Self-dual codes over $\mathbb{Z}_k$ from rectangular association schemes

Muhammad Bilal, Joaquim Borges,
Cristina Fernández-Córdoba

Universitat Autònoma de Barcelona

JMDA 2012, July 11-13, 2012

Outline

$\mathbb{Z}_k$-linear codes

- C is a $\mathbb{Z}_k$-linear code; that is, C is an additive subgroup of $\mathbb{Z}_k$.
- The dual of a code C is $C^\perp = \{w \in \mathbb{Z}_k \mid w \cdot v = 0, \ \forall\, v \in C\}$.
- The code is said to be *self-dual* if it is equal to its dual and *self-orthogonal* if it is contained in its dual.

Association Schemes

- Let X be a finite set, $|X| = v$. Let R_i be a subset of $X \times X$, $\forall i \in \mathcal{I} = \{0, \dots, d\}, d > 0$, $\Re = \{R_i\}_{i \in \mathcal{I}}$.
- We say that $(X, \Re)$ is a d-*class association scheme* if the following properties are satisfied:
  - (i) $R_0 = \{(x, x) : x \in X\}$ is the identity relation.
  - (ii) $\forall x, y \in X$, $\exists\, i \in \mathcal{I}$ such that $(x, y) \in R_i$ for exactly one i.
  - (iii) $\forall\, i \in \mathcal{I}$, $\exists\, i' \in \mathcal{I}$ such that $R_i^t = R_{i'}$, where $R_i^t = \{(x, y) : (y, x) \in R_i\}$.
  - (iv) If $(x, y) \in R_k$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant p_{ij}^k.
- A d-class association scheme with $d \leq 4$ is always commutative, [1], meaning that $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \mathcal{I}$.

D. G. Higman.

Coherent Configurations.

Geom.Dedicata, vol. 4, pp. 1-32, (1975).

- The adjacency matrix A_i for the relation R_i, $i \in \mathcal{I}$ is:

$$(A_i)_{x,y} = \begin{cases} 1, & if\ (x,y) \in R_i, \\ 0, & otherwise. \end{cases}$$

- The conditions (i)-(iv) in the definition of $(X, \Re)$ are equivalent to:
  (i) $A_0 = I$ (the identity matrix).
  (ii) $\sum_{i\in\mathcal{I}} A_i = J$ (the all-ones matrix).
  (iii) $\forall\, i \in \mathcal{I}, \exists\, i' \in \mathcal{I}$, such that $A_i = A_{i'}^t$.
  (iv) $\forall\, i, j \in \mathcal{I}, \quad A_i A_j = \sum_{k\in\mathcal{I}} p_{ij}^k A_k$.
- If the association scheme is symmetric, then $A_i = A_i^t$, for all $i \in \mathcal{I}$.
- If the association scheme is commutative, then $A_i A_j = A_j A_i$, for all $i, j \in \mathcal{I}$.

3-class association schemes and self-dual codes

- Let $(X, \Re)$ be a 3-class association scheme.
- The adjacency matrix for R_0 is I and the adjacency matrices of R_1, R_2 and R_3 are A_1, A_2 and $J - I - A_1 - A_2$, respectively.

Lemma

If $(X, \Re)$ is a 3-class association scheme then the following equations hold:

(i) $A_1 J = J A_1 = p^0_{11} J$, $A_2 J = J A_2 = p^0_{22} J$.

(ii) $A_1 A_2 = A_2 A_1 = p^0_{12} I + p^1_{12} A_1 + p^2_{12} A_2 + p^3_{12}(J - I - A_1 - A_2)$.

Note that the number of ones per row (or column) in A_1 is p^0_{11}, A_2 is p^0_{22} and A_3 is p^0_{33}.

- For arbitrary values of $r, s, t, u \in \mathbb{Z}_k$

$$\begin{aligned} Q(r,s,t,u) &= rA_0 + sA_1 + tA_2 + uA_3 \\ &= (r-u)I + (s-u)A_1 + (t-u)A_2 + uJ. \end{aligned}$$

- The generator matrix for a code generated using *pure* construction is

$$\mathcal{P}(r,s,t,u) = (I \mid Q(r,s,t,u)).$$

- The generator matrix for a code generated using *bordered* construction is

$$\mathcal{B}(r,s,t,u) = \left(\begin{array}{c|c|c|c} 1 & 0\ldots0 & a & 1\ldots1 \\ \hline 0 & & c & \\ \vdots & I & \vdots & Q(r,s,t,u) \\ 0 & & c & \end{array}\right).$$

- We write Q, $\mathcal{P}$ and $\mathcal{B}$ for $Q(r,s,t,u)$, $\mathcal{P}(r,s,t,u)$ and $\mathcal{B}(r,s,t,u)$.

Rectangular association schemes

Definition

Consider two sets A and B with $|A| = n \geq 2$ and $|B| = m \geq 2$. Let $X = A \times B$ and define the binary relations over X:

$$R_0 = \left\{((x, y), (x, y)) \in X^2\right\};$$
$$R_1 = \left\{ ((x, y), (x, y')) \in X^2 \middle| y \neq y' \right\};$$
$$R_2 = \left\{ ((x, y), (x', y)) \in X^2 \middle| x \neq x' \right\};$$
$$R_3 = \left\{ ((x, y), (x', y')) \in X^2 \middle| x \neq x' \, and \, y \neq y' \right\}.$$

$(X, \Re)$ is a symmetric 3-class association scheme with parameters:

$$v = nm, p_{11}^0 = m - 1; p_{22}^0 = n - 1; p_{33}^0 = (m-1)(n-1);$$
$$p_{11}^1 = m - 2; p_{23}^1 = p_{32}^1 = n - 1; p_{33}^1 = (n-1)(m-2);$$
$$p_{13}^2 = p_{31}^2 = m - 1; p_{22}^2 = n - 2; p_{33}^2 = (n-2)(m-1);$$
$$p_{12}^3 = p_{21}^3 = 1; p_{31}^3 = p_{13}^3 = m - 2;$$
$$p_{23}^2 = p_{32}^2 = n - 2 = p_{33}^3 = (n-2)(m-2);$$

and $p_{ij}^k = 0$, for all other cases.

Lemma

If $(X, \Re)$ is a $n \times m$ symmetric rectangular association scheme, then the following equations hold:

(i) $A_1 J = J A_1 = (m-1)\, J$, $A_2 J = J A_2 = (n-1)\, J$, $J^2 = n^2 m^2 J$;

(ii) $A_1^2 = (m-1)\, I + (m-2)\, A_1$; $A_2^2 = (n-1)\, I + (n-2)\, A_2$;

(iii) $A_1 A_2 = A_2 A_1 = A_3 = J - I - A_1 - A_2$.

Self-dual codes from rectangular association schemes

- The case of binary self-dual codes from non-symmetric 3-class association schemes was studied in [1].
- For the symmetric case the number of conditions and equations increase.
- We limit ourselves to the rectangular association scheme $n \times m$ $(n, m \geq 2)$.

M. Bilal, J. Borges, S. T. Dougherty, C. Fernández-Córdoba.
Binary Self-dual codes from 3-class association schemes.
III International Castle Meeting on Coding Theory and Applications, UAB vol. 5 , pp: 59 - 64.UAB- (September 2011). ISBN: 978-84-490-2688-1.

- For a code generated by $\mathcal{P}$ to be self-dual we need

$$(I \mid Q)(I \mid Q)^t = \mathbf{0}.$$

Namely, we need $QQ^t = -I$.

- For the code generated by $\mathcal{B}$ to be self-dual we need the following:

$$1 + a^2 + vb^2 = 0; \tag{1}$$

$$ac + b(r + s\kappa + t\kappa + u(v - 2\kappa - 1)) = 0; \tag{2}$$

$$I + c^2 J + QQ^T = \mathbf{0}. \tag{3}$$

Let $\rho = r - u$, $\sigma = s - u$ and $\tau = t - u$. We can write Equation $QQ^t = Q^2$ as

$$\begin{aligned} Q^2 &= \left[\rho^2 + \sigma^2 (m-1) + \tau^2 (n-1) - 2\sigma\tau\right] I \\ &+ \left[2\rho\sigma + \sigma^2 (m-2) - 2\sigma\tau\right] A_1 \\ &+ \left[2\rho\tau + \tau^2 (n-2) - 2\sigma\tau\right] A_1 \\ &+ \left[u\left[2\rho + 2\sigma (m-1) + 2\tau (n-1) + un^2m^2\right] + 2\sigma\tau\right] J. \end{aligned} \tag{4}$$

For the code generated by $\mathcal{P}$ to be self-orthogonal we need

$$\begin{aligned}
\rho^2 + \sigma^2 (m-1) + \tau^2 (n-1) - 2\sigma\tau &= -1, \\
2\rho\sigma + \sigma^2 (m-2) - 2\sigma\tau &= 0, \\
2\rho\tau + \tau^2 (n-2) - 2\sigma\tau &= 0, \\
u\left[2\rho + 2\sigma (m-1) + 2\tau (n-1) + un^2m^2\right] + 2\sigma\tau &= 0.
\end{aligned} \tag{5}$$

For a code generated by $\mathcal{B}$ to be self-orthogonal, along with Equations (1) and (2), we need

$$\begin{aligned} \rho^2 + \sigma^2(m-1) + \tau^2(n-1) - 2\sigma\tau &= -1; \\ 2\rho\sigma + \sigma^2(m-2) - 2\sigma\tau &= 0; \\ 2\rho\tau + \tau^2(n-2) - 2\sigma\tau &= 0; \\ u\left[2\rho + 2\sigma(m-1) + 2\tau(n-1) + un^2m^2\right] + 2\sigma\tau &= -c^2. \end{aligned} \tag{6}$$

Theorem

Let C be a code generated from a $n \times m$ rectangular association scheme over $\mathbb{Z}_k$ by using the pure or the bordered construction. Let $k = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factor decomposition of k. If C is a self-dual code, then

$$\alpha_0 \leq 1 \quad \textit{and} \quad p_i \equiv 1 \pmod 4 \;\; \forall i = 1, \ldots, r. \tag{7}$$

Moreover, if (7) is satisfied, then there exist values of n and m such that C is a self-dual code.

Example

There exists a self-dual code over $\mathbb{Z}_k$ from 3-class rectangular association scheme when $k = 2, 5, 10, 13, 17, 25, 26, \ldots$

Example

For $n = 2$ and $m = 6$. The adjacency matrices are:

$$A_0 = I,\ A_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix},$$

Example

The code C generated by $\mathcal{P}$, with $Q = 2I + 4A_1$, is a self-dual code over $\mathbb{Z}_5$.
We can generate two self-dual codes over $\mathbb{Z}_5$ with $\mathcal{B}$, using $Q = 2I + 4A_1$ with $a \equiv 2 \pmod 5$ or $a \equiv 3 \pmod 5$ along with $b \equiv c \equiv 0 \pmod 5$.

Future Work

We have generated binary self-dual codes from 3-class association schemes, BDF11, and we have also generated self-dual codes over $\mathbb{Z}_k$ from 3-class association schemes.

- We want to generate self-dual codes from Hamming and Johnson 3-class association schemes over $\mathbb{Z}_k$.

Bibliography

S. T. Dougherty, J. L. Kim, and P. Solé.
Double Circulant Codes from Two Class Association Schemes.
Advances in Mathematics of Communications, vol. 1, no. 1, pp. 45-64, (2007).

E. Rains and N. J. A. Sloane.
Self-dual codes in the Handbook of Coding Theory, V. S. Pless and W. C. Huffman.
eds., Elsevier, Amsterdam, pp. 177-294, (1998).

Thank You