Designs, permutations, and transitive groups

Patrick Solé
joint work with Minjia Shi and XiaoXiao Li

CNRS/I2M, Marseilles France

Rijeka, Croatia

The symmetric group as a metric space

Consider the *symmetric group* on n letters S_n with metric

$$d_S(\sigma, \theta) = n - F(\sigma\theta^{-1}),$$

where $F(\nu)$ denotes the number of fixed points of ν.
It is clear that d_S is not a shortest path distance since $d_S(\sigma, \theta) = 1$ is impossible.
Codes in (S_n, d_S) were studied by Tarnanen in 1999 by using the conjugacy association scheme of the group S_n.

Distance Degree Regular (DDR) spaces

A finite metric space (X, d) is *distance degree regular* (DDR) if its distance degree sequence is the same for every point.
Assume (X, d) to be of *diameter* n.
In that case (X, d) is DDR iff for each $0 \leq i \leq n$ the graph $\Gamma_i = (X, E_i)$ which connects vertices at distance i in (X, d) is regular of *degree* v_i.
Thus $E_0 = \{(x, x) \mid x \in X\}$ is the diagonal of X^2.
Note that the E_i's form a partition of X^2.

Examples:

- Distance regular graphs, Hamming graph, Johnson graph,...
- Distance degree regular graphs, Cayley graphs, vertex-transitive graphs

The symmetric group as a DDR space

Let w_k denote the numbers of permutations on n letters with k fixed points.
A generating function for these numbers (sometimes called rencontres numbers) is

$$\sum_{k=0}^{n} w_k u^k = n! \sum_{j=0}^{n} \frac{(u-1)^j}{j!}.$$

Thus, we have $v_i = n - w_i$.
(S_n, d_S) is a DDR space that does not come from a distance regular graph, not even from a DDR graph, because d_S is not a shortest path distance.

Frequencies in DDR spaces

If D is any non void subset of X we define its *frequencies* as

$$\forall i \in [0..n],\ f_i = \frac{|D^2 \cap E_i|}{|D|^2}.$$

Thus $f_0 = \frac{1}{|D|}$, and $\sum_{i=0}^{n} f_i = 1$.

Note also that if $D = X$, then $f_i = \frac{v_i}{|X|}$.

Example: If $X = H(n, q)$ and D is a linear code then $f_i = \frac{A_i}{|D|}$ is proportional to the weight distribution.

Designs in DDR spaces

The set $D \subseteq X$ is a *t-design* for some integer t if

$$\sum_{j=0}^{n} f_j j^i = \sum_{j=0}^{n} \frac{v_j}{v} j^i.$$

for $i = 1, \ldots, t$.

Examples:

- If $X = H(n, q)$ then D is an Orthogonal Array of strength t
- If $X = J(v, k)$ then D is a $t - (v, k, *)$ design

Designs in the symmetric group

Godsil  proved in 1988:

If $D \subseteq S_n$ is a t-transitive permutation group then it is a t-design in (S_n, d_S).

Partial converse in Conder-Godsil (1993):

If $D \subseteq S_n$ is a t-design that is a subgroup of S_n, then it is a t-transitive permutation group.

Examples of t-designs that are not subgroups in 3 slides.

Orthogonal polynomials

We define a scalar product on $\mathbb{R}[x]$ attached to D by the relation

$$\langle f, g \rangle_D = \sum_{i=0}^{n} f_i f(i) g(i).$$

Thus, in the special case of $D = X$ we have

$$\langle f, g \rangle_X = \frac{1}{|X|} \sum_{i=0}^{n} v_i f(i) g(i).$$

We shall say that a sequence $\Phi_i(x)$ of polynomials of degree i is *orthonormal of size $N+1$* if it satisfies

$$\forall i, j \in [0..N], \ \langle \Phi_i, \Phi_j \rangle_X = \delta_{ij},$$

where $N \leq n$.

Charlier polynomials and permutations

Let

$$C_k(x) = (-1)^k + \sum_{i=1}^{k} (-1)^{k-i} \binom{k}{i} x(x-1)\cdots(x-i+1).$$

Thus, for concreteness,
$C_0(x) = 1,\ C_1(x) = x - 1,\ C_2(x) = x^2 - 3x + 1.$
The scalar product attached to the DDR space (S_n, d_S) is then

$$\langle f, g \rangle_n = \frac{1}{n!} \sum_{k=0}^{n} w_{n-k} f(k) g(k).$$

Building on Tarnanen (1999) we can prove that
the reversed Charlier polynomials $\widehat{C_k(x)} = C_k(n-x)$ satisfy the orthogonality relation

$$\langle \widehat{C_r}, \widehat{C_s} \rangle_n = r!\delta_{rs},$$

for $r, s \leq n/2$.

Spectral characterization of designs

For a given $D \subseteq X$ the *dual frequencies* are defined for $i = 0, 1, \ldots, N(X)$ as

$$\widehat{f_i} = \sum_{k=0}^{n} \Phi_i(k) f_k.$$

We recall the characterization of t-designs in terms of dual frequencies obtained in reference below.
Let t be an integer $\in [1..N(X)]$.
The set $D \subseteq X$ is a t-design iff $\widehat{f_i} = 0$ for $i = 1, \ldots, t$.

M. Shi, O. Rioul, P. Solé,
Designs in finite metric spaces: a probabilistic approach, Graphs and Combinatorics, special issue Bannai-Enomoto 75 (2021).

Spectral characterization of designs: $t = 1$

A subset $D \subseteq S_n$ is a 1-design in (S_n, d_S) iff $\sum_{j=0}^{n} j f_j = n - 1$.

In particular, this condition is satisfied if we have n permutations at pairwise distance n when $f_1 = f_2 = \cdots = f_{n-1} = 0$, and $f_n = \frac{n-1}{n}$.

The existence of n permutations of S_n at pairwise Hamming distance n is trivially equivalent to the existence of a **Latin square** of order n.

This is the case when Y is the group generated by a cycle of length n. The Latin square is then the addition table of $(\mathbb{Z}_n, +)$.

A non-group example of a 1-design

Here is a non-group example when $n = 5$, obtained from the smallest Latin Square that is not the multiplication table of a group.

$$Y = \{12345, 24153, 35421, 41532, 53214\},$$

when $24153 \circ 35421 = 13542 \notin Y$.

Spectral characterization of designs: $t = 2$

A subset $D \subseteq S_n$ is a 2-design in (S_n, d_S) iff

$$\sum_{j=0}^{n} j f_j = n - 1, \& \sum_{j=0}^{n} j^2 f_j = 1 + (n-1)^2.$$

In particular, this condition is satisfied if we have $n(n-1)$ permutations with frequencies $f_1 = f_2 = \cdots = f_{n-2} = 0$, and $f_{n-1} = \frac{n-2}{(n-1)}$, $f_n = \frac{1}{n}$.

A non-group example of a 2-design

A nongroup example of 2-design can be obtained by considering

$$\{x \mapsto ax^3 + b \mid a, b \in \mathbb{F}_9,\ a \neq 0\}.$$

The conditions of the criterion can be checked in Magma.

Main result

If D is a t-design in (S_n, d_S), then

$$|D| \geq n(n-1)\dots(n-t+1).$$

In case of equality $f_i = 0$ for $i \in [1..n-t]$.
In particular met for sharply transitive group of permutations, eg for $t = 2$ projective planes .

Main open problem: Improve this lower bound when there is no sharply t-transitive subgroup of S_n.
$\Rightarrow$ Can we prove that $PG(2,10)$ does not exist by linear programming bounds?

Excerpt from Peter Cameron's  blog

Lower bounds are more problematic. There is a machine invented by Philippe Delsarte for finding lower bounds of sets in association schemes satisfying certain t-design-like conditions. These could in principle by applied to the conjugacy class association scheme of the symmetric group. I don't know whether anyone has done this, and I rather doubt that it will do better than the trivial lower bound of $n!/(n-t)!$ corresponding to sharply transitive sets. The reason for my belief is that, if there were a possibility of getting a better bound this way, someone would no doubt have used it to prove the non-existence of a sharply 2-transitive set of permutations on $\{1, \ldots, 10\}$ (and hence of a projective plane of order 10), for example.