The construction of combinatorial structures and linear codes from orbit matrices of strongly regular graphs

Sanja Rukavina
sanjar@math.uniri.hr

Department of Mathematics
University of Rijeka, Croatia

Symmetry vs Regularity
The first 50 years since Weisfeiler-Leman stabilization
July 1 - July 7, 2018, Pilsen, Czech Republic

Supported by CSF under the project 1637.

OM of strongly regular graphs

M. Behbahani and C. Lam have studied orbit matrices of strongly regular graphs that admit an automorphism group of prime order.

M. Behbahani, C. Lam, Strongly regular graphs with non-trivial automorphisms, *Discrete Math.*, 311 (2011), 132-144

Let Γ be a srg(v, k, λ, μ) and A be its adjacency matrix. Suppose an automorphism group G of Γ partitions the set of vertices V into t orbits $O_1, \dots, O_t$, with sizes $n_1, \dots, n_t$, respectively. The orbits divide A into submatrices $[A_{ij}]$, where A_{ij} is the adjacency matrix of vertices in O_i versus those in O_j. We define matrices $C = [c_{ij}]$ and $R = [r_{ij}]$, $1 \leq i, j \leq t$, such that

$$c_{ij} = \text{column sum of } A_{ij},$$
$$r_{ij} = \text{row sum of } A_{ij}.$$

R is related to C by $r_{ij} n_i = c_{ij} n_j$. Since the adjacency matrix is symmetric, $R = C^T$. The matrix R is the row orbit matrix of the graph Γ with respect to G, and the matrix C is the column orbit matrix of the graph Γ with respect to G.

srg(10,3,0,1)

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

$$R = \begin{bmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 \\ 3 & 1 & 0 & 1 \\ 0 & 2 & 1 & 0 \end{bmatrix}$$

Definition

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

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

$$\sum_{s=1}^{t} \frac{n_s}{n_j} r_{si} r_{sj} = \delta_{ij}(k-\mu) + \mu n_i + (\lambda - \mu) r_{ji} \tag{2}$$

is called a **row orbit matrix** for a strongly regular graph with parameters (v, k, λ, μ) and orbit lengths distribution $(n_1, \ldots, n_t)$. A $(t \times t)$-matrix $C = [c_{ij}]$ with entries satisfying conditions

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

$$\sum_{s=1}^{t} \frac{n_s}{n_j} c_{is} c_{js} = \delta_{ij}(k-\mu) + \mu n_i + (\lambda - \mu) c_{ij} \tag{4}$$

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

If all orbits have the same length w, *i.e.* $n_i = w$ for $i = 1, \ldots, t$, then $C = R$, and the following holds

$$\sum_{s=1}^{t} r_{is} r_{js} = \delta_{ij}(k-\mu) + \mu w + (\lambda - \mu) r_{ij}.$$

Linear codes from orbit matrices of strongly regular graphs

A **code** C of length n over the alphabet Q is a subset $C \subseteq Q^n$. Elements of a code are called **codewords**. A code C is called a p-ary **linear code** of dimension m if $Q = \mathbb{F}_p$, for a prime p, and C is an m-dimensional subspace of a vector space $\mathbb{F}_p^n$.

Let $C \subseteq \mathbb{F}_p^n$ be a linear code. Its **dual code** is the code $C^\perp = \{x \in \mathbb{F}_p^n | x \cdot c = 0,\ \forall c \in C\}$, where $\cdot$ is the standard inner product. A code C is **self-orthogonal** if $C \subseteq C^\perp$ and **self-dual** if $C = C^\perp$.

Theorem **[D. Crnković, M. Maksimović, B. G. Rodrigues, SR, 2016]**

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 F_q.

Theorem [D. Crnković, M. Maksimović, SR, 2018]

Let Γ be a SRG(v, k, λ, μ) having an automorphism group G which acts on the set of vertices of Γ with b orbits of lengths $n_1, \dots, n_b$, respectively, with f fixed vertices, and the other $b - f$ orbits of lengths $n_{f+1}, \dots, n_b$ divisible by p, where p is a prime dividing k, λ and μ. Let C be the column orbit matrix of the graph Γ with respect to G. If q is a prime power such that $q = p^n$, then the code spanned by the rows of the fixed part of the matrix C is a self-orthogonal code of length f over F_q.

$$
\begin{array}{c|ccc|ccc}
C & 1 & \cdots & 1 & n_{f+1} & \cdots & n_b \\
\hline
1 & & & & & & \\
\vdots & & & & & & \\
1 & & & & & & \\
\hline
n_{f+1} & & & & & & \\
\vdots & & & & & & \\
n_b & & & & & & \\
\end{array}
$$

Theorem [D. Crnković, M. Maksimović, SR, 2018]

Let Γ be a SRG(v, k, λ, μ) having an automorphism group G which acts on the set of vertices of Γ with b orbits of lengths $n_1, \ldots, n_b$, respectively, such that there are f fixed vertices, h orbits of length w, and $b - f - h$ orbits of lengths $n_{f+h+1}, \ldots, n_b$. Further, let $pw|n_s$ if $w < n_s$, and $pn_s|w$ if $n_s < w$, for $s = f + h + 1, \ldots, b$, where p is a prime number dividing k, λ, μ and w. Let C be the column orbit matrix of the graph Γ with respect to G. If q is a prime power such that $q = p^n$, then the code over F_q spanned by the part of the matrix C (rows and columns) determined by the orbits of length w is a self-orthogonal code of length h.

C	$1 \;\cdots\; 1$	$w \;\cdots\; w$	$n_{f+h+1} \;\cdots\; n_b$
1 $\vdots$ 1			
w $\vdots$ w			
n_{f+h+1} $\vdots$ n_b			

C	1	$\cdots$	1	2	$\cdots$	2	4	$\cdots$	4
1									
$\vdots$									
1									
2									
$\vdots$									
2									
4									
$\vdots$									
4									

C	1	$\cdots$	1	2	$\cdots$	2	4	$\cdots$	4
1									
$\vdots$									
1									
2									
$\vdots$									
2									
4									
$\vdots$									
4									

C	1	$\cdots$	1	2	$\cdots$	2	4	$\cdots$	4
1									
$\vdots$									
1									
2									
$\vdots$									
2									
4									
$\vdots$									
4									

Theorem [D. Crnković, M. Maksimović, SR, 2018]

Let Γ be a SRG(v, k, λ, μ) with an automorphism group G which acts on the set of vertices of Γ with b orbits of lengths $n_1, \ldots, n_b$, respectively, and $w = max\{n_1, \ldots, n_b\}$. Further, let p be a prime dividing k, λ, μ and w, and let $pn_s|w$ if $n_s \neq w$. Let C be the column orbit matrix of the graph Γ with respect to G. If q is a prime power such that $q = p^n$, then the code over F_q spanned by the rows of C corresponding to the orbits of length w is a self-orthogonal code of length b.

C	n_1	$\cdots$	n_{i_1}	n_{i_1+1}	$\cdots$	n_{i_2}	$\cdots$	w	$\cdots$	w
n_1										
$\vdots$										
n_{i_1}										
n_{i_1+1}										
$\vdots$										
n_{i_2}										
$\vdots$										
w										
$\vdots$										
w										

Theorem [D. Crnković, M. Maksimović, SR, 2018]

Let Γ be a SRG(v, k, λ, μ) with an automorphism group G which acts on the set of vertices of Γ with b orbits of lengths $n_1, \dots, n_b$, respectively, and $w = min\{n_1, \dots, n_b\}$. Further, let p be a prime dividing k, λ, μ and w, and let $pw | n_s$ if $n_s \neq w$. Let R be the row orbit matrix of the graph Γ with respect to G. If q is a prime power such that $q = p^n$, then the code over F_q spanned by the rows of R corresponding to the orbits of length w is a self-orthogonal code of length b.

R	w	$\cdots$	w	n_{i_1+1}	$\cdots$	n_{i_2}	$\cdots$	n_{i_l+1}	$\cdots$	n_b
w										
$\vdots$										
w										
n_{i_1+1}										
$\vdots$										
n_{i_2}										
$\vdots$										
n_{i_l+1}										
$\vdots$										
n_b										

Combinatorial structures from orbit matrices of strongly regular graphs

Theorem **[D. Crnković, SR, A. Švob, 2018]**

Let $C = [c_{ij}]$ be a $(t \times t)$ column orbit matrix for a strongly regular graph Γ with parameters (v, k, λ, μ) and orbit lengths distribution $(n_1, \ldots, n_t)$, $n_1 = \ldots = n_t = n$, with constant diagonal. Further, let the off-diagonal entries of C have exactly two values, *i.e.* $c_{ij} \in \{x, y\}$, $x \neq y$, $1 \leq i, j \leq t$, $i \neq j$. Replacing every x with 1 and all diagonal elements and every y in C with 0, one obtains the adjacency matrix of a strongly regular graph $\widetilde{\Gamma}$ on t vertices.