Groups acting on combinatorial designs and related codes

Dean Crnković

Department of Mathematics
University of Rijeka
Croatia

Symmetries and Covers of Discrete Objects
Queenstown, New Zealand, February 2016

This work has been fully supported by Croatian Science Foundation under the project 1637.

A $t-(v,k,\lambda)$ **design** is a finite incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$ satisfying the following requirements:

1. $|\mathcal{P}|=v$,
2. every element of $\mathcal{B}$ is incident with exactly k elements of $\mathcal{P}$,
3. every t elements of $\mathcal{P}$ are incident with exactly λ elements of $\mathcal{B}$.

Every element of $\mathcal{P}$ is incident with exactly $r=\frac{\lambda(v-1)}{k-1}$ elements of $\mathcal{B}$. The number of blocks is denoted by b. If $b=v$ (or equivalently $k=r$) then the design is called **symmetric**.

If $\mathcal{D}$ is a t-design, then it is also a s-design, for $1\leq s\leq t-1$.

Theorem 1 [J. D. Key, J. Moori]

Let G be a **finite primitive permutation group** acting on the set Ω of size n. Further, let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. If

$$\mathcal{B} = \{\Delta g : g \in G\}$$

and, given $\delta \in \Delta$,

$$\mathcal{E} = \{\{\alpha, \delta\}g : g \in G\},$$

then $\mathcal{D} = (\Omega, \mathcal{B})$ is a **symmetric** $1-(n, |\Delta|, |\Delta|)$ **design**. Further, if Δ is a **self-paired orbit** of G_α then $\Gamma(\Omega, \mathcal{E})$ is a **regular connected graph** of valency $|\Delta|$, $\mathcal{D}$ is **self-dual**, and G acts as an **automorphism group** on each of these structures, **primitive** on vertices of the graph, and on points and blocks of the design.

Instead of taking a single G_α-orbit, we can take Δ to be any **union of G_α-orbits**. We will still get a symmetric 1-design with the group G acting as an automorphism group, primitively on points and blocks of the design.

Theorem 2 [DC, V. Mikulić]

Let G be a finite permutation group **acting primitively on the sets Ω_1 and Ω_2 of size m and n, respectively**. Let $\alpha \in \Omega_1$, $\delta \in \Omega_2$, and let $\Delta_2 = \delta G_\alpha$ be the G_α-orbit of $\delta \in \Omega_2$ and $\Delta_1 = \alpha G_\delta$ be the G_δ-orbit of $\alpha \in \Omega_1$.
If $\Delta_2 \neq \Omega_2$ and

$$\mathcal{B} = \{\Delta_2 g : g \in G\},$$

then $\mathcal{D}(G, \alpha, \delta) = (\Omega_2, \mathcal{B})$ is a $1-(n, |\Delta_2|, |\Delta_1|)$ **design** with m blocks, and G acts as an **automorphism group, primitive on points and blocks** of the design.

In the construction of the design described in Theorem 2, instead of taking a single G_α-orbit, we can take Δ_2 to be any **union of G_α-orbits**.

Corollary 1

Let G be a finite permutation group acting primitively on the sets Ω_1 and Ω_2 of size m and n, respectively. Let $\alpha \in \Omega_1$ and $\Delta_2 = \bigcup_{i=1}^{s} \delta_i G_\alpha$, where $\delta_1, ..., \delta_s \in \Omega_2$ are representatives of distinct G_α-orbits. If $\Delta_2 \neq \Omega_2$ and

$$\mathcal{B} = \{\Delta_2 g : g \in G\},$$

then $\mathcal{D}(G, \alpha, \delta_1, ..., \delta_s) = (\Omega_2, \mathcal{B})$ is a 1-design $1 - (n, |\Delta_2|, \sum_{i=1}^{s} |\alpha G_{\delta_i}|)$ with m blocks, and G acts as an automorphism group, primitive on points and blocks of the design.

In fact, this construction gives us **all 1-designs on which the group G acts primitively on points and blocks**.

Corollary 2

If a group G acts primitively on the points and the blocks of a 1-design $\mathcal{D}$, then $\mathcal{D}$ can be obtained as described in Corollary 1, *i.e.*, such that Δ_2 is a union of G_α-orbits.

We can interpret the design $(\Omega_2, \mathcal{B})$ from Corollary 1 in the following way:

- the point set is Ω_2,
- the block set is $\Omega_1 = \alpha G$,
- the block $\alpha g'$ is incident with the set of points $\{\delta_i g : g \in G_\alpha g',\ i = 1, \ldots s\}$.

Let G be a **simple group** and let H_1 and H_2 be **maximal subgroups** of G. G **acts primitively** on $ccl_G(H_1)$ and $ccl_G(H_2)$ by conjugation. We can construct a **primitive** $1-$**design** such that:

- the point set of the design is $ccl_G(H_2)$,
- the block set is $ccl_G(H_1)$,
- the block $H_1^{g_i}$ is incident with the point $H_2^{h_j}$ if and only if $H_2^{h_j} \cap H_1^{g_i} \cong G_i$, $i = 1, \ldots, k$, where $\{G_1, ..., G_k\} \subset \{H_2^x \cap H_1^y \mid x, y \in G\}$.

We denote a $1-$design constructed in this way by $\mathcal{D}(G, H_2, H_1; G_1, ..., G_k)$.

From the conjugacy class of a **maximal subgroup** H of a simple group G one can construct a **regular graph**, denoted by $\mathcal{G}(G, H; G_1, ..., G_k)$, in the following way:

- the vertex set of the graph is $ccl_G(H)$,
- the vertex H^{g_i} is adjacent to the vertex H^{g_j} if and only if $H^{g_i} \cap H^{g_j} \cong G_i$, $i = 1, \ldots, k$, where $\{G_1, ..., G_k\} \subset \{H^x \cap H^y \mid x, y \in G\}$.

G **acts primitively** on the set of vertices of $\mathcal{G}(G, H; G_1, ..., G_k)$.

Theorem 3 [DC, V. Mikulić, A. Švob]

Let G be a finite permutation group **acting transitively** on the sets Ω_1 and Ω_2 of size m and n, respectively. Let $\alpha \in \Omega_1$ and $\Delta_2 = \bigcup_{i=1}^{s} \delta_i G_\alpha$, where $\delta_1, ..., \delta_s \in \Omega_2$ are representatives of distinct G_α-orbits. If $\Delta_2 \neq \Omega_2$ and

$$\mathcal{B} = \{\Delta_2 g : g \in G\},$$

then the incidence structure $\mathcal{D}(G, \alpha, \delta_1, ..., \delta_s) = (\Omega_2, \mathcal{B})$ is a $1 - (n, |\Delta_2|, \frac{|G_\alpha|}{|G_{\Delta_2}|} \sum_{i=1}^{s} |\alpha G_{\delta_i}|)$ design with $\frac{m \cdot |G_\alpha|}{|G_{\Delta_2}|}$ blocks. Then the group $H \cong G / \bigcap_{x \in \Omega_2} G_x$ acts as an automorphism group on $(\Omega_2, \mathcal{B})$, **transitive on points and blocks** of the design.

Corollary 3

If a group G acts transitively on the points and the blocks of a 1-design $\mathcal{D}$, then $\mathcal{D}$ can be obtained as described in Theorem 3.

Let M be a **finite group** and $H_1, H_2, G \leq M$. G **acts transitively** on the conjugacy classes $ccl_G(H_i)$, $i = 1, 2$, by conjugation. We can construct a $1-$design such that:

- the point set of the design is $ccl_G(H_2)$,
- the block set is $ccl_G(H_1)$,
- the block $H_1^{g_i}$ is incident with the point $H_2^{h_j}$ if and only if $H_2^{h_j} \cap H_1^{g_i} \cong G_i$, $i = 1, \ldots, k$, where $\{G_1, ..., G_k\} \subset \{H_2^x \cap H_1^y \mid x, y \in G\}$.

The group $G / \bigcap_{K \in ccl_G(H_2) \bigcup ccl_G(H_1)} N_G(K)$ acts as an automorphism group of the constructed design, **transitive on points and blocks**.

Using the described approach we have constructed a number of 2-designs and strongly regular graphs from the groups $U(3,3)$, $U(3,4)$, U(3,5), $U(3,7)$, $U(4,2)$, $U(4,3)$, $U(5,2)$, $L(2,32)$, $L(2,49)$, $L(3,5)$, $L(4,3)$ and $S(6,2)$.

Let $\mathbf{F}_q$ be the finite field of order q. A **linear code** of **length** n is a subspace of the vector space $\mathbf{F}_q^n$. A k-dimensional subspace of $\mathbf{F}_q^n$ is called a linear $[n, k]$ code over $\mathbf{F}_q$.
For $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbf{F}_q^n$ the number $d(x, y) = |\{i \,|1 \leq i \leq n, \, x_i \neq y_i\}|$ is called a Hamming distance.
The **minimum distance** of a code C is
$d = min\{d(x, y) \,| x, y \in C, x \neq y\}$.
A linear $[n, k, d]$ code is a linear $[n, k]$ code with the minimum distance d.
An $[n, k, d]$ linear code can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.
The **dual** code $C^\perp$ is the orthogonal complement under the standard inner product $(,)$. A code C is **self-orthogonal** if $C \subseteq C^\perp$ and **self-dual** if $C = C^\perp$.

Codes constructed from block designs have been extensively studied.

- E. F. Assmus Jnr, J. D. Key, Designs and their codes, Cambridge University Press, Cambridge, 1992.
- A. Baartmans, I. Landjev, V. D. Tonchev, On the binary codes of Steiner triple systems, Des. Codes Cryptogr. 8 (1996), 29–43.
- V. D. Tonchev, Quantum Codes from Finite Geometry and Combinatorial Designs, Finite Groups, Vertex Operator Algebras, and Combinatorics, Research Institute for Mathematical Sciences 1656, (2009) 44-54.

An automorphism of a code is any permutation of the coordinate positions that maps codewords to codewords.

The **code** $C_F(\mathcal{D})$ **of the design** $\mathcal{D}$ over the finite field $\mathbf{F}$ is the vector space spanned by the incidence vectors of the blocks over $\mathbf{F}$. It is known that $Aut(\mathcal{D}) \leq Aut(C_F(\mathcal{D}))$.

Any linear code is isomorphic to a code with generator matrix in so-called **standard form**, *i.e.* the form $[I_k|A]$; a check matrix then is given by $[-A^T|I_{n-k}]$. The first k coordinates are the **information symbols** and the last $n-k$ coordinates are the **check symbols**.

Permutation decoding was first developed by MacWilliams in 1964, and involves finding a set of automorphisms of a code called a **PD-set**.

Definition 1

If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a **PD-set** for C is a set S of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of S into the check positions $\mathcal{C}$.

The property of having a PD-set will not, in general, be invariant under isomorphism of codes, *i.e.* it depends on the choice of information set.

If S is a PD-set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n - k$, then

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \dots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \dots \right\rceil \right\rceil \right\rceil.$$

Good candidates for permutation decoding are linear codes with a large automorphism group and the large size of the check set (small dimension).

By the construction described in Teorem 3 we can construct designs admitting a large transitive automorphism group. Codes of these designs are good candidates for permutation decoding.

Let $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$ be a $2-(v,k,\lambda)$ design and $G \leq Aut(\mathcal{D})$. We denote the $G-$orbits of points by $\mathcal{P}_1,\ldots,\mathcal{P}_n$, $G-$orbits of blocks by $\mathcal{B}_1,\ldots,\mathcal{B}_m$, and put $|\mathcal{P}_r|=\omega_r$, $|\mathcal{B}_i|=\Omega_i$, $1 \leq r \leq n$, $1 \leq i \leq m$.
Denote by γ_{ij} the number of points of $\mathcal{P}_j$ incident with a representative of the block orbit $\mathcal{B}_i$. For these numbers the following equalities hold:

$$\sum_{j=1}^{n} \gamma_{ij} = k\,, \qquad (1)$$

$$\sum_{i=1}^{m} \frac{\Omega_i}{\omega_j}\gamma_{ij}\gamma_{is} = \lambda\omega_s + \delta_{js}\cdot(r-\lambda)\,. \qquad (2)$$

Definition 2

A $(m \times n)$-matrix $M = (\gamma_{ij})$ with entries satisfying conditions (1) and (2) is called an **orbit matrix** for the parameters $2-(v,k,\lambda)$ and orbit lengths distributions $(\omega_1,\dots,\omega_n)$, $(\Omega_1,\dots,\Omega_m)$.

Orbit matrices are often used in construction of designs with a presumed automorphism group.

The intersection of rows and columns of an orbit matrix M that correspond to non-fixed points and non-fixed blocks form a submatrix called the **non-fixed part of the orbit matrix** M.

Example

The incidence matrix of the symmetric (7,3,1) design

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

Corresponding orbit matrix for Z_3

	1	3	3
1	0	3	0
3	1	1	1
3	0	1	2

Theorem 4 [M. Harada, V. D. Tonchev]

Let $\mathcal{D}$ be a 2-(v, k, λ) design with a **fixed-point-free** and **fixed-block-free automorphism** ϕ of order q, where q is prime. Further, let M be the orbit matrix induced by the action of the group $G = \langle \phi \rangle$ on the design $\mathcal{D}$. If p is a prime dividing r and λ then the **orbit matrix** M generates a **self-orthogonal code** of length $b|q$ over $\mathbf{F}_p$.

Using Theorem 4 Harada and Tonchev constructed a ternary [63,20,21] code with a record breaking minimum weight from the symmetric 2-(189,48,12) design found by Janko.

Theorem 5 [V. D. Tonchev]

If G is a cyclic group of a prime order p that does not fix any point or block and $p|(r-\lambda)$, then the rows of the orbit matrix M generate a self-orthogonal code over $\mathbf{F}_p$.

Theorem 6 [DC, L. Simčić]

Let $\mathcal{D}$ be a 2-(v,k,λ) design with an automorphism group G which acts on $\mathcal{D}$ with f fixed points, h fixed blocks, $\frac{v-f}{w}$ point orbits of length w and $\frac{b-h}{w}$ block orbits of length w. If a prime p divides w and $r-\lambda$, then the **columns** of the non-fixed part of the orbit matrix M for the automorphism group G generate a self-orthogonal code of length $\frac{b-h}{p}$ over $\mathbf{F}_p$.

Theorem 7

Let Ω be a finite non-empty set, $G \leq S(\Omega)$ and H a normal subgroup of G. Further, let x and y be elements of the same G-orbit. Then $|xH| = |yH|$.

Theorem 8

Let Ω be a finite non-empty set, $H \lhd G \leq S(\Omega)$ and $xG = \bigsqcup_{i=1}^{h} x_i H$, for $x \in \Omega$. Then a group G/H acts transitively on the set $\{x_i H \mid i = 1, 2, \ldots, h\}$.

Let $\mathcal{D}$ be a 2-(v,k,λ) design with an automorphism group G, and $H \lhd G$. Further, let H acts on $\mathcal{D}$ with f fixed points, h fixed blocks, $\frac{v-f}{w}$ point orbits of length w and $\frac{b-h}{w}$ block orbits of length w. If a prime p divides w and $r-\lambda$, then the **columns** of the non-fixed part of the orbit matrix M for the automorphism group H generate a self-orthogonal code C of length $\frac{b-h}{p}$ over $\mathbf{F}_p$, and G/H acts as an automorphism group of C.

If G acts transitively on $\mathcal{D}$, then G/H acts transitively on C. Thus, we can construct codes admitting a large transitive automorphism group, which are good candidates for permutation decoding.