Transitive designs constructed from finite groups and related codes

Dean Crnković

Department of Mathematics
University of Rijeka
Croatia

Algebraic Representation Theory 2015
Cape Town, July 2015

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 $1\leq s\leq t-1$.

A graph is **regular** if all its vertices have the same degree; a regular graph is **strongly regular** of type (v, k, λ, μ) if it has v vertices of degree k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

An **incidence matrix** of a design $\mathcal{D}$ is a matrix $A = [a_{ij}]$ where $a_{ij} = 1$ if jth point is incident with the ith block and $a_{ij} = 0$ otherwise.

Let M be the incidence matrix of a symmetric design. If M is symmetric matrix with constant diagonal, then M is the adjacency matrix of a strongly regular graph.

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.

Theorem 4

Suppose that C is the code over $\mathbf{F}_p$ spanned by the incidence matrix of a symmetric (v, k, λ) design.

1. If $p \mid (k - \lambda)$, then $dim(C) \leq \frac{1}{2}(v + 1)$.
2. If $p \nmid (k - \lambda)$ and $p \mid k$, then $dim(C) = v - 1$.
3. If $p \nmid (k - \lambda)$ and $p \nmid k$, then $dim(C) = v$.

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

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

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

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 A be the incidence matrix of a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$. A **decomposition** of A is any partition $B_1, \ldots, B_s$ of the rows of A (blocks of $\mathcal{D}$) and a partition $P_1, \ldots, P_t$ of the columns of A (points of $\mathcal{D}$).

For $i \leq s$, $j \leq t$ define

$$\alpha_{ij} = |\{P \in P_j |\ P\mathcal{I}x\}|, \text{ for } x \in B_i \text{ arbitrarily chosen,}$$
$$\beta_{ij} = |\{x \in B_i |\ P\mathcal{I}x\}|, \text{ for } P \in P_j \text{ arbitrarily chosen.}$$

We say that a decomposition is **tactical** if the α_{ij} and β_{ij} are well defined (independent from the choice of $x \in B_i$ and $P \in P_j$, respectively).

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 $|\mathcal{P}_r| = \omega_r$, $|\mathcal{B}_i| = \Omega_i$, $1 \leq r \leq n$, $1 \leq i \leq m$.

The **group action** of G induces a **tactical decomposition of** $\mathcal{D}$. 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:

$$\sum_{j=1}^{n} \gamma_{ij} = k\,, \tag{1}$$

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

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 $(\omega_1, \ldots, \omega_n)$, $(\Omega_1, \ldots, \Omega_m)$.

Orbit matrices are often used in construction of designs with a presumed automorphism group. Construction of designs admitting an action of the presumed automorphism group consists of two steps:

1. Construction of orbit matrices for the given automorphism group,
2. Construction of block designs for the obtained orbit matrices.

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 5 [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 5 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.

DC with B. G. Rodrigues:

We studied some non-binary self-orthogonal codes obtained from the row span of orbit matrices of symmetric designs corresponding to Bush-type Hadamard matrices that admit a fixed-point-free (and fixed-block-free) automorphism of prime order.

Some codes of length 20 over $\mathbf{F}_5$ obtained from symmetric $(100, 45, 20)$ designs are optimal, some are near-optimal.

Theorem 6 [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 7

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

Theorem 8 [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 9

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 10

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.

In 2009 M. Behbahani and C. Lam introduced the notion of orbit matrices of strongly regular graphs. They have studied orbit matrices of strongly regular graphs that admit an automorphism group of prime order.

Definition 3

A $(t \times t)$-matrix $R = [r_{ij}]$ with entries satisfying conditions

$$\sum_{j=1}^{t} r_{ij} = \sum_{i=1}^{t} \frac{n_i}{n_j} r_{ij} = k \tag{3}$$

$$\sum_{s=1}^{t} \frac{n_s}{n_j} r_{si} r_{sj} = \delta_{ij}(k-\mu) + \mu n_i + (\lambda - \mu) r_{ji} \tag{4}$$

is called a **row orbit matrix** for a strongly regular graph with parameters (v, k, λ, μ) and orbit lengths distribution $(n_1, \ldots, n_t)$.

Definition 4

A $(t \times t)$-matrix $C = [c_{ij}]$ with entries satisfying conditions

$$\sum_{i=1}^{t} c_{ij} = \sum_{j=1}^{t} \frac{n_j}{n_i} c_{ij} = k \tag{5}$$

$$\sum_{s=1}^{t} \frac{n_s}{n_j} c_{is} c_{js} = \delta_{ij}(k - \mu) + \mu n_i + (\lambda - \mu) c_{ij} \tag{6}$$

is called a **column orbit matrix** for a strongly regular graph with parameters (v, k, λ, μ) and orbit lengths distribution $(n_1, \ldots, n_t)$.

Theorem 11

Let Γ be a srg(v, k, λ, μ) with an automorphism group G which acts on the set of vertices of Γ with $\frac{v}{w}$ orbits of length w. Let R be the row orbit matrix of the graph Γ with respect to G. If q is a prime dividing k, λ and μ, then the matrix R generates a self-orthogonal code of length $\frac{v}{w}$ over $\mathbf{F}_q$.

Remark In this case the row orbit matrix is equal to the column orbit matrix.

Let Γ be a srg(v, k, λ, μ) with an automorphism group G, and $H \lhd G$. Further, let H acts on the set of vertices of Γ with $\frac{v}{w}$ orbits of length w. Let R be the row orbit matrix of the graph Γ with respect to H. If q is a prime dividing k, λ and μ, then the matrix R generates a self-orthogonal code C of length $\frac{v}{w}$ over $\mathbf{F}_q$, and G/H acts as an automorphism group of C.

If G acts transitively on Γ, then G/H acts transitively on C. So, we can construct codes admitting a large transitive automorphism group, which are good candidates for permutation decoding.

In the rest of the talk we will study codes spanned by orbit matrices for a symmetric (v, k, λ) design and orbit lengths distribution $(\Omega, \ldots, \Omega)$, where $\Omega = \frac{v}{t}$. We follow the ideas presented in:

- E. Lander, Symmetric designs: an algebraic approach, Cambridge University Press, Cambridge (1983).
- R. M. Wilson, Codes and modules associated with designs and t-uniform hypergraphs, in: D. Crnković, V. Tonchev, (eds.) Information security, coding theory and related combinatorics, pp. 404–436. NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. 29 IOS, Amsterdam (2011).

(Lander and Wilson have considered codes from incidence matrices of symmetric designs.)

Theorem 12 [DC, S. Rukavina]

Let a group G acts on a symmetric (v, k, λ) design $\mathcal{D}$ with $t = \frac{v}{\Omega}$ orbits of length Ω, on the set of points and the set of blocks, and let M be an orbit matrix of $\mathcal{D}$ induced by the action of G. Suppose that C is the code over $\mathbf{F}_p$ spanned by the rows of M.

1. If $p \mid (k - \lambda)$, then $dim(C) \leq \frac{1}{2}(t + 1)$.
2. If $p \nmid (k - \lambda)$ and $p \mid k$, then $dim(C) = t - 1$.
3. If $p \nmid (k - \lambda)$ and $p \nmid k$, then $dim(C) = t$.

Let a group G acts on a symmetric (v, k, λ) design $\mathcal{D}$ with $t = \frac{v}{\Omega}$ orbits of length Ω, on the set of points and the set of blocks, and let M be the corresponding orbit matrix.

If a prime p divides k and λ, then the rows of M span a **self-orthogonal** code (Theorem 1, Harada and Tonchev).

If p divides $k - \lambda$, but does not divide k, we use a different code. Define the **extended orbit matrix**

$$M^{ext} = \left[\begin{array}{ccc|c} & & & 1 \\ & M & & \vdots \\ & & & 1 \\ \hline \lambda\Omega & \cdots & \lambda\Omega & k \end{array}\right],$$

and denote by C^{ext} the **extended code** spanned by M^{ext}.

Define the **symmetric bilinear** form ψ by

$$\psi(\bar{x}, \bar{y}) = x_1 y_1 + \ldots + x_t y_t - \lambda \Omega x_{t+1} y_{t+1},$$

for $\bar{x} = (x_1, \ldots, x_{t+1})$ and $\bar{y} = (y_1, \ldots, y_{t+1})$. Since $p \mid n$ and $p \nmid k$, it follows that $p \nmid \Omega$ and $p \nmid \lambda$. Hence ψ is a **nondegenerate** form on $\mathbf{F}_p$.

The extended code C^{ext} over $\mathbf{F}_p$ is **self-orthogonal** (or totally isotropic) **with respect to** ψ.

The matrix of the bilinear form ψ is the $(t+1) \times (t+1)$ matrix

$$\Psi = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & -\lambda\Omega \end{bmatrix}.$$

Theorem 13 [DC, S. Rukavina]

Let $\mathcal{D}$ be a symmetric (v, k, λ) design admitting an automorphism group G that acts on the set of points and the set of blocks with $t = \frac{v}{\Omega}$ orbits of length Ω. Further, let M be the orbit matrix induced by the action of the group G on the design $\mathcal{D}$, and let C^{ext} be the corresponding extended code over F_p. If a prime p divides $(k - \lambda)$, but $p^2 \nmid (k - \lambda)$ and $p \nmid k$, then C^{ext} is **self-dual** with respect to ψ.

This theorem is proved by using the Smith normal form of the matrix M^{ext}.

Theorem 14

If there exists a self-dual p-ary code of length n with respect to a nondegenerate scalar product ψ, where p is an odd prime, then $(-1)^{\frac{n}{2}} det(\psi)$ is a square in $\mathbf{F}_p$.

As a consequence of Theorems 13 and 14 we have

Theorem 15

Let $\mathcal{D}$ be a symmetric (v, k, λ) design admitting an automorphism group G that acts on the set of points and the set of blocks with $t = \frac{v}{\Omega}$ orbits of length Ω. If an odd prime p divides $(k - \lambda)$, but $p^2 \nmid (k - \lambda)$ and $p \nmid k$, then $-\lambda\Omega(-1)^{\frac{t+1}{2}}$ is a square in $\mathbf{F}_p$.

If $p^2 \mid (k - \lambda)$ we use a **chain of codes** to obtain a self-dual code from an orbit matrix.

Given an $m \times n$ integer matrix A, denote by $row_{\mathbf{F}}(A)$ the linear code over the field $\mathbf{F}$ spanned by the rows of A. By $row_p(A)$ we denote the p-ary linear code spanned by the rows of A.
For a given matrix A, we define, for any prime p and nonnegative integer i,

$$\mathcal{M}_i(A) = \{x \in \mathbb{Z}^n : p^i x \in row_{\mathbb{Z}}(A)\}.$$

We have $\mathcal{M}_0(A) = row_{\mathbb{Z}}(A)$ and

$$\mathcal{M}_0(A) \subseteq \mathcal{M}_1(A) \subseteq \mathcal{M}_2(A) \subseteq \ldots.$$

Let

$$C_i(A) = \pi_p(\mathcal{M}_i(A))$$

where π_p is the homomorphism (projection) from $\mathbb{Z}^n$ onto $\mathbf{F}_p^n$ given by reading all coordinates modulo p. Then each $C_i(A)$ is a p-ary linear code of length n, $C_0(A) = row_p(A)$, and

$$C_0(A) \subseteq C_1(A) \subseteq C_2(A) \subseteq \ldots.$$

Theorem 16

Suppose A is an $n \times n$ integer matrix such that $AUA^T = p^e V$ for some integer e, where U and V are square matrices with determinants relatively prime to p. Then $C_e(A) = \mathbf{F}_p^n$ and

$$C_j(A)^U = C_{e-j-1}(A), \quad \text{for} \quad j = 0, 1, \ldots, e-1.$$

In particular, if $e = 2f + 1$, then $C_f(A)$ is a **self-U-dual** p-ary code of length n.

In the next theorem the above result is used to associate a self-dual code to an orbit matrix of a symmetric design.

Theorem 17 [DC, S. Rukavina]

Let $\mathcal{D}$ be a symmetric (v, k, λ) design admitting an automorphism group G that acts on the set of points and the set of blocks with $t = \frac{v}{\Omega}$ orbits of length Ω. Suppose that $n = k - \lambda$ is exactly divisible by an odd power of a prime p and λ is exactly divisible by an even power of p, *e.g.* $n = p^e n_0$, $\lambda = p^{2a}\lambda_0$ where e is odd, $a \geq 0$, and $(n_0, p) = (\lambda_0, p) = 1$. If $p \nmid \Omega$, then there exists a **self-dual** p-ary code of length $t + 1$ with respect to the scalar product corresponding to $U = diag(1, \ldots, 1, -\lambda_0\Omega)$.

If λ is exactly divisible by an odd power of p, we apply the above case to the complement of the given symmetric design, which is a symmetric (v, k', λ') design, where $k' = v - k$ and $\lambda' = v - 2k + \lambda$.

Theorem 18 [DC, S. Rukavina]

Let $\mathcal{D}$ be a symmetric (v, k, λ) design admitting an automorphism group G that acts on the set of points and the set of blocks with $t = \frac{v}{\Omega}$ orbits of length Ω. Suppose that $n = k - \lambda$ is exactly divisible by an odd power of a prime p and λ is also exactly divisible by an odd power of p, *e.g.* $n = p^e n_0$, $\lambda = p^{2a+1}\lambda_0$ where e is odd, $a \geq 0$, and $(n_0, p) = (\lambda_0, p) = 1$. If $p \nmid \Omega$, then there exists a **self-dual** p-ary code of length $t + 1$ with respect to the scalar product corresponding to $U = diag(1, \ldots, 1, \lambda_0 n_0 \Omega)$.

As a consequence of Theorems 14, 17 and 18, we have

Theorem 19

Let $\mathcal{D}$ be a symmetric (v, k, λ) design admitting an automorphism group G that acts on the set of points and the set of blocks with $t = \frac{v}{\Omega}$ orbits of length Ω. Suppose that p is an odd prime such that $n = p^e n_0$ and $\lambda = p^b \lambda_0$, where $(n_0, p) = (\lambda_0, p) = 1$, and $p \nmid \Omega$. Then

- $-(-1)^{(t+1)/2}\lambda_0\Omega$ is a square $\pmod p$ if b is even,
- $(-1)^{(t+1)/2} n_0\lambda_0\Omega$ is a square $\pmod p$ if b is odd.