Self-orthogonal codes constructed from orbit matrices

Dean Crnković

Department of Mathematics
University of Rijeka
Croatia

BIRS, January 2015
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 $\mathcal{B}$.

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 $|\mathcal{P}| = |\mathcal{B}|$ (or equivalently $k = r$) then the design is called symmetric.

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

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

We say that a decomposition is **tactical** if the $\alpha_{ij}$ and $\beta_{ij}$ are well defined (independent from the choice of $x \in B_i$ and $P \in P_j$, respectively).
Let $D = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be a $2-(v, k, \lambda)$ design and $G \leq \text{Aut}(D)$. 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 $D$.

Denote by $\gamma_{ij}$ 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:

\[
\sum_{j=1}^{n} \gamma_{ij} = k, \quad (1)
\]

\[
\sum_{i=1}^{m} \frac{\Omega_i}{\omega_j} \gamma_{ij} \gamma_{is} = \lambda \omega_s + \delta_{js} \cdot (r - \lambda). \quad (2)
\]
Definition 1

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

\[
\begin{bmatrix}
0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 \\
\end{bmatrix}
\]

Corresponding orbit matrix for $\mathbb{Z}_3$

\[
\begin{array}{c|cc}
  & 1 & 3 & 3 \\
\hline
1 & 0 & 3 & 0 \\
3 & 1 & 1 & 1 \\
3 & 0 & 1 & 2 \\
\end{array}
\]
Codes

Let $\mathbb{F}_q$ be the finite field of order $q$. A linear code of length $n$ is a subspace of the vector space $\mathbb{F}_q^n$. A $k$-dimensional subspace of $\mathbb{F}_q^n$ is called a linear $[n, k]$ code over $\mathbb{F}_q$.

For $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ the number $d(x, y) = |\{i | 1 \leq i \leq n, x_i \neq y_i\}|$ is called a Hamming distance. A 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 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 $C = C^\perp$. 

D. Crnković: Self-orthogonal codes from orbit matrices
Codes constructed from block designs have been extensively studied.

Theorem 1 [M. Harada, V. D. Tonchev, 2003]

Let $\mathcal{D}$ be a 2-$(v, k, \lambda)$ design with a fixed-point-free and fixed-block-free automorphism $\phi$ 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 $\lambda$ then the orbit matrix $M$ generates a self-orthogonal code of length $b|q$ over $\mathbb{F}_p$.

Using Theorem 1 Harada and Tonchev classified all codes over $\mathbb{F}_3$ and $\mathbb{F}_7$ derived from symmetric 2-$(v, k, \lambda)$ designs with fixed-point-free automorphisms of order $p$ for the parameters $(v, k, \lambda, p) = (27, 14, 7, 3), (40, 27, 18, 5)$ and $(45, 12, 3, 5)$, and 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 $\mathbb{F}_5$ obtained form (100, 45, 20) design are optimal, some are near-optimal.
Theorem 2 [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 $\mathbb{F}_p$.

Theorem 3

Let $D$ be a symmetric $(v, k, \lambda)$ design with an automorphism group $G$ which acts on $D$ 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 $\mathbb{F}_p$. 
Theorem 4 [DC, L. Simčić]

Let $\mathcal{D}$ be a 2-$(v, k, \lambda)$ design with an automorphism $\phi$ of order $p$, where $p$ is prime. If $p$ divides $r - \lambda$, then the columns of the non-fixed part of the orbit matrix $M$ for automorphism $\phi$ generate a self-orthogonal code of length $\frac{b-h}{p}$ over $\mathbb{F}_p$, where $h$ is the number of fixed blocks.
The matrix $O_M$

$$O_M = \begin{bmatrix}
0 & 0^T_q & p j_q^T & 0^T_q \\
0_q & 0_{q \times q} & p (\bar{C} - I_q) & p \bar{C} \\
0_q & 0_{q \times q} & p (\bar{C} - I_q) & p \bar{C} \\
0_q & 0_{q \times q} & p (\bar{C} - I_q) & p \bar{C}
\end{bmatrix}$$

is an orbit matrix of a symmetric design for parameters $(4p^2, 2p^2 - p, p^2 - p)$ and the orbit length distribution with $q + 1$ fixed points and $2q$ orbits of length $p$ for points and blocks, whenever $q$ is a prime power, $q \equiv 1 \pmod{4}$, and $p = \frac{q+1}{2}$. 
Let $q$ be a prime power, $q \equiv 1 \pmod{4}$, and $p$ be a prime dividing $\frac{q+1}{2}$. It follows from Theorem 3 that the rows of the matrix

$$R = \begin{bmatrix}
\frac{q-1}{4} J_q + \frac{q-1}{4} I_q & \frac{q-1}{4} C + \frac{q+3}{4} (C - I_q) \\
\frac{q+3}{4} C + \frac{q-1}{4} (C - I_q) & \frac{q-1}{4} J_q + \frac{q-1}{4} I_q
\end{bmatrix}$$

span a self-orthogonal code over $\mathbb{F}_p$ of length $2q$.

The dimension of this code is $q - 1$. 
### Table: Parameters of the self-orthogonal codes

<table>
<thead>
<tr>
<th>$q$</th>
<th>$p$</th>
<th>parameters of the code</th>
<th>parameters of the dual code</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3</td>
<td>$[10, 4, 6]_3$ *</td>
<td>$[10, 6, 4]_3$ *</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>$[18, 8, 8]_5$ *</td>
<td>$[18, 10, 6]_5$ *</td>
</tr>
<tr>
<td>13</td>
<td>7</td>
<td>$[26, 12, 10]_7$</td>
<td>$[26, 14, 8]_7$</td>
</tr>
<tr>
<td>17</td>
<td>3</td>
<td>$[34, 16, 12]_3$ *</td>
<td>$[34, 18, 10]_3$ *</td>
</tr>
<tr>
<td>29</td>
<td>3</td>
<td>$[58, 28, 18]_3$ *</td>
<td>$[58, 30, 16]_3$ *</td>
</tr>
<tr>
<td>41</td>
<td>3</td>
<td>$[82, 40, 21]_3$ *</td>
<td>$[82, 42, 19]_3$ *</td>
</tr>
</tbody>
</table>

* Largest minimum distance among all known codes of the given length and dimension.
Conjecture 1

Let $q$ be a prime power, $q \equiv 1 \pmod{4}$, and $p = \frac{q+1}{2}$ be a prime. The code spanned by rows of the matrix $R$ is a self-orthogonal $[2q, q - 1, p + 3]_p$ code, and a dual code is a $[2q, q + 1, p + 1]_p$ code.
The rows of the matrix $S$, obtained from $R$ by adding first two rows and last two columns,

$$
S = \begin{bmatrix}
0_q & 0_q & \frac{q-1}{4} J_q + \frac{q-1}{4} I_q & \frac{q-1}{4} C + \frac{q+3}{4} (\overline{C} - I_q) \\
0_q & 0_q & \frac{q+3}{4} C + \frac{q-1}{4} (\overline{C} - I_q) & \frac{q-1}{4} J_q + \frac{q-1}{4} I_q \\
1 & 0 & j_q & 0_q \\
0 & 1 & 0_q & j_q
\end{bmatrix}
$$

span a self-dual $[2q + 2, q + 1]$ code over $\mathbb{F}_p$.

If $q$ is a prime and $q = 12m + 5$, where $m$ is a non-negative integer, then the code spanned by $S$ is equivalent to the Pless symmetry code $C(q)$.
Table: Parameters of the self-dual codes

* Largest minimum distance among all known codes of the given length and dimension.

Conjecture 2

Let $q$ be a prime power, $q \equiv 1 \ (mod \ 4)$, and let $p = \frac{q+1}{2}$ be a prime. The code spanned by rows of the matrix $S$ is a self-dual $[2q + 2, q + 1, p + 3]_p$ code.
A graph is **regular** if all the vertices have the same degree; a regular graph is **strongly regular** of type \((v, k, \lambda, \mu)\) if it has \(v\) vertices, degree \(k\), and if any two adjacent vertices are together adjacent to \(\lambda\) vertices, while any two non-adjacent vertices are together adjacent to \(\mu\) vertices.

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 2

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 \((v, k, \lambda, \mu)\) and orbit lengths distribution \((n_1, \ldots, n_t)\).
Definition 3

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

\begin{align*}
\sum_{i=1}^{t} c_{ij} &= \sum_{j=1}^{t} \frac{n_j}{n_i} c_{ij} = k \quad (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} \quad (6)
\end{align*}

is called a **column orbit matrix** for a strongly regular graph with parameters $(\nu, k, \lambda, \mu)$ and orbit lengths distribution $(n_1, \ldots, n_t)$. 
Theorem 5

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

Remark In this case the row orbit matrix is equal to the column orbit matrix.
In the rest of the talk we will study codes spanned by orbit matrices for a symmetric \((v, k, \lambda)\) design and orbit lengths distribution \((\Omega, \ldots, \Omega)\), where \(\Omega = \frac{v}{t}\). We follow the ideas presented in:


(Lander and Wilson have considered codes from incidence matrices of symmetric designs.)
Theorem 6

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

1. If $p \mid (k - \lambda)$, then $\text{dim}(C) \leq \frac{1}{2}(v + 1)$.
2. If $p \nmid (k - \lambda)$ and $p \mid k$, then $\text{dim}(C) = v - 1$.
3. If $p \nmid (k - \lambda)$ and $p \nmid k$, then $\text{dim}(C) = v$. 
Theorem 7 [DC, S. Rukavina]

Let a group $G$ acts on a symmetric $(v, k, \lambda)$ design $D$ with $t = \frac{v}{\Omega}$ orbits of length $\Omega$, on the set of points and the set of blocks, and let $M$ be an orbit matrix of $D$ induced by the action of $G$. Suppose that $C$ is the code over $\mathbb{F}_p$ 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 $V$ be a vector space of finite dimension $n$ over a field $\mathbf{F}$, let $b : V \times V \rightarrow \mathbf{F}$ be a symmetric bilinear form, i.e. a scalar product, and $(e_1, \ldots, e_n)$ be a basis of $V$. The bilinear form $b$ gives rise to a matrix $B = [b_{ij}]$, with

$$b_{ij} = b(e_i, e_j).$$

The matrix $B$ determines $b$ completely. If we represent vectors $x$ and $y$ by the row vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, then

$$b(x, y) = xBy^T.$$

Since the bilinear form $b$ is symmetric, $B$ is a symmetric matrix.
A bilinear form $b$ is nondegenerate if and only if its matrix $B$ is nonsingular. We may use a symmetric nonsingular matrix $U$ over a field $\mathbb{F}_p$ to introduce a scalar product $\langle \cdot, \cdot \rangle_U$ for row vectors in $\mathbb{F}_p^n$, namely

$$\langle a, c \rangle_U = aUc^\top.$$ 

For a linear $p$-ary code $C \subset \mathbb{F}_p^n$, the $U$-dual code of $C$ is

$$C^U = \{ a \in \mathbb{F}_p^n : \langle a, c \rangle_U = 0 \text{ for all } c \in C \}.$$ 

We call $C$ self-$U$-dual, or self-dual with respect to $U$, when $C = C^U$. 

Let a group $G$ acts on a symmetric $(v, k, \lambda)$ design $\mathcal{D}$ with $t = \frac{v}{\Omega}$ orbits of length $\Omega$, 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 $\lambda$, 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

$$M^{ext} = \begin{bmatrix}
M & 1 \\
\lambda \Omega & \ldots & \lambda \Omega & 1 \\
\lambda \Omega & \ldots & \lambda \Omega & k
\end{bmatrix},$$

and denote by $C^{ext}$ the extended code spanned by $M^{ext}$. 
Define the symmetric bilinear form $\psi$ by

$$\psi(\bar{x}, \bar{y}) = x_1y_1 + \ldots + x_ty_t - \lambda\Omega x_{t+1}y_{t+1},$$

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

The extended code $C^{ext}$ over $\mathbb{F}_p$ is self-orthogonal (or totally isotropic) with respect to $\psi$. 
The matrix of the bilinear form $\psi$ 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 8 [DC, S. Rukavina]

Let \( D \) be a symmetric \((v, k, \lambda)\) 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 \( \Omega \). Further, let \( M \) be the orbit matrix induced by the action of the group \( G \) on the design \( D \), and \( C^{\text{ext}} \) 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 \( C^{\text{ext}} \) is self-dual with respect to \( \psi \).

This theorem is proved by using the Smith normal form of the matrix \( M^{\text{ext}} \).
Theorem 9

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

As a consequence of Theorems 8 and 9 we have

Theorem 10

Let $\mathcal{D}$ be a symmetric $(v, k, \lambda)$ 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 $\Omega$. 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 $\mathbb{F}_p$. 
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 $\text{row}_F(A)$ the linear code over the field $F$ spanned by the rows of $A$. By $\text{row}_p(A)$ 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 $i$,

$$M_i(A) = \{ x \in \mathbb{Z}^n : p^i x \in \text{row}_\mathbb{Z}(A) \}.$$  

We have $M_0(A) = \text{row}_\mathbb{Z}(A)$ and

$$M_0(A) \subseteq M_1(A) \subseteq M_2(A) \subseteq \ldots.$$
Let

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

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

$$C_0(A) \subseteq C_1(A) \subseteq C_2(A) \subseteq \ldots .$$
Theorem 11

Suppose $A$ is an $n \times n$ integer matrix such that $A U A^T = p^e V$ for some integer $e$, where $U$ and $V$ are square matrices with determinants relatively prime to $p$. Then $C_e(A) = \mathbb{F}_p^n$ 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 12

Let $\mathcal{D}$ be a symmetric $(v, k, \lambda)$ 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 $\Omega$. Suppose that $n = k - \lambda$ is exactly divisible by an odd power of a prime $p$ and $\lambda$ 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 $U = \text{diag}(1, \ldots, 1, -\lambda_0 \Omega)$.

If $\lambda$ 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 $(v, k', \lambda')$ design, where $k' = v - k$ and $\lambda' = v - 2k + \lambda$. 
Theorem 13

Let $\mathcal{D}$ be a symmetric $(v, k, \lambda)$ 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 $\Omega$. Suppose that $n = k - \lambda$ is exactly divisible by an odd power of a prime $p$ and $\lambda$ 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 $U = \text{diag}(1, \ldots, 1, \lambda_0 n_0 \Omega)$. 
As a consequence of Theorems 9, 12 and 13, we have

**Theorem 14**

Let $\mathcal{D}$ be a symmetric $(v, k, \lambda)$ 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 $\Omega$. 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

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