

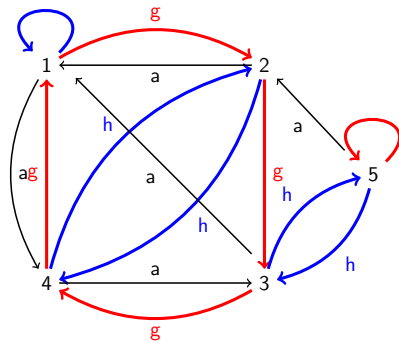
# A Tale of Two Design Theories

William J. Martin

Department of Mathematical Sciences  
and  
Department of Computer Science  
Worcester Polytechnic Institute

Combinatorics Seminar  
Brandeis University  
February 23, 2016

## A Puzzle



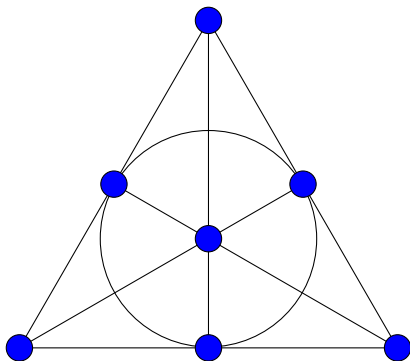
Without knowing the initial state of the system, send a sequence of instructions to move to State 1.

## A Small Finite Geometry

In finite geometry we enjoy incidence structures in which any two lines meet in at most one point and any two points are joined by at most one line.

If we insist on “exactly one point” and “exactly one line”, and avoid degenerates, we are studying finite projective planes.

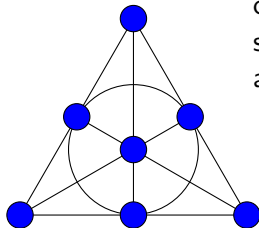
# The Fano plane



1	2	4
2	3	5
3	4	6
4	5	0
5	6	1
6	0	2
0	1	3

## The Fano Plane

The Fano plane is the smallest finite projective plane: its points are the 1-dimensional subspaces of  $\mathbb{F}_2^3$  and its lines are the 2-dimensional subspaces. Each line contains three points and any two points are joined by a unique line.



The Fano plane can also be constructed from the quadratic residues  $\mathcal{D} = \{1, 2, 4\}$  in  $\mathbb{Z}_7$  by viewing lines (or “blocks”) as all possible cyclic shifts  $x + \mathcal{D} \subseteq \mathbb{Z}_7$  for  $x \in \mathbb{Z}_7$ .

## Biplanes?

By the same token, we can obtain a design from the quadratic residues modulo 11; but here any two distinct points lie in two common blocks and any two blocks have exactly two points in common.

Some people call these *biplanes* it is very frustrating that we know only 17 non-trivial examples.

# Block Designs

More generally, a  $2$ - $(n, k, \mu)$  design is a collection  $\mathcal{B}$  of  $k$ -element subsets of  $[n] = \{1, \dots, n\}$  such that any two points  $x, y \in [n]$  occur together in exactly  $\mu$  blocks.

These have been of interest to statisticians and are known as “balanced incomplete block designs”.

## A 3-Design

The codewords of the extended binary Hamming code

$$C = \text{rowsp} \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

give us a design

$$\mathcal{D} = \{4567, 2367, 2345, 1357, 1346, 1245, 1247, \\ 1238, 1458, 1678, 2468, 2578, 3678, 3568\}$$

in which every triple appears exactly once!



## $t$ -Designs

In 1959, Haim Hanani defined  $t$ -designs.

A  $t$ - $(n, k, \mu)$  design is a collection  $\mathcal{D}$  of  $k$ -element subsets of  $[n] = \{1, \dots, n\}$  having the property that every  $t$ -element subset  $T \subset [n]$  is contained in exactly  $\mu$  blocks from  $\mathcal{D}$ .

## $t$ -Designs

In 1959, Haim Hanani defined  $t$ -designs.

A  $t$ - $(n, k, \mu)$  design is a collection  $\mathcal{D}$  of  $k$ -element subsets of  $[n] = \{1, \dots, n\}$  having the property that every  $t$ -element subset  $T \subset [n]$  is contained in exactly  $\mu$  blocks from  $\mathcal{D}$ .

Now statisticians fall asleep.

## $t$ -Designs

In 1959, Haim Hanani defined  $t$ -designs.

A  $t$ - $(n, k, \mu)$  design is a collection  $\mathcal{D}$  of  $k$ -element subsets of  $[n] = \{1, \dots, n\}$  having the property that every  $t$ -element subset  $T \subset [n]$  is contained in exactly  $\mu$  blocks from  $\mathcal{D}$ .

Now statisticians fall asleep.

But finite group theorists get excited.

## Can we use groups?

Let  $G$  be any  $t$ -transitive (or  $t$ -homogeneous) permutation group on  $[n]$ . For  $k > t$ , let  $\mathcal{D}$  be any orbit of  $G$  on  $k$ -subsets. Then  $\mathcal{D}$  is a  $t$ - $(n, k, \mu)$  design.

So if there exist  $t$ -transitive groups for all  $t$ , then there exist  $t$ -designs for all  $t$ .

## 5-Designs from Beautiful Groups

But the CLASSIFICATION of finite simple groups tells us that, apart from the symmetric and alternating groups, there are no  $t$ -transitive groups for  $t > 5$ .

For  $t = 5$ , two Mathieu groups are  $t$ -transitive, but that's all we get; these give us  $5$ -(24, 8, 1) and  $5$ -(12, 6, 1) designs.

# Steiner Systems

A design with  $\mu = 1$  is as small as possible; these are called *Steiner systems*.

Until recently, no non-trivial Steiner systems with  $t > 5$  were known and, for  $t = 5$ , the only known examples had  $k = 6$  and  $n \in \{12, 24, 48, 72, 84, 108, 132\}$ .

## They exist! They exist!

Today, we require  $\mathcal{D}$  contains no repeated blocks.

In 1987, Luc Teirlinck proved that non-trivial  $t$ -designs exist for all values of  $t$ . But these designs have astronomically large  $\mu$  values.

In the 1990s, various people used basis reduction (LLL) to piece together orbits of nice groups ( $PSL_2(q)$  acting on the projective line seemed to be fruitful) and obtain  $t$ -designs with  $t = 6, 7, 8, 9$  and  $\mu$  not “too bad” (2-,3-,4-digit numbers).

## Keevash's Theorem

In January 2014, Peter Keevash (now at Oxford) proved that Steiner systems exist for all values of  $t$ . (In fact, once you take divisibility into account, only finitely many  $n$  are bad for a given  $t$  and  $k$ ). This answers a question of Plücker from 1835.



# Incidence Matrices

We want to look at these objects from a linear-algebraic viewpoint.

Our matrices are functions on Cartesian products:

$$W : \binom{[n]}{k} \times \binom{[n]}{t} \rightarrow \mathbb{C}$$

## Incidence Matrix of $k$ -Sets versus $t$ -Sets

The *incidence matrix* (“Wilson matrix”, “Riemann matrix”)  $W_{k,t} = W_{k,t}^{(n)}$  has rows indexed by  $\binom{[n]}{k}$  and columns indexed by  $\binom{[n]}{t}$  and entries

$$(W_{k,t})_{a,b} = \begin{cases} 1 & b \subseteq a; \\ 0 & \text{otherwise.} \end{cases}$$

## Incidence Matrices

Some properties of the incidence matrices:

$$W_{k,t}W_{t,s} = \binom{k-s}{t-s} W_{k,s}$$

so  $\text{colsp } W_{k,t}$  contains  $\text{colsp } W_{k,t-1}$ .

$$W_{k,t}^{(n)} = \left[ \begin{array}{c|c} W_{k-1,t-1}^{(n-1)} & W_{k-1,t}^{(n-1)} \\ \hline 0 & W_{k,t}^{(n-1)} \end{array} \right]$$

so, for  $t \leq k \leq n/2$ ,  $W_{k,t}$  has full column rank.

# The Johnson Association Scheme

Now fix  $n$ . We consider the algebra generated by the matrices

$$C_t = W_{k,t} W_{k,t}^\top$$

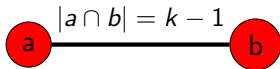
We have

$$C_r C_s = \sum_{t=0}^{\min(r,s)} \binom{k-t}{r-t} \binom{k-t}{s-t} \binom{v-r-s}{v-k-t} C_t$$

so that  $\text{span}_{\mathbb{C}}\{C_0, \dots, C_t\}$  is closed under matrix multiplication for  $0 \leq t \leq k$ .

## The Johnson Graph

Consider the graph  $J(n, k)$  with vertex set  $\binom{[n]}{k}$  and adjacency rule

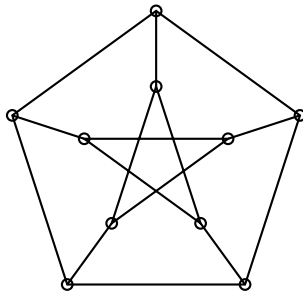
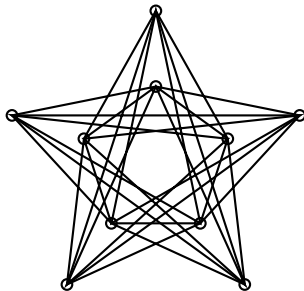


This graph  $J(n, k)$  is called the *Johnson graph*. It's eigenvalues are  $(k - j)(n - k - j) - j$  for  $0 \leq j \leq k$ .

I should note that these graphs play a special role in Babai's new quasipolynomial time algorithm for graph isomorphism.

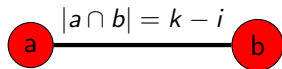
Example:  $J(5, 2)$ 

For 2-subsets of  $[5] = \{1, 2, 3, 4, 5\}$  we get the Johnson graph and its familiar complement:



# The Johnson Scheme

Two vertices  $a$  and  $b$  are at distance  $i$  in the Johnson graph  $J(n, k)$  if



Denote the adjacency matrix of this graph by  $A_i$ .

## Bose-Mesner Algebra

One easily checks that

$$C_t = \sum_{i=0}^t \binom{i}{t} A_{k-i}$$

So the algebra  $\mathbb{A}$  generated by  $C_0, \dots, C_k$  is also closed under entrywise (*Schur*) multiplication.

Also,  $I \in \mathbb{A}$  and  $J \in \mathbb{A}$  where  $J = \sum_i A_i$  is the all-ones matrix.

A transpose-closed vector space of matrices closed under both ordinary and Schur multiplication and containing the identities for both is called a *Bose-Mesner algebra*.



## Bose-Mesner Algebra

A transpose-closed vector space of matrices closed under both ordinary and Schur multiplication and containing the identities for both is called a *Bose-Mesner algebra*.

These are equivalent to *association schemes* (Bose/Mesner, 1959). Here's a definition in the symmetric case:

We have a finite set  $X$  together with a partition  $\mathcal{R} = \{R_0, \dots, R_d\}$  of  $X \times X$  into symmetric relations satisfying

- ▶  $R_0$  is the identity relation on  $X$
- ▶ there exist *intersection numbers*  $p_{ij}^h$  such that, whenever  $(a, b) \in R_h$ ,

$$\#\{c \in X \mid (a, c) \in R_i, (c, b) \in R_j\} = p_{ij}^h$$

## Bases for the Bose-Mesner Algebra

In general, we let  $A_i$  denote the adjacency matrix of the graph  $(X, R_i)$ . Then

$$A_i A_j = \sum_{h=0}^d p_{ij}^h A_h,$$

$$\mathbb{A} = \text{span}_{\mathbb{R}} \{A_0, \dots, A_d\}$$

is closed under both ordinary and Schur multiplication and contains both  $I$  and  $J$ .

So  $\mathbb{A}$  admits a basis of mutually orthogonal idempotents  $\{E_0, \dots, E_d\}$

$$E_i E_j = \delta_{i,j} E_i$$

with  $E_0 + E_1 + \dots + E_d = I$ . Without loss,  $E_0 = \frac{1}{|X|} J$ .

## Three Bases

In the case of the Johnson scheme, the algebra  $\mathbb{A}$  has a useful third basis  $\{C_t\}_{t=0}^k$ .

$$C_t = \sum_{i=0}^t \binom{i}{t} A_{k-i}, \quad A_i = \sum_{j=0}^k H_i(j) E_j, \quad E_j = \sum_{t=0}^j \varrho_j(t) C_t$$

where

$$H_i(j) = \sum_{\ell=0}^i (-1)^\ell \binom{j}{\ell} \binom{k-j}{i-\ell} \binom{n-k-j}{i-\ell}$$

is the dual Hahn polynomial.

## Designs as 01-Vectors

Now let  $\mathcal{D} \subseteq \binom{[n]}{k}$  be encoded as a 01-vector of length,  $x$  say,  $\binom{n}{k}$ .  
Then  $\mathcal{D}$  is a  $t$ -design

- ▶ if and only if

## Designs as 01-Vectors

Now let  $\mathcal{D} \subseteq \binom{[n]}{k}$  be encoded as a 01-vector of length,  $x$  say,  $\binom{n}{k}$ .  
Then  $\mathcal{D}$  is a  $t$ -design

- ▶ if and only if  $x^\top W_{k,t} = \mu \mathbf{1}$  for some constant  $\mu$
- ▶ if and only if

## Designs as 01-Vectors

Now let  $\mathcal{D} \subseteq \binom{[n]}{k}$  be encoded as a 01-vector of length,  $x$  say,  $\binom{n}{k}$ .  
Then  $\mathcal{D}$  is a  $t$ -design

- ▶ if and only if  $x^\top W_{k,t} = \mu \mathbf{1}$  for some constant  $\mu$
- ▶ if and only if  $x^\top W_{k,j}$  is a constant vector for  $0 \leq j \leq t$
- ▶ if and only if

## Designs as 01-Vectors

Now let  $\mathcal{D} \subseteq \binom{[n]}{k}$  be encoded as a 01-vector of length,  $x$  say,  $\binom{n}{k}$ .  
Then  $\mathcal{D}$  is a  $t$ -design

- ▶ if and only if  $x^\top W_{k,t} = \mu \mathbf{1}$  for some constant  $\mu$
- ▶ if and only if  $x^\top W_{k,j}$  is a constant vector for  $0 \leq j \leq t$
- ▶ if and only if  $x^\top C_j$  is a constant vector for  $0 \leq j \leq t$
- ▶ if and only if

## Designs as 01-Vectors

Now let  $\mathcal{D} \subseteq \binom{[n]}{k}$  be encoded as a 01-vector of length,  $x$  say,  $\binom{n}{k}$ .  
Then  $\mathcal{D}$  is a  $t$ -design

- ▶ if and only if  $x^\top W_{k,t} = \mu \mathbf{1}$  for some constant  $\mu$
- ▶ if and only if  $x^\top W_{k,j}$  is a constant vector for  $0 \leq j \leq t$
- ▶ if and only if  $x^\top C_j$  is a constant vector for  $0 \leq j \leq t$
- ▶ if and only if  $x^\top E_j = 0$  for  $0 < j \leq t$ .



## Designs as 01-Vectors

Now let  $\mathcal{D} \subseteq \binom{[n]}{k}$  be encoded as a 01-vector of length,  $x$  say,  $\binom{n}{k}$ .  
Then  $\mathcal{D}$  is a  $t$ -design

- ▶ if and only if  $x^\top W_{k,t} = \mu \mathbf{1}$  for some constant  $\mu$
- ▶ if and only if  $x^\top W_{k,j}$  is a constant vector for  $0 \leq j \leq t$
- ▶ if and only if  $x^\top C_j$  is a constant vector for  $0 \leq j \leq t$
- ▶ if and only if  $x^\top E_j = 0$  for  $0 < j \leq t$ .

This leads us to a powerful *linear programming bound* for designs (and codes).

# Posets

For any subset  $S \subseteq [n]$  of size  $s \leq k$ , we identify  $S$  with the 01-vector which is the corresponding column of  $W_{k,s}$ . The map

$$S \mapsto |S|$$

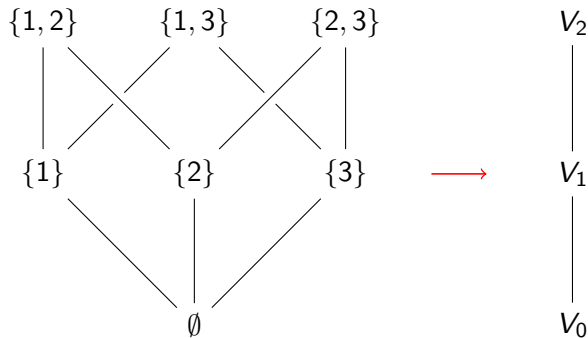
from the Boolean lattice to the chain captures the decomposition of colsp  $W_{k,t}$  into eigenspaces

$$V_0 + V_1 + \cdots + V_t$$

for the Johnson graph

## Posets

For  $n = 3$ ,  $k = 2$  (ignore top element  $\{x, y, z\}$ ), we have an order-preserving map



## General Situation

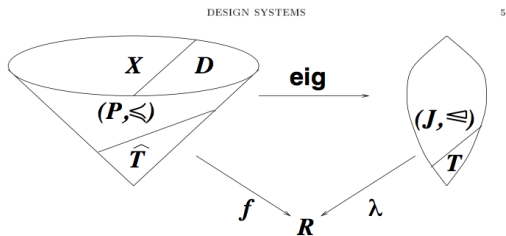


FIGURE 1. Subset  $D$  is a poset  $\mathcal{T}$ -design if and only if  $f|_D = \lambda \circ \text{eig}$  for some function  $\lambda$ .

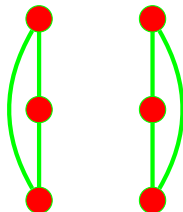
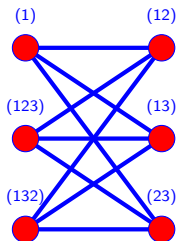
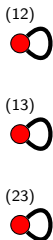
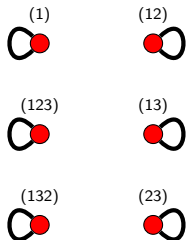
## The Association Scheme of $\mathfrak{S}_n$

From a matrix theory viewpoint, this is just the center of the group algebra, in the right regular representation.

- ▶ An *association scheme* is a highly regular edge decomposition of the complete graph
- ▶ Our graphs will have one vertex for each  $\sigma \in \mathfrak{S}_n$
- ▶ We have one graph for each conjugacy class  $\mathcal{C}_\lambda$
- ▶  $\sigma \sim \tau$  in graph  $G_\lambda$  iff  $\sigma^{-1}\tau \in \mathcal{C}_\lambda$
- ▶ the vector space spanned by these  $p(n)$  matrices is closed under both ordinary and entrywise multiplication (*Bose-Mesner algebra*)

Recall

$$p(n) = [x^n] \prod_{k=1}^{\infty} \frac{1}{1 - x^k}$$

The Association Scheme of  $\mathfrak{S}_3$ 

The Association Scheme of  $\mathfrak{S}_3$ 

$$A_0 = \left[ \begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right],$$

$$A_1 = \left[ \begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{array} \right],$$

$$A_2 = \left[ \begin{array}{ccc|ccc} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{array} \right]$$

# Latin Squares

6	1	2	3	4	5
1	6	3	4	5	2
2	4	6	5	1	3
3	5	1	2	6	4
4	2	5	1	3	6
5	3	4	6	2	1

We will view this as a design consisting of six permutations

$(123456)$ ,  $(26)$ ,  $(1542)(36)$ ,  $(13)(2465)$ ,  $(14)(35)$ ,  $(164325)$



## Transitive Set of Permutations

What special property does this set of permutations enjoy?  
It is *transitive* in the sense that, for every  $i$  and  $j$  there is a (unique, in fact) permutation in the design that maps  $i$  to  $j$ .

## $t$ -Transitive Permutation Groups

Every Cayley table for a group achieves this. But some groups act on sets  $t$ -transitively for  $t > 1$ .

A group  $G$  acts  $t$ -transitively on set  $\Omega$  if, for any distinct  $x_1, \dots, x_t$  and any distinct  $y_1, \dots, y_t$  from  $\Omega$ , there exists a  $g \in G$  mapping each  $x_i$  to the corresponding  $y_i$ .

In fact, if such  $g$  exists for all choices of the  $x_i$  and  $y_i$ , then the *number* of such  $g$  is independent of the  $x_i$  and  $y_i$ .

## $t$ -Homogeneous Groups

A group  $G$  acts  $t$ -homogeneously on set  $\Omega$  if, for any distinct  $x_1, \dots, x_t$  and any distinct  $y_1, \dots, y_t$  from  $\Omega$ , there exists a  $g \in G$  mapping the set  $\{x_1, \dots, x_t\}$  to the set  $\{y_1, \dots, y_t\}$ .

## Transitivity versus Homogeneity

Let's always assume  $t < (n - 1)/2$ .

- ▶ Obvious:  $t$ -transitive implies  $t$ -homogeneous
- ▶ Obvious:  $t$ -transitive implies  $(t - 1)$ -transitive
- ▶ Not-so-Obvious:  $t$ -homogeneous implies  $(t - 1)$ -homogeneous
- ▶ Livingstone-Wagner Theorem (1965): The number of orbits of  $G$  on  $(t - 1)$ -sets cannot exceed the number of orbits of  $G$  on  $t$ -sets
- ▶ the  $t$ -homogeneous groups which are not  $t$ -transitive were characterized by Kantor (1968,1972)

## $\lambda$ -Transitive Permutation Groups

There is a natural common generalization of these two ideas. Let  $\lambda = (\lambda_1, \dots, \lambda_k)$  be a partition of  $n$ . A group  $G \leq \mathfrak{S}_n$  is  $\lambda$ -transitive if for every two ordered set partitions

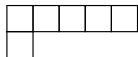
$$P = (P_1, \dots, P_k), \quad Q = (Q_1, \dots, Q_k)$$

with  $|P_i| = |Q_i| = \lambda_i$  for all  $i$ , there is a  $g \in G$  mapping each  $P_i$  setwise to each  $Q_i$ .

For hooks, this specializes to  $t$ -transitive groups; for  $\lambda = (n - t, t)$ , these specialize to  $t$ -homogeneous groups.

## $\lambda$ -Transitive Sets of Permutations

But our latin square is not a group — it's a *set* of permutations which is  $\lambda$ -transitive for  $\lambda = (n - 1, 1)$ .



## $\lambda$ -Transitive Sets of Permutations

A partition  $P = (P_1, \dots, P_k)$  of  $[n]$  has *shape*  $\lambda = (\lambda_1, \dots, \lambda_k)$  if  $|P_i| = \lambda_i$  for all  $i$ . A set  $\mathcal{D} \subseteq \mathfrak{S}_n$  is  $\lambda$ -transitive if there exists a constant  $\mu$  such that, for any set partitions  $P$  and  $Q$  of shape  $\lambda$ ,  $\mathcal{D}$  contains exactly  $\mu$  permutations mapping  $P_i$  to  $Q_i$  (setwise) for each  $1 \leq i \leq k$ .

## Examples

The alternating group is  $(2, 1, \dots, 1)$ -transitive.

Other than symmetric and alternating groups,  $\lambda$ -transitive subgroups of  $\mathfrak{S}_n$  all have  $\lambda_1 \geq n - 5$ .

But  $\lambda$ -transitive sets with  $|\mathcal{D}| \ll n!$  exist for  $n$  sufficiently large (here we fix  $\lambda_2, \dots, \lambda_k$ ). We don't know much about small  $\mu$ .



## Young Subgroups and their Cosets

A *Young subgroup* of  $\mathfrak{S}_n$  is a subgroup of the form

$$Y(P) = \{\sigma \in \mathfrak{S}_n \mid \sigma P_i = P_i \forall i\}$$

where  $P = (P_1, \dots, P_k)$  is any partition of  $[n]$ .

**Lemma:** A subset  $\mathcal{D} \subseteq \mathfrak{S}_n$  is a  $\lambda$ -transitive set of permutations if and only if  $|\mathcal{D} \cap \tau Y(P)|$  is constant for all cosets  $\tau Y(P)$  of all Young subgroups of shape  $\lambda$ .

# Incidence Matrix of Cosets of Young Subgroups

For  $\lambda \vdash n$ , the incidence matrix  $W_\lambda$  has rows indexed by  $\mathfrak{S}_n$  and columns indexed by all cosets of all Young subgroups of shape  $\lambda$  with entries

$$(W_\lambda)_{\tau, C} = \begin{cases} 1 & \tau \in C; \\ 0 & \text{otherwise.} \end{cases}$$

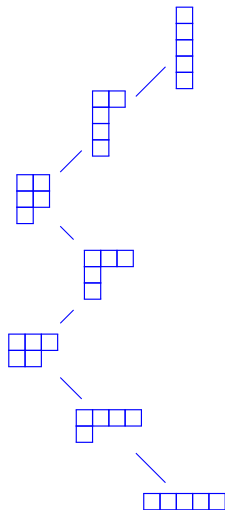
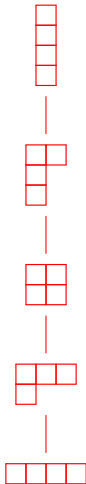
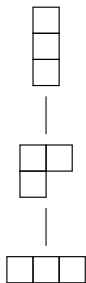
## The Eigenspaces of $\mathfrak{S}_n$ (as an association scheme)

Like all (commutative) Bose-Mesner algebras, the Bose-Mesner of the symmetric group is diagonalizable. There is one maximal common eigenspace  $V_\beta$  of the  $A_\alpha$  for each partition  $\beta \vdash n$ ; its dimension is  $f_\beta^2$  where  $f_\beta$  is the number of standard Young tableaux of shape  $\beta$  and can be computed, e.g., using the hook length formula.

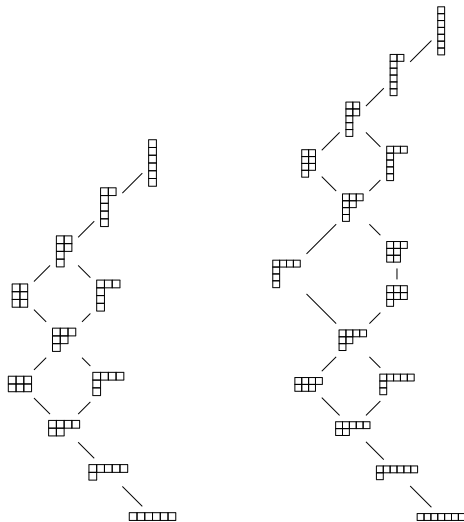
## Dominance Order

Now we use *dominance order*: for partitions  $\lambda, \mu$  of  $n$ , write  $\lambda \trianglelefteq \mu$  if, for all  $j$   $\lambda_1 + \cdots + \lambda_j \leq \mu_1 + \cdots + \mu_j$ . (Set  $\mu_j = 0$  for larger  $j$ .)

# Dominance Order, $n = 3, 4, 5$



## Dominance Order, $n = 6, 7$



## Telescoping Sums of Eigenspaces

We know that

$$V_\mu \subseteq \text{colsp } W_\mu \subseteq \bigoplus_{\lambda \trianglelefteq \mu} V_\lambda$$

This gives us a third basis for the Bose-Mesner algebra of  $\mathfrak{S}_n$ : for  $\mu \vdash n$ , define  $C_\mu = W_\mu W_\mu^\top$ . Then

$$C_\mu = \sum_{\lambda} \varrho_{\mu,\lambda} E_\lambda$$

with  $\varrho_{\mu,\lambda} = 0$  unless  $\lambda \trianglelefteq \mu$ .

It follows that  $\mathcal{D} \subseteq \mathfrak{S}_n$  with characteristic vector  $x$  of length  $n!$  is  $\lambda$ -transitive set of permutations if and only if

$$x^\top E_\mu = 0$$

for all  $1^n \neq \mu \trianglelefteq \lambda$ .

# Mapping Cosets of Young Subgroups to Their Shapes

So we have an order-preserving map

$$\text{sh} : \mathcal{P} \rightarrow \mathcal{E}$$

which captures the “lower triangular” nature of the change-of-basis matrix.

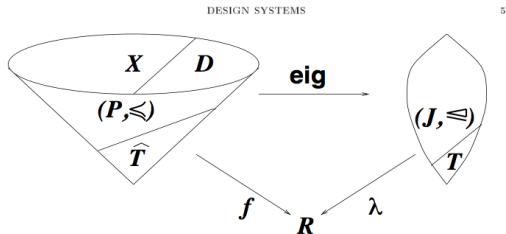


FIGURE 1. Subset  $D$  is a poset  $\mathcal{T}$ -design if and only if  $f|_{\mathcal{T}} = \lambda \circ \text{eig}$  for some function  $\lambda$ .



## $\lambda$ -Homogeneous Groups

In a recent paper (J. Algebra 2016), André, Araújo and Cameron generalized this idea a bit more. They studied  $\lambda$ -homogeneous groups, allowing the  $g \in G$  to permute the various  $P_i$ :

Let  $\lambda = (\lambda_1, \dots, \lambda_k)$  be a partition of  $n$ . A group  $G \leq \mathfrak{S}_n$  is  $\lambda$ -homogeneous if for every two unordered set partitions

$$P = (P_1, \dots, P_k), \quad Q = (Q_1, \dots, Q_k)$$

of shape  $\lambda$ , there is a  $g \in G$  such that

$$(gP_1, \dots, gP_k) = Q.$$

## $\lambda$ -Homogeneous Groups

André et al. classify those permutation groups which are  $\lambda$ -homogeneous but not  $\lambda$ -transitive.

Setting aside symmetric and alternating groups, and those classified by Kantor, the shapes that arise are

$$(3, 3), (5, 5), (3, 2, 1, \dots, 1), (2, 2, 1, \dots, 1)$$

with  $n \in \{9, 11, 12, 23, 24\}$ .

# Transformation Semigroups

Denote by  $\mathcal{T}_n$  the *full transformation semigroup* consisting of all functions from  $[n]$  to itself.

For a function  $a : [n] \rightarrow [n]$  denote by  $\ker(a)$  the partition of  $[n]$  into preimages of the elements of the range of  $a$ .

**Theorem** (*André et al.*): For  $a \in \mathcal{T}_n \setminus \mathfrak{S}_n$ ,

$$\langle a, \mathfrak{S}_n \rangle = \{b \in \mathcal{T}_n \mid (\exists \tau \in \mathfrak{S}_n)(\tau \ker(a) \subseteq \ker(b))\}.$$

## A Group Can Synchronize a Function

We say  $G \leq \mathfrak{S}_n$  synchronizes  $a \in \mathcal{T}_n \setminus \mathfrak{S}_n$  if  $\langle a, G \rangle$  contains a constant function. (This happens iff  $S = \langle a, G \rangle \setminus G$  is generated by its idempotents. Many equivalent statements.)

**Theorem** (*André et al.*): Let  $a \in \mathcal{T}_n \setminus \mathfrak{S}_n$  and  $G \leq \mathfrak{S}_n$ ,

$$\langle a, G \rangle \setminus G = \langle a, \mathfrak{S}_n \rangle \setminus \mathfrak{S}_n$$

iff

- ▶  $G$  is  $k$ -homogeneous where  $a$  has image of size  $k$ , and
- ▶  $G$  is  $\lambda$ -homogeneous where  $\ker(a)$  has shape  $\lambda$ .

## Synchronizing Automata

Using these tools, André et al. gave the following characterization of pairs  $(a, G)$  for which

$$\langle a, G \rangle \setminus G = \langle a, \mathfrak{S}_n \rangle \setminus \mathfrak{S}_n .$$

Let  $r$  be the rank (image size) of  $a$ .

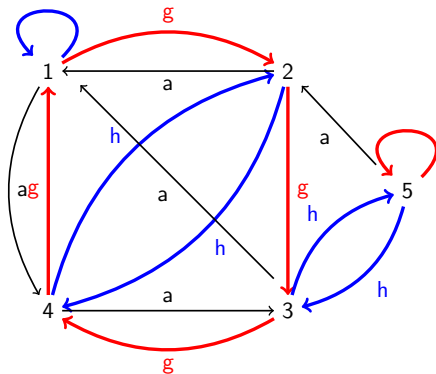
Except for  $G = \mathcal{S}_n, \mathcal{A}_n$  and  $n \in \{5, 6, 9\}$ , we have

- ▶  $r = 1$  and  $G$  is transitive
- ▶  $r > n/2$ ,  $G$  is  $(n - r)$ -homogeneous and  $\lambda = (n - r + 1, 1, \dots, 1)$
- ▶  $r = n - 2$ ,  $G$  is 4-transitive and  $\lambda = (2, 2, 1, \dots, 1)$
- ▶  $r = n - 3$ ,  $G$  is 5-transitive and  $\lambda = (3, 2, 1, \dots, 1)$
- ▶  $\lambda = (n - t, \lambda_2, \dots, \lambda_r)$ ,  $G$  is  $t$ -homogeneous ( $t < n/2$ ) and some extra conditions.

# Černý Conjecture

**Conjecture** (J. Černý, 1964): If a constant function exists, then it is a word of length at most  $(n - 1)^2$  in the generators of the semigroup.

## The Solution to the Puzzle



Shortest synchronizing word:  $a a h g a g a$

# The End

Thank you.

