Regular digraphs and related linear codes

Vedrana Mikulić Crnković
(vmikulic@math.uniri.hr)
joint work with Ivona Traunkar and Matea Zubović Žutolija

Faculty of Mathematics, University of Rijeka

Combinatorial Designs and Codes 2024
(Satellite event of the 9th European Congress of Mathematics)

This work has been supported by Croatian Science Foundation under the project 4571 and by the University of Rijeka under the project uniri-iskusni-prirod-23-155.

UNIVERSITY OF RIJEKA
FACULTY OF MATHEMATICS

Groups and designs
Construction of 1-designs from groups

Digraphs
Construction of k-regular digraphs from groups

Codes
Construction of codes from incidence matrix of 1-designs

Group action

A group G acts on a set S if there exists function $f : G \times S \mapsto S$ such that

1. $f(e, x) = x, \forall x \in S$,
2. $f(g_1, f(g_2, x)) = f(g_1 g_2, x), \forall x \in S, \forall g_1, g_2 \in G$.

Denote the described action by $xg, \forall x \in S, \forall g \in G$.

The set $G_x = \{g \in G \mid xg = x\}$ is a group called stabilizer of the element $x \in S$. The set $xG = \{xg \mid g \in G\}$ is orbit of the element $x \in S$. If there is only one orbit than the action is transitive.

Designs

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is called a t-(v, k, λ) design, if

1. $\mathcal{P}$ contains v points,
2. each block $B \in \mathcal{B}$ is incident with k points, and
3. every t distinct points are incident with λ blocks.

The incidence matrix of a design is a $b \times v$ matrix $[m_{ij}]$ where b and v are the numbers of blocks and points respectively, such that $m_{ij} = 1$ if the point P_j and the block B_i are incident, and $m_{ij} = 0$ otherwise.

A bijective mapping of points to points and blocks to blocks which preserves incidence of a design $\mathcal{D}$ is called an automorphism of $\mathcal{D}$. The set of all automorphisms of $\mathcal{D}$ forms its full automorphism group denoted by $\mathrm{Aut}(\mathcal{D})$.

UNIVERSITY OF RIJEKA
FACULTY OF MATHEMATICS

- A design is block design if $t = 2$.
- A design is symmetric if the number of points is equal to the number of blocks.
- A design is weakly p-self-orthogonal (p-WSO) if all the block intersection numbers gives the same residue modulo p. A weakly p-self-orthogonal design is p-self-orthogonal if the block intersection numbers and the block sizes are multiples of p.
- Specially, weakly 2-self-orthogonal design is called weakly self-orthogonal (WSO) design, and 2-self-orthogonal design is called self-orthogonal.

UNIVERSITY OF RIJEKA
FACULTY OF MATHEMATICS

Construction of 1-designs from groups

Theorem (D. Crnković, VMC, 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 $\Delta_2 = \cup_{i=1}^{s} G_\alpha.\delta_i$, where $\delta_1, \ldots, \delta_s \in \Omega_2$ are representatives of distinct G_α-orbits. If $\Delta_2 \neq \Omega_2$ and

$$\mathcal{B} = \{g.\Delta_2 \ : \ g \in G\},$$

then $\mathcal{D}(G, \alpha, \delta_1, \ldots, \delta_s) = (\Omega_2, \mathcal{B})$ is a $1 - (n, |\Delta_2|, \frac{|G_\alpha|}{|G_{\Delta_2}|} \sum_{i=1}^{s} |G_{\delta_i}.\alpha|)$ design with $\frac{m \cdot |G_\alpha|}{|G_{\Delta_2}|}$ blocks. The group $H \cong G/ \cap_{x \in \Omega_2} G_x$ acts as an automorphism group on $(\Omega_2, \mathcal{B})$, transitively on points and blocks of the design.

- D. Crnković, VMC, A. Švob, On some transitive combinatorial structures constructed from the unitary group $U(3,3)$, J. Statist. Plann. Inference, 144, (2014) 19–40.
- D. Crnković, VMC, A. Švob, New 3-designs and 2-designs having $U(3,3)$ as an automorphism group, Discrete Math. 340 (2017), 2507-2515.
- D. Crnković, S. Rukavina, A. Švob, New strongly regular graphs from orthogonal groups $O^+(6,2)$ and $O^-(6,2)$, Discrete Math. 341 (2018) 2723-2728.
- A. E. Brouwer, D. Crnković, A. Švob, A construction of directed strongly regular graphs with parameters (63,11,8,1,2), Discrete Math. 347 (2024), 114146, 3 pages.

UNIVERSITY OF RIJEKA
FACULTY OF MATHEMATICS

- The incidence matrix of a symmetric 1-design is the adjacency matrix of a regular digraph.
- The incidence matrix of a symmetric 1-design with symmetric incidence matrix is the adjacency matrix of a regular graph.

Quasi-strongly regular digraphns

A quasi-strongly regular digraph[1] (QSRD) $\mathcal{G}$ with parameters $(n, k, t, a; c_1, c_2, \ldots, c_p)$ is a k-regular digraph on n vertices such that

- each vertex is incident with t undirected edges,
- for any two distinct vertices x, y the number of paths of length 2 from x to y is a if $x \to y$,
- for any two distinct vertices x, y the number of paths of length 2 from x to y is c_i, for $i \in \{1, \ldots, p\}$, if $x \nrightarrow y$
- for each c_i, $i \in \{1, \ldots, p\}$, there exist two distinct vertices $x \nrightarrow y$ such that the number of paths of length 2 from x to y is c_i.

Number p is grade of $\mathcal{G}$ and $c_1 > c_2 > \cdots > c_p$.

[1] D. Jia, Z. Guo, G. Zhang, *Some constructions of quasi-strongly regular graphs, Graphs and Combinatorics*, **38**, (2022)

Quasi-strongly regular digraphns

A quasi-strongly regular digraph[1] (QSRD) $\mathcal{G}$ with parameters $(n, k, t, a; c_1, c_2, \dots, c_p)$ is a k-regular digraph on n vertices such that

- each vertex is incident with t undirected edges,
- for any two distinct vertices x, y the number of paths of length 2 from x to y is a if $x \to y$,
- for any two distinct vertices x, y the number of paths of length 2 from x to y is c_i, for $i \in \{1, \dots, p\}$, if $x \nrightarrow y$
- for each c_i, $i \in \{1, \dots, p\}$, there exist two distinct vertices $x \nrightarrow y$ such that the number of paths of length 2 from x to y is c_i.

Number p is grade of $\mathcal{G}$ and $c_1 > c_2 > \dots > c_p$.

- If $p = 1$, a quasi-strongly regular digraph is strongly regular digraph (SRD) with paramters (n, k, a, c_1, t).
- If $p = 1$ and $k = t$, a quasi-strongly regular digraph is strongly regular graph.

[1] D. Jia, Z. Guo, G. Zhang, *Some constructions of quasi-strongly regular graphs, Graphs and Combinatorics*, 38, (2022)

Construction of k-regular digraphs from groups

Theorem (VMC, Matea Zubović Žutolija)

Let G be a finite permutation group acting transitively on the set Ω. Let $\alpha \in \Omega$ and let $\Delta = \cup_{i=1}^{s} \delta_i G_\alpha$ be a union of orbits of the stabilizer G_α of α, where $\delta_1, \ldots, \delta_s$ are representatives of different G_α-orbits. Let $T = \{g_1, \ldots, g_t\}$ be a set of representatives of left cosets in $G/G_\alpha = \{g_1 G_\alpha, \ldots, G_t G_\alpha\}$. Let $\mathcal{V} = \{g_i.\alpha | i = 1, \ldots, t\}$ and let $\mathcal{E} = \{(g_i.\alpha, g_i.\beta) | i = 1, \ldots, t, \beta \in \Delta\}$.
Then $\Gamma = (\mathcal{V}, \mathcal{E})$ is a directed graph with $|\Omega|$ vertices that is $|\Delta|$-regular and such that $g_i.\Delta$ is a set of out-neighbours of the vertex $g_i.\alpha$, $i = 1, \ldots, t$. The group G acts on the constructed graph as automorphism group, transitively on the set of vertices.

Theorem

If a group G acts transitively on a set of vertices of a directed regular graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, then there exists a set Ω such that vertices and arcs of a digraph $\mathcal{G}$ are defined in the way described in Theorem.

Classifications

- There are, up to isomorphism, 2920 QSRD, on which a transitive automorphism group of degree n, $n \in \{1, \dots, 30\} \backslash \{22, 24, 28, 30\}$, is acting. 478 of them are SRD.
- There are, up to isomorphism, 18 QSRD on which the transitive irregular automorphism group of degree 22 acts. Two of them are SRD.
- There are, up to isomorphism, 68235 QSRD on which the transitive irregular automorphism group of degree 24 acts, of which 64 are SRD.
- There are, up to isomorphism, 469 QSRDs on which the transitive irregular automorphism group of degree 28 acts, of which 22 are SRD.
- There are, up to isomorphism, 642 QSRD on which the transitive irregular automorphism group of degree 30 acts, of which 12 are directed SRD.
- There are, up to isomorphism, 124 QSRD, on which the primitive automorphism group of degree n, $n \in \{31, \dots, 110\}$, is acting, no SRD.

More results

- There is no SRD with parameters $(22, 9, 3, 4, 6)$ such that the automorphism group G acts transitively on the set of vertices of that directed graph.
- There is no SRD with parameters (24,10,3,5,5) such that the automorphism group G acts transitively on the set of vertices of that directed graph.
- There is no SRD with parameters $(28, 6, 2, 1, 3)$ such that the automorphism group G acts transitively on the set of vertices of that directed graph.
- There is no SRD with parameters $(30, 11, 2, 5, 9)$ and $(30, 12, 4, 5, 11)$ such that the automorphism group G acts transitively on the set of vertices of that directed graph.

Codes

We will talk only about linear codes, i.e. subspaces of the ambient vector space over a field $\mathbb{F}_q$ of order $q = p^l$, where p is prime.
A code C of length n and dimension k over the field $\mathbb{F}_q$ is denoted by $[n, k]_q$.
Specially, if $q = 2$, parameters of code C with minimum distance d are denoted by $[n, k, d]$.

A generator matrix of a $[n, k]$ code C is a $k \times n$ matrix whose rows form basis of C.

The dual code of a code C is code $C^\perp$, $C^\perp = \{v \in (\mathbb{F}_q)^n \mid (v, c) = 0, \ \forall c \in C\}$.
A code is self-orthogonal (SO) if $C \subseteq C^\perp$, self-dual if $C = C^\perp$, and LCD if $C \cap C^\perp = \{0\}$.

The code $C_{\mathbb{F}}(\mathcal{D})$ of a design $\mathcal{D}$ over the finite field $\mathbb{F}$ is the space spanned by the incidence vectors of the blocks over $\mathbb{F}$.

Two linear codes are isomorphic if they can be obtained from one another by permuting the coordinate positions. An automorphism of a code C is an isomorphism from C to C. The full automorphism group will be denoted by $\mathrm{Aut}(C)$.

If code $C_{\mathbb{F}}(\mathcal{D})$ is a linear code of a design $\mathcal{D}$ over a finite field $\mathbb{F}$, then the full automorphism group of $\mathcal{D}$ is contained in the full automorphism group of code $C_{\mathbb{F}}(\mathcal{D})$.

SO codes from p-WSO 1-designs

Theorem (VMC, I. Traunkar)

Let $q = p^l$ be prime power and $\mathbb{F}_q$ a finite field of order q. Let $\mathcal{D}$ be a weakly p-self-orthogonal design such that $k \equiv a \pmod{p}$ and $|B_i \cap B_j| \equiv d \pmod{p}$, for all $i, j \in \{1, \ldots, b\}$, $i \neq j$, where B_i and B_j are two blocks of a design $\mathcal{D}$. Let M be it's $b \times v$ incidence matrix.

1. *If $\mathcal{D}$ is p-self-orthogonal design, then M generates a self-orthogonal code over $\mathbb{F}_q$.*
2. *If $a = 0$ and $d \neq 0$, then the matrix $[\sqrt{d} \cdot I_b, M, \sqrt{-d} \cdot \mathbf{1}]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-d$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*
3. *If $a \neq 0$ and $d = 0$, then the matrix $[M, \sqrt{-a} \cdot I_b]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-a$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*
4. *If $a \neq 0$ and $d \neq 0$, there are two cases:*
   - 4.1 *if $a = d$, then the matrix $[M, \sqrt{-d} \cdot \mathbf{1}]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-a$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise, and*
   - 4.2 *if $a \neq d$, then the matrix $[\sqrt{d-a} \cdot I_b, M, \sqrt{-d} \cdot \mathbf{1}]$ generates a self-orthogonal code over $\mathbb{F}$, where $\mathbb{F} = \mathbb{F}_q$ if $-d$ is a square in $\mathbb{F}_q$, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise.*

LCD codes from p-WSO designs

Theorem (VMC, I. Traunkar)

Let $\mathcal{D}$ be such that $k \equiv a \pmod{p}$ and $|B_i \cap B_j| \equiv d \pmod{p}$, for all $i, j \in \{1, \dots, b\},\ i \neq j$, where B_i and B_j are two blocks of the design $\mathcal{D}$.

1. *If $a = d = 0$ then*
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b]$ for $x \neq 0$, and
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b, y\mathbf{1}]$ for $y \neq 0$ and $x^2 + b \cdot y^2 \neq 0$
   generate an LCD code over the field $\mathbb{F}_q$.
2. *If $a = 0$ and $d \neq 0$ then*
   the matrix $\mathbf{M}$ for $(b-1) \cdot d \neq 0$ and if $\mathbf{M}$ is of full rank,
   the matrix $[\mathbf{M}, y\mathbf{1}]$ for $by^2 + (b-1) \cdot d \neq 0$ and if $\mathbf{M}$ is of full rank,
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b]$ for $x - d \neq 0$ and $x^2 + (b-1) \cdot d \neq 0$, and
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b, y\mathbf{1}]$ for $x^2 - d \neq 0$ and $b \cdot y^2 + x^2 + (b-1) \cdot d \neq 0$
   generate an LCD code over the field $\mathbb{F}_q$.

Theorem (VMC, I. Traunkar)

3. *If $a \neq 0$ and $d = 0$ then*
   the matrix $\mathbf{M}$ *if* $\mathbf{M}$ *is of full rank,*
   the matrix $[\mathbf{M}, y\mathbf{1}]$ *for* $b \cdot y^2 + a \neq 0$ *and if* $\mathbf{M}$ *is of full rank,*
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b]$ *for* $x^2 + a \neq 0$, *and*
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b, y\mathbf{1}]$ *for* $x^2 + a \neq 0$ *and* $b \cdot y^2 + x^2 + a \neq 0$
   generate an LCD code over the field $\mathbb{F}_q$.
4. *If $a = d \neq 0$ then*
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b]$ *for* $x \neq 0$ *and* $x^2 + ba \neq 0$, *and*
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b, y\mathbf{1}]$ *for* $x \neq 0$ *and* $b \cdot y^2 + x^2 + b \cdot d \neq 0$
   generate an LCD code over the field $\mathbb{F}_q$.
5. *If $a \neq 0$, $d \neq 0$, $a \neq d$ then*
   the matrix $\mathbf{M}$ *for* $a + (b-1) \cdot d \neq 0$ *and if* $\mathbf{M}$ *is of full rank,*
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b]$ *for* $x^2 - d + a \neq 0$ *and* $x^2 + a + (b-1) \cdot d \neq 0$,
   the matrix $[\mathbf{M}, y\mathbf{1}]$ *for* $by^2 + a + (b-1) \cdot d \neq 0$ *and if* $\mathbf{M}$ *is of full rank, and*
   the matrix $[\mathbf{M}, x \cdot \mathbf{I}_b, y\mathbf{1}]$ *for* $x^2 - d + a \neq 0$ *and*
   $b \cdot y^2 + x^2 + a + (b-1) \cdot d \neq 0$
   generate an LCD code over $\mathbb{F}_q$.

Examples of SO and LCD codes over the field $\mathbb{F}_q$ constructed by described extensions of incidence matrix and similar extensions of orbit matrices and submatrices of orbit matrices:

V. Tonchev, Self-Orthogonal Designs and Extremal Doubtly-Even Codes, Journal of Combinatorial Theory, Series A 52, 197-205 (1989).

D. Crnković, VMC, B. G. Rodrigues, On self-orthogonal designs and codes related to Held's simple group, Adv. Math. Commun. 12 (2018)

VMC, I. Traunkar, Self-orthogonal codes constructed from weakly self-orthogonal designs invariant under an action of M_{11}, AAECC (2023)

VMC, B. G. Rodrigues, I. Traunkar, LCD codes constructed from weakly p-self-orthogonal 1-designs, submitted

Examples of SO and LCD codes over the field $\mathbb{F}_q$ constructed by described extensions of incidence matrix and similar extensions of orbit matrices and submatrices of orbit matrices:

- V. Tonchev, Self-Orthogonal Designs and Extremal Doubtly-Even Codes, Journal of Combinatorial Theory, Series A 52, 197-205 (1989).
- D. Crnković, VMC, B. G. Rodrigues, On self-orthogonal designs and codes related to Held's simple group, Adv. Math. Commun. 12 (2018)
- VMC, I. Traunkar, Self-orthogonal codes constructed from weakly self-orthogonal designs invariant under an action of M_{11}, AAECC (2023)
- VMC, B. G. Rodrigues, I. Traunkar, LCD codes constructed from weakly p-self-orthogonal 1-designs, submitted

Examples of SO codes from adjacency and orbit matrix of graphs and digraphs:

- D. Crnković, A. Švob, Self-orthogonal codes from Deza graphs, normally regular digraphs and Deza digraphs, Graphs Combin. 40 (2024), article no. 35, 12 pages.

If A is adjacency matrix of a QSRD with parameters $(n, k, t, a; c_1, c_2, \dots, c_p)$ then:

- A is square matrix and $AJ_n = J_nA = kJ$
- $A^2 = tI_n + aA + c_1C_1 + c_2C_2 + \cdots + c_pC_p$ for some non-zero $(0,1)$-matrices $C_1, C_2, \dots, C_p$ such that $C_1 + C_2 + \cdots + C_p = J_n - I_n - A$
- $(A^T)^2 = tI_n + aA^T + c_1C_1^T + c_2C_2^T + \cdots + c_pC_p$ for some non-zero $(0,1)$-matrices $C_1, C_2, \dots, C_p^T$ such that $C_1^T + C_2^T + \cdots + C_p^T = J_n - I_n - A^T$

From that one can eliminate some graphs whose adjacency matrix will generate non-interesting SO or LCD codes.

Examples: Binary SO codes constructed from SRDs and QSRDs on 12 vertices

SRD	code
(12,4,0,2,2)	[12,3,4]
(12,5,2,2,3)	[12,3,6]*
(12,65,2,2,3)	[12,4,4]

QSRD or its complement	code
(12,2,0,0;1,0)	[12,6,2]
(12,4,0,0;4,0)	[12,3,4]
(12,4,3,0;3,2,0)	[12,4,4]
(12,4,3,0;3,1)	[12,5,4]*
(12,1,0,0;1,0)	[24,12,2]
(12,3,0,0;3,2,0)	[24,12,4]
(12,5,4,0;5,4,0)	[24,12,4]
(12,3,2,1;1,0)	[12,4,4]
(12,3,2,1;2,0)	[12,5,4]*
(12,5,1,2;4,2)	[12,6,4]*
(12,5,3,2;4,1)	[12,6,2]
(12,4,0,1;4,2,1)	[24,12,8]*

Thank you for your attention!