Constructing doubly even self-dual codes from Hadamard matrices

Dean Crnković

Faculty of Mathematics
University of Rijeka
Croatia

Joint work with Andrea Švob

Combinatorial Designs and Codes
Satellite event of the 9th European Congress of Mathematics
Sevilla, Spain, July 2025

This work has been fully supported by Croatian Science Foundation under the project 4571.

The talk is based on the results presented in the paper

- D. Crnković, A. Švob, Constructing doubly even self-dual codes and even unimodular lattices from Hadamard matrices, Appl. Algebra Engrg. Comm. Comput., to appear.

A **Hadamard matrix** of order n is a $n \times n$ $\{\pm 1\}$ matrix H such that $HH^{\top} = nI_n$. A Hadamard matrix of order n can exist only if n $= 1$, 2 or $n \equiv 0 \mod 4$. The Hadamard conjecture states that these necessary conditions are also sufficient. Since the discovery of a Hadamard matrix of order 428, the smallest open case is $n =$ 668.

A matrix A is skew-symmetric if $A^T = -A$. A Hadamard matrix H of order $4k$ is **skew-type** if $H = A + I_{4k}$, where $A^T = -A$. It was conjectured by J. Seberry that a skew-type Hadamard matrix exists if and only if n=1,2, or $4k$, where k is a positive integer (smallest open case $4k = 276$).

A $t-(v,k,\lambda)$ **design** is a finite incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},\mathcal{I})$ satisfying the following requirements:

1. $|\mathcal{P}|=v$,
2. every element of $\mathcal{B}$ is incident with exactly k elements of $\mathcal{P}$,
3. every t elements of $\mathcal{P}$ are incident with exactly λ elements of $\mathcal{B}$.

Every element of $\mathcal{P}$ is incident with exactly r elements of $\mathcal{P}$. The number of blocks is denoted by b.
If $|\mathcal{P}|=|\mathcal{B}|$ (or equivalently $k=r$) then the design is called **symmetric**.

The existence of a symmetric design with parameters $(4n-1, 2n-1, n-1)$ is equivalent to the existence of a Hadamard matrix of order $4n$. Such a symmetric design is called a **Hadamard 2-design**.

A $(0,1)$-matrix D is skew if $D+D^T$ is a $(0,1)$-matrix. A skew-type Hadamard matrix corresponds to a Hadamard 2-design with the skew incidence matrix, and vice versa.

Any 3-design with parameters 3-$(4t, 2t, t-1)$ is called a **Hadamard** 3-**design**, since it is related to a Hadamard matrix of order $4t$.

A q-ary linear code of length n, dimension k, and minimum distance d is called a $[n, k, d]_q$ code.

The **dual** code $C^\perp$ is the orthogonal complement under the standard inner product $\langle \cdot \, , \cdot \rangle$.

A code C is **self-orthogonal** if $C \subseteq C^\perp$ and **self-dual** if $C = C^\perp$.

The **weight** of a codeword x, denoted by $w(x)$, is its distance from the zero vector.

A code for which all codewords have weight divisible by four is called **doubly-even**, and **singly even** if all weights are even and there is at least one codeword x with $w(x) \equiv 2 \mod 4$.

Theorem 1 [M. Harada, K. Saito, 2018]

A doubly even self-dual code of length n exists if and only if $n \equiv 0 \mod 8$, while a singly even self-dual code of length n exists if and only if n is even.

The **binary code of a Hadamard matrix** H, denoted by $C_2(H)$, is the binary linear code spanned by the rows of the block-by-point incidence matrix of the 3-design defined by H.

Equivalent Hadamard matrices produce equivalent codes.

Alternatively, for a normalized Hadamard matrix H of order n, the binary code of H can be defined as the binary code generated by the row vectors of the binary Hadamard matrix $B = \frac{1}{2}(H + J_n)$ associated to H.

Let $\mathbb{R}^m$ be an m-dimensional Euclidean space with the standard inner product $\langle \cdot , \cdot \rangle$.

An n-**dimensional lattice** L in $\mathbb{R}^m$ is a free $\mathbb{Z}$-module spanned by n linearly independent vectors $v_1, v_2, \ldots, v_n$, called a **basis** of the lattice.

An $n \times m$ matrix M whose rows are the vectors $v_1, v_2, \ldots, v_n$ is called a generator matrix of L.

We say that the **rank** of the lattice L is n and its **dimension** is m. If $n = m$, the lattice is called a full-rank lattice.

In this talk, we will consider full-rank lattices.

The **dual lattice** of L is $L^* = \{x \in \mathbb{R}^n : \langle x, a \rangle \in \mathbb{Z}, \text{ for all } a \in L\}$.

An **unimodular lattice** L is an integral lattice which is its own dual.

In other words, $\det L = \det(MM^\top) = 1$ and $\langle u, v \rangle$ is an integer for all $u, v \in L$.

If the norm $\langle x, x \rangle$ is even integer for all $x \in L$, then the lattice L is called **even**. Unimodular lattices which are not even are called **odd**.

The **minimum norm** of a lattice L is the smallest norm among all nonzero vectors of L.

- E. Bannai, S. T. Dougherty, M. Harada, M. Oura, Type II codes, even unimodular lattices, and invariant rings, IEEE Trans. Inform. Theory 45 (1999), 1194–1205.

Construction A

Let C be a binary self-dual code of length n. Further, let $\varphi : \mathbb{Z} \to \mathbb{F}_2^n$ be a mapping such that $\varphi(x) = x \mod 2$. Then the lattice

$$L_C = \frac{1}{\sqrt{2}}\{x \in \mathbb{Z}^n : \varphi(x) \in C\}$$

is an unimodular lattice of rank n. If C is doubly even, then L_C is an even unimodular lattice. This construction of lattices is known as Construction A. The minimum norm of L_C is 2.

- T. Miezaki, Design-theoretic analogies between codes, lattices, and vertex operator algebras, Des. Codes Cryptogr. 89 (2021), 763–780.

A doubly even self-dual code of length $8t$ yields an even unimodular lattice of rank $8t$ (Construction A).

Even unimodular lattices yield holomorphic vertex operator algebras.

This Miezaki's paper motivated us to construct doubly even self-dual codes from Hadamard matrices.

- M. Hall Jr., Combinatorial Theory, second ed., Wiley, New York, 1986.

The binary code of a Hadamard matrix of order n is doubly even self-dual if $n \equiv 8 \mod 16$.

- A. Munemasa, H. Tamura, The codes and the lattices of Hadamard matrices, European J. Combin. 33 (2012), 519–533.

Theorem 2

Let H be a normalized Hadamard matrix of order n, B the binary Hadamard matrix associated to H. Let $\ell \geq 2$ be an integer such that $4\ell|n$ and $(\ell, \frac{n}{4\ell}) = 1$. Then the row vectors of B generate a self-dual code over $\mathbb{Z}/\ell\mathbb{Z}$ of length n, which is type II if ℓ is even.

Note that a self-dual code over $\mathbb{Z}/2m\mathbb{Z}$ is called type II if the Euclidean norm of every codeword is divisible by $4m$.

- We study binary Hadamard codes, i.e. the case when $\ell = 2$.
- We construct type II (i.e. doubly even) self-dual codes even in cases when $(2, \frac{n}{8}) \neq 1$, i.e. when $n \equiv 0 \mod 16$, which is not the case covered by Theorem 2.

A Hadamard 3-design with parameters 3-$(4t, 2t, t-1)$ is quasi-symmetric with intersection numbers 0 and t.

Theorem 3 [DC, A Švob, 2023]

Let H be a Hadamard matrix of order $8t$. Then $C_2(H)$ is a doubly even self-orthogonal binary linear code of length $8t$.

It follows from Theorem 3 that in case $C_2(H)$ is a $[8t, 4t]_2$ code, then it is doubly even and self-dual.

The Hadamard matrix of order $4n$ obtained from a Paley design with parameters $(4q-1, 2q-1, q-1)$, where q is a prime power $\equiv 3 \mod 4$, is called a **Paley type I Hadamard matrix**.

- T. Beth, D. Jungnickel, H. Lenz, Design Theory: Volume 1, Cambridge University Press, Cambridge, 1999.

Theorem 4

Let $\mathcal{D}$ be the symmetric design belonging to a skew difference set D in an abelian group of order q, where q is a prime power $\equiv 3 \mod 4$. If p is a prime divisor of $m = \frac{q+1}{4}$, then $rank_p(\mathcal{D}) = 2m$.

The following corollary is a direct consequence of Theorems 3 and 4.

Corollary 5 [DC, A. Švob, 2023]

Let H be a Paley type I Hadamard matrix of order $8t$. Then $C_2(H)$ is a doubly even self-dual code of length $8t$.

Corollary 5 shows that a Paley type I Hadamard matrix of order $8t$ can be used to construct an even lattice of rank $8t$.

Theorem 6 [DC, A. Švob, 2023]

Let $\mathcal{D}$ be a Hadamard 2-design with parameters $(4t-1, 2t-1, t-1)$, having a skew incidence matrix M and M' is the incidence matrix of the complement of $\mathcal{D}$. Then

$$M_1 = \left[\begin{array}{c|cc} 0 & j_{4t-1}^{\top} & 0_{4t-1}^{\top} \\ \hline 0_{4t-1} & M & M + I_{4t-1} \\ j_{4t-1} & M & M' - I_{4t-1} \end{array}\right]$$

is the incidence matrix of a Hadamard 2-design $\mathcal{D}_1$ with parameters $(8t-1, 4t-1, 2t-1)$, and $rank_2(\mathcal{D}_1) = 4t$.

Remarks:

- Since Paley designs have skew incidence matrices, Theorem 6 can be applied to any Paley design.
- The matrix M_1 from Theorem 6 is skew, so we can apply Theorem 6 to the matrix M_1. Consequently, any Hadamard 2-design with parameters $(4t-1, 2t-1, t-1)$ having a skew incidence matrix yield a series of Hadamard 2-designs $\mathcal{D}_i$ with parameters $(2^{i+2}t-1, 2^{i+1}t-1, 2^{i}t-1)$ and $rank_2(\mathcal{D}_i) = 2^{i+1}t$, where i is any positive integer i.e. a series of doubly even self-dual binary codes of length $2^{i+2}t$ and even unimodular lattices of rank $2^{i+2}t$, where i is a positive integer.

Lemma 7 [DC, A. Švob, 2023]

A Hadamard 2-**design** $\mathcal{D}$ with parameters $(4t-1, 2t-1, t-1)$ having a skew incidence matrix exists if and only if there exists a **skew-type Hadamard matrix** of order $4t$.

As a consequence of Lemma 7, we have the following theorem.

Theorem 8 [DC, A. Švob, 2023]

Suppose that there exists a skew-type Hadamard matrix H of order $4t$. Then there exists a skew-type Hadamard matrix H_1 of order $8t$ such that the code $C_2(H_1)$ is doubly even and self-dual.

It follows that a skew Hadamard matrix of order $4t$ yields a series of doubly even self-dual binary codes of length $2^{i+2}t$ and even unimodular lattices of rank $2^{i+2}t$, where i is a positive integer.

A **conference matrix** of order n is a $(n \times n)$ $(0, \pm 1)$-matrix W satisfying $WW^T = (n-1)I_n$. If W is a conference matrix of order n, then either $n \equiv 0 \ (mod\ 4)$ or $n \equiv 2 \ (mod\ 4)$.

- If $n \equiv 0 \ (mod\ 4)$, then W is equivalent to a skew-symmetric matrix.
- If $n \equiv 2 \ (mod\ 4)$, then W is equivalent to a symmetric conference matrix, and $n-1$ is the sum of two squares.

A **graph** is **regular** if all the vertices have the same valency. A regular graph is **strongly regular** of type (v, k, λ, μ) if it has v vertices, valency k, and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices.

If thee exists a symmetric conference matrix of order n, then there exists a strongly regular graph with parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$, where $v = n - 1$. Strongly regular graphs with parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ are called **conference graphs**.

Theorem 9 [DC, A. Švob, 2023]

Let M be an adjacency matrix of a conference graph with parameters $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$. Then the matrices

$$M_1 = \left[\begin{array}{ccc|cccc}
0 & 1 & 0 & j_v^\top & j_v^\top & 0_v^\top & 0_v^\top \\
1 & 0 & 0 & j_v^\top & 0_v^\top & j_v^\top & 0_v^\top \\
0 & 0 & 1 & j_v^\top & 0_v^\top & 0_v^\top & j_v^\top \\
\hline
j_v & j_v & j_v & M & M' - I_v & M & M' - I_v \\
j_v & 0_v & 0_v & M' - I_v & M' & M' - I_v & M' \\
0_v & j_v & 0_v & M & M' - I_v & M' & M + I_v \\
0_v & 0_v & j_v & M' - I_v & M' & M + I_v & M
\end{array}\right],$$

$$M_2 = \left[\begin{array}{ccc|cccc}
0 & 0 & 1 & j_v^\top & 0_v^\top & 0_v^\top & j_v^\top \\
1 & 0 & 0 & j_v^\top & j_v^\top & 0_v^\top & 0_v^\top \\
0 & 1 & 0 & j_v^\top & 0_v^\top & j_v^\top & 0_v^\top \\
\hline
0_v & 0_v & 0_v & M' - I_v & M + I_v & M' & M' \\
j_v & 0_v & j_v & M' - I_v & M' - I_v & M' & M \\
j_v & j_v & 0_v & M & M & M' - I_v & M + I_v \\
0_v & j_v & j_v & M & M' & M' - I_v & M' - I_v
\end{array}\right],$$

where $M' = J_v - M$, are incidence matrices of Hadamard 2-designs with parameters $(4v+3, 2v+1, v)$.

Remark

The design $\mathcal{D}_1$ having the incidence matrix M_1 is self-dual, while the design $\mathcal{D}_2$ having the incidence matrix M_2 is in general not isomorphic to its dual design with the incidence matrix $M_3 = M_2^\top$. Let H_1, H_2 and H_3 be Hadamard matrices of order $4(v+1)$ corresponding to the Hadamard 2-designs $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$. Since $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$ have parameters 2-$(4v+3, 2v+1, v)$ and $4(v+1) \equiv 8 \mod 16$, the binary codes of the matrices H_1 and H_2 are **self-dual and doubly even**.

Remark

Let q be a prime power, $q \equiv 1 \mod 4$, and let M be the adjacency matrix of the Paley graph with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$. Then M can be used for the construction of Hadamard 2-designs with parameters $(4q+3, 2q+1, q)$ by applying Theorem 9.

Since many skew-type Hadamard matrices and conference graphs are known, the constructions presented in this talk give a rich source of matrices that could be used to construct doubly even self-dual codes, and consequently even unimodular lattices (and holomorphic vertex operator algebras).

Are unimodular lattices having the minimum norm 2 interesting?

- I. B. Frenkel, J. Lepowsky, A. Meurman, Vertex operator algebras and the Monster, Pure and Applied Mathematics, Vol. 134, Academic Press, 1988.

The vectors of norm 2 form a Lie algebra. If V_L is the holomorphic vertex operator algebra associated to an unimodular lattice L, then the vectors of norm 2 yield an affine vertex algebra which is a subalgebra of V_L.

Unimodular lattices constructed in this talk have minimum norm 2, since they are constructed using the Construction A. Hence the vectors of minimum norm in these lattices yield an affine vertex algebra.

Thank you for your attention!