AIMS Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 10(12): 28264–28276.
DOI: 10.3934/math.20251243
Received: 09 September 2025
Revised: 21 October 2025
Accepted: 10 November 2025
Published: 01 December 2025

Research article

On codes induced from Hadamard matrices

Ted Hurley*

University of Galway (previously National University of Ireland Galway), Ireland

* **Correspondence:** Email: Ted.Hurley@universityofgalway.ie.

Abstract: Unit derived schemes applied to Hadamard matrices are used to construct and analyse linear block and convolutional codes. Codes are constructed to prescribed types, lengths and rates and multiple series of self-dual, dual-containing, linear complementary dual and quantum error-correcting of both linear block and convolutional codes are derived.

Keywords: Hadamard; code; linear; convolutional; self-dual; dual-containing; quantum code
Mathematics Subject Classification: 15B99, 94B05, 94B10

1. Introduction

Unit schemes form a basis for the algebraic construction and analysis of linear block and convolutional codes and these are described in [22] and references therein. The non-existence of general algebraic methods for constructing, designing and studying convolutional codes has often been a problem and limited very much their size and availability; see for example McEliece [30] and also [1, 2, 13, 33]. Here methods derived in [22] are extended for use on Hadamard matrices to provide constructions of linear block and convolutional codes and to construct these to required types, distances and rates. The work here can be read independently of [22] although the ideas initiated in [22] are in the background. The types constructed include self-dual, dual-containing, linear complementary dual and quantum codes and large lengths, rates and distances are achievable. The codes are given over finite fields and types of code required are constructed in both the linear block and convolutional cases. Methods using orthogonal units, Fourier/Vandermonde units, group ring units and related units for constructing and analysing such codes is devised in [21, 22]. The methods are applied to Hadamard matrices to construct algebraically the linear block and convolutional codes and properties of Hadamard matrices allows these to be constructed to required length, rate and type. Infinite series are derived. From a single Hadamard matrix, multiple linear block and convolutional codes are formed and formed to required types.

The distances achieved can often be calculated algebraically; for example the distance of a rate $\frac{1}{2}$ convolutional code obtained is of the order of twice the distance of the linear block rate $\frac{1}{2}$ codes obtained from the same Hadamard matrix.

$C^{\perp}$ denotes the dual of the code C. See Section 1.1 for precise definition of dual of a convolutional code. C is a dual-containing (DC) code if $C \cap C^{\perp} = C^{\perp}$; C is a linear complementary dual (LCD) code if $C \cap C^{\perp} = 0$. C is a self-dual code provided $C^{\perp} = C$ and is an important type of dual-containing code. Dual-containing codes, which include self-dual codes, can be used to construct quantum error-correcting codes (QECC) by the CSS method [5, 6, 36]; here convolutional quantum error-correcting codes are constructed in this way from Hadamard matrices.

A Hadamard matrix is an $n \times n$ matrix H with entries ± 1 satisfying $HH^{\mathrm{T}} = nI_n$. Such a matrix can only exist for $n = 2$ or $n = 4m$ for a positive integer m, [25] Theorem 18.1; see [18] for a beautifully written book on Hadamard matrices. Here these ± 1 entries may be considered as elements in a general field.

The Walsh-Hadamard codes can be formed from Walsh-Hadamard matrices of size $2^k \times 2^k$ by equating the entries (-1) to 0 and then forming binary codes from the $(k + 1)$ linearly independent rows remaining. Using the unit-derived methods on a general Hadamard $n \times n$ matrix gives much more scope, arbitrary rates, good distances, required types but also both linear block and convolutional codes are formed. Several algorithms exist for decoding convolutional codes, the most common ones being the Viterbi algorithm and the sequential decoding algorithm.

Propositions 2.1–2.5 on codes derived from Hadamard are proven and these form a basis for specific algorithms. The following general algorithms are noted:

- Algorithm 1 constructs LCD rate $\frac{r}{n}$, for r, $0 < r < n$, linear block codes from Hadamard $n \times n$ matrices.
- Algorithm 2 constructs self-dual length $2n$ codes from Hadamard $n \times n$ matrices.
- Algorithm 3 constructs self-dual length n convolutional codes from Hadamard $n \times n$ matrices.
- Algorithm 4 constructs dual-containing, length n, rate $\frac{r}{n}$, $(n > r \geq \frac{n}{2})$, convolutional codes from an $n \times n$ Hadamard matrices.

The codes are readily implemented once an expression for the Hadamard matrix is available. Large lengths and rates are obtainable. The brilliant Computer Algebra system GAP with included packages Guava and Gauss, [38], proves extremely useful in manipulating submatrices, working over finite field, constructing applications and computing and verifying distances.

Higher memory convolutional codes may also be generated by breaking the Hadamard matrices further into blocks; see [22] for this. The general process for constructing higher memory convolutional codes from Hadamard matrices is left for later development; however an example, 2.10, is given for a small case to show how the process can proceed for Hadamard matrices.

The notation and parameters used in the following applications may be found in Section 1.1. The notation for linear block codes is standard; however the notation and parameters used for convolutional codes vary in the literature and the specifics used need to be clarified.

Explicit samples of applications. Applications are obtained by applying the propositions and algorithms to particular cases. Once the Hadamard matrix is formed, the propositions and algorithms may then be applied to produce multiple cases of required codes.

$H(n)$ denotes a Hadamard matrix of size n.

From $H(20)$ the following are formed:

(1) LCD $[20, 13, 4]_3$, $[20, 7, 6]_3$ codes;
(2) Self-dual convolutional $(20, 10, 10; 1, 12)_{3^2}$ codes;
(3) DC convolutional $(20, 13, 7; 1, 8)_{3^2}$ codes;
(4) Quantum codes of length 20, distance 8 and rate $\frac{6}{20}$ over $GF(3^2)$;
(5) Self-dual $[20, 10, 8]_5$ codes;
(6) $(20, 10, 10; 1, 14)_{7^2}$ self-dual convolutional codes;
(7) $[40, 20, 12]_3$ self-dual codes are given directly in systematic form, see Proposition 2.2.

From $H(28)$ the following are formed:

- LCD $[28, 16, 6]_3$, $[28, 12, 9]_5$ codes;
- Convolutional self-dual $(28, 14, 14; 1, 12)_3$ codes over $GF(3)$;
- DC convolutional $(28, 18, 10; 1, 8)$ codes over $GF(3)$;
- Quantum codes of length 28, distance 8, rate $\frac{8}{28}$ over $GF(3)$;
- Self-dual convolutional $(28, 14, 14; 1, 16)$ codes over $GF(5)$
- DC convolutional $(28, 16, 12; 1, 14)$ codes over $GF(5)$;
- $[28, 14, 9]_7$ self-dual codes.

Generally from $H(n)$ with $p \nmid n$, self-dual $(n, \frac{n}{2}, \frac{n}{2}; 1, d)$ convolutional codes and DC $(n, r, n-r; 1; d)$, $r > \frac{n}{2}$, convolutional codes are formed. In prototype Example 2.9, it is shown how the different types of LCD, self-dual, DC, quantum, linear block and convolutional codes may be derived for a small Hadamard matrix case. Self-dual codes over $GF(p)$ can often be obtained from a Hadamard matrix of size n when $p \mid n, p \neq 2$, see Proposition 2.8. For example, self-dual $[12k, 6k, d]_3$ codes are produced from Paley-Hadamard matrices of size $12k$, see Section 2.1.

An understanding of the propositions and algorithms allows one to take a Hadamard matrix and construct LCD, self-dual, DC and QECC codes therefrom. Section 2.1 is given over to considering ternary codes and codes over fields of characteristic 3. Codes over $GF(5)$ from Hadamard matrices may similarly be worked on. Using non-separable Hadamard matrices in applications seems to work out better.

1.1. Additional notation and background

The notation for linear block codes is standard and may be found in [3, 24, 26, 30] and many others. $GF(q)$ denotes the finite field with q elements and $\mathbb{Z}_m$ denotes the integers modulo m; in particular $\mathbb{Z}_p = GF(p)$ for a prime p. A $[n, r, d]$ code denotes a linear block code of length n, dimension r, and (minimum) distance d; the *rate* is $\frac{r}{n}$. A $[n, r, d]_q$ code denotes a linear block code of length n, dimension r and distance d over the field $GF(q)$.

Different equivalent definitions for convolutional codes are given in the literature. The notation and definitions used here follow that given in [34, 35, 37]. A rate $\frac{k}{n}$ convolutional code with parameters (n, k, δ) over a field $\mathcal{F}$ is a submodule of $\mathcal{F}[z]^n$ generated by a reduced basic matrix $G[z] = (g_{ij}) \in$

$\mathcal{F}[z]^{r\times n}$ of rank r where n is the length, $\delta = \sum_{i=1}^{r}\delta_i$ is the degree with $\delta_i = \max_{1\le j\le r}\deg g_{ij}$. Then $\mu = \max_{1\le i\le r}\delta_i$ is known as the memory of the code and the code is then given with parameters $(n,k,\delta;\mu)$. The parameters $(n,k,\delta;\mu,d_f)$ are used for such a code with free (minimum) distance d_f. Further $(n,k,\delta;\mu,d_f)_q$ is used to specify that the code is over the field $GF(q)$.

Suppose C is a convolutional code in $\mathcal{F}[z]^n$ of rank k. A generating matrix $G[z] \in \mathcal{F}[z]_{k\times n}$ of C having rank k is called a generator or encoder matrix of C. A matrix $H \in \mathcal{F}[z]_{n\times(n-k)}$ satisfying $C = \ker H = \{v \in \mathcal{F}[z]^n : vH = 0\}$ is said to be a control matrix or check matrix of the code C.

Convolutional codes can be catastrophic or non-catastrophic; see for example [30] for the basic definitions. A catastrophic convolutional code is prone to catastrophic error propagation and is not much use. A convolutional code described by a generator matrix with right polynomial inverse is a non-catastrophic code; this is sufficient for our purposes. The designs given here for the generator matrices allow for specifying directly the control matrices and the right polynomial inverses. Lack of algebraic construction methods for designing convolutional codes limited their size and availability, see McEliece [30] for discussion and also [1, 2, 13, 33]. It is shown here how Hadamard matrices can be used to construct convolutional codes but see also [22, 23]. Several algorithms exist for decoding convolutional codes, the most common ones being the Viterbi algorithm and the sequential decoding algorithm.

Let $G(z)$ be the generator matrix for a convolutional code C with memory m. Suppose $G(z)H^{\mathrm{T}}(z) = 0$, so that $H^{\mathrm{T}}(z)$ is a control matrix, and then $H(z^{-1})z^m$ generates the convolutional dual code of C, see [4] and [12]. This is also known as the module-theoretic dual code.* The code is then dual-containing provided the code generated by $H(z^{-1})z^m$ is contained in the code generated by $G(z)$.

The dual of a code C is denoted by $C^{\perp}$.

Dual-containing (DC) codes, which contain self-dual codes, are an important class of codes for theoretical and practical purposes. Besides their direct applications, DC codes are used to construct quantum error correcting codes (QECC) by the CSS method [5, 6, 36]. Here then quantum error correcting linear and convolutional codes of different lengths and rates are constructed explicitly from Hadamard matrices.

Linear complementary dual, LCD, codes have been studied extensively for their theoretical and practical importance's by Carlet, Mesnager, Tang, Qi and Pelikaan, [7–9, 31], and were originally introduced by Massey in [28, 29]. They have been used for improving the security of information on sensitive devices against side-channel attacks (SCA) and fault non-invasive attacks, see [10, 11], and in data storage and communications' systems. Here LCD linear block and convolutional codes are constructed from Hadamard matrices using the unit-derived and associated methods.

The unit-derived and associated methods for constructing and analysing linear block codes was initiated in [14–17] and developed further in [19, 20]. The papers [22, 23] and references therein extend the unit-derived and related methods ideas to form in addition convolutional codes and algebraic methods for constructing whole series of linear block and convolutional codes to prescribed length, distance, rate and type are derived. The unit-derived methods give further information on the code in addition to describing the generator and control matrices. McEliece - see for example [30] - remarks: 'A most striking fact is the lack of algebraic constructions of families of convolutional codes';

*In convolutional coding theory, the idea of dual code has two meanings. The other dual convolutional code defined is called the sequence space dual; the generator matrices for these two types are related by a specific formula.

constructing convolutional codes of reasonable length was beyond computer generation.

Which Hadamard matrix of a particular size n should one work? It is not an issue in cases where just the main properties of a Hadamard matrix are required. It seems best from practice and intuition to work with non-separable Hadamard matrices. Here non-separable means the Hadamard matrix is not a non-trivial tensor product of other Hadamard matrices. The Walsh-Hadamard matrices are separable except for size 2.

2. Linear block and convolutional codes induced from Hadamard matrices

The Walsh-Hadamard binary linear block codes $[2^k, k, 2^{k-1}]_2$ and $[2^k, k+1, 2^{k-1}]_2$ have very small rates but have found use probably on account of the distances and decoding methods available. Codes from general Hadamard matrices as now described allow much more scope with much better rates, good distances, and required types and both linear block and convolutional codes may be formed.

Let H be a Hadamard matrix with $HH^{\mathrm{T}} = nI_n$. Break H as $H = \binom{A}{B}$ for A an $r \times n$ matrix and then $\binom{A}{B}(A^{\mathrm{T}}\ B^{\mathrm{T}}) = nI_n$. When $n \neq 0$ in the field under consideration, a code is obtained in which A is the generator matrix and B^{T} is a check matrix. This is the basic method for producing the linear block codes from Hadamard matrices. A more general method is to take any r rows of the Hadamard matrix to generate a code and a check matrix is obtained by eliminating the corresponding columns of the transpose of the Hadamard matrix. The convolutional codes are essentially obtained from breaking the Hadamard matrix into blocks and using the blocks as 'components' of the generator matrix of a convolutional code. Properties of the Hadamard matrix are used to construct the type of code required.

The following Propositions 2.1–2.5 form the basis for deriving algorithms with which series of codes, both linear block and convolutional, are derived. These allow linear block and convolutional codes of particular types, such as self-dual, DC, LCD and quantum, to be constructed and enables these to be devised to the required length and rate. Algorithms 1–4 follow from which numerous applications can be devised.

It is worth noting that arithmetic over $GF(p) = \mathbb{Z}_p$ is simply modular arithmetic and is easily implemented. Let $d(X)$ denote the distance of the linear block code generated by the matrix X.

Proposition 2.1. *Let H be a Hadamard matrix of size n and $n \neq 0$ in a field $\mathcal{F}$. Suppose H has the form $H = \binom{A}{B}$, where A has size $r \times n$, implying $\binom{A}{B}(A^T\ B^T) = nI_n$. Then the code generated by A over $\mathcal{F}$ is an LCD $[n, r]$ code $\mathcal{A}$ and B generates the dual code of $\mathcal{A}$.*

Proof. Both A and B have full ranks as H is invertible. Now $AB^{\mathrm{T}} = 0$ and so B^{T} is a control matrix for the code $\mathcal{A}$ and thus B generates the dual code of $\mathcal{A}$. Since H is invertible in $\mathcal{F}$ a combination of the rows of A cannot be a non-trivial combination of the rows of B and thus $\mathcal{A}$ is an LCD code. □

Algorithm 1. *Construct LCD rate $\frac{r}{n}$ linear block codes from Hadamard $n \times n$ matrices H as follows:*

Let $\mathcal{F} = GF(p)$ where $p \nmid n$. Choose any r rows of H to form the generator matrix of an $[n, r]$ code over $\mathcal{F}$. This code is an $[n, r]$ LCD code.

Proposition 2.2. *Let $n \neq 0$ in a field $\mathcal{F}$ and H be a Hadamard matrix with $HH^T = nI_n$. Then there exists $\alpha \in \mathcal{F}$ or in a quadratic extension of $\mathcal{F}$ such that $(I_n, \alpha H)$ generates a self-dual code.*

Proof. Let $I = I_n$. Now $(I, \alpha H)\begin{pmatrix} I \\ \alpha H^{\mathrm{T}} \end{pmatrix} = I + \alpha^2 nI = (1 + \alpha^2 n)I$. Now $(1 + x^2 n = 0)$ has a solution in $\mathcal{F}$ or else $(1 + x^2 n)$ is irreducible over $\mathcal{F}$. Thus in $\mathcal{F}$ or in a quadratic extension of F there exists an α such that $(1 + \alpha^2 n) = 0$. Then $(I, \alpha H)\begin{pmatrix} I \\ \alpha H^{\mathrm{T}} \end{pmatrix} = 0$ and so $K^{\mathrm{T}} = \begin{pmatrix} I \\ \alpha H^{\mathrm{T}} \end{pmatrix}$ of rank n is a control matrix. Thus $K = (I, \alpha H)$ generates the dual of the code and hence the code is self-dual. □

The distance of the codes in Proposition 2.2 may be worked out from Proposition 2.6 but not always easily. From the self-dual code, by the CSS construction, a quantum error-correcting code may be constructed with the same distance.

An example of how this Proposition 2.2 works is given with Prototype example 2.9 which uses a Hadamard matrix of size 12.

Algorithm 2. Construct $[2n, n]$ self-dual codes using Hadamard matrices of size n:

Let $\mathcal{F} = GF(p)$ where $p \nmid n$ and $A = (I_n, \alpha H)$ where α satisfies $(1 + \alpha^2 n = 0)$ in $\mathcal{F}$ or in a quadratic extension of $\mathcal{F}$. Then the code generated by A is self-dual.

Proposition 2.3. *Let H be a Hadamard matrix of size n and $n \neq 0$ in a field $\mathcal{F}$. Suppose H has the form $H = \binom{A}{B}$ implying $\binom{A}{B}\left(A^T \; B^T \right) = nI_n$ where $n = 2m$ and A and B have size $m \times n$. Let $G(z) = A + iBz$ where $i = \sqrt{-1}$ in $\mathcal{F}$ or in a quadratic extension of F. Then $G(z)$ generates a self-dual convolutional (non-catastrophic) code with parameters $(2m, m, m; 1, d)$ where $d = d(A) + d(B)$.*

Proof. Now $G(z)(iB^{\mathrm{T}} + A^{\mathrm{T}} z) = (A + iBz)(iB^{\mathrm{T}} + A^{\mathrm{T}} z) = 0 + nI_m z - nI_m z + 0 = 0$ and so $H^{\mathrm{T}}(z) = (iB^{\mathrm{T}} + A^{\mathrm{T}} z)$ is a control matrix. Hence $H(z^{-1})z = A + iB$ generates the dual of the code and so the code is self-dual. Also $(A + iBz)A^{\mathrm{T}} = nI_m$ and so $(A + iBz)$ has a right polynomial inverse and thus the code generated by $G(z)$ is non-catastrophic.

The proof of the distance is straight forward and omitted. □

Algorithm 3. *Construct self-dual convolutional codes from Hadamard matrices.*

Let H be a Hadamard matrix of size $n = 2m$ and $\mathcal{F} = GF(p)$ where $p \nmid n$. Let A consist of any m rows of H and B consist of the other m rows of H. Define $G(z) = A + iB$ where $i = \sqrt{-1}$ in $\mathcal{F}$ or in a quadratic extension of $\mathcal{F}$. Then $G(z)$ generates a self-dual convolutional code with parameters $(2m, m, m; 1, d)$ where $d = d(A) + d(B)$.

Proposition 2.4. *Let H be a Hadamard matrix of size n so that $HH^T = nI_n$ and $n \neq 0$ in a field $\mathcal{F}$. Suppose H has the form $H = \binom{A}{B}$ implying $\binom{A}{B}\left(A^T \; B^T \right) = nI_n$ where A has size $r \times n$ and B has size $(n - r) \times n$ with $r > (n - r)$. Let $t = (2r - n)$ and define $B_1 = \binom{0_{t \times n}}{B}$. Then $G(z) = A + iB_1 z$ generates a convolutional dual-containing $(n, r, n - r; 1, d)$ code C where $i = \sqrt{-1}$ in $\mathcal{F}$ or in a quadratic extension of $\mathcal{F}$.*

Proof. Define $0_t = 0_{t \times n}$. Thus $B_1 = \begin{pmatrix} 0_t \\ B \end{pmatrix}$ is an $r \times n$ matrix. Now A^{T} is an $n \times r$ matrix and thus has the form $A^{\mathrm{T}} = (X, C_1)$ where C_1 has size $n \times (n - r)$ and X has size $n \times (2r - n)$. As $AA^{\mathrm{T}} = nI_r$ then $AC_1 = n\begin{pmatrix} 0_{(2r-n)\times(n-r)} \\ I_{(n-r)\times(n-r)} \end{pmatrix}$ and also $B_1 B = n\begin{pmatrix} 0_{(2r-n)\times(n-r)} \\ I_{(n-r)\times(n-r)} \end{pmatrix}$. Now $A = \begin{pmatrix} X^{\mathrm{T}} \\ {C_1}^{\mathrm{T}} \end{pmatrix}, B_1 = \begin{pmatrix} 0_t \\ D^{\mathrm{T}} \end{pmatrix}$. Then $(A + iB_1 z)(iB^{\mathrm{T}} + C_1 z) = 0$ so $H^{\mathrm{T}}(z) = (iB^{\mathrm{T}} + C_1 z)$ is a control matrix and $H(z^{-1})z = {C_1}^{\mathrm{T}} + iB$ generates the dual of the code. The code generated by ${C_1}^{\mathrm{T}} + iB$ is easily seen to be contained in the code generated by $(A + iB_1)$ and so the code generated by $(A + iB_1)$ is dual-containing. That the code is non-catastrophic follows in a similar manner to the proof in Proposition 2.3. □

Suppose $H = \left(\begin{smallmatrix} P \\ Q \end{smallmatrix}\right)$ so that $\left(\begin{smallmatrix} P \\ Q \end{smallmatrix}\right)\left(P^{\mathrm{T}} \; Q^{\mathrm{T}} \right) = nI_n$ where P has size r with $r > \frac{n}{2}$. Then this can be written $\left(\begin{smallmatrix} A \\ B \\ C \end{smallmatrix}\right)\left(A^{\mathrm{T}} \; B^{\mathrm{T}} \; C^{\mathrm{T}} \right) = nI_n$ where C has the same size as B. Another way to look at Proposition 2.4 is as follows:

Proposition 2.5. *Let H be a Hadamard $n \times n$ matrix and $n \neq 0$ in $\mathcal{F}$. Suppose $H = \left(\begin{smallmatrix} A \\ B \\ C \end{smallmatrix}\right)$ where C has the same size as B and thus $\left(\begin{smallmatrix} A \\ B \\ C \end{smallmatrix}\right)\left(A^{T} \; B^{T} \; C^{T} \right) = nI_n$.*

Then $G(z) = \left(\begin{smallmatrix} A \\ B \end{smallmatrix}\right) + i\left(\begin{smallmatrix} \underline{0} \\ C \end{smallmatrix}\right)$ defines a dual-containing convolutional $(n, r, n-r; 1, d)$ code where $i = \sqrt{-1}$ in $\mathcal{F}$ or in a quadratic extension of $\mathcal{F}$, $\underline{0}$ is the zero matrix of the same size as A and $r \times n$ is the size of $\left(\begin{smallmatrix} A \\ B \end{smallmatrix}\right)$.

This is equivalent to Proposition 2.4 but a proof is given as it's instructive for the algorithm that follows.

Proof. Note that $BB^{\mathrm{T}} = nI_t = CC^{\mathrm{T}}$ for some t. Use 0 for a zero matrix whose size is clear from the context. Now $(\left(\begin{smallmatrix} A \\ B \end{smallmatrix}\right) + i\left(\begin{smallmatrix} 0 \\ C \end{smallmatrix}\right)z)(iC^{\mathrm{T}} + B^{\mathrm{T}}z) = 0 + \left(\begin{smallmatrix} 0 \\ I_t \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 \\ I_t \end{smallmatrix}\right) + 0 = 0$ and so $H^{\mathrm{T}}(z) = iC^{\mathrm{T}} + B^{\mathrm{T}}z$ is a control matrix for the code. Hence $H(z^{-1})z = B + iC$ generates the dual of the code. It is easy to see that the code is dual-containing. Also a right inverse for $G(z)$ is readily written down and so the code is non-catastrophic. □

This can be used to find or estimate the distances of the dual-containing codes derived.

Algorithm 4. *Construct rate $\frac{r}{n}$, $n > r \geq n/2$, dual-containing convolutional codes from Hadamard matrices of size n.*

Let $\mathcal{F} = GF(p)$ where $p \nmid n$, A consist of r rows of H and B consist of the other $(n-r)$ rows of H. Define $G(z) = A + iB_1 z$ where $B_1 = \left(\begin{smallmatrix} 0_{t\times n} \\ B \end{smallmatrix}\right)$, $t = 2r - n$ and $i = \sqrt{-1}$ in $\mathcal{F}$ or in a quadratic extension of $\mathcal{F}$. Then $G(z)$ generates a dual-containing convolutional code $(n, r, n-r, 1, d)$.

The distance d in Algorithm 4 can be estimated from Proposition 2.4 as follows: Let A_1 be the matrix of the first $(2r-n)$ of A in Proposition 2.4; the distance of C is then $\min\{d(A_1), d(A) + d(\left(\begin{smallmatrix} A_1 \\ B \end{smallmatrix}\right))\}$.

Note that from a dual-containing code, by the CSS construction, a quantum error-correcting codes, QECC, of the same length and distance as that of the dual-containing code is constructible.

The Hadamard matrix over $GF(3)$ has entries $\{1, -1\}$ which are all the non-zero entries of $GF(3)$. $GF(5)$ has the property that it contains a square root of (-1) as $2 = \sqrt{-1}$ in $GF(5)$. But also $GF(3)$ may be extended to $GF(3^2)$ which has a square root of (-1); the significance of $\sqrt{-1}$ is clear from the convolutional codes is derived as in Propositions 2.3 and 2.4.

For characteristic dividing n the rank of a Hadamard $n \times n$ matrix is then less than n. When the characteristic does not divide n then the Hadamard $n\times n$ matrix has rank n and its rows are independent; this is used in Propositions 2.3 and 2.4. Proposition 2.2 uses a Hadamard matrix to give a generator matrix of a self-dual code in systematic form, [3]. The distance can be obtained from the Hadamard matrix as follows.

Proposition 2.6. *(Proposition 3.8 in [22].) Let C be the code generated by $G = (I_n, P)$. Suppose the code generated by any s rows of P has distance $\geq (d - s)$ and for some choice of r rows the code generated by these r rows has distance exactly $(d - r)$, then the distance of C is d.*

For a matrix K the following notation, as suggested by [38], is adopted: $K[s..t][u..v]$ is the submatrix of K consisting of the rows s to t of K and the columns u to v of K.

Lemma 2.7. *Let $H = H(n)$ be a Hadamard matrix of size n and and let $p \neq 2$ be a prime divisor of n. Then* $\operatorname{rank}(H) \leq \frac{n}{2}$ *in $\mathbb{Z}_p = GF(p)$.*

Proof. Modulo p, $HH^{\mathrm{T}} = nI_n = 0_{n\times n}$. If A is an $m\times n$ matrix and B is $n\times k$, then $\operatorname{rank}(A)+\operatorname{rank}(B)-n \leq \operatorname{rank}(AB)$. Let $H = A, B = H^{\mathrm{T}}$. Then $\operatorname{rank}(H)+\operatorname{rank}(H^{\mathrm{T}})-n \leq \operatorname{rank} HH^{\mathrm{T}} = 0$. But $\operatorname{rank}(H) = \operatorname{rank}(H^{\mathrm{T}})$ and so $2\operatorname{rank}(H) \leq n$ and hence $\operatorname{rank}(H) \leq \frac{n}{2}$. □

It is easy to check the rank as required in such cases when $p \mid n$. In many cases it works that the rank is actually $\frac{n}{2}$ but it's not necessary that the first $\frac{n}{2}$ rows are independent.

Proposition 2.8. *Let $H = H(2n)$ be a Hadamard matrix of size $2n$ and $p \mid n$, p a prime, $p \neq 2$. Suppose over $GF(p)$ that H has rank n and let A be an $n \times 2n$ submatrix of rank n. Then A generates a self-dual $[2n, n]_p$ code over $GF(p)$.*

Proof. It may be assumed that A consists of the first n rows of H as interchanging rows of a Hadamard matrix results in a Hadamard matrix of the same rank. Thus over $GF(p)$, HH^{T} has the form $\binom{A}{B}\begin{pmatrix} A^{\mathrm{T}} & B^{\mathrm{T}} \end{pmatrix} = 0$. Thus $AA^{\mathrm{T}} = 0$. Now $\operatorname{rank}(A) = n$ and thus $\operatorname{rank}(A^{\mathrm{T}}) = n$. Hence A generates a $[2n, n]$ code $\mathcal{A}$ and A is a control matrix of this code. Thus the dual code of $\mathcal{A}$ is generated by A and so $\mathcal{A}$ is self-dual. □

In Proposition 2.8 any n rows of H that form a matrix of rank n can be used to generate a self-dual code. In many cases the matrix of the first n rows has rank n and also in many cases a selection of any n rows has rank n. The distance may be found for lengths up to about a 100 by computer and after that algebraic methods are required.

Applications/examples Applications are derived by applying the propositions and algorithms. The introduction lists some applications and the following is a further selection.

The first application is a small prototype example with $H = H(12)$ and this demonstrates how the different methods for constructing linear block and convolutional codes from Hadamard matrices codes can be developed.

Prototype Example 2.9. *Let H be a 12×12 Hadamard matrix. This is a good example and is the first case of a Hadamard matrix with size $n > 2$ where H cannot be derived as a Walsh-Hadamard matrix type.*

- *Then $HH^T = I_{12}$ is broken up as: $\binom{A}{B}\begin{pmatrix} A^T & B^T \end{pmatrix} = 12I_{12}$. Let A consist of the first 6 rows of H, $A = K[1..6][1..12]$, and B consist of the last 6 rows of H. Over $GF(3)$ this becomes $\binom{A}{B}\begin{pmatrix} A^T & B^T \end{pmatrix} = 0$. Now A (and B) have rank 6 as does A^T giving $AA^T = 0$. Thus the code generated by A has dual code generated by $A^{TT} = A$ and so is self-dual. The distance of the code, $\mathcal{A}$, generated by A is 6 and so $\mathcal{A}$ is a $[12, 6, 6]$ self-dual code over $GF(3)$. This is best possible. The code can correct up to 2 errors and thus a combination of one or two rows of A^T is unique and can be used to correct up to two errors in a straight-forward manner.*

- *Over $GF(5)$ the code generated by A is an LCD code as is the dual code is generated by B. Both are $[12, 6, 6]_5$ codes over $GF(5)$.*
  Over $GF(5)$ define $G(z) = A+iBz$ where $i = \sqrt{-1}$; in this case $i = 2$ as $2^2 = 4 = -1$ in $GF(5)$. $G(z)$ generates a convolutional memory 1 code which is non-catastrophic as $(A + iBz)A^T = 6I_6 = I_6$ so that $A + iBz$ has a right polynomial inverse. Now $(A + iBz)(iB^T + A^T z) = 0$ so $K^T(z) = iB^T + A^T z$ is a control matrix giving that $K(z^{-1})z = A + iBz$ generates the dual code code and so the code is self-dual. The free distance of the code is the sum of the distances of the codes generated by A and by B which is 12, see Proposition 2.3. Thus a self-dual convolutional $(12, 6, 6; 1, 12)_5$ code is obtained. From this a quantum error-correcting convolutional code is obtained with length 12 and distance 12 over $GF(5) = \mathbb{Z}_5$.
- *Let H again be a Hadamard 12×12 matrix and let C be the $[24, 12]$ code generated by $(I_{12}, \alpha H)$ with α to be determined. Then $(I, \alpha H)\begin{pmatrix} I \\ \alpha H^T \end{pmatrix} = I + 12\alpha^2 I = (1 + 12\alpha^2)I$. Require now that $(1 + 12\alpha^2) = 0$ in a field to be decided. In this case $K^T = \begin{pmatrix} I \\ \alpha H^T \end{pmatrix}$, which has rank 12, is a control matrix and then $K = (I, \alpha H)$ generates the dual code of C and so C is self-dual.*
- *In item 2.9 require that $1 + 2\alpha^2 = 0$ in characteristic 5 which requires $2\alpha^2 = -1 = 4$ which requires $\alpha^2 = 2$. Now $x^2 - 2$ is irreducible over $GF(5)$ and so extend $GF(5)$ to $GF(5^2)$ which has an element $\alpha^2 = 2$. Then over this field $(I, \alpha H)$ generates a self-dual code. The length of the code turns out to be 8 and thus get a $[24, 12, 8]$ self-dual code over $GF(5^2)$.*
  In $GF(7) = \mathbb{Z}_7$, $\alpha = 2$ satisfies $1 + 12\alpha^2 = 0$ and so $(I, 2H)$ generates a self-dual $[24, 12, 8]_7$ code.

Example 2.10. *Hadamard matrices can be used to construct higher memory convolutional codes. Let H be a Hadamard 12×12 matrix, $A = H[1.3][1..12], B = H[4..6][1..12], C = H[7..9][1..12], D = H[10..12][1..12]$. Then $G(z) = A + Bz + Cz^2 + Dz^3$ gives a $(12, 3, 9; 3, 24)$ convolutional code. The distance is easily computed as $d(A) = 6 = d(B) = d(C) = d(D)$ and $d((\begin{smallmatrix} X \\ Y \end{smallmatrix}) = 6$ for X, Y different elements of $\{A, B, C, D\}$.*

Further applications/examples are given below.

Example 2.11. *With $H = H(72)$ any 36 rows generate a $[72, 36, 18]_3$ self-dual code. With $H = H[144]$ over $GF(3)$, 72 rows of H generate a $[144, 72, d]_3$ code.*

Example 2.12. *Let $H = Hadamard(20)$. Let $A = H[1..10][1..20], B = H[11..20][1..20]$. Over $GF(3)$ the codes generated by both A and B are $[20, 10, 6]$ LCD codes. Using $G(z) = A + iBz$ gives by Proposition 2.3 a convolutional $(20, 10, 10; 1; 12)$ self-dual code over $GF(3^2)$ where $i = \sqrt{-1}$ in $GF(3^2)$. From this a QECC convolutional code of length 20 and distance 12 is obtained.*

Over $GF(5)$ a $[20, 10, 8]_5$ self-dual code is obtained from H. But also $A = H[1..10][1..20]$ and $B = H[11..20][1..20]$ give $[20, 10, 8]_5$ codes over $GF(5)$.

Example 2.13. *$H = H(24)$. Over $GF(3)$ this has rank 12. But also $A = H[1..12][1..24]$ has rank 12 over $GF(3)$ and generates a self-dual $[24, 12, 9]$ code over $GF(3)$.*

Let $B = H[11..24][1..24]$. Then both A and B generate $[24, 12, 7]_5$ codes over $GF(5)$. Let $G(z) = A + iBz$ where $i = \sqrt{-1} = 2$ in $GF(5)$. Then by Proposition 2.3, $G(z)$ generates a convolutional self-dual $[24, 12, 12; 1, 14)$ code over $GF(5)$. From this a QECC convolutional code of length 24 and distance 14 is derived over $GF(5)$.

Example 2.14. *Let $H = H(40), A = H[1..20][1..40], B = H[21..40][1..40]$. Over $GF(5)$ H has rank 20 but A has rank 10 over $GF(5)$. Now $C = H[1..10][1..40]$ has rank 10 over $GF(5)$ and generates* *a* $[40, 10, 16]$ *LCD code over* $GF(5)$. *Over* $GF(3)$ *define* $G(z) = A + iBz$ *where* $i = \sqrt{-1}$ *in* $GF(3^2)$. *Then* $G(z)$ *generates a self-dual convolutional* $(40, 20, 20; 1, d)$ *code where* $d = d(A) + d(B)$, *Proposition 2.3. From this a QECC convolutional code of length* 40 *and distance d is obtained.*

Example 2.15. $H = H(36), A = H[1..18][1..36], B = H[19..36][1..36]$. *Over* $GF(3)$ *A generates a self-dual* $[36, 18, 12]_3$ *code as does B. Define* $G(z) = A + iBz$ *where* $i = \sqrt{-1} = 2$ *in* $GF(5)$ *and then* $G(z)$ *generates a convolutional self-dual code* $(36, 18, 18; 1, d)$ *where* $d = d(A) + d(B)$ *from which a QECC convolutional code of length* 36 *and distance d is obtained.*

2.1. Ternary codes from Hadamard matrices

Ternary codes, codes over $GF(3)$, have their own interest and are the next are the next obvious cases after binary; see for example [32] but many more in the literature. Arithmetic in $GF(3) = \mathbb{Z}_3$ is easily implemented. Some applications given previously are ternary codes. The entries of a Hadamard matrix are the non-zero elements of $\mathbb{Z}_3 = GF(3)$ and looking at unit-derived codes formed from Hadamard matrices over $GF(3) = \mathbb{Z}_3$ is particularly interesting and beneficial.

Lemma 2.7 shows that when $3 \mid n$ then $\text{rank}(H) \leq \frac{n}{2}$ in $\mathbb{Z}_3 = GF(3)$ for a Hadamard matrix of size n. For a Paley-Hadamard matrix H of size n, $\text{rank}(H) = \frac{n}{2}$. Is it true in other cases? In cases where the rank is $\frac{n}{2}$ a self-dual $[n, \frac{n}{2}, d]_3$ code is constructible from any $\frac{n}{2}$ independent rows of the Hadamard matrix.

The following is a consequence of Proposition 2.8:

Proposition 2.16. *Let H be a Hadamard matrix of size n such that* $3 \mid n$ *and that* $\text{rank}(H) = \frac{n}{2}$. *Then any submatrix of size* $\frac{n}{2} \times n$ *of rank* $\frac{n}{2}$ *over* $GF(3)$ *generates a self-dual* $[n, \frac{n}{2}, d]_3$ *code.*

Corollary 2.17. *Let* $H = H(12k)$ *be a Hadamard matrix of rank* $6k$ *over* $GF(3)$. *Then* $6k$ *linearly independent rows over* $GF(3)$ *of H generate a self-dual* $[n, \frac{n}{2}, d]_3$ *code.*

It is interesting to find the distances attained. For a self-dual $[n, \frac{n}{2}, d]_3$ ternary code it is known that $d \leq \lfloor \frac{n}{12} \rfloor + 3$ [27]. For $n = 12k$ extremal ternary self-dual codes exist for lengths $n = 12, 24, 36, 48, 60$ and do not exist for $n = 72, 96, 120$ and for $n \geq 144$. Now by Corollary 2.17 $\frac{n}{2}$ linearly independent rows over $GF(3)$ of a Hadamard matrix of size $n = 12k$ generate a self-dual ternary code; when $n = 12, 24, 36, 48, 60$ it is verified by computer that these are optimal.

Lemma 2.18. *In characteristic* 3 *a non-zero sum of r rows of a Hadamard* $n \times n$ *matrix is the same as the sum of the first r rows of a Hadamard* $n \times n$ *matrix.*

Proof. In characteristic 3 the non-zero coefficients in a sum of rows are ± 1 only. Interchanging rows of a Hadamard matrix or multiplying any row by -1 results in a Hadamard matrix. Thus taking the relevant rows and placing them in the first r places and multiplying the row by -1 if the coefficient is -1 results in a Hadamard matrix whose sum of the first r rows is the same as the vector sum of the required rows. □

Thus if a lower bound on the support of the sum of the first s rows of a particular type of Hadamard matrix over $\mathbb{Z}_3$ can be obtained then distances of the unit-derived codes from such a matrix H are calculated and also the distances of the self-dual codes $(I, \alpha H)$ as in Proposition 2.2 are obtained. The following proposition is a special case of Proposition 2.1.

Proposition 2.19. *Let H be a Hadamard $n \times n$ and $3 \nmid n$. Then any r rows of H generates an LCD ternary $[n, r, d]_3$ code over $\mathbb{Z}_3$.*

Application: With $n = 20$ the following LCD codes are obtained:

$[20, 5, 10]_3, [20, 6, 10]_3, [20, 10, 6]_3, [20, 11, 5]_3, [20, 13, 4]_3$.

With $n = 28$ the following LCD codes are obtained: $[28, 7, 12], [28, 14, 6], [28, 18, 4]$.

The following proposition is immediate from propositions 2.3–2.5.

Proposition 2.20. *Let $H = H(n)$ be a Hadamard matrix of size n where $3 \nmid n$.*

(i) Suppose A consists of $\frac{n}{2}$ rows of H and B consists of the other $\frac{n}{2}$ rows of H. Then $G(z) = A + iB$ with $i = \sqrt{-1}$ in $GF(3^2)$ generates a self-dual convolutional $(n, \frac{n}{2}, \frac{n}{2}; 1, d)$ code in $GF(3^2)$ where $d = d(A) + d(B)$.

(ii) Suppose A consists of r rows of H with $r > \frac{n}{2}$ and B consists of the other $(n-r)$ rows of H. Define $B_1 = \left(\begin{smallmatrix} \underline{0} \\ B \end{smallmatrix}\right)$ where $\underline{0}$ is the zero $(2n - r) \times n$ matrix. Then $G(z) = A + iB_1x$ generates a dual-containing convolutional $(n, r, n - r; 1, d)$ code in $GF(3^2)$ where $i = \sqrt{-1}$.

Proposition 2.5 is used to calculate the distance d in part (ii) of Proposition 2.20.

3. Conclusions

Using units in Hadamard matrices to design and analyse linear block and convolutional codes is a unique method in coding theory. Infinite new series of both linear block and convolutional are now available by the methods. Codes, both linear block and convolutiona, can be designed to required length, rate and type; distances can often be calculated directly. Interesting new examples are given but the methods are inherently algebraic with no restrctions on size leaving many new codes for particular purposes yet to be designed by the methods.

Use of Generative-AI tools declaration

The author declares he has not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

The author declares no conflict of interest.

References

1. P. Almeida, D. Napp, R. Pinto, A new class of superregular matrices and MDP convolutional codes, *Linear Algebra Appl.*, **439** (2013), 2145–2157. https://doi.org/10.1016/j.laa.2013.06.013
2. P. J. Almeida, D. Napp, R. Pinto, Superregular matrices and applications to convolutional codes, *Linear Algebra Appl.*, **499** (2016), 1–25. https://doi.org/10.1016/j.laa.2016.02.034

3. R. E. Blahut, *Algebraic Codes for data transmission*, Cambridge University Press, 2012. https://doi.org/10.1017/CBO9780511800467
4. I. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov, Dual convolutional codes and the MacWilliams identities, *Probl. Inf. Transm.*, **48** (2012), 21–30. https://doi.org/10.1134/S0032946012010036
5. A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inform. Theory*, **44** (1998), 1369–1387. https://doi.org/10.1109/18.681315
6. A. R. Calderbank, P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A*, **54** (1996), 1098–1105. https://doi.org/10.1103/PhysRevA.54.1098
7. C. Carlet, S. Mesnager, C. Tang, Y. Qi, Euclidean and Hermitian LCD MDS codes, *Des. Codes Cryptogr.*, **86** (2018), 2605–2618. https://doi.org/10.1007/s10623-018-0463-8
8. C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pelikaan, Linear codes over F_q are equivalent to LCD codes for $q > 3$, *IEEE Trans. Inform. Theory*, **64** (2018), 3010–3017. https://doi.org/10.1109/TIT.2018.2789347
9. C. Carlet, S. Mesnager, C. Tang, Y. Qi, New characterization and parametrization of LCD codes, *IEEE Trans. Inform. Theory*, **65** (2019), 39–49. https://doi.org/10.1109/TIT.2018.2829873
10. C. Carlet, Boolean functions for cryptography and error correcting codes, In: *Boolean models and methods in mathematics, computer science, and engineering*, Cambridge University Pres, 2010, 257–397. https://doi.org/10.1017/CBO9780511780448.011
11. C. Carlet, S. Guilley, Complementary dual codes for counter measures to side-channel attacks, In: *Coding theory and applications*, Cham: Springer, **3** (2015), 97–105. https://doi.org/10.1007/978-3-319-17296-5_9
12. H. Gluesing-Luerssen, G. Schneider, A MacWilliams identity for convolutional codes: The general case, *IEEE Trans. Inform. Theory*, **55** (2009), 2920–2930. https://doi.org/10.1109/TIT.2009.2021302
13. G. G. La Guardia, On negacyclic MDS-convolutiona codes, *Linear Algebra Appl.*, **448** (2014), 85–96. https://doi.org/10.1016/j.laa.2014.01.033
14. P. Hurley, T. Hurley, Module codes in group rings, In: *2007 IEEE international symposium on information theory*, Nice: IEEE, 2007, 1981–1985. https://doi.org/10.1109/ISIT.2007.4557511
15. P. Hurley, T. Hurley, Codes from zero-divisors and units in group rings, *Int. J. Inf. Coding Theory*, **1** (2009), 57–87. https://doi.org/10.1504/IJICoT.2009.024047
16. P. Hurley, T. Hurley, Block codes from matrix and group rings, In: *Selected topics in information and coding theory*, World Scientific Publishing Co., 2010, 159–194. https://doi.org/10.1142/9789812837172_0005
17. P. Hurley, T. Hurley, LDPC and convolutional codes from matrix and group rings, In: *Selected topics in information and coding theory*, World Scientific Publishing Co., 2010, 195–237. https://doi.org/10.1142/9789812837172_0006
18. K. J. Horadam, *Hadamard matrices and their applications*, Princeton University Press, 2007.
19. T. Hurley, D. Hurley, Coding theory: The unit-derived methodology, *Int. J. Inf. Coding Theory*, **5** (2018), 55–80. https://doi.org/10.1504/IJICOT.2018.10013082
20. T. Hurley, D. Hurley, B. Hurley, Quantum error-correcting codes: The unit design strategy, *Int. J. Inf. Coding Theory*, **5** (2018), 169–182. https://doi.org/10.1504/IJICOT.2018.095018

21. T. Hurley, D. Hurley, B. Hurley, Maximum distance separable codes to order, *arXiv:1902.06624*, 2019. https://doi.org/10.48550/arXiv.1902.06624
22. T. Hurley, Ultimate linear block and convolutional codes, *AIMS Mathematics*, **10** (2025), 8398–8421. https://doi.org/10.3934/math.2025387
23. T. Hurley, Linear block and convolutional MDS codes to equired rate, distance and type, In: *Intelligent computing*, Cham: Springer, **507** (2022), 129–157. https://doi.org/10.1007/978-3-031-10464-0_10
24. R. Johannesson, K. Sh. Zigangirov, *Fundamentals of convolutional coding*, Wiley-IEEE Press, 2015.
25. J. H. van Lint, R. M. Wilson, *A course in combinatorics*, Cambridge University Press, 2001.
26. F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, Elsevier, 1977.
27. C. L. Mallows, N. J. A. Sloan, An upper bound for self-dual codes, *Inf. Control*, **22** (1973), 188–200. https://doi.org/10.1016/S0019-9958(73)90273-8
28. J. L. Massey, Reversible codes, *Inf. Control*, **7** (1964), 369–380. https://doi.org/10.1016/S0019-9958(64)90438-3
29. J. L. Massey, Linear codes with complementary duals, *Discrete Math.*, **106-107**, (1992), 337–342. https://doi.org/10.1016/0012-365X(92)90563-U
30. R. J. McEliece, *The theory of information and coding*, 2 Eds., Cambridge University Press, 2002. https://doi.org/10.1017/CBO9780511606267
31. S. Mesnager, C. Tang, Y. Qi, Complementary dual algebraic geometry codes, *IEEE Trans. Inform. Theory*, **64** (2018), 2390–2397. https://doi.org/10.1109/TIT.2017.2766075
32. V. Pless, Symmetry codes over GF(3) and new five-designs, *J. Combin. Theory Ser. A*, **12** (1972), 119–142. https://doi.org/10.1016/0097-3165(72)90088-X
33. J. M. M. Porras, J. A. D. Pérez, J. I. I. Curto, G. S. Sotelo, Convolutional goppa codes, *IEEE Trans. Inf. Theory*, **52** (2006), 340–344. https://doi.org/10.1109/TIT.2005.860447
34. J. Rosenthal, R. Smarandache, Maximum distance separable convolutional codes, *Appl. Algebra Engrg. Comm. Comput.*, **10** (1999), 15–32. https://doi.org/10.1007/s002000050120
35. J. Rosenthal, Connections between linear systems and convolutional codes, In: *Codes, systems, and graphical models*, New York: Springer, **123** (2001), 39–66. https://doi.org/10.1007/978-1-4613-0165-3_2
36. A. M. Steane, Simple quantum error-correcting codes, *Phys. Rev. A*, **54** (1996), 4741–4751. https://doi.org/10.1103/PhysRevA.54.4741
37. R. Smarandache, H. Gluesing-Luerssen, J. Rosenthal, Constructions for MDS-convolutional codes, *IEEE Trans. Inform. Theory*, **47** (2001), 2045–2049. https://doi.org/10.1109/18.930938
38. The GAP Group, *Groups, algorithms, and programming*, Version 4.12.2; 2022. Available from: `https://www.gap-system.org`