Self-orthogonal and LCD subspace codes

Dean Crnković

Faculty of Mathematics
University of Rijeka
Croatia

(joint work with Keita Ishizuka, Hadi Kharaghani, Sho Suda and Andrea Švob)

8th Workshop on Design Theory, Hadamard Matrices and Applications (Hadamard 2025)
Seville, Spain, May 2025

This work was supported by the Croatian Science Foundation under the project number HRZZ–IP–2022–10–4571.

Most of the talk is based on the results presented in the paper

1. D. Crnković, K. Ishizuka, H. Kharaghani, S. Suda, A. Švob, Constructions of self-orthogonal and LCD subspace codes, preprint, arXiv:2407.05695.
2. D. Crnković, A. Švob, LCD subspace codes, Des. Codes Cryptogr. 91 (2023), 3215–3226,

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

For $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbf{F}_q^n$ the number $d(x, y) = |\{i \,|1 \leq i \leq n,\, x_i \neq y_i\}|$ is called a Hamming distance. The **minimum distance** of a code C is $d = min\{d(x, y)\,|x, y \in C, x \neq y\}$.

A linear $[n, k, d]_q$ code is a linear $[n, k]$ code over $\mathbf{F}_q$ with the 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 linear code C is called **self-orthogonal** if $C \subseteq C^\perp$ and **self-dual** if $C = C^\perp$.

A linear code C over $\mathbb{F}_q$ is called a **Euclidean** or **classical linear complementary dual code** (shortly **LCD code**) if $C \cap C^\perp = \{0\}$.

Let G be a generator matrix for a q-ary linear code C. The code C is self-orthogonal if and only if $GG^\top = O$ over the finite field $\mathbb{F}_q$, where O denotes the zero matrix.

An $[n, k]$ code C is self-dual if and only if it is self-orthogonal and $k = \frac{n}{2}$.

There is many research dealing with self-orthogonal codes.

LCD codes were introduced by Massey in 1992.

- J. L. Massey, Linear codes with complementary duals, Discrete Math. 106/107 (1992), 337–342.

Massey showed that that the nearest-codeword (or maximum-likelihood) decoding problem for an LCD code C reduces to a simpler problem: given a word in $C^{\perp}$, find the nearest codeword in C.

Massey also showed that asymptotically good LCD codes exist and that LCD codes provide an optimum linear coding solution for the two-user binary adder channel.

The following characterization of LCD codes is also given by Massey.

Let G be a generator matrix of a linear code C over a finite field. Then C is an LCD code if and only if $\det(GG^\top) \neq 0$.

LCD codes can be used to protect systems against side channel attacks (SCA) and fault injection attacks (FIA).

It was shown by Sendrier in 2004 that LCD codes meet the asymptotic Gilbert-Varshamov bound.

A multisecret-Sharing scheme based on LCD codes was introduced in 2020 by A. Alahmadi et al.

In 2018 Carlet et al. showed that for $q > 3$, the existence of an $[n, k, d]_q$ linear code implies the existence of an $[n, k, d]_q$ LCD code.

In 2000, Ahlswede, Cai, Li and Yeung introduced **network coding**. A network is a directed graph which consists of source vertices, inner vertices and sink vertices. The source vertices transmit messages to the sink vertices through a channel of inner vertices. A receiver sees the data packets and deduces from them the messages that were originally intended for the sinks.

Mixing of data is allowed at the network vertices. A special case arises when the packets are interpreted as vectors of symbols from a finite field, and the mixing functions are linear transformations. This is the case of **linear network coding**.

In 2006, Ho, Médard, Kötter, Karger, Effros, Shi and Leong demonstrated that the so-called multicast capacity of a network is achieved, with high probability in a sufficiently large field, by a random choice of local mixing functions. In that way, **random network coding** was introduced.

Since the linear transformation by the channel of the transmitted vectors is not known in advance by the transmitter or any of the receivers, such a model is sometimes referred to as a **non-coherent transmission model.**

In 2008, in their seminal, paper Kötter and Kschischang considered information transmission not via the transmitted vectors, but rather by the vector space that they span. These types of codes are called **subspace codes**.

Kötter and Kschischang proved that subspace codes are efficient for transmission in networks and because of their applications in error correction for random network coding they attract a wide attention in recent research.

A **subspace code** C_S is a nonempty set of subspaces of $\mathbb{F}_q^n$.

A **subspace distance** is given by

$$d_s(U, W) = dim(U + W) - dim(U \cap W),$$

where $U, W \leq \mathbb{F}_q^n$. The **minimum distance** of C_S is given by

$$d = min\{d_S(U, W)|\ U, W \in C_S, U \neq W\}.$$

A subspace code C_S in $\mathbb{F}_q^n$ is called an $(n, \#C_S, d; K)_q$ subspace code if the dimensions of the codewords of C_S are contained in a set $K \subseteq \{0, 1, 2, ..., n\}$.

In the case $K = \{k\}$, a subspace code C_S is called a **constant dimension code** with the parameters $(n, \#C_S, d; k)_q$.

Otherwise, *i.e.* if all codewords do not have the same dimension, C_S is called a **mixed dimension code**. Such subspace code is denoted by $(n, \#C_S, d)_q$.

The **injection distance**, introduced in 2008 by Kötter, Kschischang and Silva, is given as follows

$$d_I(U, W) = \max\{\dim(U), \dim(W)\} - \dim(U \cap W).$$

If $\dim(U) = \dim(W)$, then $d_S(U, W) = d_I(U, W)$. So, for constant dimension codes $d_S = d_I$.

An useful overview of subspace codes is given in

- M. Greferath, M. O. Pavčević, N. Silberstein, M. Vázquez-Castro (eds.), Network coding and subspace designs, Signals and Communication Technology, Springer, Cham, 2018.

As an analog of the definition of an LCD linear code we introduce the definition of an LCD subspace code.

Definition 1

Let $\mathcal{P}_q(n)$ be the set of all subspaces of $\mathbb{F}_q^n$, and let $C_S \subseteq \mathcal{P}_q(n)$ be a subspace code. If $C_i \cap C_j^{\perp} = \{0\}$, for all $C_i, C_j \in C_S$, then C_S is called an **LCD subspace code**.

Each codeword of an LCD subspace code C_S is an LCD code, since for every $C_i \in C_S$ it holds that $C_i \cap C_i^{\perp} = \{0\}$.

The following theorem generalizes the Massey's characterization of LCD codes.

Theorem 1 [DC, A. Švob, 2023]

Let C_1 and C_2 be $[n, k]$ codes over the field $\mathbb{F}_q$, and let G_1 and G_2 be their generator matrices, respectively. If the matrix $G_2 G_1^\top$ is nonsingular, then $C_2 \cap C_1^\perp = C_1 \cap C_2^\perp = \{0\}$.

We use this property for a construction of LCD subspace codes.

In his paper from 1992 Massey gave a decoding method for LCD codes. We propose a decoding algorithm for LCD subspace codes based on the following property.

If $X \leq V$ such that $X \cap X^{\perp} = \{0\}$ and $Y \leq V$, then

$$\dim(X + Y) = \dim(X) + \dim(\pi_{X^{\perp}}(Y)).$$

Further, if $Y = \langle y_1, \ldots, y_k \rangle$ then

$$\pi_{X^{\perp}}(Y) = \langle \pi_{X^{\perp}}(y_1), \ldots, \pi_{X^{\perp}}(y_k) \rangle .$$

Let $C \leq \mathbb{F}_q^n$. Using the formula given in the following theorem we can calculate distances between C and the elements of an LCD subspace code $\{C_1, \dots C_m\}$.

Theorem 2 [DC, A. Švob, 2023]

Let $\{C_1, \dots C_m\}$ be an LCD subspace code and let $C \leq \mathbb{F}_q^n$. Then,

$$d_s(C_i, C) = \dim(C_i) + 2\dim(\pi_{C_i^\perp}(C)) - \dim(C). \qquad (1)$$

Proof.

Since

$$\dim(C_i + C) = \dim(C_i) + \dim(C) - \dim(C_i \cap C)$$

and

$$\dim(C_i + C) = \dim(C_i) + \dim(\pi_{C_i^\perp}(C)),$$

the following holds

$$\dim(C_i \cap C) = \dim(C) - \dim(\pi_{C_i^\perp}(C)).$$

Since

$$d_s(C_i, C) = \dim(C_i + C) - \dim(C_i \cap C),$$

the formula (1) holds. □

Remark 1

Let $C_S = \{C_1, \dots C_m\}$ be an LCD subspace code. Suppose that a codeword (subspace) $C_i = \langle x_1^i, x_2^i, \dots, x_k^i \rangle$ is sent through a noisy channel, and the subspace $C = \langle x_1, x_2, \dots, x_k \rangle$ is received. Calculate the distance between C and $C_i \in C_S$ as follows

$$d_s(C_i, C) = \dim(C_i) + 2\dim(\pi_{C_i^\perp}(C)) - \dim(C),$$

where

$$\dim(\pi_{C_i^\perp}(C)) = \dim(\langle \pi_{C_i^\perp}(x_1), \pi_{C_i^\perp}(x_2), \dots, \pi_{C_i^\perp}(x_k) \rangle).$$

Note that a minimum distance decoder for subspace codes chooses the closest codeword to the received word with respect to the subspace distance. If there is more than one closest codeword, the decoder returns "failure".

Let X be a finite set. An **association scheme** with d classes is a pair $(X, \mathcal{R})$ such that

1. $\mathcal{R} = \{R_0, R_1, \ldots, R_d\}$ is a partition of $X \times X$,
2. $R_0 = \triangle = \{(x, x) | x \in X\}$,
3. $R_i = R_i^\top$ (*i.e.* $(x, y) \in R_i \Rightarrow (y, x) \in R_i$) for all $i \in \{0, 1, \ldots, d\}$,
4. there are numbers p_{ij}^k (the intersection numbers of the scheme) such that for any pair $(x, y) \in R_k$ the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ equals p_{ij}^k.

The relations R_i, $i \in \{0, 1, \ldots, d\}$, of an association scheme can be described by the set of symmetric $(0,1)$-adjacency matrices $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$, $A_i = [a^i_{x,y}]$ for $i = 0, 1, \ldots, d$, where $a^i_{xy} = 1$ if $(x, y) \in R_i$. The matrices $\{A_0, A_1, \ldots, A_d\}$ satisfy

$$A_i A_j = \sum_{k=0}^{d} p^k_{i,j} A_k = A_j A_i. \tag{2}$$

Each of the matrices A_i, $i \in \{1, 2, \ldots, d\}$, represents a simple graph Γ_i on the set of vertices X (vertices x and y are adjacent in Γ_i if and only if $(x, y) \in R_i$).

Theorem 3 [DC, A. Švob, 2023]

Let $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$ be the set of $n \times n$ adjacency matrices of a d-class association scheme $(X, \mathcal{R})$. Further, let $I = \{i_1, i_2, \ldots, i_s\} \subseteq \{0, 1, \ldots, d\}$ and $p | p_{i,j}^k$, for all $k \in \{0, 1, \ldots, d\}$ and all $i, j \in I$, where p is a prime number. Then the set of row spaces of the matrices $N_x = \left[\begin{array}{c|c} X & \alpha_x I_n \end{array} \right]$, $\alpha_x \in \mathbb{F}_q \setminus \{0\}$, where X is a nonzero element of the linear space spanned by the matrices A_i, $i \in I$, forms an LCD subspace code $C_S \subseteq \mathbb{F}_q^{2n}$, for some positive integer r after $q = p^r$.

Proof.

For two matrices N_x and N_y, the matrix $N_x N_y^\top = \alpha_x \alpha_y I_n$ is nonsingular. Theorem 1 leads us to the conclusion that C_S is an LCD subspace code. □

Let us consider a square $n \times n$ real matrix A whose rows and columns are indexed by elements of $X = \{1, 2, \ldots, n\}$. Let $\Pi = \{X_1, X_2, \ldots, X_t\}$ be a partition of X. We partition the matrix A according to Π as $A = [A_{ij}]$, $1 \leq i, j \leq t$.

If q_{ij} denotes the average row sum of A_{ij} then the matrix $Q = [q_{ij}]$ is called a **quotient matrix** of A.

If the row sum of each block A_{ij} is a constant then the partition Π is called **row equitable**. Similarly, if the column sum of each block A_{ij} is a constant then the partition Π is called **column equitable**.

If Π is both row and column equitable, then Π is said to be **equitable**.

If A is an adjacency matrix of a graph Γ and Π is an equitable partition of A, then we say that Π is an equitable partition of the graph Γ. An equitable (or regular) partition of an association scheme $(X, \mathcal{R})$ with d classes is a partition of X which is equitable with respect to each adjacency matrix of the graphs Γ_i, $i \in \{1, 2, \ldots, d\}$, corresponding to the association scheme $(X, \mathcal{R})$.

We use the following result by C. D. Godsil, W. J. Martin in order to prove Theorem 5.

Theorem 4

Let Π be an equitable partition of a d-class association scheme $(X, \mathcal{R})$ with t cells, and let M_i, $i = 0, 1, \ldots, d$, denote the quotient matrix of the graph Γ_i with respect to Π. Then

$$M_i M_j = \sum_{k=0}^{d} p_{i,j}^k M_k = M_j M_i,$$

where integers p_{ij}^k are the intersection numbers of the scheme.

Theorem 5 [DC, A. Švob, 2023]

Let Π be an equitable partition of a d-class association scheme $(X, \mathcal{R})$ with t cells of the same length $\frac{|X|}{t}$, $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$ be the set of adjacency matrices of $(X, \mathcal{R})$, and let M_i denote the corresponding quotient matrix of A_i with respect to Π. Further, let $I = \{i_1, i_2, \ldots, i_s\} \subseteq \{0, 1, \ldots, d\}$ and $p | p_{i,j}^k$, for all $k \in \{0, 1, \ldots, d\}$ and all $i, j \in I$, where p is a prime number. Then the set of row spaces of the matrices $N_x = \left[\begin{array}{c|c} X & \alpha_x I_t \end{array} \right]$, $\alpha_x \in \mathbb{F}_q \setminus \{0\}$, where X is a nonzero element of the linear space spanned by the matrices M_i, $i \in I$, forms an LCD subspace code $C_S \subseteq \mathbb{F}_q^{2t}$, for some positive integer r after $q = p^r$.

Theorem 5 is a generalization of Theorem 3.

Example

A graph Γ with diameter d is called **distance-regular** if the distance relations of Γ give the relations of a d-class association scheme.

Theorem 5 can be applied to the association scheme corresponding to a distance-regular graph. The action of an automorphism group of a distance-regular graph on the set of vertices induces an equitable partition of the association scheme.

For example, from a distance-regular graph having 200 vertices, diameter $d = 5$, and the intersection array $\{22, 21, 16, 6, 1; 1, 6, 16, 21, 22\}$ known as Doubled Higman-Sims graph, we constructed LCD subspace codes with parameters $(20, 16, 2; 10)_2$ and $(40, 5, 2; 20)_2$.

Two Hadamard matrices H and K of order n are called **unbiased** if $HK^\top = \sqrt{n}L$, where L is a Hadamard matrix of order n. Unbiased Hadamard matrices exist only in square orders.

If $\{H_1, H_2, \ldots, H_m\}$ is a set of mutually unbiased Hadamard matrices of order $2n$, then $m \leq n$. That was shown in 2010 by W. H. Holzmann, H. Kharaghani, W. Orrick.

By a result of P. J. Cameron and J. J. Seidel from 1973, this upper bound is attained for Hadamard matrices of order 4^k.

Theorem 6 [DC, A. Švob, 2023]

Let $\{H_1, H_2, \ldots, H_m\}$ be **a set of mutually unbiased Hadamard matrices of order** n. Further, **let** p **be a prime number dividing** $\sqrt{n}$ and $\mathbb{F}_q$ be the finite field of order q, where $q = p^r$. Then the set of row spaces of the matrices $N_x = \left[\begin{array}{c|c} X & \alpha_x I_n \end{array} \right]$, $\alpha_x \in \mathbb{F}_q \setminus \{0\}$, where X is a nonzero element of the linear space spanned by the matrices H_i, $i = 1, 2, \ldots, m$, forms an LCD subspace code $C_S \subseteq \mathbb{F}_q^{2n}$.

Proof.

For matrices H_i and H_j, $1 \leq i, j \leq m$, $i \neq j$, iz holds that $H_i H_i^\top = H_j H_j^\top = nI_n$ and $H_i H_j^\top = \sqrt{n}L$, where L is a Hadamard matrix. Hence, for two matrices N_x and N_y, the matrix $N_x N_y^\top = \alpha_x \alpha_y I_n$ is a nonsingular matrix. C_S is an LCD subspace code. □

Weighing matrices are a generalization of Hadamard matrices. A matrix $W = [w_{ij}]$ of order n and $w_{ij} \in \{-1, 0, 1\}$ is called a **weighing matrix** with weight k, if $WW^\top = kI_n$. If $k = n$, then $WW^\top = nI_n$ and the weighing matrix W is a Hadamard matrix.

Two weighing matrices W_1 and W_2 of order n and weight k are called **unbiased**, if $W_1 W_2^\top = \sqrt{k}W$, where W is a weighing matrix of order n and weight k.

Theorem 7 [DC, A. Švob, 2023]

Let $\{W_1, W_2, \ldots, W_m\}$ be a set of mutually unbiased weighing matrices of order n and weight k. Further, let p be a prime number dividing $\sqrt{k}$ and $\mathbb{F}_q$ be the finite field of order q, for some positive integer r after $q = p^r$. Then the set of row spaces of the matrices $N_x = \left[\begin{array}{c|c} X & \alpha_x I_n \end{array} \right]$, $\alpha_x \in \mathbb{F}_q \setminus \{0\}$, where X is a nonzero element of the linear space spanned by the matrices W_i, $i = 1, 2, \ldots, m$, forms an LCD subspace code $C_S \subseteq \mathbb{F}_q^{2n}$.

Example

From mutually unbiased weighing matrices of order 16 and weight nine $\{W_1, W_2, W_3, K\}$ constructed in

- W. H. Holzmann, H. Kharaghani, W. Orrick, On the real unbiased Hadamard matrices, in: R. A. Brualdi, S. Hedayat, H. Kharaghani, G. B. Khosrovshahi, S. Shahriari (eds), Combinatorics and graphs, Contemp. Math. 531, Amer. Math. Soc., Providence, RI, 2010, 243–250,

by applying Theorem 7 we obtained LCD subspace code with parameters $(32, 81, 6; 16)_3$ and its subcode with parameters $(32, 27, 8; 16)_3$.

An equitable partition of the set $\{W_1, W_2, \ldots, W_m\}$ of mutually unbiased weighing matrices is a partition $\Pi = \{C_1, C_2, \ldots, C_t\}$ of X which is equitable with respect to each of the matrices W_i, $i = 1, 2, \ldots, m$.

Let W_1 and W_2 be unbiased weighing matrices of order n and weight k. Further, let Π be an equitable partition of the set $\{W_1, W_2\}$ with t cells of the same length $\frac{n}{t}$, and let C be the characteristic matrix of Π. It holds that

$$M_1 M_2^\top = (C^\top C)^{-1} C^\top C C^\top \sqrt{k} L C (C^\top C)^{-1}.$$

Hence, the following theorem holds.

Theorem 8 [DC, A. Švob, 2023]

Let $S = \{W_1, W_2, \ldots, W_m\}$ be a set of mutually unbiased weighing matrices of order n and weight k. Further, let Π be an equitable partition of the set S, with t cells of the same length $\frac{n}{t}$, and let M_i denote the corresponding quotient matrix of W_i with respect to Π, $i = 1, 2, \ldots, m$. Let p be a prime number dividing $\sqrt{k}$. Then the set of row spaces of the matrices $N_x = \left[\begin{array}{c|c} X & \alpha_x I_t \end{array} \right]$, $\alpha_x \in \mathbb{F}_q \setminus \{0\}$, where X is a nonzero element of the linear space spanned by the matrices $M_1, M_2, \ldots, M_m$, forms an LCD subspace code $C_S \subseteq \mathbb{F}_q^{2t}$, for some positive integer r after $q = p^r$.

Clearly, Theorem 8 applies to Hadamard matrices.

The following theorem generalizes the above given constructions.

Theorem 9 [DC, K. Ishizuka, H. Kharaghani, S. Suda, A. Švob, 202?]

Let $S = \{M_1, M_2, \ldots, M_m\}$ be a set of integer square matrices of order n, and let p be a prime number dividing the entries of $M_i M_j^\top$ for any $i, j \in \{1, 2, \ldots, m\}$. Further, let Π be an equitable partition of the set S, with t cells of the same length $\frac{n}{t}$, and let M_i' denote the corresponding quotient matrix of M_i with respect to Π, $i = 1, 2, \ldots, m$.
Let $\mathbb{F}_q$ be the finite field of order q with characteristic p. Then the set of row spaces of the matrices $N_x = \left[\begin{array}{c|c} X & \alpha_x I_t \end{array} \right]$, $\alpha_x \in \mathbb{F}_q \setminus \{0\}$, where X is a nonzero element of the linear space spanned by the matrices $M_1', M_2', \ldots, M_m'$, forms an LCD subspace code $\mathcal{C} \subseteq \mathbb{F}_q^{2t}$.

Using Theorem 9, we also constructed LCD subspace codes from

- mutually quasi-unbiased weighing matrices,
- orthogonal designs,
- linked system of symmetric designs,
- linked system of symmetric group divisible designs,
- linked system of symmetric group divisible designs of type II,
- Deza digraphs of type II,

and their quotient (orbit) matrices.

Definition 2

Let $\mathcal{P}_q(n)$ be the set of all subspaces of $\mathbb{F}_q^n$. The *dual* code of a subspace code $C_S \subseteq \mathcal{P}_q(n)$ is the set $C_S^\perp$ of all vector spaces in $\mathcal{P}_q(n)$ that are orthogonal to each vector space in C_S. If $C_S \subseteq C_S^\perp$, then C_S is called a **self-orthogonal** subspace code.

The following theorem is a counterpart to Theorem x.

Theorem 10 [DC, K. Ishizuka, H. Kharaghani, S. Suda, A. Švob, 202?]

Let $S = \{M_1, M_2, \ldots, M_m\}$ be a set of integer square matrices of order n, and let p be a prime number dividing the entries of $M_i M_j^\top$ for any $i, j \in \{1, 2, \ldots, m\}$. Further, let Π be an equitable partition of the set S, with t cells of the same length $\frac{n}{t}$, and let M_i' denote the corresponding quotient matrix of M_i with respect to Π, $i = 1, 2, \ldots, m$.
Let $\mathbb{F}_q$ be the finite field of order q with characteristic p. Then the set of row spaces of the nonzero elements of the linear space spanned by the matrices $M_1', M_2', \ldots, M_m'$ forms a self-orthogonal subspace code $\mathcal{C} \subseteq \mathbb{F}_q^t$.

By applying Theorem 10, we constructed self-orthogonal subspace codes from

- association schemes,
- mutually (quasi-)unbiased weighing matrices,
- orthogonal designs,
- linked system of symmetric designs,
- linked system of symmetric group divisible designs,
- linked system of symmetric group divisible designs of type II,
- Deza digraphs of type II,

and their quotient (orbit) matrices.

Happy birthday Rob!

Happy birthday Dane!