HALF-CYCLIC, DIHEDRAL AND HALF-DIHEDRAL CODES

R. JAJCAY, P. POTOČNIK, S. WILSON

Abstract. This note discusses, in elementary terms, linear codes over $\mathbb{Z}_2$ which are closed under 2-step cyclic shifts, and classifies them in terms of special linear combinations of polynomials. Codes which are preserved under order-reversing automorphisms are also discussed, and a classification result in terms of special linear combinations of polynomials is obtained.

1. Introduction

The results in this note were motivated by the study of the *Praeger-Xu* graphs, $\Gamma = \mathrm{PX}(n, k)$ for $k < n$ as defined in [5, 10]. With three small exceptions, these graphs have symmetry groups $\mathrm{Aut}(\Gamma)$ isomorphic to $\mathbb{Z}_2^n \rtimes \mathbb{D}_n$. In investigating vertex-transitive subgroups of $\mathrm{Aut}(\Gamma)$, in particular the Cayley subgroups, one needs to understand binary linear codes of length n which generalize the well-known cyclic codes. The more general codes needed in the study of the Praeger-Xu graphs are linear subspaces of $\mathbb{Z}_2^n$ invariant under the actions of subgroups of the dihedral group $\mathbb{D}_n = \langle R, M\rangle$ where R is the cyclic rotation of the positions (columns) of the code and M reverses the codewords. In this paper, we use the terms *half-cyclic, dihedral* and *half-dihedral* to indicate the three types of codes of interest. These are binary linear codes invariant under the action of $\langle R^2\rangle$, $\langle R, M\rangle$, and $\langle R^2, M\rangle$, respectively. This paper's primary results are Theorem 2.11 which classifies half-cyclic codes, Theorem 3.3 which classifies the dihedral codes, and Theorem 3.5 which classifies half-dihedral codes.

It should be noted that half-cyclic codes constitute the simplest case of codes known under the name of *quasi-cyclic codes*. Quasi-cyclic codes are linear subspaces of $\mathbb{Z}_2^n$ invariant under R^i, for some fixed $1 \leq i \leq n-1$. They have been the focus of a number of articles (e.g.,[1, 2, 3, 6, 7, 8, 9, 11]), the majority of which seek a unified theory for all possible $1 \leq i \leq n-1$, and tend to require quite a bit of algebraic machinery. Our approach differs in two significant ways. First, by focusing on the single case $i = 2$, our approach allows us to use only elementary linear algebra, and, second, the obtained results are close in flavor to the well-known classification of cyclic codes that relates these codes to divisors of $t^n - 1$ over $\mathbb{Z}_2$ and is given later in this section as Theorem 1.1.

In this note, we will write elements of $\mathbb{Z}_2^n$ as bitstrings. Let R be the the linear transformation of $\mathbb{Z}_2^n$ mapping the string $u = u_0u_1u_2\dots u_{n-1}$ to $uR = u_{n-1}u_0u_1u_2\dots u_{n-2}$. We call this R a *cyclic shift*. An even power of R is an

Key words and phrases. linear codes, cyclic codes, half-cyclic codes, code symmetries, 94Bxx.

The first author is supported by the projects VEGA 1/0474/15, VEGA 1/0596/17, VEGA 1/0423/20, APVV-15-0220, and by the Slovenian Research Agency (research projects N1-0038, N1-0062, J1-9108). The second author gratefully acknowledges the support of the Slovenian Research Agency, Programme P1–0294, and all three authors acknowledge the support of the bilateral project BI-US/16-17-031.

even shift, and an odd power is an odd shift. The substring of a vector $u = u_0u_1u_2 \dots u_{n-1}$ consisting of positions starting from the first 1 (the *leading* 1) to the last 1 (the *trailing* 1) will be called the *core* of u. For example, if $u = 01101000$, its leading 1 is in position 1 ($u_1 = 1$), its trailing 1 is in position 4 ($u_4 = 1$), and its core is the string 1101.

A non-trivial subspace C of $\mathbb{Z}_2^n$ which is invariant under R is called a *cyclic code* (even though cyclic codes can be defined over any finite alphabet, in this paper we will only consider binary codes). Cyclic codes are well-known [4] and completely classified via identification of the elements of $\mathbb{Z}_2^n$ with polynomials. Specifically, let V_n be the additive subgroup of polynomials within $\mathbb{Z}_2[t]$ of degrees smaller than n. Then the vector $u = u_0u_1u_2 \dots u_{n-1}$ is identified with the polynomial $u(t) = u_0 + u_1t + u_2t^2 + \dots u_{n-1}t^{n-1}$ in $\mathbb{Z}_2[t]$. In what follows, when referring to the *degree* of the bitstring u we mean the degree of the corresponding polynomial $u(t)$; the degree is equal to the position of the trailing 1 of u.

The following theorem on cyclic codes is well-known:

Theorem 1.1. *If C is a cyclic code, consider the non-trivial element u of C ending in the greatest number of zeroes; it is unique and corresponds to the polynomial $u(t)$ of smallest possible degree. Then the following are true:*

(1) The polynomial $u(t)$ divides $t^n - 1$.
(2) If the degree of $u(t)$ is k, then C has dimension $n - k$.
(3) C has a basis consisting of all uR^i having the same core as u, i.e., a basis consisting of the vectors uR^i, $0 \leq i \leq n - k - 1$.

We call the unique u from Theorem 1.1 the *generator* of C and $u(t)$ its *generating polynomial.*

2. Half-cyclic codes

The types of codes that we wish to consider in this note are not cyclic, but still exhibit similar symmetry properties.

Definition 2.1. If n is even, a subspace C of $\mathbb{Z}_2^n$ will be called a *half-cyclic code* provided it is invariant under the even shift R^2.

All codes invariant under R are obviously invariant under R^2, and if n is odd, all codes invariant under R^2 are also invariant under R. That is why, in the above definition, n is assumed to be an even positive integer. This will be assumed throughout our paper; $n = 2m$, with m being a positive integer.

Our goal is to develop theorems similar to Theorem 1.1, classifying half-cyclic codes and their canonical bases in terms of polynomials, and then do the same for the related dihedral and half-dihedral codes defined in Section 3.

Let π_e and π_o denote the projection of $\mathbb{Z}_2^n$ onto $\mathbb{Z}_2^m$ defined via the formulas $\pi_e(u_0u_1u_2 \dots u_{n-1}) = u_0u_2 \dots u_{n-2}$ and $\pi_o(u_0u_1u_2 \dots u_{n-1}) = u_1u_3 \dots u_{n-1}$ (projections onto the even and odd positions). Given a half-cyclic code C, both projections $\pi_e(C), \pi_o(C)$, are necessarily cyclic codes, and correspond to generating polynomials $u_o(t), u_e(t)$ which are divisors of $t^m - 1$ over $\mathbb{Z}_2$. Thus, any half-cyclic code $C \subseteq \mathbb{Z}_2^n$ can be viewed as a 'merging' of two cyclic codes $C_1, C_2 \subseteq \mathbb{Z}_2^m$. More precisely, let $w = w_0w_1 \dots w_{m-1}, w' = w'_0w'_1 \dots w'_{m-1} \in \mathbb{Z}_2^m$. The *merged bitstring* of w, w' is the bitstring $v = w_0w'_0w_1w'_1 \dots w_{m-1}w'_{m-1} \in \mathbb{Z}_2^n$. If $v_1, v_2, \dots, v_k$ is a basis for C, then $\pi_o(v_1), \pi_o(v_2), \dots, \pi_o(v_k)$ must generate the cyclic code $\pi_o(C)$, and $\pi_e(v_1), \pi_e(v_2), \ldots, \pi_e(v_k)$ must generate the cyclic code $\pi_e(C)$. It is important to observe that we do not claim the two sets form bases for the corresponding cyclic codes, as they do not need to. The following examples illustrate these ideas.

Example 2.2. Let $m = 3, n = 6$, and let $C_1 = \mathbb{Z}_2^3 = \langle 100, 010, 001\rangle$. The code obtained by merging each word of C_1 with each word of C_1 can be easily seen to be equal to the entire space $\mathbb{Z}_2^6$ and is therefore of dimension 6. Neither of the projections π_e or π_o is injective; not even when restricted to the basis of $\mathbb{Z}_2^6$. On the other hand, considering the repetition code obtained by merging each codeword of C_1 with itself yields a 3-dimensional subspace of $\mathbb{Z}_2^6$ generated by the vectors $110000, 001100, 000011$ and with each projection being injective and mapping a basis to a basis.

Example 2.3. Let $m = 3, n = 6$, and let $C_1 = \mathbb{Z}_2^3 = \langle 100, 010, 001\rangle$, $C_2 = \langle 000\rangle$ be cyclic codes of length 3. The bitstrings $100000, 0010000, 000010$ obtained by merging the generators of C_1 with the vector 000 can be easily seen to form a basis for a half-cyclic code of length 6.

It is also easy to see that for any two cyclic codes C_1 and C_2 of length m, the code of length $n = 2m$ consisting of all the merges of a word from C_1 with a word from C_2 is a half-cyclic code.

Example 2.4. Taking all the merges of the code $C_1 = \mathbb{Z}_2^3 = \langle 100, 010, 001\rangle$ with the code $C_3 = \langle 110, 011\rangle$ yields a half-cyclic code C_{1+3} of length 6 and dimension 5. The code C_{1+3} is not cyclic.

Finally, the code generated by the vectors $100000, 110000, 001100, 000011$ is a 4-dimensional linear code which is not half-cyclic, while both the even and odd projections of this code are cyclic. Thus, the condition that both the even and odd projections of the basis of a linear code C generate cyclic codes of half-length is not sufficient for C being half-cyclic. Equivalently, each half-cyclic C of length $n = 2m$ is associated with two divisors of $t^m - 1$ (the generating polynomials for the even and odd projection codes), however, knowing these two divisors does not suffice for reconstructing C, and one needs to understand the relation by which these two polynomials are tied together. These additional requirements needed to guarantee that C is half-cyclic will be determined in Theorem 2.11.

The reader will probably agree that the repetition code from Example 2.2 and the code constructed in Example 2.3 are, in a way, degenerate. In what follows, we first define precisely what we mean by degenerate, and in Lemma 2.6 we classify such codes.

For an integer $h, 0 < h < n$, let $\pi_h : \mathbb{Z}_2^n \to \mathbb{Z}_2^h$ denote the linear projection sending each $u_0u_1u_2 \ldots u_{n-1}$ to $u_0u_1u_2 \ldots u_{h-1}$. We say that a code C is *h-full* provided the dimension of $\pi_h(C)$ is equal to h. The maximum h for which C is h-full is its *fullness* (clearly, a k-dimensional code is at most k-full). We will call a code which is not 2-full a *degenerate* code.

Degenerate half-cyclic codes in $\mathbb{Z}_2^n$ are relatively easy to understand. In stating our result, we rely on three merging functions from $\mathbb{Z}_2^m$ to $\mathbb{Z}_2^{2m}$:

Definition 2.5. Let m be an integer, and $n = 2m$. For each $u \in \mathbb{Z}_2^m$, $u = u_0u_1u_2 \ldots u_{m-1}$, let $\theta_1(u) = 0u_00u_10u_2 \ldots 0u_{m-1}$ be the merge of $00 \ldots 0$ with u, let $\theta_2(u)$ to be the merge of u with $00 \ldots 0$, and finally, let $\theta_3(u)$ to be the merge of u with itself.

Thus, $\theta_1(110) = 010100$, $\theta_2(110) = 101000$, and $\theta_3(110) = 111100$.

Lemma 2.6. *If C' is a cyclic code of length m and dimension s, then each of the codes $C_1 = \theta_1(C')$, $C_2 = \theta_2(C')$, and $C_3 = \theta_3(C')$ is a degenerate half-cyclic code of length $n = 2m$ and dimension s. Moreover, every degenerate half-cyclic code arises in this way.*

Proof. All three codes are obviously invariant under R^2, and therefore half-cyclic. The dimension of $\pi_2(C_i)$ is at most 1, for all $1 \le i \le 3$. Finally, if C is a half-cyclic code and $dim(\pi_2(C)) \le 1$, then $\pi_2(C)$ is equal to one of the one-dimensional spaces $\langle 10\rangle$, $\langle 01\rangle$, or $\langle 11\rangle$, in which case $C = \theta_2(C')$, $C = \theta_1(C')$ or $C = \theta_3(C')$, respectively, for some cyclic code C'. □

If C is a half-cyclic code, so is its cyclic shift CR. We will call C and CR *associates* of each other. Then the associate of a degenerate half-cyclic code of type 1 is one of type 2 and vice versa. However the associate of a code of type 3 might be a non-degenerate half-cyclic code. A non-degenerate half-cyclic code is associate to a degenerate one if and only if every codeword has the first entry the same as the last.

In order to state our result about non-degenerate half-cyclic codes, we need the following concepts and notation.

Definition 2.7. If $u(t), v(t)$ and $w(t)$ are polynomials, we say the $w(t)$ is an *alternating linear combination* (ALC for short) of $u(t)$ and $v(t)$, in that order, if there are polynomials $f(t), g(t) \in \mathbb{Z}_2[t]$ such that $w(t) = f(t^2)u(t) + tg(t^2)v(t)$ (with the multiplication performed in $\mathbb{Z}_2[t]$). In other words, $w(t)$ is an ALC of $u(t)$ and $v(t)$ if $w(t)$ is a linear combination of $u(t)$ and $v(t)$ over $\mathbb{Z}_2[t]$ with the coefficient of $u(t)$ being an even polynomial and the coefficient of $v(t)$ being an odd polynomial. If $w(t)$ is both an ALC of $u(t)$ and $v(t)$ and also an ALC of $v(t)$ and $u(t)$, we will say that $u(t)$ and $v(t)$ are *semi-divisors* of $w(t)$.

In this paper, we will need to consider only semi-divisors of $w(t) = t^n - 1$. Then polynomials $u(t)$ and $v(t)$ are semidivisors of $t^n - 1$ iff there exist polynomials f_1, g_1, f_2, g_2 such that

$$t^n - 1 = f_1(t^2)u(t) + tg_1(t^2)v(t),$$
$$t^n - 1 = f_2(t^2)v(t) + tg_2(t^2)u(t).$$

Example 2.8. In $\mathbb{Z}_2^8$, let $u = 11000110$ and $v = 11100000$, with the corresponding polynomials $u(t) = 1 + t + t^5 + t^6$ and $v(t) = 1 + t + t^2$. Then,

$$t^8 - 1 = (1 + t^2)u(t) + t(1 + t^4)v(t), \text{ and } t^8 - 1 = (1 + t^6)v(t) + tu(t),$$

which shows that $u(t)$ and $v(t)$ are semi-divisors of $t^8 - 1$.

Definition 2.9. For vectors u and v in $\mathbb{Z}_2^n$, of degrees a and b, respectively, suppose that

(1) $u_0 = 1$ and $v_0 = 1$,
(2) a and b are of the same parity,
(3) $b < n - 1$, and
(4) $u(t)$ and $v(t)$ are semi-divisors of $t^n - 1$.

We will call an ordered pair (u, v) satisfying the above conditions a *generating pair* of vectors, and we define the *stepped set* generated by u and v to be the set of vectors

$$\{uR^{2i} | 0 \leq 2i < n - a\} \cup \{vR^{2i+1} | 1 \leq 2i + 1 < n - b\}.$$

Note that the stepped set generated by (u, v) consists of all even shifts of u having the same core as u and all odd shifts of v having the same core as v. Note also that the order of the vectors u and v matters; i.e., the stepped set generated by (u, v) might be different from the stepped set generated by the vectors (v, u).

Example 2.10. Consider the vectors $u = 10011000$ and $v = 10100000$ in $\mathbb{Z}_2^8$, of degrees 4 and 2 respectively. Then $u(t) = 1+t^3+t^4$ while $v(t) = 1+t^2$. We see that

$$t^8 - 1 = (1 + t^4)u(t) + t(t^2 + t^4)v(t),$$
and
$$t^8 - 1 = (1 + t^2 + t^4 + t^6)v(t) + t(0)u(t),$$

showing that $u(t)$ and $v(t)$ are semi-divisors of t^8-1. Thus, (u, v) forms a generating pair and generates the stepped set
$x_0 = uR^0 = 10011000$
$x_1 = vR^1 = 01010000$
$x_2 = uR^2 = 00100110$
$x_3 = vR^3 = 00010100$
$x_4 = vR^5 = 00000101.$

Theorem 2.11 (The Half-Cyclic Code Theorem). *Let C be a non-degenerate half-cyclic code of length n. Then C has a basis which is a stepped set generated by a generating pair of vectors (u, v).*

Conversely, given a generating pair (u, v), the stepped set generated by (u, v) is a basis for a non-degenerate half-cyclic code C.

Moreover, if C is the half-cyclic code generated by a stepped basis formed from a generating pair (u, v), and a and b denote the degrees of $u(t)$ and $v(t)$, respectively, the dimension of C is $n - \frac{a+b}{2}$, and the fullness h of C is

$$h = \begin{cases} \min\{n - a, n + 1 - b\}, & \textit{if } a \textit{ and } b \textit{ are both even,} \\ \min\{n + 1 - a, n - b\}, & \textit{if } a \textit{ and } b \textit{ are both odd.} \end{cases}$$

Proof. For any subspace C of $\mathbb{Z}_2^n$, let $\mathcal{J}$ be the *leading set* of C, i.e., the set of all j, $0 \leq j \leq n - 1$, such that some element of C has its leading 1 in position j. Further, if the elements of $\mathcal{J}$ are $j_0 < j_1 < j_2 < \cdots < j_{s-1}$, define a *transversal* for $\mathcal{J}$ to be any set of vectors $x_0, x_1, \ldots, x_{s-1}$ in C with the property that the leading 1 of x_i is in position j_i, for all i. Clearly, every basis for C is equivalent, via Gaussian reduction, to a transversal, and each transversal is a basis for C. Hence, the cardinality s of $\mathcal{J}$ is the dimension of C. While there may be many transversal bases for C, the vector x_{s-1} is necessarily the same in all of them. This uniqueness follows from the fact that the sum of two distinct vectors with leading 1's in position j_{s-1} is necessarily a non-zero vector with leading 1 in a position further to the right than j_{s-1}, while j_{s-1} is assumed to be the last position for a leading 1.

Now assume that C is a non-degenerate half-cyclic code, that $\mathcal{J}$ is its leading set, and that the vectors $x_0, x_1, \ldots, x_{s-1}$ form a transversal for $\mathcal{J}$. By non-degeneracy, j_0 must be 0, and j_1 must be 1. Moreover, if $j \in \mathcal{J}$ and $j \geq 2$, then $j - 2 \in \mathcal{J}$. Thus, $\mathcal{J}$ must consist of all even numbers from 0 up to some last even number,

j_e, and of all odd numbers from 1 up to some j_o. Let x_e be the vector in this transversal basis whose leading 1 is in position j_e; similarly, let x_o be that for j_o. It follows that x_e and x_o must have their trailing 1's in position $n-1$ or $n-2$. By subtraction, and non-degeneracy, we can assume that one of them ends in 1 and the other in 10. With x_e and x_o so chosen, let $u = x_e R^{-j_e}$ and $v = x_o R^{-j_o}$. Then both u and v have their leading 1's in position 0, $u \in C$ and, while v need not be in C, vR *is* in C. Since $j_o \geq 1$, $\deg(v) < n-1$. Because x_e and x_o have their trailing 1's in positions of opposite parity, u and v must have their trailing 1's in positions of the same parity, and so the polynomials $u(t)$ and $v(t)$ have degrees of the same parity. Thus (u, v) satisfies the first three conditions of a generating pair. We now need to show that $u(t)$ and $v(t)$ are semi-divisors of $t^n - 1$.

For each $i \in \{0, 1, \dots, s-1\}$, replace x_i, the vector having its leading 1 in position $j_i \in \mathcal{J}$, with uR^{j_i} if j_i is even, and with vR^{j_i} if j_i is odd. This new set $\mathcal{B}$ is still a transversal for $\mathcal{J}$, and so a basis for C. The core of each bitstring in $\mathcal{B}$ is the same as the core of u or the core of v, depending on the parity of the corresponding j_i. It is also easy to see that the basis $\mathcal{B}$ is the stepped set generated by (u, v).

In terms of polynomials, each $x_i(t)$ is $t^{j_i}u(t)$ or $t^{j_i}v(t)$, again depending on the parity of j_i, with even j_i's appearing in $t^{j_i}u(t)$ and odd j_i's appearing in $t^{j_i}v(t)$. Let $\mathcal{B}(t)$ stand for this set of polynomials. Because of this parity division, every linear combination over $\mathbb{Z}_2$ of the polynomials in $\mathcal{B}(t)$ is an ALC of $u(t)$ and $v(t)$.

Recall that $\mathcal{B}$ contains a vector w which ends in 10 (which is either x_e or x_o). Since C is a half-cyclic code, wR^2 is in C, and therefore it is a linear combination of the vectors in $\mathcal{B}$. Now, let $z(t)$ be the polynomial corresponding to wR^2. Then, $z(t) = t^2 w(t) - t^n + 1$, and so $t^n - 1 = t^2 w(t) - z(t)$. Since both w and z belong to C, their corresponding polynomials are ALC's of $u(t)$ and $v(t)$, and so is the expression $t^2 w(t) - z(t)$. It follows that $t^n - 1$ is an ALC of $u(t)$ and $v(t)$, in that order.

Similarly, assume that w' is the vector in $\mathcal{B}$ which ends in 1 (this is the other of the vectors x_o or x_e), and let $\epsilon = w'_{n-2}$. Then w' is of the form $00\dots01\dots\epsilon1$. Since, $w'R^2 \in C$, the corresponding polynomial $z'(t)$ is an ALC of $u(t)$ and $v(t)$. At the same time, $z'(t) = t^2 w'(t) - t^{n+1} + t - \epsilon(t^n - 1)$. Since we already know that $t^n - 1$ is an ALC of $u(t)$ and $v(t)$, subtracting $t^2 w'(t) - \epsilon(t^n - 1)$ from both sides yields that $t^{n+1} - t$ is an ALC of $u(t)$ and $v(t)$. Since the constant term of $t^{n+1} - t$ is zero, the coefficient polynomial of $u(t)$ must have zero constant term as well. Thus, we can divide both sides by t and obtain an expression for $t^n - 1$ as an ALC of $v(t)$ and $u(t)$ (in *that* order). In this way, we have established that $u(t)$ and $v(t)$ are semi-divisors of $t^n - 1$, which completes the proof of the first statement of our theorem.

To prove the second statement, suppose that $u(t)$ and $v(t)$ are semi-divisors of $t^n - 1$ such that (u, v) is a generating pair. The stepped set $\mathcal{B} = x_0, x_1, \dots, x_{s-1}$ generated by u and v is an independent set of vectors, and is therefore a basis for a subspace C of $\mathbb{Z}_2^n$. To show that C is closed under R^2, it is enough to show that the images of the elements in $\mathcal{B}$ under R^2 all belong to C. By the very definition of the stepped set, all of the vectors in $\mathcal{B}$ except x_e and x_o end in at least two zeros and thus their images under R^2 belong to $\mathcal{B}$. Moreover, since the degrees of $u(t)$ and $v(t)$ are of the same parity, one of the two vectors x_e and $x_o \in \mathcal{B}$ ends in 1 and one ends in 10. Reversing the argument from the previous paragraph implies that both $x_e R^2$ and $x_o R^2$ belong to the span of $\mathcal{B}$. Namely, if we denote the polynomials corresponding to x_e and x_o by $z(t)$ and $z'(t)$, both $t^2z(t)$ and $t^2z'(t)$ take the form of a polynomial that is a sum of polynomials corresponding to elements in $\mathcal{B}$ plus t^n-1, or $t^{n+1}-t$, or both. Since we assume that t^n-1 is an ALC of $u(t)$ and $v(t)$, and thus $t^{n+1}-t$ is an ALC of $v(t)$ and $u(t)$, both t^n-1 and $t^{n+1}-t$ are also sums of polynomials corresponding to elements in $\mathcal{B}$. Hence, $z(t)$ and $z'(t)$ are sums of polynomials corresponding to elements in $\mathcal{B}$ which means that x_eR^2 and x_oR^2 belong to the span of $\mathcal{B}$.

To prove the third part of the theorem, we consider separately the case in which $a=\deg(u(t))$ and $b=\deg(v(t))$ are both even and the case in which a and b are both odd.

(1) Suppose that a and b are both even. Then the elements of the basis which are in the orbit of u are the even cyclic shifts uR^{2i}, where $a+2i\le n-1$. Moreover, since a is even, it must be the case that $a+2i\le n-2$. The set of i's that satisfy this inequality is $\{0,1,\dots,\frac{n-2-a}{2}\}$, and this is a set of cardinality $\frac{n-a}{2}$. Similarly, all elements of the basis that belong to the orbit of v are of the form vR^{2i+1}, where $b+2i+1\le n-1$. The solutions to this inequality belong to the set $\{0,1,\dots,\frac{n-2-b}{2}\}$ of cardinality $\frac{n-b}{2}$. Combining the two cardinalities yields that the dimension s of C is equal to $\frac{n-a}{2}+\frac{n-b}{2}=n-\frac{a+b}{2}$.

Furthermore, j_e is $n-2-a$ and j_o is $n-1-b$. Let j' be the smaller of j_e, j_o. Then the leading set includes all of 0, 1, 2, $\dots$, $j', j'+1$, but does not include $j'+2$. The fullness of C is then $j'+2$, which is, in this case, $\min\{n-a, n+1-b\}$, as required.

(2) Suppose that both a and b are odd. An argument similar to the one above about dimension shows that the number of basis elements which are even shifts of u is $\frac{n+1-a}{2}$, while the number of odd shifts of v is $\frac{n-1-b}{2}$. Thus, $s=\frac{n+1-a}{2}+\frac{n-1-b}{2}=n-\frac{a+b}{2}$. Finally, a proof similar to the previous one about fullness shows that when a and b are both odd, then the fullness is $\min\{n+1-a, n-b\}$, as required. □

Example 2.12. Let $n=8$, let $w=01110000$, and let C_4 be the code generated by the four elements of the R^2-orbit of w. Then C_4 consists of the following $2^4=16$ elements:

00000000	01110000	00011100	00000111
11000001	10110001	11011101	11000110
01110110	01101100	00011011	10101101
10110110	11011010	01101011	10101010

An easy inspection yields $\mathcal{J}=\{0,1,3,5\}$, $j_e=0$, $j_o=5$, and the unique vector with leading 1 in position 5 is 00000111. Following the proof, we choose $x_3=00000111$, $x_2=x_3R^{-2}=00011100$, and $x_1=x_3R^{-4}=01110000$. Also, $v=x_3R^{-j_o}=x_3R^{-5}=11100000$ (which is not in C_4). Next, we are to choose $x_0=u$ to be a vector with leading 1 in position 0, and trailing 1 in position 6. The code C_4 contains four vectors with these properties: 11000110, 10110110, 11011010, and 10101010, and any one of these four vectors, together with x_1, x_2 and x_3, forms a stepped basis for C_4. If we choose the first of them, $u=11000110$, we obtain the following stepped basis for C_4:

$$x_0=11000110,\quad x_1=01110000,\quad x_2=00011100,\quad x_3=00000111.$$

Referring to Example 2.8, we see that the pair $(11000110, 11100000)$ is a generating pair for C_4.

Here, $a = 6$ and $b = 2$, and so the dimension s is $8 - \frac{6+2}{2} = 8 - 4 = 4$. Both degrees are even, which means that the fullness of C_4 is equal to $\min\{8-6, 8+1-2\} = 2$.

The other candidates for u, $10110110 = x_0 + x_1, 11011010 = x_0 + x_2$, and $10101010 = x_0 + x_1 + x_2$, yield similar results.

Example 2.13. The code C_{1+3} introduced in Example 2.4 is half-cyclic. Its generating pair is $u = 100000$, $v = 101000$. Here, $a = 0, b = 2$, so that the dimension of the code is $6 - \frac{0+2}{2} = 6$ - 1 = 5.

In general, any half-cyclic code having $a = 0$ is formed as the code in Example 2.4, i.e., by merging every vector in $\mathbb{Z}_2^m$ with every vector in some cyclic code in $\mathbb{Z}_2^m$.

Of all the generating pairs of a non-degenerate C we wish to select one such pair to be the *canonical* pair. If $a = b$ (where a and b are the degrees of u and v), the proof of Theorem 2.11 shows that there is only one choice for both u and v and that is, by default, the canonical choice. If $a \neq b$, let v be the one with smaller degree, b; remember that this v is uniquely determined. Define the canonical choice for u to be the one for which $u_i = 0$ and $u_{a-i} = 0$ for all odd i less than $D = \frac{a-b}{2}$; if D is odd, we require $u_D = 0$ as well.

When $a > b$, we claim, such a canonical choice is always possible. If u and v are any generating pair with $a > b$, odd shifts of v are positioned to have leading 1's in positions 1, 3, 5, ..., and trailing ones in positions $a-1, a-3, a-5, \ldots$. By subtracting odd shifts of v from u, alternately matching leading and trailing ones of v with corresponding 1's in u, we can cause 0's to appear in positions $1, a-1, 3, a-3, 5, a-5 \ldots$. When i is odd and $a - 2i$ is more than b, we can cause both u_i and u_{a-i} to be 0 by subtracting different odd shifts of v. When $a - 2i$ is equal to b, we may not be able to make both equal to 0 simultaneously. This happens when $i = D$ is an odd number; i.e., when b and a differ by an odd multiple of 2.

Thus, for example, the canonical choice for Example 2.12 would be $u = 10101010$, $v = 11100000$, with the corresponding stepped basis

$$x_0 = 10101010, \;\; x_1 = 01110000, \;\; x_2 = 00011100, \;\; x_3 = 00000111.$$

Example 2.15 below shows a more interesting case of finding a canonical pair.

Corollary 2.14. *Non-degenerate half-cyclic codes of length n are in a one-to-one correspondence with canonical choices of generating pairs.*

Since each choice of x_j must lead to the same number of generators in the stepped basis $\mathcal{B}$, all choices for x_j must have cores of the same length. Note also that the stepped basis constructed in Theorem 2.11 is a *shortest-core* basis; that is, for each $j \in \mathcal{J}, x_j$ has the shortest core among all vectors with leading 1 in position j over all transversal bases of C.

The next example shows that the associate of a degenerate code need not be degenerate.

Example 2.15. Consider the cyclic code C' of length 5 and dimension 4 generated by $u' = 11000$. Let C_5 be the length 10 degenerate code $\theta_3(C')$ described in Lemma 2.6, and let C_5^* be its associate. Then C_5^* is non-degenerate. Applying the generator construction from Theorem 2.11, we may choose the generators $w = 1110000001$ and $v = 1111000000 = wR$.

In this example, where the degrees, 3 and 9, differ by an odd multiple of 2, we would subtract vR and then vR^3 from $w = 1110000001$, and so the canonical pair would be $u = 1000011001, v = 1111000000$, and the stepped basis is then

$$x_0 = 1000011001, \quad x_1 = 0111100000, \quad x_2 = 0001111000, \quad x_3 = 0000011110.$$

Notice that u has degree $9 = n - 1$. This is typical of the associate-of-degenerate case, as we see in the following lemma:

Lemma 2.16. *A non-degenerate half-cyclic code C of length n is the associate of a degenerate code if and only if one of the generators for C has degree $n - 1$.*

Proof. First, if C is the associate of a degenerate code C', then C' must be degenerate of type 3. As observed already, in this case, the first and last entries of every word in C must be the same. Since one of the generators must have its leading 1 in position 0, its trailing 1 must be in position $n - 1$. Every such vector corresponds to a polynomial of degree $n - 1$.

On the other hand, assume that C is a non-degenerate half-cyclic code for which one of its generators has degree $n - 1$. Then this generator must be u, by which we mean that in the stepped basis $\mathcal{B}$, x_0 must be u itself. Clearly, no even shifts of u are possible. Thus, the remaining basis members $x_1, x_2, \ldots, x_{s-1}$ must be odd shifts of v, where v is of odd degree less than $n - 1$. But odd shifts of odd degree vectors must have their trailing 1's in even positions, and so all of them have their first and final entries both equal to 0. Hence, all basis vectors in the basis $\mathcal{B}$ have the property that their first and last entry are equal, and so this necessarily holds for all vectors in the span of $\mathcal{B}$, i.e., for each vector of C. It follows that the associate code of C is degenerate. □

The following theorem gathers the results of Lemma 2.6 and the discussion following it, Lemma 2.16, and The Half-Cyclic Code Theorem, Theorem 2.11, to summarize the four possibilities for associate pairs of half-cyclic codes:

Theorem 2.17. *Let C be a half-cyclic code in $\mathbb{Z}_2^{2m}$, and let CR be its associate code, which must also be half-cyclic. Then exactly one of these four statements holds:*

(1) There exists a cyclic code C' in $\mathbb{Z}_2^m$, such that C and CR are the merged codes $\theta_1(C')$ and $\theta_2(C')$, both degenerate, in some order.
(2) There exists a cyclic code C' in $\mathbb{Z}_2^m$ with a generating vector u', of degree less than $m - 1$, such that one of C, CR is the degenerate code $\theta_3(C')$, while the other is the non-degenerate half-cyclic code with generating pair $\theta_3(u')R^{-1}, \theta_3(u')$.
(3) The code $C = CR$ is the one-dimensional code whose only non-zero vector is $\alpha = 111\ldots1$. Here, C and CR are both degenerate.
(4) There exists a generating pair (u, v) of vectors, each of degree less than $n - 1$, with the property that the two stepped sets generated by (u, v) and (v, u) are bases for the codes C and CR, in some order.

3. Dihedral and half-dihedral codes

One way to see cyclic and half-cyclic codes is as subspaces of $\mathbb{Z}_2^n$ invariant under the action of specific cyclic groups acting on the coordinates. We extend this idea and consider the actions of dihedral groups containing these cyclic groups. To do that, for each $j \in \mathbb{Z}_n$ we define the j^{th} *reflection* to be the linear transformation $M_j : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ sending a vector $u = u_0u_1u_2 \dots u_{n-1}$ to the vector whose i-th entry is u_{j-i} (with the indices calculated in $\mathbb{Z}_n$). For example, $110100M_2 = 011001$, and $110100M_3 = 101100$. Note that

$$M_jM_{j+1} = R \text{ and } M_jM_{j+2} = R^2, \tag{1}$$

for all $j \in \mathbb{Z}_n$.

Using reflections, we define for any vector u with leading and trailing 1's in positions j and k respectively its *reverse* to be the vector $\bar{u} = uM_{j+k}$. Then u and $\bar{u}$ have leading and trailing 1's in the same positions and the core of one is the reverse of the core of the other. If $u = \bar{u}$, we say that u is *palindromic*.

A pair of vectors is said to be *nearly palindromic* provided that both vectors are palindromic or one is palindromic and the second differs from its reverse by a single odd shift of the first (palindromic) vector.

To clarify this definition, a generating pair of vectors (u, v), of degrees $a \geq b$ respectively, is nearly palindromic if and only if u and v are both palindromic or $D = \frac{a-b}{2}$ is odd, v is palindromic, and $u + \bar{u} = vR^D$. In this last case, u must be of the form $u = yxy'$, where y is an arbitrary string of odd length D satisfying $y_0 = 1$, $y' = yM_{D-1}$, x is a string of the same length as v, and $x + \bar{x} = v$. In order for such a pair to be canonical, all y_i's must be 0 for odd values of i, while x must begin with a 0 and end with a 1.

Following are definitions of the linear codes that are the focus of this section.

Definition 3.1. A non-trivial linear code $C \subseteq \mathbb{Z}_2^n$ invariant under R and some M_j (and hence, under all M_j's) is called a *dihedral* code.

Definition 3.2. For even n, a non-trivial code $C \subseteq \mathbb{Z}_2^n$ invariant under R^2 and some M_j is called a *half-dihedral* code. A half-dihedral code C is *even half-dihedral* if it is preserved by R^2 and all M_j's for even values of j, or it is *odd half-dihedral* if it is preserved by R^2 and all M_j's for odd values of j. Even half-dihedral codes will be said to be of *even parity*, and odd half-dihedral codes will be of *odd parity.*

As noted already, in case of odd n, linear codes are invariant under R if and only if they are invariant under R^2. Moreover, even if one assumes an even n, identities (1) show that non-trivial linear codes C invariant under R^2 and *all* M_j's are also invariant under R, and are therefore dihedral. By definition, dihedral codes are cyclic, and thus can be described with respect to their generators.

Theorem 3.3. *A subspace $C \subseteq \mathbb{Z}_2^n$ is a dihedral code if and only if it is a cyclic code whose generator is palindromic.*

Proof. If C is a dihedral code, then it is a cyclic code as well, and thus admits a generator u. If we denote the degree of the polynomial $u(t)$ by k, the reflection M_k sends u to a vector whose leading and trailing 1's are in positions 0 and k again. Since u is unique with this property, $\bar{u} = uM_k$ must be u itself, making u palindromic.

On the other hand, if C is a cyclic code whose generator is palindromic of degree k, then $\mathcal{B} = \{x_i = uR^i \mid 0 \leq i \leq n-1-k\}$ is a basis for C. Furthermore, for each $i \in \mathbb{Z}_n$, $x_iM_{n-1} = uR^iM_{n-1} = uM_{n-1}R^{-i}$. Since u has palindromic core, and has its leading and trailing 1's in positions 0 and k, it must be that uM_{n-1} has the same core as u and has its leading and trailing 1's in positions

$n-1-k$ and $n-1$. Because $x_{n-1-k} = uR^{n-1-k}$ is the unique element of C with a leading 1 in position $n-1-k$, it must be that $x_{n-1-k} = uM_{n-1}$. Then $x_iM_{n-1} = uM_{n-1}R^{-i} = uR^{n-1-k}R^{-i} = uR^{n-1-k-i} = x_{n-1-k-i}$, for all $i \in \mathbb{Z}_n$. Thus, $\mathcal{B}$ is closed under M_{n-1}, and therefore C must also be closed under M_{n-1}. It follows that C is dihedral. □

The corresponding situation for half-dihedral codes is more complex. We derive separate results for the degenerate and non-degenerate cases.

Theorem 3.4. *Let C be a degenerate half-cyclic code of length $n = 2m$. It is half-dihedral if and only if there is a dihedral code C' of length m such that C is one of $\theta_1(C')$, $\theta_2(C')$, or $\theta_3(C')$.*

Proof. We know from Lemma 2.6 that a degenerate half-cyclic code must be of the form $\theta_i(C')$ for some cyclic C' in $\mathbb{Z}_2^m$ and some $i \in \{1,2,3\}$. Note that R^2 acts on $\mathbb{Z}_2^n$ as R does on $\mathbb{Z}_2^m$, M_{2j} acts on $\theta_1(C')$ and $\theta_2(C')$ as M_j does on C', and M_{2j+1} acts on $\theta_3(C')$ as M_j does on C'. We see that C is half-dihedral if and only if C' is dihedral. □

Theorem 3.5 (The Half-Dihedral Code Theorem). *Let $C \subseteq \mathbb{Z}_2^n$ be a non-degenerate half-cyclic code. Suppose that its canonical generators are u and v of degrees a and b, respectively. Then*

(1) C is half-dihedral of parity opposite to the parity of a and b if and only if $v = \bar{u}$.

(2) C is half-dihedral of the same parity as the parity of a and b if and only if (u, v) is nearly palindromic.

Proof. Let $\{x_0, x_1, \ldots, x_{s-1}\}$ be a stepped basis for C. If C is a half-dihedral code of parity opposite to the parity of a and b, then C is invariant under M_{a+1} and M_{b+1} (among others). The reflection M_{a+1} sends x_0, with leading and trailing 1's in positions 0 and a, to a vector in C with leading and trailing 1's in positions 1 and $a+1$. Since $x_1 = vR$ has the shortest core of all vectors with leading 1 in position 1, $b \le a$. Similarly considering the action of M_{b+1} on x_1, which has leading and trailing 1's in positions 1 and $b+1$, M_{b+1} sends x_1 to a vector in C with leading and trailing 1's in positions 0 and b. Employing the same argument as before yields $a \le b$. Thus $a = b$, the core of v is the reverse of the core of u, and hence $v = \bar{u}$.

Conversely, suppose that C has generators u and $v = \bar{u}$. Since C is assumed to be half-cyclic, it is invariant under R^2 and therefore contains the set $\mathcal{E}$ of *all* even shifts of u and the set $\mathcal{O}$ of *all* odd shifts of v; moreover, C is spanned by $\mathcal{E} \cup \mathcal{O}$. Since $v = \bar{u}$, the degree of u matches the degree of v, and thus, $M_{a+1} = M_{b+1}$ swaps u and vR. Consequently, M_{a+1} swaps the two sets $\mathcal{E}$ and $\mathcal{O}$, and therefore fixes $\mathcal{E} \cup \mathcal{O}$. Thus C is half-dihedral of parity $a+1$, the opposite parity of a.

If C is a half-dihedral code of the same parity as that of a and b, then C is invariant under M_a. Moreover, every entry x in the stepped basis $\mathcal{B}$ generated by u and v whose leading 1 is in place i has its trailing one in place $i+a$ or $i+b$, and so one of the symmetries M_{2i+a} or M_{2i+b} (each of which preserves C) sends x to a vector $\bar{x} \in C$ having the same leading and trailing 1's as x and reversed core. Thus, $x + \bar{x}$ is either equal to the zero vector, in which case x is palindromic, or $x + \bar{x}$ is a non-trivial palindrome with core shorter than that of x.

Since both C and CR are non-degenerate, we can choose to be working in the one in which the core of x_0 is not shorter than that of x_1. That is, we can assume that $a = \deg(u(t)) \geq b = \deg(v(t))$. Then v has the shortest core of all non-trivial elements of C, and therefore $v + \bar{v}$ must be 0, forcing v to be palindromic.

If $a = b$, u has the same degree as v and it too must be palindromic for the same reason. Thus, suppose that $a > b$ and apply the above arguments to the vector u. Then $w = u + \bar{u}$ must be palindromic of degree less than a, and it must belong to C. Once again, if w were equal to the zero vector, u would have to be palindromic and the claim of the theorem would follow.

Thus assume that w is not the zero vector. Since it is a linear combination of the elements in $\mathcal{B}$ and its degree is less than a, it must be a combination of odd cyclic shifts of v whose leading 1's are in odd positions to the right of the position 0 and whose trailing 1's are in positions to the left of a.

Let j be the position of the leading 1 in $w = u + \bar{u}$. Then j must be odd, and the trailing 1 of the palindrome w is in position $a - j$. Since v has the shortest core among the non-zero vectors in C, the length of the core of $u + \bar{u}$, $a - 2j$, must be greater than or equal to b. We claim that $a - 2j = b$, for if that were not the case, i.e., if $a - 2j$ were bigger than b, then u_j and $u_{a-j} = \bar{u}_j$ would both have to be equal to 0, because of our assumption that u, v is a canonical pair. This would force $1 = w_j = u_j + \bar{u}_j = 0 + 0$, a contradiction. It follows that w must simply be $vR^j = vR^{\frac{a-b}{2}}$, which completes the proof of the fact that the pair u, v is nearly palindromic.

Finally, suppose that C is half-cyclic with generating pair (u, v) which is nearly palindromic. Again, let $\mathcal{E}$ be the set of all even shifts of u and let $\mathcal{O}$ be the set of all odd shifts of v. Because C is half-cyclic, it contains, and is generated by, $\mathcal{E} \cup \mathcal{O}$. Assume that $a \geq b$. Then v is a palindrome, so that $\mathcal{O}M_b = \mathcal{O}$. Since a and b are of the same parity and $\mathcal{O}$ is invariant under R^2, it must also be true that $\mathcal{O}M_a = \mathcal{O}$. If u is a palindrome, then $\mathcal{E}M_a = \mathcal{E}$, and so C, generated by $\mathcal{E} \cup \mathcal{O}$, is also preserved by M_a. Otherwise $u + uM_a$ is some odd shift of v. Specifically, it must be that a and b differ by an odd nultiple of 2. Suppose that $\frac{a-b}{2}$ is the odd number D. Then $u + uM_a = vR^D$, so that $uM_a = u + vR^D$. Then for each element uR^{2j} of $\mathcal{E}$, the corresponding element of $\mathcal{E}M_a$ is

$$(uR^{2j})M_a = uM_aR^{-2j} = (u + vR^D)R^{-2j} = uR^{-2j} + vR^{D-2j}.$$

The first of the summands is in $\mathcal{E}$, the second is in $\mathcal{O}$. Thus every element of $\mathcal{E}M_a$ is an element of $\mathcal{E}$ plus an element of $\mathcal{O}$, and so the span of $\mathcal{E} \cup \mathcal{O}$ is equal to the span of its image under M_a, and thus C is half-dihedral of the same parity as a. □

Example 3.6. Consider first the half-cyclic code C_6 of length 6 generated by $u = 110000$ and $w = 110100$ (in that order). A stepped basis for C_6 is

$$x_0 = 110000 = u, x_1 = 011010 = wR, x_2 = 001100 = uR^2, x_3 = 000011 = uR^4.$$

Then $u(t) = 1 + t$ and $w(t) = 1 + t + t^3$, with each polynomial being of odd degree. Furthermore,

$$t^6 - 1 = (1 + t^2)u(t) + t(1 + t^2)w(t), \text{ and } t^6 - 1 = (1 + t^2)w(t) + t(1 + t^4)u(t),$$

and so $u(t)$ and $w(t)$ are semi-divisors of $t^n - 1$. In addition, this pair is nearly palindromic, as u is palindromic, and $w + \bar{w} = 110100 + 101100 = 011000$, where the last sum is an odd shift of u, $w + \bar{w} = uR^{\frac{3-1}{2}}$. This basis is not canonical because w_1 is not zero. Taking $v = w + uR = 101100$ gives the canonical choice, and $\mathcal{B} = \{u, vR, uR^2, uR^4\}$ is the corresponding stepped basis for C_6.

Example 3.7. Consider the code C_7 associated to the code C_6 from Example 3.6, $C_7 = C_6R$. This has generators v and u (in that order). The change of the order of generators causes an interestingly different choice for the stepped basis:

$$x_0 = 101100 = v, x_1 = 011000 = uR, x_2 = 001011 = vR^2, x_3 = 000110 = uR^3,$$

and again, with a and b odd, this is a canonical basis for an odd dihedral code.

4. Appendix

Tables 1 and 2 display all half-cyclic code of length 8 or less. One of each associate pair of generating pairs is given. The triple of parameters $[n, k, m]$ denotes, as usual, the length, the dimension and the minimal distance of the code, while $[a, b]$ is the pair of the degrees of the generators. The next columns present canonical generators u and v without their trailing zeroes. The 'type' column shows

Cyc	cyclic
Dih	dihedral
HC	half-cyclic
HDiEvn	even half-dihedral
HDiOdd	odd half-dihedral
–DG	degenerate

A more complete listing of codes up to length 14 (some 540 in all) is available on the website `http://euler.doa.fmph.uniba.sk/half-dihedral-codes.html`

In general coding theory, two codes are considered *equivalent* if some permutation of coordinates applied uniformly across one code produces the other. For a half-cyclic code, most permutations of coordinates applied to it do not yield a half-cyclic code. There are, however, two permutations from the full symmetric group $\mathbb{S}_n$ under which the collection of half-cyclic codes is obviously closed, namely, $\varphi = (1, 3, 5, \ldots, n-1)$, and $\psi = (0, 2, 4, \ldots, n-2)$. For any half-cyclic code C, both $C\varphi$ and $C\psi$ are also half-cyclic. The generators for $C\varphi$ and $C\psi$ generally differ from those of C, and they are not always the images of the generators of C under φ or ψ. The basic parameters $[n, k, m]$, though, remain unchanged. The type may change quite freely.

The following example illustrates some of these possibilities:

Example 4.1. Consider the six codes of length 10 given in Table 3 (in the form of entries from Table 1). If, for any half-cyclic code H generated by u and v, we let $\bar{H}$ denote the code generated by $\bar{u}$ and $\bar{v}$, the reader may easily check that $A\varphi = \bar{B}$, $B\varphi = \bar{E}$, $C\varphi = \bar{C}$, $D\varphi = \bar{F}$, $E\varphi = \bar{E}R$, and $F\varphi = DR$.

Final Remark: While this paper has been concerned exclusively with codes over $\mathbb{Z}_2$, almost all our definitions, techniques and results would apply to codes over other fields as well.

Acknowledgement: The authors would like to thank Prof. Bahattin Yildiz of Northern Arizona University for many enlightening conversations on coding theory and for his contributions to the accuracy and readability of this note.

[n, k, m]	[a, b]	u	v	type
[2, 1, 2]	[1, 1]	11	11	Dih-DG
[2, 2, 1]	[0, 0]	1	1	Dih
[4, 1, 4]	[3, 3]	1111	1111	Dih-DG
[4, 2, 2]	[3, 1]	1001	11	HDiEvn-DG
[4, 2, 2]	[2, 2]	101	101	Dih
[4, 2, 2]	[2, 2]	111	101	HDiOdd
[4, 3, 1]	[2, 0]	101	1	HDiOdd
[4, 3, 2]	[1, 1]	11	11	Dih
[4, 4, 1]	[0, 0]	1	1	Dih
[6, 1, 6]	[5, 5]	111111	111111	Dih-DG
[6, 2, 4]	[5, 3]	100111	1111	HDiEvn-DG
[6, 2, 3]	[4, 4]	10101	10101	Dih
[6, 2, 4]	[4, 4]	11011	11011	Dih
[6, 3, 2]	[5, 1]	100001	11	HDiEvn-DG
[6, 3, 2]	[4, 2]	10101	101	HDiOdd
[6, 3, 2]	[4, 2]	10111	101	HDiOdd
[6, 3, 3]	[4, 2]	10101	111	HDiOdd
[6, 3, 2]	[3, 3]	1001	1001	Dih
[6, 3, 3]	[3, 3]	1111	1101	HC
[6, 4, 1]	[4, 0]	10101	1	HDiOdd
[6, 4, 2]	[3, 1]	1011	11	HDiEvn
[6, 4, 2]	[2, 2]	101	101	Dih
[6, 4, 2]	[2, 2]	111	111	Dih
[6, 5, 1]	[2, 0]	101	1	HDiOdd
[6, 5, 2]	[1, 1]	11	11	Dih
[6, 6, 1]	[0, 0]	1	1	Dih

Table 1. Half-cyclic codes of length up to 6

References

[1] N. Aydin, N. Connolly, J. Murphree, *New binary linear codes from quasi-cyclic codes and an augmentation algorithm*, Appl. Algebra Eng. Commun. Comput. 28, No. 4 (2017), 339-350.

[2] M. Barbier, C. Chabot, G. Quintin, *On quasi-cyclic codes as a generalization of cyclic codes*, Finite Fields Appl. 18 (2012), 904–919.

[3] P.-L. Cayrel, Ch. Chabot, A. Necer, *Quasi-cyclic codes as codes over rings of matrices*, Finite Fields Appl. 16, No. 2 (2010), 100-115.

[4] R. Hill, *A first course in coding theory*, Oxford Applied Mathematics and Computing Science Series, Oxford, Clarendon Press. XII (1986).

[5] R. Jajcay, P. Potočnik, S. Wilson, *The Praeger-Xu graphs: Cycle structures, maps and semitransitive orientations*, Acta Math. Univ. Comenianae 88 (2) (2019), 269-291.

[6] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes. I: Finite fields*, IEEE Trans. Inf. Theory 47, No. 7 (2001), 2751-2760.

[7] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes. II: Chain rings*, Des. Codes Cryptography 30, No. 1 (2003), 113-130.

[8] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes. III: Generator theory*, IEEE Trans. Inf. Theory 51, No. 7 (2005), 2692-2700.

[9] S. Ling, H. Niederreiter, P. Solé, *On the algebraic structure of quasi-cyclic codes. IV: Repeated roots*, Des. Codes Cryptography 38, No. 3 (2006), 337-361.

[10] P. Potočnik, S. Wilson, *Recipes for Edge-transitive Tetravalent Graphs*, arXiv:1608.04158 [math.CO], August 2016.

[11] M. Shi, Y. Zhang, Quasi-twisted codes with constacyclic constituent codes, Finite Fields and Their Applications 39, (2016), 159-178.

[n, k, m]	[a, b]	u	v	type
[8, 1, 8]	[7, 7]	11111111	11111111	Dih-DG
[8, 2, 4]	[7, 5]	10011001	110011	HDiEvn-DG
[8, 2, 4]	[6, 6]	1010101	1010101	Dih
[8, 2, 4]	[6, 6]	1110111	1010101	HDiOdd
[8, 3, 4]	[7, 3]	10011001	1111	HDiEvn-DG
[8, 3, 2]	[6, 4]	1010101	10001	HDiOdd
[8, 3, 2]	[6, 4]	1011111	10001	HDiOdd
[8, 3, 4]	[6, 4]	1010101	11011	HDiOdd
[8, 3, 4]	[5, 5]	100111	111001	HDiOdd
[8, 3, 4]	[5, 5]	110011	101101	HDiEvn
[8, 3, 4]	[5, 5]	110011	110011	Dih
[8, 4, 2]	[7, 1]	10000001	11	HDiEvn-DG
[8, 4, 2]	[6, 2]	1010101	101	HDiOdd
[8, 4, 2]	[6, 2]	1011101	101	HDiOdd
[8, 4, 3]	[6, 2]	1010101	111	HDiOdd
[8, 4, 2]	[5, 3]	100001	1001	HDiEvn
[8, 4, 3]	[5, 3]	100111	1101	HC
[8, 4, 4]	[5, 3]	101011	1111	HDiEvn
[8, 4, 4]	[5, 3]	101101	1111	HDiEvn
[8, 4, 2]	[4, 4]	10001	10001	Dih
[8, 4, 2]	[4, 4]	10011	10001	HC
[8, 4, 2]	[4, 4]	11001	10001	HC
[8, 4, 2]	[4, 4]	11011	10001	HDiOdd
[8, 4, 3]	[4, 4]	11111	11011	HDiOdd
[8, 4, 4]	[4, 4]	10111	11101	HDiEvn
[8, 5, 1]	[6, 0]	1010101	1	HDiOdd
[8, 5, 2]	[5, 1]	101101	11	HDiEvn
[8, 5, 2]	[4, 2]	10001	101	HDiOdd
[8, 5, 2]	[4, 2]	10001	111	HDiOdd
[8, 5, 2]	[4, 2]	10011	101	HDiOdd
[8, 5, 2]	[3, 3]	1011	1101	HDiOdd
[8, 5, 2]	[3, 3]	1111	1001	HDiEvn
[8, 5, 2]	[3, 3]	1111	1111	Dih
[8, 6, 1]	[4, 0]	10001	1	HDiOdd
[8, 6, 2]	[3, 1]	1001	11	HDiEvn
[8, 6, 2]	[2, 2]	101	101	Dih
[8, 6, 2]	[2, 2]	111	101	HDiOdd
[8, 7, 1]	[2, 0]	101	1	HDiOdd
[8, 7, 2]	[1, 1]	11	11	Dih
[8, 8, 1]	[0, 0]	1	1	Dih

Table 2. Half-cyclic codes of length 8

Robert Jajcay,
Faculty of Mathematics, Physics and Informatics, Comenius University, Bratislava, Slovakia; also affiliated with Faculty of Mathematics, Natural Sciences and Information Technology, University of Primorska, Koper, Slovenia
E-mail address: robert.jajcay@fmph.uniba.sk

A:	[10, 5, 3]	[2, 8]	111	101010101	HDiEvn
B:	[10, 5, 3]	[3, 7]	1101	10011101	HC
C:	[10, 5, 3]	[4, 6]	11001	1001011	HC
D:	[10, 5, 3]	[4, 6]	11011	1001001	HDiEvn
E:	[10, 5, 3]	[5, 5]	101001	111011	HC
F:	[10, 5, 3]	[5, 5]	110001	111001	HC

Table 3. Some related codes of length 10

Primož Potočnik,
Faculty of Mathematics and Physics, University of Ljubljana, Slovenia; also affiliated with Institute of Mathematics, Physics, and Mechanics, Ljubljana, Slovenia
E-mail address: primoz.potocnik@fmf.uni-lj.si

Stephen E. Wilson,
Department of Mathematics and Statistics, Northern Arizona University, Flagstaff, Arizona, USA; also affiliated with Faculty of Mathematics, Natural Sciences and Information Technology, University of Primorska, Koper, Slovenia
E-mail address: stephen.wilson@nau.edu