Construction of isodual codes from polycirculant matrices

Minjia Shi, Li Xu, Patrick Solé

Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-020-00799-8

Construction of isodual codes from polycirculant matrices

Minjia Shi[1] · **Li Xu**[1] · **Patrick Solé**[2]

Received: 30 November 2019 / Revised: 15 July 2020 / Accepted: 25 August 2020

Abstract
Double polycirculant codes are introduced here as a generalization of double circulant codes. When the matrix of the polyshift is a companion matrix of a trinomial, we show that such a code is isodual, hence formally self-dual. Numerical examples show that the codes constructed have optimal or quasi-optimal parameters amongst formally self-dual codes. Self-duality, the trivial case of isoduality, can only occur over $\mathbb{F}_2$ in the double circulant case. Building on an explicit infinite sequence of irreducible trinomials over $\mathbb{F}_2$, we show that binary double polycirculant codes are asymptotically good.

Keywords Quasi-polycyclic codes · Isodual codes · Formally self-dual codes · Double circulant codes · Trinomials

Mathematics Subject Classification Primary 94B05 · Secondary 11C08

1 Introduction

Self-dual codes is one of the most fascinating class of codes as witnessed by their many connections with modular forms [25], invariant theory and combinatorial designs [21]. This class has been enlarged, in recent years, to *isodual* codes that is to say codes that are equivalent

Communicated by V. A. Zinoviev.

This research is supported by National Natural Science Foundation of China (61672036), Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), Academic fund for outstanding talents in universities (gxbjZD03).

✉ Minjia Shi
smjwcl.good@163.com

Li Xu
xuli1451@163.com

Patrick Solé
sole@enst.fr

[1] Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Mathematical Sciences, Anhui University, Anhui 230601, China

[2] CNRS, University of Aix Marseille, Centrale Marseille, I2M, Marseille, France

to their duals [1,7,17,21]. These constitute in turn a subclass of the larger class of *formally self-dual codes* that is to say codes the weight enumerator of which is a fixed point of the MacWilliams transform [6,8–10]. A very popular and successful construction technique for isodual codes is the use of circulant matrices. In particular double circulant codes are easily shown to be isodual [5]. In the present paper, we generalize this technique to polycirculant matrices, and introduce double polycirculant codes.

In [2,20] was studied the notion of polycyclic codes, that is linear codes over a finite field F, that are invariant under a generalized shift (called here a *polyshift*), and affording a structure of ideal over a ring of the form $R_f = F[x]/\langle f \rangle$ for some $f \in F[x]$ (the case $f = x^n - 1$ is that of classical cyclic codes). While the name was coined in [20], the concept (under the name pseudo-cyclic code) has been known for a long time [23]. As is well known, polycyclic codes are shortened cyclic codes, and conversely shortened cyclic codes are polycyclic [23, p .241].

In the present paper, we introduce and study a class of codes called double polycirculant codes (DP) from the standpoint of duality, minimum distance, and asymptotic performance. A matrix is called *polycirculant* if its rows are successive polyshifts of its first row. A DP code is then a linear code with generator matrix of the form (I, A) where I is an identity matrix, and A a polycirculant matrix. Thus DP codes reduce to double circulant codes when the polyshift is the classical shift. When $A^t = QAQ$ for Q a permutation matrix it is easy to show that the DP code is equivalent to its dual, and is, in particular, formally self-dual (FSD). FSD codes have been studied extensively over $\mathbb{F}_2$ [6,10,18], $\mathbb{F}_3$ [8], $\mathbb{F}_4$ [12], and even over $\mathbb{F}_5$, or $\mathbb{F}_7$ [9]. Indeed, we can show that DP codes can be binary self-dual only if they are double circulant. We focus on the special case when the matrix of the polyshift is the companion matrix of a trinomial with nonzero constant term. In that situation, every polycirculant matrix satisfies the condition on its transpose mentioned above. For $q = 2, 3, 5, 7$ numerical examples in short to medium lengths show the DP codes have parameters equal or up to one unit of the best-known FSD codes. Further, by random coding, we can show that the relative distances of long binary codes in that family satisfy a family of lower bounds that is, up to epsilons, the Gilbert–Varshamov bound for linear codes of rate one half. They thus constitute a class of asymptotically good codes. The argument relies on the construction of an infinite family of irreducible trinomials, a fact of independent interest, and on some properties of cyclic vectors in linear algebra [13, chap. 7]. This generalizes the asymptotic properties of self-dual double-circulant codes [3], and of self-dual negacirculant codes [4,24]. The proof is restricted to $\mathbb{F}_2$ where we can show that an infinite family of irreducible trinomials exists.

The material is arranged as follows. Section 2 collects the notations and notions needed to follow the rest of the paper. Section 3 studies duality properties of DP codes: isoduality, self-duality and evenness. Section 4 derives asymptotic bounds by random coding. Section 5 displays some numerical examples of parameters of DP codes. Section 6 concludes the article and points out some significant and challenging open problems.

2 Preliminaries

Throughout the paper the notation M^t denotes the transpose of the matrix M.

2.1 Linear codes

Throughout, F denotes a finite field. If q is a prime power, we denote by $\mathbb{F}_q$ the finite field of order q. Let N denote a nonnegative integer. A **(linear) code** C of length N over a finite field $\mathbb{F}_q$ is a $\mathbb{F}_q$ vector subspace of $\mathbb{F}_q^N$. The dimension of the code is its dimension as a $\mathbb{F}_q$ vector space, and is denoted by k. The elements of C are called **codewords**. Two codes C and D are (monomially) **equivalent** if there is a monomial matrix M such that $MC = D$ [14, §1.7] (recall that a matrix is **monomial** if it contains exactly one nonzero element per row and per column; in particular any permutation matrix is a monomial matrix). The **(Hamming) weight** of $x \in \mathbb{F}_q^N$ is denoted by $W(x)$. The **weight distribution** of a code C is the set of numbers A_i's for $i = 0, 1, \ldots, n$, where

$$A_i = |\{x \in C \mid W(x) = i\}|.$$

The minimum nonzero weight d of a linear code is called the **minimum distance**. The **dual** $C^\perp$ of a code C is understood w.r.t. the standard inner product. A code is **self-dual** if it is equal to its dual, and **isodual** if it is equivalent to its dual. A code is **formally self-dual** (FSD) if it has the same weight distribution as its dual. Thus isodual codes are FSD. A binary code is **even** if the weights of all its codewords are even, and **odd** otherwise. If $C(N)$ is a sequence of codes of parameters $[N, k_N, d_N]$, the **rate** r and **relative distance** δ are defined as

$$r = \limsup_{N\to\infty} \frac{k_N}{N} \text{ and } \delta = \liminf_{N\to\infty} \frac{d_N}{N}.$$

A family of codes is said to be **asymptotically good** if it contains a sequence with rate and relative distance such that $r\delta > 0$. Recall the classical **entropy function** $H(x)$ of the real variable x defined for $0 < x < 1$, by the formula

$$H(x) = -x \log(x) - (1 - x) \log(1 - x).$$

See [21, Chap. 10, §11] for background material. We recall, for context, but are not going to invoke, the classical Gilbert–Varshamov bound

$$r \geq 1 - H(\delta).$$

2.2 Polycyclic codes

We say that a linear code C of length n over a field F is **polycyclic** if there exists a vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in F^n$ such that for every $(a_0, a_1, \ldots, a_{n-1}) \in C$ we have

$$(0, a_0, a_1, \ldots, a_{n-2}) + a_{n-1}\,(c_0, c_1, \ldots, c_{n-1}) \in C.$$

We refer to $\mathbf{c}$ as an **associate vector** of C. Note that such a vector may be not unique.

To an associate vector $\mathbf{c}$ we attach the polynomial $c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$. Let $f(x) = x^n - c(x)$. It is shown in [20] that polycyclic codes are ideals in $R_f = F[x]/\langle f(x)\rangle$ with the usual correspondence between vectors and polynomials.

It is shown in [20], that a polycyclic code with the associate vector $\mathbf{c}$ is left invariant by right multiplication of the matrix D of the form:

$$D = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ c_0 & c_1 & c_2 & \dots & c_{n-1} \end{pmatrix}. \tag{1}$$

We call the endomorphism of F^n with matrix D^t the **polyshift** associated with $\mathbf{c}$, and denote it by $T_{\mathbf{c}}$. The matrix D^t is called in linear algebra the **companion matrix** of $f(x)$ [13, §7.1]. If $\mathbf{c} = (1, 0, \dots, 0)$ then $T_{\mathbf{c}}$ is just the standard cyclic shift to the right. Sometimes, to avoid double indices, we will write T for $T_{\mathbf{c}}$.

2.3 Double polycirculant codes

A matrix A of size $n \times n$ is **polycirculant** for a polyshift $T_{\mathbf{c}}$ if its rows are in succession

$$\mathbf{a}, T_{\mathbf{c}}(\mathbf{a}), T_{\mathbf{c}}^2(\mathbf{a}), \dots, T_{\mathbf{c}}^{n-1}(\mathbf{a}).$$

Such a matrix is uniquely determined by its first row and the associate vector $\mathbf{c}$. If $\mathbf{c} = (1, 0, \dots, 0)$ then A is just a circulant matrix. A linear code C of length $2n$ is said to be **double polycirculant** (DP) if its generator matrix G is of the form $G = (I, A)$, where I is the identity matrix of size $n \times n$, and A is a polycirculant matrix of the same size. If $\mathbf{c} = (1, 0, \dots, 0)$, then C is a (pure) double circulant code [3].

Caveat: We use N for the length of the DP code, and n for the size of A. Thus $N = 2n$ in the whole paper.

3 Duality results

3.1 Isoduality

The following proposition is our main motivation to introduce double polycirculant codes.

Proposition 1 *Let A be a matrix satisfying $A^t = QAQ$, with Q a monomial matrix that satisfies $Q^2 = I$, where I is identity of order n. The code $C = \langle (I, A) \rangle$ is an isodual code of length $2n$.*

Proof The parity-check matrix of C is then $H = (-A^t, I)$. Recall that H spans $C^\perp$. Using the hypothesis, we have $H\mathcal{Q} = (-QA, Q)$, where $\mathcal{Q} = \begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix}$. Hence $QH\mathcal{Q} = (-A, I)$, a matrix which spans a code equivalent to C. The result follows. □

Remark 1 In general it is known that any matrix A, invertible over some field satisfies $A^t = uAu$, with $u^2 = I$ [11]. It is not known when u can be a monomial matrix.

Now we exhibit a class of DP codes where this proposition applies.

Theorem 1 *Given an associate vector* $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$*, and the vector* $\mathbf{a} = (a_1, a_2, \ldots, a_n)$*, define the polycirculant matrix A by the equation*

$$A = \begin{pmatrix} \mathbf{a} \\ T_{\mathbf{c}}(\mathbf{a}) \\ T_{\mathbf{c}}^2(\mathbf{a}) \\ \cdots \\ T_{\mathbf{c}}^{n-1}(\mathbf{a}) \end{pmatrix}.$$

The matrix $T_{\mathbf{c}}$ *is the companion matrix of some polynomial* f*. If* f *is of the form* $x^n - ax^m - b$ *with* $a, b \in F \setminus \{0\}$*, then there is a monomial matrix* Q *of order 2 such that* $AQ = QA^t$*. Namely, one can take*

$$Q_{i,j} = \begin{cases} 1, & \text{if} \quad i + j = m + 1, \\ b, & \text{if} \quad i + j = n + m + 1, \\ 0, & \text{otherwise}. \end{cases}$$

In particular, under these hypotheses, the code $C = \langle (I, A) \rangle$ *is isodual.*

Proof We know that for any vector $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$, the matrix

$$T_{\mathbf{c}} = T = \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & c_{n-2} \\ 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix},$$

and it's the companion matrix of $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0$ over $\mathbb{F}_q$. So, if $f(x) = x^n - ax^m - b$, then $c_0 = b$, $c_m = a$, $c_1 = \cdots = c_{m-1} = c_{m+1} = \cdots = c_{n-1} = 0$. If we let $E = AQ$, $F = QA^t$, $E = (E_{i,j})_{n\times n}$, $F = (F_{i,j})_{n\times n}$, $A = (A_{i,j})_{n\times n}$, then we obtain $E_{i,j} = \sum_{k=1}^{n} A_{i,k} Q_{k,j}$, $F_{i,j} = \sum_{k=1}^{n} Q_{i,k} A_{j,k}$, and, by the definition of Q, we can obtain

$$E_{i,j} = \begin{cases} A_{i,m+1-j}, & 1 \le j \le m; \\ bA_{i,n+m+1-j}, & m < j \le n; \end{cases} \quad F_{i,j} = \begin{cases} A_{j,m+1-i}, & 1 \le i \le m; \\ bA_{j,n+m+1-i}, & m < i \le n. \end{cases}$$

Now we have to prove $E_{i,j} = F_{i,j}$ for $i, j = 1, 2, \ldots, n$.

Let T_j be the j-th row of the matrix T. By the definition of A, we can get

$$\left(A_{i,1}, A_{i,2}, \ldots, A_{i,n}\right) = T_c \left(A_{i-1,1}, A_{i-1,2}, \ldots, A_{i-1,n}\right) = \left(A_{i-1,1}, A_{i-1,2}, \ldots, A_{i-1,n}\right) T^t.$$

Then

$$A_{i,j} = (A_{i-1,1}, A_{i-1,2}, \ldots, A_{i-1,n}) T_j^t = \begin{cases} bA_{i-1,n}, & j = 1; \\ A_{i-1,m} + aA_{i-1,n}, & j = m + 1; \\ A_{i-1,j-1}, & otherwise. \end{cases}$$

We distinguish four cases depending on the relative positions of i and j with respect to m.

(i) **If** $1 \le i \le m$ **and** $1 \le j \le m$, then we have $E_{i,j} = A_{i,m+1-j}$ and $F_{i,j} = A_{j,m+1-i}$. In this case, $1 \le m + 1 - i \le m$ and $1 \le m + 1 - j \le m$. If $i \ge j$, when $j = m$, we can get $i = j = m$, $E_{i,j} = A_{m,i} = F_{i,j}$; when $1 \le j < m$, we can get $A_{i,m+1-j} = A_{i-(i-j),m+1-j-(i-j)} = A_{j,m+1-i}$. If $i < j$, we can get $A_{j,m+1-i} = A_{j-(j-i),m+1-i-(j-i)} = A_{i,m+1-j}$. It means that $E_{i,j} = F_{i,j}$.

(ii) **If** $1 \le i \le m$ **and** $m < j \le n$, then we have $E_{i,j} = bA_{i,n+m+1-j}$ and $F_{i,j} = A_{j,m+1-i}$. In this case $1 \le m+1-i \le m$ and $m+1 \le n+m+1-j \le n$. Furthermore, $m+1-i \le j-i$, implying $A_{j,m+1-i} = A_{j-(m-i),m+1-i-(m-i)} = A_{i+j-m,1} = bA_{i+j-m-1,n} = bA_{i,n+m+1-j}$, thus $E_{i,j} = F_{i,j}$.

(iii) **If** $m < i \le n$ **and** $1 \le j \le m$, then we have $E_{i,j} = A_{i,m+1-j}$ and $F_{i,j} = bA_{j,n+m+1-i}$. The proof follows as in case (ii).

(iv) **If** $m < i \le n$ **and** $m < j \le n$, then we have $E_{i,j} = bA_{i,n+m+1-j}$ and $F_{i,j} = bA_{j,n+m+1-i}$. In this case $m+1 \le n+m+1-i \le n$ and $m+1 \le n+m+1-j \le n$. The proof follows as in case (i).

The last assertion follows by Proposition 1. This completes the proof. □

3.2 Self-duality criterion when $q = 2$

In this subsection, and the next one, we work over $\mathbb{F}_2$. Given the vector $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ where $c_1 = c_m = 1, c_i = 0, i \ne 1, m$, and the first row $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ define the matrix $A = \begin{pmatrix} \mathbf{a} \\ T_{\mathbf{c}}(\mathbf{a}) \\ T_{\mathbf{c}}^2(\mathbf{a}) \\ \cdots \\ T_{\mathbf{c}}^{n-1}(\mathbf{a}) \end{pmatrix}$. When $\mathbf{c}$ satisfies the above conditions, $T_{\mathbf{c}}$ is the companion matrix of the trinomial $f(x) = x^n - x^{m-1} - 1$.

Theorem 2 *With the above notation, the code $C = \langle (I, A) \rangle$ where I is identity matrix of order n is a binary self-dual code if and only if $A = I$. In other words, a binary DP code with a trinomial induced polyshift is a self-dual code iff it is equivalent to a direct sum of repetition codes of length* 2.

Proof The code $C = \langle (I, A) \rangle$ is a self-dual code iff $AA^t = -I = I$ over $\mathbb{F}_2$, where A^t is the transpose of A. Now we need to prove $AA^t = I$ iff $A = I$. On the one hand, let $B = AA^t$, $B = (B_{i,j})_{n \times n}$, $A = (A_{i,j})_{n \times n}$, then $B_{i,j} = \sum_{k=1}^{n} A_{i,k} A_{j,k}$.

With the definition of A, we can get the i-th row of A is

$$\begin{aligned}(A_{i,1}, A_{i,2}, \ldots, A_{i,n}) &= (0, A_{i-1,1}, A_{i-1,2}, \ldots, A_{i-1,n-1}) + A_{i-1,n}\mathbf{c} \\ &= (0, A_{i-1,1}, A_{i-1,2}, \ldots, A_{i-1,n-1}) + A_{i-1,n}(1, 0, \ldots, 0, 1, 0, \ldots, 0),\end{aligned}$$

then

$$\begin{aligned}A_{i,1}^2 + A_{i,2}^2 + \cdots + A_{i,n}^2 &= A_{i-1,1}^2 + A_{i-1,2}^2 + \cdots + A_{i-1,n-1}^2 + A_{i-1,n}^2 + A_{i-1,n}^2, \\ \sum_{k=1}^{n} A_{i,k} &= \sum_{k=1}^{n} A_{i-1,k} + A_{i-1,n}.\end{aligned}$$

With the definition of B, we have

$$\begin{aligned}
B_{1,1} &= \sum_{k=1}^{n} A_{1,k}^2 = \sum_{k=1}^{n} A_{1,k} = a_1 + a_2 + \cdots + a_{n-1} + a_n;\\
B_{2,2} &= \sum_{k=1}^{n} A_{2,k}^2 = \sum_{k=1}^{n} A_{2,k} = B_{1,1} + A_{1,n};\\
B_{3,3} &= \sum_{k=1}^{n} A_{3,k}^2 = \sum_{k=1}^{n} A_{3,k} = B_{2,2} + A_{2,n};\\
&\cdots\\
B_{n-1,n-1} &= \sum_{k=1}^{n} A_{n-1,k}^2 = \sum_{k=1}^{n} A_{n-1,k} = B_{n-2,n-2} + A_{n-2,n};\\
B_{n,n} &= \sum_{k=1}^{n} A_{n,k}^2 = \sum_{k=1}^{n} A_{n,k} = B_{n-1,n-1} + A_{n-1,n}.
\end{aligned}$$

If $B = I$, $B_{1,1} = B_{2,2} = \cdots = B_{n,n} = 1$, then we can get $A_{1,n} = A_{2,n} = \cdots = A_{n-1,n} = 0$. Let T_j be the j-th row of matrix T. Since the vector $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ with $c_1 = c_m = 1$, $c_i = 0$, $i \neq 1, m$, we have

$$T_j = \begin{cases} e_n, & j = 1;\\ e_{m-1} + e_n, & j = m;\\ e_{j-1}, & otherwise. \end{cases}$$

where $e_i, i = 1, 2, \ldots, n$ is the canonical basis of F^n, defined by $(e_i) = \delta_{ij}, i, j = 1, 2, \ldots, n$. Thus, by computations similar to those in the proof of Theorem 1, we have

$$A_{i,j} = T_j \begin{pmatrix} A_{i-1,1}\\ A_{i-1,2}\\ \cdots\\ A_{i-1,n} \end{pmatrix} = \begin{cases} A_{i-1,n}, & j = 1; \quad (1)\\ A_{i-1,m-1} + A_{i-1,n}, & j = m; \quad (2)\\ A_{i-1,j-1}, & otherwise \quad (3) \end{cases}$$

If $1 \leq t \leq n - m$, by (3) we can get

$$A_{t,n} = A_{t-(t-1),n-(t-1)} = A_{1,n-t+1} = a_{n-t+1}.$$

So for each $m + 1 \leq j \leq n$ we have

$$a_j = A_{n-j+1,n}.$$

If $n - m + 1 \leq t \leq n$, by (3) we can get

$$A_{t,n} = A_{t-(n-m),n-(n-m)} = A_{t+m-n,m}.$$

So for each $1 \leq i \leq m$ we have

$$A_{i,m} = A_{n-m+i,n}.$$

By applying (2) and then (3), it follows that for each $1 < i \leq m$ we have

$$A_{i,m} = A_{i-1,m-1} + A_{i-1,n} = A_{1,m-i+1} + A_{i-1,n} = a_{m-i+1} + A_{i-1,n}.$$

Then for $1 \leq j < m$ we have

$$a_j = A_{m-j+1,m} - A_{m-j,n} = A_{n-j+1,n} - A_{m-j,n}.$$

What's more, $a_m = A_{1,m} = A_{n-m+1,n}$.

Because $A_{1,n} = A_{2,n} = \cdots = A_{n-1,n} = 0$, so $a_n = a_{n-1} = \cdots = a_2 = 0$; further, $B_{1,1} = 1$, yielding $a_1 = 1$. Then with $\mathbf{a} = (a_1, a_2, \ldots, a_n) = (1, 0, \ldots, 0)$, we check from its definition the matrix $A = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = I$.

On the other hand, if $A = I$, it is immediate that $AA^t = I$. □

3.3 Even isodual codes

An important class of binary isodual codes is the class of even isodual codes that is those isodual codes all weights of which are even [10,18]. The next result shows that over $\mathbb{F}_2$ many isodual codes coming from our construction are odd.

Theorem 3 *Let A be a polycirculant matrix of size $n \times n$, for a polyshift $T_{\mathbf{c}}$. If $\mathbf{c}$ is an even weight vector, then the binary code $C = \langle (I, A) \rangle$ is an even code if and only if the first row of A is $\mathbf{a} = (1, 0, \ldots, 0)$.*

Proof If $C = \langle (I, A) \rangle$ is an even code, then each row of A has an odd weight.

Firstly, suppose the weight of $\mathbf{a}$ is $W(\mathbf{a}) = 1$, namely, $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ with only $a_m = 1$. By the definition of A, we can get the first $n - m + 1$ rows of A as:

$$\begin{aligned} \mathbf{a} &= (0, \ldots, 0, 1, 0, 0, 0, \ldots, 0, 0); \\ T_{\mathbf{c}}(\mathbf{a}) &= (0, \ldots, 0, 0, 1, 0, 0, \ldots, 0, 0); \\ T_{\mathbf{c}}^2(\mathbf{a}) &= (0, \ldots, 0, 0, 0, 1, 0, \ldots, 0, 0); \\ &\cdots \\ T_{\mathbf{c}}^{n-m}(\mathbf{a}) &= (0, \ldots, 0, 0, 0, 0, 0, \ldots, 0, 1). \end{aligned}$$

Then the $(n - m + 2)$-th row is

$$T_{\mathbf{c}}^{n-m+1}(\mathbf{a}) = (0, 0, \ldots, 0, 0) + 1 \cdot \mathbf{c},$$

and the weight of this row is $W(T_{\mathbf{c}}^{n-m+1}(\mathbf{a})) = W(\mathbf{c}) \equiv 0 \pmod 2$. So in this case, if we expect that the weight of each row of A is odd, it requires $n - m = n - 1$, then $m = 1$ and $\mathbf{a} = (1, 0, \ldots, 0)$.

More generally, suppose that the weight of $\mathbf{a}$ is odd, with rightmost nonzero a_i for $i = t$. If we let $W(\mathbf{a}) = 2k + 1$, $k \geq 0$, and $\mathbf{a} = (0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 0)$ with rightmost nonzero $a_t = 1$, reasoning as before, by the definition of A, we can get the first $n - t + 1$ rows of A as:

$$\begin{aligned} \mathbf{a} &= (0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 1, 0, 0, 0, \ldots, 0); \\ T_{\mathbf{c}}(\mathbf{a}) &= (0, 0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 1, 0, 0, \ldots, 0); \\ T_{\mathbf{c}}^2(\mathbf{a}) &= (0, 0, 0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 0); \\ &\cdots \\ T_{\mathbf{c}}^{n-t}(\mathbf{a}) &= (0, \ldots, 0, 0, 0, 0, \ldots, 1, 0, \ldots, 1, 0, \ldots, 1). \end{aligned}$$

Then the $(n-t+2)$-th row is

$$T_{\mathbf{c}}^{n-t+1}(\mathbf{a}) = (0,0,\ldots,0,0,0,0,\ldots,1,0,\ldots 1,0,\ldots,0) + 1\cdot\mathbf{c},$$

and the weight of this row is $W(T_{\mathbf{c}}^{n-t+1}(\mathbf{a})) = 2k + W(\mathbf{c})$. Because $W(\mathbf{c}) \equiv 0 \pmod 2$, in this case, if we expect that the weight of each row of A is odd, it requires $n-t = n-1$, then $t = 1$. It means that $a_1 = 1$ is the rightmost nonzero element of $\mathbf{a}$. Therefore, $\mathbf{a} = (1,0,\ldots,0)$.

On the other hand, if the vector $\mathbf{a} = (1,0,\ldots,0)$, then we can check from the definition of A that $A = I$. It is immediate to check that $C = \langle (I, A)\rangle = \langle (I, I)\rangle$ is an even code. □

Remark 2 When $\mathbf{c}$ has odd weight, we can get that the weight of each row of A is odd if and only if the weight of $\mathbf{a}$ is odd by a similar argument as in the proof of Theorem 3. Namely, the binary code $C = \langle (I, A)\rangle$ is even if and only if $\mathbf{a}$ has odd weight. This extension is left to the reader.

4 Asymptotic performance

We prepare for the main result of the section by the following lemma. Recall that the **Cyclotomic polynomial** of index m denoted here by $Q_m(.)$, is the $\mathbb{Z}$-polynomial with roots all the elements of order m in the algebraic closure of $\mathbb{Q}$ [19].

Lemma 1 ([19, Exercise 3.96]) *For any positive integer n, the trinomial* $H_n(x) = x^{2\cdot 3^n} + x^{3^n} + 1$ *is irreducible over* $\mathbb{F}_2$.

Proof The cyclotomic polynomial $Q_m(x)$ is irreducible over $\mathbb{F}_2$ iff its degree $\phi(m)$ is equal to the order of 2 $\pmod m$, that is the minimal positive integer k such that $2^k \equiv 1 \pmod m$ [19, Th. 2.47 (ii)]. Let $m = 3^{n+1}$. Thus, by [19, Ex. 2.46], we know that $Q_m(x) = H_n(x) = x^{2\cdot 3^n} + x^{3^n} + 1$, and well-known properties of Euler totient function show that $\phi(m) = 2\cdot 3^n$. By [16, Thm 1], because 2 is a primitive root $\pmod 3$, it is a primitive root $\pmod{3^n}$ for all $n \geq 1$. Thus $Q_m(x) = H_n(x)$ is irreducible. □

The number of DP codes of length $2n$ is important to count.

Proposition 2 *For a given polyshift, the number of DP codes of length* $2n$ *over* $\mathbb{F}_q$ *is* q^n.

The easy proof is omitted. We prepare for the proof of the next theorem by a lemma from linear algebra.

Lemma 2 *Let* $0 \neq \mathbf{w} \in \mathbb{F}_q^n$. *Let R be a matrix of size* $n \times n$ *over* $\mathbb{F}_q$ *with an irreducible characteristic polynomial. The matrix with successive rows* $\mathbf{w}, R\mathbf{w}, \ldots, R^{n-1}\mathbf{w}$ *is nonsingular.*

Proof The result is immediate from [13, Chap. 7, Theorem 1 (ii)]. We give an alternative proof as follows. Consider the $\mathbb{F}_q$ vector space

$$V = \{R^i\mathbf{w} \mid i = 0, 1, \ldots, n\}.$$

This vector space is invariant by R. Let h (resp.χ) denote the minimal (resp. characteristic) polynomial of R restricted to V. Let g be the characteristic polynomial of R on the whole space $\mathbb{F}_q^n$. Then by the lemma of [13, p. 200], the polynomial χ divides g. By Cayley-Hamilton theorem, h divides χ. Hence h divides g. By [13, §7, Theorem 1] the degree of h equals the dimension of V. Since g is irreducible, this means that $h = g$ and $V = \mathbb{F}_q^n$. The result follows. □

Theorem 4 *Let* $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$. *For a given polyshift, the matrix of which is the companion matrix of an irreducible trinomial, the number of DPs of length* $2n$ *over* $\mathbb{F}_q$ *that contains the vector* $(\mathbf{u}, \mathbf{v}) \neq 0$ *is at most one.*

Proof We need to solve $A^t \mathbf{u}^t = \mathbf{v}^t$, when $A^t = QAQ$, and Q is as in Theorem 1. Letting $\mathbf{u}' = Q\mathbf{u}^t$ and $\mathbf{v}' = Q\mathbf{v}^t$, $\mathbf{v}' = (v_1', v_2', \ldots, v_n')^t$, we obtain the system of n equations

$$v_1' = \mathbf{a} \cdot \mathbf{u}', \ldots, v_i' = T_{\mathbf{c}}^{i-1}(\mathbf{a}) \cdot \mathbf{u}', \ldots, v_n' = T_{\mathbf{c}}^{n-1}(\mathbf{a}) \cdot \mathbf{u}'.$$

By transposition, we obtain a system in the a_i's whose matrix has successive columns

$$\mathbf{u}', \ldots, T_{\mathbf{c}}^t \mathbf{u}', \ldots, (T_{\mathbf{c}}^t)^{n-1} \mathbf{u}'.$$

By the lemma this matrix is non singular. The result follows. □

We are now in a position to state and prove the main result of this section. The proof technique is the classical method of expurgated random coding.

Theorem 5 *For all* $0 < \delta < H^{-1}(\frac{1}{2})$, *there are sequences of binary DP codes of relative distance* δ *with a polyshift whose matrix is the companion of an irreducible trinomial.*

Proof By Lemma 1, there are infinitely many irreducible trinomials over $\mathbb{F}_2$. For a given n, by Proposition 2 there are $\Omega_n = 2^n$ DP codes of length $2n$ w.r.t. a polyshift whose matrix is the companion matrix of a given irreducible trinomial. We will require the following entropic estimate. The total number of binary vectors of length $2n$, and Hamming weight $< d_n = \lfloor 2\delta n \rfloor$, V_n say, is at most

$$V_n \leq 2^{2nH(\delta)} \tag{2}$$

by [21, Chap. 10, Cor. 9].

By Theorem 4, a nonzero vector $(\mathbf{u}, \mathbf{v})$ with weight $< d_n$ can be contained in at most one such code. If

$$\Omega_n > V_n, \tag{3}$$

then there is at least one such DP code of length $2n$ with minimum distance $\geq d_n$. (Note that it is essential that inequality (3) be strict to derive that conclusion).

By (2) we see that inequality (3) will hold for n large enough if

$$2^{2nH(\delta)} = o(2^n),$$

which will hold in particular if $H(\delta) < 1/2$. □

Remark Thus this theorem means that for every $\epsilon > 0$, there are sequences of DP codes with a relative distance $> H^{-1}(\frac{1}{2}) - \epsilon$. Note, for sake of comparison, that the quantity $H^{-1}(\frac{1}{2})$ is the Gilbert–Varshamov bound on the relative distance of linear binary codes of rate $1/2$.

5 Numerics

In Tables 1, 2 and 3, 4, for, respectively, $q = 2, 3, 5, 7$ we denote by

- $d_F(q, 2n)$ the highest minimum weight of formally self-dual codes over $\mathbb{F}_q$ as per [6,8,9],
- $d_F^*(q, 2n)$ the highest minimum weight of FSD DP codes constructed over $\mathbb{F}_q$.

Table 1 The highest minimum weight for $\mathbb{F}_2$

Length $2n$	$d_F^*(2, 2n)$	$d_F(2, 2n)$
4	2*	2
6	3*	3
8	3*	3
10	3	4
12	4*	4
14	4*	4
16	5*	5
18	5*	5
20	5	6
22	6	7
24	6	7
26	6	7
28	6	7
30	7*	7 or 8
32	7	8
34	7	8
36	8*	8
38	8*	8 or 9
40	8	9 or 10

Table 2 The highest minimum weight for $\mathbb{F}_3$

Length $2n$	$d_F^*(3, 2n)$	$d_F(3, 2n)$
4	3*	3
6	3*	3
8	4*	4
10	4	5
12	5	6
14	5	6
16	6*	6
18	6*	6
20	6	7
22	7	8
24	8	9
26	8*	8 or 9
28	8	9 or 10
30	8	9, 10 or 11

We put a star exponent on the entry $d_F^*(q, 2n)$ whenever $d_F^*(q, 2n) = d_F(q, 2n)$. In Table 5 we denote by $d_{fsdao}(4, 2n)$ the highest minimum weight of formally self-dual additive odd codes over $\mathbb{F}_4$ ([12]); and by $d_{fsdao}^*(4, 2n)$ the highest minimum weight of FSD DP codes that we can find over $\mathbb{F}_4$. We put a star exponent on the entry $d_{fsdao}(4, 2n)^*$ whenever $d_{fsdao}(4, 2n)^* = d_{fsdao}(4, 2n)$. We constructed a large number of random DP codes with trinomial polyshifts as in Theorem 1, and the Tables collect the best found. All binary codes

Table 3 The highest minimum weight for $\mathbb{F}_5$

Length $2n$	$d_F^*(5, 2n)$	$d_F(5, 2n)$
4	3*	3
6	4*	4
8	4*	4
10	5*	5
12	6*	6
14	6*	6
16	7*	7
18	7*	7 or 8
20	7	8 or 9
22	8*	8, 9 or 10
24	8	9 or 10

Table 4 The highest minimum weight for $\mathbb{F}_7$

Length $2n$	$d_F^*(7, 2n)$	$d_F(7, 2n)$
4	3*	3
6	4*	4
8	4	5
10	5*	5
12	6*	6
14	6	7
16	7*	7 or 8
18	7	8 or 9
20	8	9 or 10
22	8	9, 10 or 11
24	9	10, 11 or 12

Table 5 The highest minimum weight for $\mathbb{F}_4$

Length $2n$	$d_{fsdao}^*(4, 2n)$	$d_{fsdao}(4, 2n)$
4	3*	3
6	3*	3
8	4*	4
10	5*	5
12	5	6
14	6*	6 or 7

constructed are odd. All the DP codes constructed in this section are FSD codes by Theorem 1. All computations were performed in Magma [15].

6 Conclusion and open problems

In this work we have introduced a new class of codes of rate one half: double polycirculant codes. These codes are the natural generalization of double circulant codes when going from standard shift to the polyshift of polycylic codes. When the matrix of the polyshift is the companion matrix of a trinomial of the form $x^n + ax^m + b$, these codes are isodual, and in particular formally self-dual. In short lengths, their parameters are optimal or quasi-optimal amongst FSD codes. More importantly, when $q = 2$, we could show that they are asymptotically good.

Many open problems remain. Characterizing the matrices over finite fields that are monomially equivalent to their transpose could lead to new constructions of isodual codes. At a more structural level, it might be possible to derive isoduality for a larger class of polyshifts. The characterization of evenness is only done for half the associate vectors. It would be worth constructing even FSD codes over $\mathbb{F}_2$, the first studied class of FSD codes [10,18], by DP codes, or to prove they do not exist. Eventually, DP codes over finite rings is a wide open area, which is well worth investigating, in view of the double circulant codes over rings of [5].

References

1. Alahmadi A., Alsulami S., Hijazi R., Solé P.: Isodual cyclic codes over finite fields of odd characteristic. Discret. Math. **339**(1), 344–353 (2016).
2. Alahmadi A., Dougherty S.T., Leroy A., Solé P.: On the duality and the direction of polycyclic codes. Adv. Math. Commun. **10**(4), 921–929 (2016).
3. Alahmadi A., Ozdemir F., Solé P.: On self-dual double circulant codes. Des. Codes Cryptogr. **86**(6), 1257–1265 (2018).
4. Alahmadi A., Güneri C., Ozkaya B., Shohaib H., Solé P.: On self-dual double negacirculant codes. Discret. Appl. Math. **222**, 205–212 (2017).
5. Bachoc C., Gulliver A., Harada M.: Isodual codes over $\mathbb{Z}_{2k}$ and Isodual lattices. J. Algebr. Comb. **12**, 223–240 (2000).
6. Betsumiya K., Harada M.: Binary optimal odd formally self-Dual codes. Des. Codes Cryptogr. **23**(1), 11–22 (2001).
7. Blackford T.: Isodual constacyclic codes. Finite Fields Appl. **24**, 29–44 (2013).
8. Dougherty S.T., Gulliver T.A., Harada M.: Optimal ternary formally self-dual codes. Discrete Math. **196**, 117–135 (1999).
9. Dougherty S.T., Gulliver T.A., Harada M.: Optimal formally self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$, Appl. Algebra Eng. Commun. Comput. **10**(3), 227–236 (2000).
10. Fields J., Gaborit P., Pless V., Huffman W.C.: On the classification of extremal even formally self-dual codes of lengths 20 and 22. Discret. Appl. Math. **111**, 75–86 (2001).
11. Gow R.: The equivalence of an invertible matrix to its transpose. Linear Multilinear Algebra **8**(4), 329–336 (2008).
12. Han S., Kim J.-L.: Formally self-dual additive codes over $\mathbb{F}_4$. J. Symbol. Comput. **45**, 787–799 (2010).
13. Hoffman K., Kunze R.: Linear Algebra, 2nd edn. Prentice-Hall, Englewood Cliffs, NJ (1971).
14. Huffman W.C., Pless V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003).
15. http://magma.maths.usyd.edu.au/calc/.
16. Jolly N.: Constructing the primitive roots of prime powers. Honors thesis, La Trobe University, Australia (2008).
17. Kim H.-J., Lee Y.: Construction of isodual codes over $GF(q)$. J. Symbol. Comput. **45**, 372–385 (2017).
18. Kim J.-L., Pless V.: A note on formally self-dual even codes of length divisible by 8. Finite Fields Appl. **13**(2), 224–229 (2007).
19. Lidl R., Niederreiter H.: Finite Fields, Encyclopedia of Math and Its Applications, vol. 20. Cambridge University Press, Cambridge (1997).

20. Lopez-Permouth S.R., Parra-Avila B.R., Szabo S.: Dual generalizations of the concept of cyclicity of codes. Adv. Math. Comput. **3**(3), 227–234 (2009).
21. MacWilliams F.J., Sloane N.J.A.: The Theory of Error Correcting Codes. North Holland, Amsterdam (1977).
22. Mihoubi C., Solé P.: Optimal and isodual ternary cyclic codes of rate 1/2, Bull. Math. Sci. **2**, 343–357 (2012).
23. Peterson W.W., Weldon E.J.: Error Correcting Codes, 2nd edn. MIT Press, Cambridge, MA (1972).
24. Shi M., Qian L., Solé P.: On self-dual negacirculant codes of index two and four. Des. Codes Cryptogr. **86**(11), 2485–2494 (2018).
25. Shi M., Choie Y.J., Sharma A., Solé P.: Codes and Modular Forms: A Dictionary. World Scientific, Singapore (2020).
26. von zur Gathen J., Irreducible trinomials over finite fields: von zur Gathen. J. Math. Comput. **72**, 1987–2000 (2003).