Strongly regular graphs constructed from groups

Dean Crnković

Department of Mathematics
University of Rijeka
Croatia

Symmetry vs Regularity
Pilsen, Czech Republic, July 2018

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 a group G acts transitively on Ω, $\alpha \in \Omega$, and Δ is an orbit of G_α, then $\Delta' = \{\alpha g \mid g \in G,\ \alpha g^{-1} \in \Delta\}$ is also an orbit of G_α. Δ' is called the orbit of G_α paired with Δ. It is obvious that $\Delta'' = \Delta$ and $|\Delta'| = |\Delta|$. The orbits Δ and Δ' are called **mutually paired orbits**. If $\Delta' = \Delta$, then Δ is said to be **self-paired**.

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.

We can interpret the graph $\Gamma(\Omega, \mathcal{E})$ from Theorem 1 in the following way:

- the set of vertices is Ω,
- the vertex $\alpha g'$ is incident with the vertices from the set $\{\delta g : g \in G_\alpha g'\}$.

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 (or a regular graph) with the group G acting as an automorphism group, primitively on points and blocks of the design.

In fact, this construction gives us **all regular graphs on which the group G acts primitively on the set of vertices**.

Corollary 1

If a group G acts primitively on the set of vertices of a regular graph Γ, then Γ can be obtained as described in Theorem 1, *i.e.*, such that Δ is a union of G_α-orbits.

From the conjugacy class of a **maximal subgroup** H of a simple group G one can construct a **regular graph**, denoted by $\Gamma(G, H; G_1, ..., G_k)$, 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 $H^{g_i} \cap H^{g_j} \cong G_i$, $i = 1, \dots, k$, 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 $\Gamma(G, H; G_1, ..., G_k)$.

Theorem 2 [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 2

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 2.

Corollary 3

If $\Omega_1 = \Omega_2$ and Δ_2 is a union of self-paired and mutually paired orbits of G_α, then the design $\mathcal{D}(G, \alpha, \delta_1, ..., \delta_s)$ is a symmetric self-dual design and its incidence matrix is the adjacency matrix of a $|\Delta_2|-$regular graph.

Let M be a **finite group** and $H, G \leq M$. G **acts transitively** on the conjugacy class $ccl_G(H)$ by conjugation. One can construct a regular graph such that:

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

The group $G / \bigcap_{K \in ccl_G(H)} N_G(K)$ acts as an automorphism group of the constructed graph, **transitive on the set of vertices**.

Example - DRGs from $U(4,2)$ [DC, S. Rukavina, A. Švob]

Applying Corollary 3 we classify all DRGs with at most 600 vertices admitting a transitive action of $U(4,2) \cong S(4,3) \cong O^-(6,2)$.

Theorem 3 [DC, S. Rukavina, A. Švob]

Up to isomorphism there are exactly 12 strongly regular graphs with at most 600 vertices, admitting a transitive action of the group $U(4,2)$. These SRGs have parameters $(27,10,1,5)$, $(36,15,6,6)$, $(40,12,2,4)$, $(45,12,3,3)$, $(120,56,28,24)$, $(135,64,28,32)$, $(216,40,4,8)$, $(540,187,58,68)$ and $(540,224,88,96)$.

Parameters of Γ	$Aut(\Gamma)$
(27,10,1,5)	$U(4,2):Z_2$
(36,15,6,6)	$U(4,2):Z_2$
(40,12,2,4)	$U(4,2):Z_2$
(40,12,2,4)	$U(4,2):Z_2$
(45,12,3,3)	$U(4,2):Z_2$
(120,56,28,24)	$O^+(8,2):Z_2$
(135,64,28,32)	$O^+(8,2):Z_2$
(216,40,4,8)	$U(4,2):Z_2$
(540,187,58,68)	$Z_2\times(U(4,2):Z_2)$
(540,187,58,68)	$Z_2\times U(4,2)$
(540,224,88,96)	$Z_2\times U(4,2)$
(540,224,88,96)	$U(4,3):D_8$

Table: SRGs from the group $U(4,2)$, $v\leq 600$

The SRG(216,40,4,8) and two SRGs with parameters (540,187,58,68) are the first known examples of strongly regular graphs with these parameters. The SRG(216,40,4,8) is the first known strongly regular graph on 216 vertices.

The SRG(540,224,88,96) having the full automorphism group isomorphic to $Z_2 \times U(4,2)$ was previously unknown.

The SRGs with parameters (40,12,2,4) are point graphs of generalized quadrangles GQ$(3,3)$, one of them corresponds to the point-hyperplane design in the projective geometry PG$(3,3)$ (see PhD thesis of W. Haemers).

The SRG(45,12,3,3) is the only vertex-transitive strongly regular graph with these parameters.

The SRG(135,64,28,32) is the complementary graph of the polar graph $O^+(8,2)$.

The SRG(540,224,88,96) having $U(4,3):D_8$ as the full automorphism group is the polar graph $NU(4,3)$.

Theorem 4 [DC, S. Rukavina, A. Švob]

Up to isomorphism there are exactly 2 distance-regular graphs with diameter $d \geq 3$ having at most 600 vertices, admitting a transitive action of the group $U(4,2)$. These distance-regular graphs have 135 or 160 vertices.

# vertices	Intersection array	$Aut(\Gamma)$
135	$\{14, 12, 8; 1, 3, 7\}$	$S(6,2)$
160	$\{6, 3, 3, 3; 1, 1, 1, 2\}$	$U(4,2):Z_2$

Table: DRGs from the group $U(4,2)$, $d \geq 3$, $v \leq 600$

The graph on 135 vertices is a dual polar graph, a primitive DRG with diameter 3.

The graph on 160 vertices is the generalized octagon of order (3,1), a primitive DRG with diameter 4.

These two DRGs are unique distance-regular graphs with the given intersection arrays.

Example - Deza graph from $U(4,2)$ [DC, A. Švob]

Combining incidence matrices of transitive 1-designs one can construct an adjacency matrix of a non-transitive graph.

The Zara graph with parameters (126,45,12,18) is a $SRG(126, 45, 12, 18)$ with the full automorphism group $U(4, 3) \times Z_4$. The group $U(4, 2)$ acts on that Zara graph in three orbits of sizes 1, 45 or 80.

The same action of $U(4, 2)$ yields a strictly Deza graph (diameter 2, not a SRG) with parameters $(126, 45, 12, 18)$ and the full automorphism group $Z_2 \times (U(4, 2) : Z_2)$.

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.

Codes constructed from adjacency matrices of SRGs have been studied, for example, in:

- A. E. Brouwer, C. A. van Eijl, On the p-Rank of the Adjacency Matrices of Strongly Regular Graphs, J. Algebraic Combin. 1 (1992), 329-346.
- W. H. Haemers, C. Parker, V. Pless, V. D. Tonchev, A Design and a Code Invariant under the Simple Group Co_3, J. Combin Theory Ser A 62 (1993), 225-233.
- W. H. Haemers, R. Peeters, J. M. van Rijckevorsel, Binary codes of strongly regular graphs, Des. Codes Cryptogr., 17 (1999), 187–209.
- V. D. Tonchev, Binary codes derived from the Hoffman-Singleton and Higman-Sims graphs, IEEE Trans. Inform. Theory 43 (1997), 1021-1025.

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

Let Γ be a graph and C_F be the code spanned by the adjacency matrix of Γ over the field $\mathbf{F}$. Then $Aut(\Gamma) \leq Aut(C_F)$.

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 Corollary 3 we can construct regular graphs admitting a large transitive automorphism group. Codes of these graphs are good candidates for permutation decoding.