On some constructions of LCD codes

Ana Grbac [abaric@math.uniri.hr]
Dean Crnković [deanc@math.uniri.hr]
Andrea Švob[asvob@math.uniri.hr]

Department of Mathematics
University of Rijeka, Croatia

Combinatorial Designs and Codes (online)
Satellite event of the 8th European Congress of Mathematics

15th July 2021

This work has been fully suported by Croatian Science Foundation under the project 5713.

Outline of the Talk

1. Preliminaries
2. Constructions of LCD codes from two-class association schemes
3. Conditions for constructing LCD codes over the field $\mathbb{F}_2$
4. LCD codes from SRGs and DRTs

Linear code

Definition

An $[\boldsymbol{n},\boldsymbol{k}]$ **linear code** $\mathcal{C}$ of length n and rank k is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field with q elements.

Definition

The **Hamming distance** between two vectors $x,y \in \mathbb{F}_q^n$ is defined by

$$d(x,y) = |\{i \mid x_i \neq y_i,\ 1 \leq i \leq n\}|.$$

The **minimum distance** of a code $\mathcal{C}$ is defined by

$$d = min\{d(x,y) \mid x,y \in \mathcal{C},\ x \neq y\}.$$

An $[n,k]$ linear code with minimum distance d will be denoted by $[n,k,d]$ code.

Linear code

Definition

Given a linear $[n, k, d]$ code $\mathcal{C}$, a **generator matrix** G of $\mathcal{C}$ is a $k \times n$ matrix whose rows form a basis for a linear code.
A generator matrix of the form $G = [I_k \mid A]$, where I_k is the identity matrix of order k and A is a $k \times (n-k)$ matrix, is called a **generator matrix in standard form**.

Definition

The **dual code** of a linear code $\mathcal{C} \subset \mathbb{F}_q^n$ is the code $\mathcal{C}^\perp \subset \mathbb{F}_q^n$ where

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0,\ \forall y \in \mathcal{C}\}.$$

A code $\mathcal{C}$ is **self-orthogonal** if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and **self-dual** if $\mathcal{C} = \mathcal{C}^\perp$.
The length n of a self-dual code is even and the dimension is $n/2$.

Strongly regular graph

Definition (SRG(v, k, λ, μ))

A simple graph G of order v is **strongly regular** with parameters (v, k, λ, μ) if

- each vertex has degree k,
- each adjacent pair of vertices has λ common neighbours,
- each nonadjacent pair of vertices has μ common neighbours.

Doubly regular tournament

Definition

A **tournament** $T = (V, E)$ of order n (**n-tournament**) is a directed graph where the vertex set V consists of n elements and the edge set $E \subset V \times V$ such that each pair of vertices x and y is joined by exactly one of the directed edges (x, y) or (y, x).

Let (x, y) be a directed edge of a tournament T. We say that x *dominates* y and y is an *out-neighbour* of x. Similarly, y *is dominated* by x and x is an *in-neighbour* of y.
The *out-degree* of the vertex x is the number of vertices that are dominated by x and the *in-degree* of the vertex x is the number of vertices that dominate x.

Doubly regular tournament

Definition

A tournament T is ***k*-regular** if each vertex dominates k vertices and is dominated by k vertices, *i.e* if every vertex in T has in-degree and out-degree k.

Definition (DRT(v, k, λ, μ))

A tournament T of order v is **doubly regular** with parameters (v, k, λ, μ) if

- T is k-regular,
- any two adjacent vertices have λ common out-neighbours,
- and each of these two vertices has additional μ out-neighbours which are not common to them.

Association scheme

Definition

Let X be a finite set of size $v \geq 2$. A **two-class association scheme** on X is a sequence of three binary relations R_0, R_1, R_2 defined on X which satisfy:

1. $X \times X = R_0 \cup R_1 \cup R_2$, $R_i \cap R_j = \emptyset$ for $i \neq j$, $i,j = 0,1,2$,
2. $R_0 = \{(x,x) \mid x \in X\}$,
3. for every $i \in \{0,1,2\}$, there exists $j \in \{0,1,2\}$ such that $R_i^T = R_j$, where $R_i^T = \{(y,x) \mid (x,y) \in R_i\}$,
4. for any triple i,j,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 which does not depend on the choice of x and y that satisfy $(x,y) \in R_k$.
5. $p_{ij}^k = p_{ji}^k$, for all $i,j,k \in \{0,1,2\}$.

Association scheme

The relations $R_i,\ i = 0, 1, 2$, of an association scheme can be described by their adjacency matrices $A_i,\ i = 0, 1, 2$, whose rows and columns are indexed by the elements of X and whose entries satisfy

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

We have two cases:

1. $A_1^T = A_1$ and $A_2^T = A_2$ in which case the undirected graph (X, R_1) is a strongly regular graph.
2. $A_1^T = A_2$ and $A_2^T = A_1$ in which case the directed graph (X, R_1) is a doubly regular tournament.

Self-dual codes from two-class association schemes

- S. T. Dougherty, J-L. Kim, P. Solé, Double circulant codes from two-class association schemes. Adv. Math. Commun. 1 (2007), 45-64.

LCD code

Definition

A **linear code with a complementary dual** (or an **LCD code**) is a linear code $\mathcal{C}$ whose dual code $\mathcal{C}^{\perp}$ satisfies $\mathcal{C} \cap \mathcal{C}^{\perp} = \{\emptyset\}$.

If $\mathcal{C}$ is an LCD code, then $\mathcal{C}^{\perp}$ is also an LCD code.

Lemma (Massey, 1992.)

Let G be a generator matrix for a code over a field. Then $\det(GG^{\top}) \neq 0$ if and only if G generates an LCD code.

LCD codes from two-class association schemes

- D. Crnković, A. Grbac, A. Švob, Formally self-dual LCD codes from two-class association schemes, Applicable Algebra in Engineering, Communication and Computing (2021), 1-18.

Constructions of LCD codes

Let A be the adjacency matrix of a graph G with v vertices, degree k, with parameters λ and μ.

1. G is an SRG $\Rightarrow A^T = A$
2. G is a DRT $\Rightarrow A^T = \overline{A} = J - I - A$

For arbitrary scalars $r, s, t \in \mathbb{F}_q$ let $Q_{\mathbb{F}_q}(r,s,t) = (rI + sA + t\overline{A})$.

The **pure** construction is

$$P_{\mathbb{F}_q}(r,s,t) = (I \mid Q_{\mathbb{F}_q}(r,s,t)).$$

The **bordered** construction is

$$B_{\mathbb{F}_q}(r,s,t) = \left(\begin{array}{c|c|c|c} 1 & 0\ldots 0 & \alpha & \beta\ldots\beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_{\mathbb{F}_q}(r,s,t) \\ 0 & & \gamma & \end{array}\right).$$

Pure construction

For the code $P_{\mathbb{F}_q}(r,s,t)$ to be LCD code we need $\det(P_{\mathbb{F}_q}P_{\mathbb{F}_q}^{\top}) \neq 0$.
It follows that

$$(I \mid Q_{\mathbb{F}_q}(r,s,t))(I \mid Q_{\mathbb{F}_q}(r,s,t))^T \neq \mathbf{0}.$$

We obtain that if we get

$$Q_{\mathbb{F}_q}(r,s,t)Q_{\mathbb{F}_q}(r,s,t)^T = (x-1)I\ ,\ x \neq 0,\ x \in \mathbb{F}_q.$$

Pure construction

Theorem

Let $r, s, t \in \mathbb{F}_q$ and let $Q_{\mathbb{F}_q} = (rI + sA + t\overline{A})$. Further, let $P_{\mathbb{F}_q}$ be an $n \times 2n$ matrix over $\mathbb{F}_q$, and suppose $P_{\mathbb{F}_q} = \left[\ I\ \middle|\ Q_{\mathbb{F}_q}(r,s,t)\ \right]$ generates a $[2n, n]$ code C over $\mathbb{F}_q$. The code $P_{\mathbb{F}_q}(r,s,t)$ formed from an $SRG(v,k,\lambda,\mu)$, with the adjacency matrix A, is an LCD code if $x \neq 0,\ x \in \mathbb{F}_q$ and

$$\begin{aligned} r^2 + s^2k - t^2 - t^2k + t^2v &= x - 1 \\ 2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2stk + t^2v - 2t^2k &= 0 \\ 2rt + s^2\mu - 2st\mu + t^2\mu + 2stk + t^2v - 2t^2 - 2t^2k &= 0\ . \end{aligned}$$

The code $P_{\mathbb{F}_q}(r,s,t)$ formed from a $DRT(v,k,\lambda,\mu)$, with the adjacency matrix A, is an LCD code if $x \neq 0,\ x \in \mathbb{F}_q$ and

$$\begin{aligned} r^2 + (s^2 + t^2)k &= x - 1 \\ rt + sr + (s^2 + t^2)(k - 1 - \lambda) + st\lambda + st\mu &= 0 \\ rt + sr + (s^2 + t^2)(k - \mu) + st\mu + st\lambda &= 0\ . \end{aligned}$$

Bordered construction

For the code $B_{\mathbb{F}_q}(r,s,t)$ to be LCD code we need $\det(B_{\mathbb{F}_q}B_{\mathbb{F}_q}^\top) \neq 0$.
We have that if $B_{\mathbb{F}_q}B_{\mathbb{F}_q}^\top$ is a diagonal matrix.
It follows that ($x \neq 0,\ y \neq 0, x, y \in \mathbb{F}_q$)

$$\begin{aligned} 1+\alpha^2+v\beta^2 &= y \\ \alpha\gamma+\beta(r+sk+t(v-k-1)) &= 0 \\ I+\gamma^2 J+Q_R(r,s,t)Q_R(r,s,t)^T &= xI. \end{aligned}$$

The third equation gives

$$Q_{\mathbb{F}_q}(r,s,t)Q_{\mathbb{F}_q}(r,s,t)^T = (x-1-\gamma^2)I - \gamma^2 A - \gamma^2\overline{A}.$$

Bordered construction

Theorem

Let $r, s, t \in \mathbb{F}_q$ *and let* $Q_{\mathbb{F}_q} = (rI + sA + t\overline{A})$*. Further, let* $B_{\mathbb{F}_q}$ *be an* $(n+1) \times (2n+2)$ *matrix over* $\mathbb{F}_q$ *and* α, β *and* γ *are scalars, and suppose*

$$B_{\mathbb{F}_q} = \left(\begin{array}{c|c|c|c} 1 & 0\dots0 & \alpha & \beta\dots\beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_{\mathbb{F}_q}(r,s,t) \\ 0 & & \gamma & \end{array}\right)$$

generates a $[2n+2, n+1]$ *code* C *over* $\mathbb{F}_q$*.*
The code $B_{\mathbb{F}_q}(r,s,t)$ *formed from an* $SRG(v,k,\lambda,\mu)$*, with the adjacency matrix* A*, is an LCD code if* $x \neq 0,\ y \neq 0$*,* $x, y \in \mathbb{F}_q$ *and*

Bordered construction

$$\begin{aligned} r^2 + s^2k - t^2 - t^2k + t^2v &= x - 1 - \gamma^2 \\ 2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2stk + t^2v - 2t^2k &= -\gamma^2 \\ 2rt + s^2\mu - 2st\mu + t^2\mu + 2stk + t^2v - 2t^2 - 2t^2k &= -\gamma^2 \\ 1 + \alpha^2 + v\beta^2 &= y \\ \alpha\gamma + \beta(r + sk + t(v - k - 1)) &= 0\ . \end{aligned}$$

The code $B_{\mathbb{F}_q}(r, s, t)$ formed from a DRT(v, k, λ, μ), with the adjacency matrix A, is an LCD code if $x \neq 0,\ y \neq 0, x, y \in \mathbb{F}_q$ and

$$\begin{aligned} r^2 + (s^2 + t^2)k &= x - 1 - \gamma^2 \\ rt + sr + (s^2 + t^2)(k - 1 - \lambda) + st\lambda + st\mu &= -\gamma^2 \\ rt + sr + (s^2 + t^2)(k - \mu) + st\mu + st\lambda &= -\gamma^2 \\ 1 + \alpha^2 + v\beta^2 &= y \\ \alpha\gamma + \beta(r + sk + t(v - k - 1)) &= 0\ . \end{aligned}$$

LCD codes over the fields $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$

We simplified the preceding conditions and we gave conditions for constructing LCD codes over the fields $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$.

We constructed LCD codes from some families of strongly regular graphs and from some doubly regular tournaments.

LCD codes from SRGs over $\mathbb{F}_2$

Over $\mathbb{F}_2$, for SRGs we obtain

$$Q_{\mathbb{F}_2}(r,s,t)Q_{\mathbb{F}_2}(r,s,t)^T = (r+sk+t+tk+tv)I + (s\lambda+t\lambda+tv)A + (s\mu+t\mu+tv)\overline{A}.$$

We use this to examine when the construction gives LCD codes.

Table: Conditions for constructing LCD codes from SRGs over the field $\mathbb{F}_2$

r	s	t	Pure construction	Bordered construction
0	0	1	$v=\lambda=\mu=1+k$	$\lambda=\mu,\ \gamma=1+k+v$
0	1	0	$k=\lambda=\mu=0$	$k=\lambda=\mu=\gamma$
0	1	1	Never	Never
1	0	0	Never	Never
1	0	1	$\lambda=\mu=v=k$	$k=\lambda=\mu=v+\gamma$
1	1	0	$k=1,\ \lambda=\mu=0$	$\lambda=\mu=\gamma=k+1$
1	1	1	$v=0$	$v=\gamma$

For the bordered case, additionally it must satisfy the necessary conditions given for α and β: $\alpha+v\beta=0,\ \alpha\gamma+\beta\gamma=0$.
In the table all equalities are given in $\mathbb{F}_2$.

LCD codes from DRTs over $\mathbb{F}_2$

Over $\mathbb{F}_2$, for DRTs we obtain

$$\begin{aligned} Q_R(r,s,t)Q_R(r,s,t)^T &= (r+(s+t)k)I \\ &+ (rt+sr+(s+t)(k-1-\lambda)+st\lambda+st\mu)A \\ &+ (rt+sr+(s+t)(k-\mu)+st\mu+st\lambda)\overline{A}. \end{aligned}$$

Lemma

If Γ is a DRT with parameters (v,k,λ,μ), then $v=4\lambda+3$, $k=2\lambda+1$ and $\mu=\lambda+1$.

Table: Conditions for constructing LCD codes from DRTs over the field $\mathbb{F}_2$

r	s	t	Pure construction	Bordered construction
0	0	1	$k=0,\ \lambda=1$	$k=\gamma,\ \lambda=1$
0	1	0	$k=0,\ \lambda=1$	$k=\gamma,\ \lambda=1$
0	1	1	Never	Never
1	0	0	Never	$\gamma=1$
1	0	1	$k=\lambda=1$	$k=\gamma+1,\ \lambda=1$
1	1	0	$k=\lambda=1$	$k=\gamma+1,\ \lambda=1$
1	1	1	Never	Never

LCD codes from SRGs

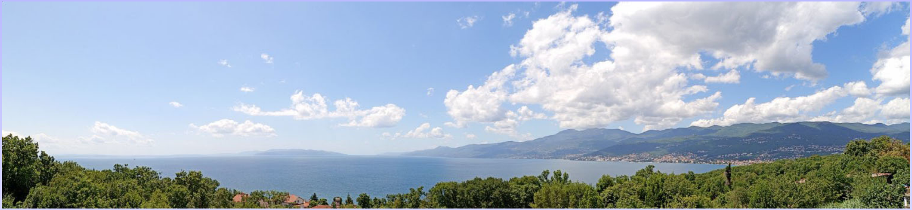
We constructed LCD codes from some families of strongly regular graphs: line graphs of complete graphs and bipartite complete graphs, some notable graphs such as the Petersen, Shrikhande, Clebsch, Hoffman-Singleton and Gewirtz graph and the Chang graphs, block graphs of Steiner triple systems, graphs obtained from orthogonal arrays and rank three permutation groups.

Graph	LCD codes	Parameters	Remark
$L(K_6)$	$B_{\mathbb{F}_2}(0,0,1)$	$[32,16,7]$	near-optimal
SRG$(15,8,4,4)$	$P_{\mathbb{F}_3}(a,0,a)$	$[30,15,8]$	
$L(K_{2,2})$	$P_{\mathbb{F}_3}(a,a,b)$, $P_{\mathbb{F}_3}(a,b,b)$	$[8,4,4]$	optimal
SRG$(4,2,0,2)$	$B_{\mathbb{F}_3}(a,a,0)$	$[10,5,4]$	near-optimal
Clebsch graph	$P_{\mathbb{F}_2}(1,0,1)$	$[32,16,8]$	optimal
SRG$(16,10,6,6)$	$B_{\mathbb{F}_2}(1,0,1)$	$[34,17,7]$	near-optimal

LCD codes from DRTs

We constructed LCD codes from DRTs of order $n = 4\lambda + 3$, $\lambda = 0, 1, \ldots, 8$.

DRT	LCD codes	Parameters	Remark
$(3,1,0,1)$	$B_{\mathbb{F}_3}(a,a,b), B_{\mathbb{F}_3}(a,b,a)$	$[8,4,4]$	optimal
	$B_{\mathbb{F}_3}(a,b,b)$	$[8,4,4]$	optimal
$(7,3,1,2)$	$P_{\mathbb{F}_3}(a,b,0), P_{\mathbb{F}_3}(a,0,b)$	$[14,7,5]$	near-optimal
	$B_{\mathbb{F}_3}(0,a,b)$	$[16,8,6]$	optimal
$(11,5,2,3)$	$B_{\mathbb{F}_3}(a,a,b), B_{\mathbb{F}_3}(a,b,a)$	$[24,12,6]$	
	$B_{\mathbb{F}_3}(0,a,0), B_{\mathbb{F}_3}(0,0,a)$	$[24,12,6]$	
$(15,7,3,4)$	$B_{\mathbb{F}_3}(a,a,b), B_{\mathbb{F}_3}(a,b,a)$	$[32,16,8]$	
	$B_{\mathbb{F}_3}(0,0,a)$	$[32,16,8]$	
$(19,9,4,5)$	$P_{\mathbb{F}_3}(a,b,0), P_{\mathbb{F}_3}(a,0,b)$	$[38,19,10]$	
	$B_{\mathbb{F}_3}(0,a,b)$	$[40,20,10]$	



Thank you for your attention!