that $\mathcal{F}$ is maximal, and that its characteristic function f has degree at most 2. Then every $m \in \mathcal{F}$ has a certificate of the form $\bigl\{\{i_1, m(i_1)\}, \dots, \{i_r, m(i_r)\}, \{i,j\}\bigr\}$.

Note that the certificate could mention the same pair twice, for example if $m(i_1) = i_2$.

Proof. The first step is to prove that for every distinct $k_1, \dots, k_r$, the restriction of f to $[i_1 \leftrightarrow k_1] \cap \cdots \cap [i_r \leftrightarrow k_r]$ has degree at most 1, assuming the coset intersection is non-empty. This part is identical to the proof of Lemma 3.2, so we do not repeat it here (the only difference is that we never consider $k_1, \dots, k_r$ such that the coset intersection is empty).

Now suppose that $m \in \mathcal{F}$. Then the restriction of f to

$$I = [i_1 \leftrightarrow m(i_1)] \cap \cdots \cap [i_r \leftrightarrow m(i_r)]$$

(which is non-empty) has degree 1. According to Theorem 2.9, $f|_I$ is either a dictator, a triangle, or an anti-triangle. If $f|_I$ is a dictator or a triangle, then $m|_I$ has a certificate of size 1, and we are done. We would like to show that the remaining case is impossible.

If $f|_I$ is an anti-triangle, then m has an extended certificate $(C', \{i,j,k\})$ of size $r+1 \leqslant n-2$. The same argument proves every perfect matching in $\mathcal{F}$ has an extended certificate of size $r+1 \leqslant n-2$; therefore, Lemma 4.1 implies that if $m' \notin \mathcal{F}$ is a perfect matching satisfying C', then $\mathcal{F} \cup \{m'\}$ is also 2-intersecting. Thus either $\mathcal{F}$ is not maximal (if such $m' \notin \mathcal{F}$ exists), or in fact C' is already a certificate for m. □

We now prove an analog of Lemma 3.3, from which Theorem 1.4 will easily follow. The only difference in the statement is the additional assumption that $\mathcal{F}$ is maximal. We omit the arguments of the proof that are identical to Lemma 3.3 *mutatis mutandis*.

Lemma 4.4 (Key Lemma). *Let $\mathcal{F} \subseteq \mathcal{M}_{2n}$ be a maximal 2-intersecting family whose characteristic function f has degree at most 2, and suppose that $C(f) \leqslant n-2$. Let $C_1(f)$ the maximum certificate complexity of any $m \in \mathcal{F}$. Then the family $\mathcal{F}$ is contained in the union of at most T many $C_1(f)$-cosets, where*

$$T = \frac{2\lfloor C_1(f)/2 \rfloor (C_1(f)-1)!}{2^{\lfloor C_1(f)/2 \rfloor}}.$$

Moreover, $C_1(f) \geqslant 2$.

Proof. Let $\mu \in \mathcal{F}$ be a perfect matching satisfying $C(f,\mu) = C_1(f)$. Lemma 2.11, applied to $m_1 = m_2 = \mu$, shows that $C(f,\mu) \geqslant 2$, and so $C_1(f) \geqslant 2$. Lemma 4.2 shows that $\mathcal{F}$ is r-covered, where $r = C(f,\mu) - 1$. Note that $r \leqslant C(f) - 1 \leqslant n-3$. Without loss of generality, we can assume that $\mathcal{F} \subseteq [1 \leftrightarrow r+1] \cup [2 \leftrightarrow r+2] \cup \cdots \cup [r \leftrightarrow 2r]$.

Lemma 4.3 shows that every $m \in \mathcal{F}$ has a certificate of the form

$$\bigl\{\{1, m(1)\}, \dots, \{r, m(r)\}, \{i,j\}\bigr\},$$

which we call the *standard certificate*. Lemma 4.3 also implies that $\mathcal{F}$ is not $(r-1)$-covered; otherwise, every member of $\mathcal{F}$ would have a certificate of size $r < C_1(f)$, which contradicts the definition of $C_1(f)$.

A standard certificate $\bigl\{\{1, m(1)\}, \dots, \{r, m(r)\}, \{i,j\}\bigr\}$ satisfies $m(1), \dots, m(r) \notin [r]$, since otherwise Lemma 4.3 would imply that $\mathcal{F}$ is $(r-1)$-covered (since some of the pairs $\{t, m(t)\}$ coincide), which is impossible. This allows us to color the pairs in a standard certificate unambiguously: a pair $\{t, m(t)\}$ is colored t, and a pair $\{i,j\}$ with $i,j \notin [r]$ is colored $r+1$. Every standard certificate contains exactly one pair of each color.

The remainder of the proof is identical to that of Lemma 3.3. □

We can now prove Theorem 1.4, whose proof is very similar to that of Theorem 1.3.

Proof of Theorem 1.4. Let $\mathcal{F}$ be a 2-intersecting subset of $\mathcal{M}_{2n}$ of size $(2n-5)!!$, where $n \geqslant 2$, and let f be its characteristic function. Our goal is to show that

$$\mathcal{F} = \{m \in \mathcal{M}_{2n} : m(i_1) = j_1 \text{ and } m(i_2) = j_2\}$$

for some distinct $i_1, j_1, i_2, j_2 \in [2n]$.

Suppose first that $n \geqslant 8$. Since $n \geqslant 3$, Theorem 2.8 shows that $\mathcal{F}$ is maximal and that $\deg f \leqslant 2$. Lemma 2.12 shows that $C_1(f) \leqslant n-2$. Lemma 4.4 implies that $C_1(f) \geqslant 2$ and $|\mathcal{F}| \leqslant T(2n-2C_1(f)-1)!!$, where $T = \lfloor C_1(f)/2 \rfloor (C_1(f)-1)!/2^{\lfloor C_1(f)/2 \rfloor}$. Therefore

$$\frac{(2n-5)!!}{(2n-2C_1(f)-1)!!} \leqslant \frac{2\lfloor C_1(f)/2\rfloor (C_1(f)-1)!}{2^{\lfloor C_1(f)/2 \rfloor}}.$$

The left-hand side is clearly increasing in n. Since $n \geqslant C_1(f)+2$, it follows that

$$\frac{(2C_1(f))!}{3 \cdot 2^{C_1(f)} C_1(f)!} = \frac{(2C_1(f)-1)!!}{3} \leqslant \frac{2\lfloor C_1(f)/2\rfloor (C_1(f)-1)!}{2^{\lfloor C_1(f)/2 \rfloor}},$$

and so

$$(2C_1(f))! \leqslant 3 \cdot 2^{\lceil C_1(f)/2 \rceil} C_1(f)!(2\lfloor C_1(f)/2 \rfloor)(C_1(f)-1)!.$$

If $C_1(f)$ is even then this reads

$$(2C_1(f))! \leqslant 3 \cdot 2^{C_1(f)/2} C_1(f)!^2.$$

When $C = C_1(f)$ increases by 1, the left-hand side increases by a factor of $(2C+2)(2C+1)$, while the right-hand side increases by a factor of $\sqrt{2}(C+1)^2$, which is smaller for $C \geqslant 2$. When $C = 3$, the inequality fails. Therefore in this case, $C_1(f) = 2$.

If $C_1(f)$ is odd then the inequality reads

$$(2C_1(f))! \leqslant 3 \cdot 2^{(C_1(f)+1)/2} C_1(f)!(C_1(f)-1)(C_1(f)-1)! < 3 \cdot 2^{(C_1(f)+1)/2} C_1(f)!^2.$$

As before, if we increase $C = C_1(f)$ by 1, the left-hand side increases by a larger factor than the (far) right-hand side. When $C = 3$, the inequality fails, and so this case cannot happen.

Now let $m \in \mathcal{F}$ be arbitrary. Since $C_1(f) = 2$, there is a certificate of the form $\bigl\{\{i_1, j_1\}, \{i_2, j_2\}\bigr\}$ for m. The number of permutations satisfying this certificate is $(2n-5)!!$, and we conclude that $\mathcal{F}$ consists of all perfect matchings satisfying the certificate, completing the proof in this case.

In order to complete the proof, we consider the case $n \leqslant 7$. It suffices to show that for $n \in \{2, 3, 4, 5, 6, 7\}$, any 2-intersecting family of size $(2n-5)!!$ which contains the perfect matching $\{1, n+1\}, \ldots, \{n+2n\}$ is of the form

$$\{m \in \mathcal{M}_{2n} : m(i_1) = n + i_1, m(i_2) = n + i_2\}$$

for some $i_1 \neq i_2 \in [n]$.

If $n = 2$ or $n = 3$ then $(2n-5)!! = 1$, and the claim can be verified directly. In order to verify the remaining cases $n \in \{4, 5, 6, 7\}$, we use exhaustive search just as in the proof of Theorem 1.3. The relevant code appears in Appendix D. $\square$

References

[1] Rudolf Ahlswede and Levon H. Khachatrian, *The complete intersection theorem for systems of finite sets*, European J. Combin. **18** (1997), no. 2, 125–136, `https://doi.org/10.1006/eujc.1995.0092`.

[2] ———, *A pushing-pulling method: new proofs of intersection theorems*, Combinatorica **19** (1999), no. 1, 1–15, `https://doi.org/10.1007/s004930050042`.

[3] Angelot Behajaina, Roghayeh Maleki, Aina Toky Rasoamanana, and A. Sarobidy Razafimahatratra, *3-setwise intersecting families of the symmetric group*, Discrete Math. **344** (2021), no. 8, Paper No. 112467, 15, `https://doi.org/10.1016/j.disc.2021.112467`.

[4] Harry Buhrman and Ronald de Wolf, *Complexity measures and decision tree complexity: a survey*, Theoret. Comput. Sci. **288** (2002), no. 1, 21–43, https://doi.org/10.1016/S0304-3975(01)00144-X, Complexity and logic (Vienna, 1998).

[5] Peter J. Cameron and C. Y. Ku, *Intersecting families of permutations*, European J. Combin. **24** (2003), no. 7, 881–890, https://doi.org/10.1016/S0195-6698(03)00078-7.

[6] Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli, *Harmonic analysis on finite groups*, Cambridge Studies in Advanced Mathematics, vol. 108, Cambridge University Press, Cambridge, 2008, https://doi.org/10.1017/CBO9780511619823, Representation theory, Gelfand pairs and Markov chains.

[7] ———, *Representation theory of the symmetric groups*, Cambridge Studies in Advanced Mathematics, vol. 121, Cambridge University Press, Cambridge, 2010, https://doi.org/10.1017/CBO9781139192361, The Okounkov-Vershik approach, character formulas, and partition algebras.

[8] Neta Dafni, *Complexity measures on the symmetric group and beyond*, Master's thesis, Technion — Israel Institute of Technology, 2022.

[9] Neta Dafni, Yuval Filmus, Noam Lifshitz, Nathan Lindzey, and Marc Vinyals, *Complexity measures on the symmetric group and beyond*, in 12th Innovations in Theoretical Computer Science Conference, LIPIcs. Leibniz Int. Proc. Inform., vol. 185, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2021, pp. Art. No. 87, 5, https://doi.org/10.1305/ndjfl/1040046140.

[10] David Ellis, *A proof of the Cameron-Ku conjecture*, J. Lond. Math. Soc. (2) **85** (2012), no. 1, 165–190, https://doi.org/10.1112/jlms/jdr035.

[11] ———, *Setwise intersecting families of permutations*, J. Combin. Theory Ser. A **119** (2012), no. 4, 825–849, https://doi.org/10.1016/j.jcta.2011.12.003.

[12] David Ellis, Ehud Friedgut, and Haran Pilpel, *Intersecting families of permutations*, J. Amer. Math. Soc. **24** (2011), no. 3, 649–682, https://doi.org/10.1090/S0894-0347-2011-00690-5.

[13] P. Erdős, Chao Ko, and R. Rado, *Intersection theorems for systems of finite sets*, Quart. J. Math. Oxford Ser. (2) **12** (1961), 313–320, https://doi.org/10.1093/qmath/12.1.313.

[14] Shaun Fallat, Karen Meagher, and Mahsa N. Shirazi, *The Erdős-Ko-Rado theorem for 2-intersecting families of perfect matchings*, Algebr. Comb. **4** (2021), no. 4, 575–598, https://doi.org/10.5802/alco.169.

[15] Yuval Filmus, *A comment on intersecting families of permutations*, arXiv:1706.10146, 2017.

[16] Yuval Filmus, Hamed Hatami, Nathan Keller, and Noam Lifshitz, *On the sum of the L_1 influences of bounded functions*, Israel J. Math. **214** (2016), no. 1, 167–192, https://doi.org/10.1007/s11856-016-1355-0.

[17] Péter Frankl and Mikhail Deza, *On the maximum number of permutations with given maximal or minimal distance*, J. Combinatorial Theory Ser. A **22** (1977), no. 3, 352–360, http://www.sciencedirect.com/science/article/pii/0097316577900097.

[18] Chris Godsil and Karen Meagher, *A new proof of the Erdős-Ko-Rado theorem for intersecting families of permutations*, European J. Combin. **30** (2009), no. 2, 404–414, https://doi.org/10.1016/j.ejc.2008.05.006.

[19] ———, *Erdős-Ko-Rado theorems: algebraic approaches*, Cambridge Studies in Advanced Mathematics, vol. 149, Cambridge University Press, Cambridge, 2016, https://doi.org/10.1017/CBO9781316414958.

[20] ———, *An algebraic proof of the Erdős-Ko-Rado theorem for intersecting families of perfect matchings*, Ars Math. Contemp. **12** (2017), no. 2, 205–217, https://doi.org/10.26493/1855-3974.976.c47.

[21] Benoit Larose and Claudia Malvenuto, *Stable sets of maximal size in Kneser-type graphs*, European J. Combin. **25** (2004), no. 5, 657–673, https://doi.org/10.1016/j.ejc.2003.10.006.

[22] Nathan Lindzey, *Erdős-Ko-Rado for perfect matchings*, European J. Combin. **65** (2017), 130–142, https://doi.org/10.1016/j.ejc.2017.05.005.

[23] Nathan Lindzey, *Intersecting families of perfect matchings*, arXiv:1811.06160, 2018.

[24] ———, *Matchings and representation theory*, Ph.D. thesis, University of Waterloo, 2018.

[25] Karen Meagher and Lucia Moura, *Erdős-Ko-Rado theorems for uniform set-partition systems*, Electron. J. Combin. **12** (2005), Research Paper 40, 12, http://www.combinatorics.org/Volume_12/Abstracts/v12i1r40.html.

[26] Karen Meagher and A. Sarobidy Razafimahatratra, *The Erdős-Ko-Rado theorem for 2-pointwise and 2-setwise intersecting permutations*, Electron. J. Combin. **28** (2021), no. 4, Paper No. 4.10, 21, https://doi.org/10.37236/9556.

[27] Sampo Niskanen and Patric R. J. Östergård, *Cliquer user's guide, version 1.0*, Tech. Report T48, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, 2003.

[28] Ryan O'Donnell, *Analysis of Boolean functions*, Cambridge University Press, New York, 2014, https://doi.org/10.1017/CBO9781139814782.

[29] Bruce E. Sagan, *The symmetric group*, second ed., Graduate Texts in Mathematics, vol. 203, Springer-Verlag, New York, 2001, https://doi.org/10.1007/978-1-4757-6804-6, Representations, combinatorial algorithms, and symmetric functions.

[30] Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 9.5)*, 2022, https://www.sagemath.org.

Appendix A. SAGE code

The code snippets below form part of the proofs of Lemma 2.5, Theorem 1.3, and Theorem 1.4. They are available to download as part of the arXiv version of the paper.

Appendix B. Code for Lemma 2.5

```
import itertools

def degree_2_functions():
    "Generate vector space of degree 2 functions, represented as truth table"
    return span(QQ, [vector(int((x & m) == m) for x in range(16)) \
                     for m in [0, 1, 2, 4, 8, 3, 5, 9, 6, 10, 12]])

def verify_no_sensitivity_4():
    "Verify that no function from {0,1}^4 to {0,1} has sensitivity 4 at zero"
    degree_2 = degree_2_functions()
    return not any(f for f in itertools.product([0,1], repeat=16) \
                   if f[0] != f[1] == f[2] == f[4] == f[8] and \
                   vector(f) in degree_2)
```

Appendix C. Code for Theorem 1.3

```
def intersection_size(a, b):
    "Size of intersection of two permutations"
    return sum(i==j for (i,j) in zip(a,b))

def generate_G_n(n, t):
    "Generate graph whose cliques are t-intersecting families
    of S_n containing id"
    idp = list(range(n))
    V = [a for a in Permutations(range(n)) if intersection_size(a, idp) >= t]
    E = [(a,b) for a in V for b in V if t <= intersection_size(a, b) < n]
    return Graph([V, E])

def verify_main_theorem_n(n):
    "Verify that all 2-intersecting families containing id are 2-cosets
     given n"
    G_n = generate_G_n(n, 2)
    return G_n.clique_number() == factorial(n - 2) and \
        len(G_n.cliques_maximum()) == binomial(n, 2)

def verify_main_theorem():
    "Verify that all 2-intersecting families containing id are 2-cosets
     for 4 <= n <= 7"
    return all(verify_main_theorem_n(n) for n in [4,5,6,7])
```

Appendix D. Code for Theorem 1.4

```
def intersection_size(a, b):
    "Size of intersection of two perfect matchings"
    return len(a.intersection(b))

def generate_G_n(n, t):
    "Generate graph whose cliques are t-intersecting families of M_2n
    containing a fixed PM"
    idm = frozenset(PerfectMatchings(2*n).__iter__().__next__())
    V = [frozenset(a) for a in PerfectMatchings(2*n) if \
```

```
        intersection_size(frozenset(a), idm) >= t]
    E = [(a,b) for a in V for b in V if t <= intersection_size(a, b) < n]
    return Graph([V, E])

def verify_main_theorem_n(n):
    "Verify that all 2-intersecting families containing a fixed PM
     are 2-cosets for given n"
    G_n = generate_G_n(n, 2)
    return G_n.clique_number() == factorial(2*n-4)/(2^(n-2)*factorial(n-2)) and \
        len(G_n.cliques_maximum()) == binomial(n, 2)

def verify_main_theorem():
    "Verify that all 2-intersecting families containing a fixed PM
     are 2-cosets for 4 <= n <= 7"
    return all(verify_main_theorem_n(n) for n in [4,5,6,7])
```

Technion – Israel Institute of Technology, The Henry and Marilyn Taub Faculty of Computer Science, CS Taub Building, Haifa 3200003, Israel.
Email address: giladchase@gmail.com

Technion – Israel Institute of Technology, The Henry and Marilyn Taub Faculty of Computer Science, CS Taub Building, Haifa 3200003, Israel.
Email address: netadafni@gmail.com

Technion – Israel Institute of Technology, The Henry and Marilyn Taub Faculty of Computer Science, CS Taub Building, Haifa 3200003, Israel.
Email address: filmus.yuval@gmail.com

Technion – Israel Institute of Technology, The Henry and Marilyn Taub Faculty of Computer Science, CS Taub Building, Haifa 3200003, Israel.
Email address: lindzeyn@gmail.com