# Transitive designs constructed from groups

Dean Crnković
Vedrana Mikulić
and
Andrea Švob

Department of Mathematics
University of Rijeka
Omladinska 14, 51000 Rijeka, Croatia

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 $\lambda$ elements of $\mathcal{B}$.

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

If $|\mathcal{P}| = |\mathcal{B}|$ then the design is called **symmetric**.

**Theorem 1 (J. D. Key, J. Moori, 2002)** Let $G$ be a finite primitive permutation group acting on the set $\Omega$ of size $n$. Further, let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer $G_\alpha$ of $\alpha$. 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 $\Delta$ is a self-paired orbit of $G_\alpha$ 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 $G_\alpha$-orbit, we can take $\Delta$ to be any union of $G_\alpha$-orbits. We will still get a symmetric 1-design with the group $G$ acting as an automorphism group, primitive on points and blocks of the design.

Moreover, if the group $G$ acts primitively on the points and the blocks of a self-dual symmetric 1-design, $\mathcal{D}$, with duality respected by $G$, then $\mathcal{D}$ can be obtained by orbiting a union of orbits of a point-stabilizer, as described in Theorem 1.

**Theorem 2 (D. C., V. Mikulić)**
Let $G$ be a finite permutation group acting primitively on the sets $\Omega_1$ and $\Omega_2$ of size $m$ and $n$, respectively. Let $\alpha \in \Omega_1$, $\delta \in \Omega_2$, and let $\Delta_2 = \delta G_\alpha$ be the $G_\alpha$-orbit of $\delta \in \Omega_2$ and $\Delta_1 = \alpha G_\delta$ be the $G_\delta$-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 $G_\alpha$-orbit, we can take $\Delta_2$ to be any union of $G_\alpha$-orbits.

**Corollary 1**

Let $G$ be a finite permutation group acting primitively on the sets $\Omega_1$ and $\Omega_2$ 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 $G_\alpha$-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 $\Delta_2$ is a union of $G_\alpha$-orbits.

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

- the point set is $\Omega_2$,
- 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 $H_1$ 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 $H_2^{h_j} \cap H_1^{g_i} \cong G_i,\ i = 1, \dots, k$, where $\{G_1, ..., G_k\} \subset \{H_2^x \cap H_1^y \mid x, y \in G\}$.

Let us 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 $\mathcal{G}(G, H; G_1, ..., G_k)$.

Combinatorial structures constructed from $U(3,4)$

| Combinatorial structure | Structure of the full automorphism group |
|---|---|
| 2-(65,5,1) design | $U(3,4):Z_4$ |
| 2-(65,15,21) design | $U(3,4):Z_4$ |
| 2-(65,26,250) design | $U(3,4):Z_4$ |
| $SRG(208,75,30,25)$ | $U(3,4):Z_4$ |
| $SRG(416,100,36,20)$ | $G(2,4):Z_2$ |

Structures constructed from $U(3,5)$

| Combinatorial structure | Structure of the full automorphism group |
|---|---|
| 2-(126,6,1) design | $U(3,5):S_3$ |
| 2-(50,14,13) design | $U(3,5):Z_2$ |
| 2-(126,36,14)design | $U(3,5):Z_2$ |
| $SRG(525,144,48,36)$ | $U(3,5):S_3$ |
| $SRG(50,7,0,1)$ | $U(3,5):Z_2$ |
| $SRG(175,72,20,36)$ | $U(3,5):Z_2$ |

Block designs on 31 points constructed from $L(3,5)$

| Combinatorial structure | Structure of the full automorphism group |
|---|---|
| 2-(31,6,1) design | $L(3,5)$ |
| 2-(31,6,100) design | $L(3,5)$ |
| 2-(31,10,300) design | $L(3,5)$ |
| 2-(31,15,700) design | $L(3,5)$ |
| 2-(31,3,25) design | $L(3,5)$ |
| 2-(31,12,550) design | $L(3,5)$ |
| 2-(31,15,875) design | $L(3,5)$ |

Strongly regular graphs constructed from $U(5,2)$

| Combinatorial structure | Structure of the full automorphism group |
|---|---|
| SRG(165,36,3,9) | $U(5,2):Z_2$ |
| SRG(176,40,12,8) | $U(5,2):Z_2$ |
| SRG(297,40,7,5) | $U(5,2):Z_2$ |
| SRG(1408,567,246,216) | $U(6,2):Z_2$ |

Block designs constructed from $U(4,2)$, $U(3,3)$, $L(2,32)$ and $L(2,49)$

| Combinatorial structure | Structure of the full automorphism group |
| --- | --- |
| 2-(36,15,6) design | $U(4,2):Z_2$ |
| 2-(36,15,6) design | $U(3,3):Z_2$ |
| 2-(40,13,4) design | $PGL(4,3)$ |
| 2-(40,13,4) design | $U(4,2):Z_2$ |
| 2-(45,12,3) design | $U(4,2):Z_2$ |
| 2-(63,31,15) design | $U(3,3):Z_2$ |
| 2-(63,31,15) design | $PGL(6,2)$ |
| 2-(28,4,1) design | $U(3,3):Z_2$ |
| 2-(28,12,11) design | $PSp(6,2)$ |
| 2-(36,16,12) design | $PSp(6,2)$ |
| 2-(50,8,4) design | $L(2,49):Z_2$ |
| 2-(50,20,152) design | $L(2,49):Z_2$ |

SRG-s constructed from $U(4,2)$, $U(3,3)$, $L(2,32)$ and $L(2,49)$

| Combinatorial structure | Structure of the full automorphism group |
|---|---|
| $SRG(27,10,1,5)$ | $U(4,2):Z_2$ |
| $SRG(36,14,4,6)$ | $U(3,3):Z_2$ |
| $SRG(36,15,6,6)$ | $U(4,2):Z_2$ |
| $SRG(40,12,2,4)$ | $U(4,2):Z_2$ |
| $SRG(40,12,2,4)$ | $U(4,2):Z_2$ |
| $SRG(45,12,3,3)$ | $U(4,2):Z_2$ |
| $SRG(63,30,13,15)$ | $U(3,3):Z_2$ |
| $SRG(63,30,13,15)$ | $PSp(6,2)$ |
| $SRG(63,32,16,16)$ | $PSp(6,2)$ |
| $SRG(63,32,16,16)$ | $U(3,3):Z_2$ |
| $SRG(528,62,31,4)$ | $S_{33}$ |
| $SRG(1225,96,48,4)$ | $S_{50}$ |

**Theorem 3 (D. C., V. Mikulić)**
Let $G$ be a finite permutation group acting transitively on the sets $\Omega_1$ and $\Omega_2$ 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 $G_\alpha$-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 $H_1$, $H_2$, and $G$ be **subgroups** of $M$. $G$ 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 $\{G_1, ..., G_k\} \subset \{H_2^x \cap H_1^y \mid x, y \in G\}$.

This design can have repeated blocks. 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**.

Block designs constructed from $S(6,2)$

| Combinatorial structure | Structure of the full automorphism group |
|---|---|
| 2-(28,12,11) design | $S(6,2)$ |
| 2-(28,4,5) design | $S(6,2)$ |
| 2-(28,10,40) design | $S(6,2)$ |
| 2-(36,16,12) design | $S(6,2)$ |
| 2-(36,8,6) design | $S(6,2)$ |
| 2-(36,12,33) design | $S(6,2)$ |
| 2-(36,6,8) design | $S(6,2)$ |
| 2-(63,31,15) design | $PGL(6,2)$ |
| 2-(28,7,16) design | $S(6,2)$ |
| 2-(28,10,45) design | $S(6,2)$ |
| 2-(28,12,66) design | $S(6,2)$ |
| 2-(36,16,72) design | $S(6,2)$ |
| 2-(63,31,90) design | $PGL(6,2)$ |

## POSSIBLE APPLICATION

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 $\mathcal{C}$.

An automorphism of a code is any permutation of the coordinate positions that maps codewords to codewords. For $s \leq t$ an $s$-**PD-set** is a set $S$ of automorphisms of $C$ which is such that every $s$-set of coordinate positions is moved by at least one member of $S$ into $\mathcal{C}$.

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

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

This result can be adapted to $s$-PD-sets for $s \leq t$ by replacing $t$ by $s$ in the formula.

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

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

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

## INFINITE DESIGNS

**Definition 2**
Let $t$ be a positive integer, $v$ an infinite cardinal, $k$ and $\overline{k}$ cardinals with $k+\overline{k}=v$, and $\Lambda$ a $(t+1)\times(t+1)$ matrix with rows and columns indexed by $\{0,\ldots,t\}$ with $(i,j)$ entry a cardinal number if $i+j\leq t$ and blank otherwise. Then a simple infinite $t-(v,(k,\overline{k}),\Lambda)$ design consists of a set $V$ of points and a set $\mathcal{B}$ of subsets of $V$, having the properties

- $|B|=k$ and $V\backslash B=\overline{k}$, for all $B\in\mathcal{B}$.

- For $0\leq i+j\leq t$, let $x_1,\ldots,x_i,y_1,\ldots,y_j$ be distinct points of $V$. Then the number of elements of $\mathcal{B}$ containing all of $x_1,\ldots,x_i$ and none of $y_1,\ldots,y_j$ is precisely $\Lambda_{i,j}$.

- No block contains another block.

In a nonsimple infinite designs repeated blocks are allowed and the last condition should be replaced by

- No block strictly contains another block.

$\Lambda_{0,0} = b$
$\Lambda_{1,0} = r$

Let $G$ be an infinite group acting transitively on the infinite sets $\Omega_1$ and $\Omega_2$. In a similar way as in Teorem 3 one constructs an infinite 1-design having an automorphism group isomorphic to $G/\bigcap_{x\in\Omega_2} G_x$ that acts transitively on points and blocks of the design.