On the duality and the direction of polycyclic codes

ON THE DUALITY AND THE DIRECTION OF POLYCYCLIC CODES

Abstract. Polycyclic codes are ideals in quotients of polynomial rings by a principal ideal. Special cases are cyclic and constacyclic codes. A MacWilliams relation between such a code and its annihilator ideal is derived. An infinite family of binary self-dual codes that are also formally self-dual in the classical sense is exhibited. We show that right polycyclic codes are left polycyclic codes with different (explicit) associate vectors and characterize the case when a code is both left and right polycyclic for the same associate polynomial. A similar study is led for sequential codes.

1. Introduction

Polycyclic codes (formerly known as pseudo-cyclic [10]) over a finite field F are defined as ideals in $R_f = F[x]/(f)$ where $f \neq 0$ is arbitrary in $F[x]$ and were studied under that name in [7]. Thus the choice $f = x^n - 1$ leads to cyclic codes of length n. Similarly $f = x^n - a$ leads to constacyclic codes. It is a classical exercise to show that polycyclic codes are shortened cyclic codes and conversely [10, p.241]. A possible engineering application is burst-error correction [5]. Still polycyclic codes never enjoyed the same popularity that cyclic codes have. One possible reason is that, for a generic f, the dual of a polycyclic code is not polycyclic.

In this paper, we introduce an alternate form of dual that is the annihilator of the ideal. Under the condition that $f(0)$ is a unit we derive a MacWilliams formula between the code and its annihilator. We construct binary self annihilating codes that are also formally self-dual codes in the classical sense that their weight enumerator is a fixed point of the MacWilliams transform. In particular we show that shortened quadratic residue codes are formally self-dual. In the second part

2010 *Mathematics Subject Classification:* Primary: 94B15, 94B05, 94B065.

Key words and phrases: Cyclic codes, formally self-dual codes.

of the paper, we study the notion of one-sided polycylic codes and the same notion for sequential codes, the dual class of polycylic codes.

The material is organized as follows. Section 2 collects the necessary notations and definitions. Section 3 studies the duality in the sense of annihilators. In Section 4, infinite families of annihilator self-dual polycyclic codes that are not self-dual are constructed. In Section 5, we show that right polycyclic codes with associate vector $\mathbf{c}$ are left polycyclic for another polynomial $\widehat{\mathbf{c}}$. We characterize the case when $\mathbf{c} = \widehat{\mathbf{c}}$. In Section 6, we do a similar study for sequential codes which are the dual class of polycyclic codes.

2. Notation and definitions

2.1. Ring theory.

Define an inner product on R_f by the rule

$$\langle g, h\rangle_f = gh(0).$$

Where $g, h \in R_f$ are represented by polynomials of degree less than the degree of f. If $C \leq R_f$ is a polycyclic code, then we define its *annihilator dual* C^0 by the formula

$$C^0 = \{g \in R_f | \, \forall h \in C, gh(0) = 0\}.$$

The name is justified by the following result. Recall that the annihilator $Ann(I)$ of an ideal I in a commutative ring R is $Ann(I) = \{x \in R | \, \forall y \in I, \, xy = 0\}$.

Proposition 1. *If the form $\langle ., .\rangle_f$ is non degenerate then, for all $C \leq R_f$, we have $C^0 = Ann(C)$.*

Proof. By definition $Ann(C) \subseteq C^0$. By hypothesis $C = \langle g\rangle$, with f a multiple of g. This implies $Ann(C) = \langle f/g\rangle$, and both $Ann(C)$ and C^0 have dimension $\deg(g)$. The result follows. $\square$

2.2. Formally self-dual codes.

The *weight enumerator* of a code $C \leq F_q^n$ is

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i,$$

where A_i counts the number of codewords of weight i.

A binary code C is said to be *formally self-dual* (fsd) if

$$W_C(x, y) = W_C(\frac{x + y}{\sqrt{2}}, \frac{x - y}{\sqrt{2}}).$$

Thus a self-dual code is fsd but not conversely. Still, invariant theory can be applied to study the weight enumerators of fsd codes. For more background, we refer to [1, 2, 4, 6].

3. Duality

We begin with an easy lemma.

Lemma 1. *If $f(0) \neq 0$ then the bilinear form $\langle ., .\rangle_f$ is non degenerate.*

Proof. We must show that the orthogonal of R_f is zero. Let g be an element in that space. Since $g \perp 1$ we see that $g = xg'$ for some g'. Observe that, by hypothesis, x is invertible in R_f with inverse $-(f(x) - f(0))(f(0))^{-1}$, and by induction that x^i is invertible for all i. Considering successively $g \perp x^{-i}$ for $i = 0, \ldots, \deg(f) - 1$, we obtain the result. $\square$

We set up a Fourier Tranform on a function ϕ with domain R_f by the formula

$$\widehat{\phi}(g) = \sum_{h \in R_f} \psi_F(\langle g, h\rangle_f)\phi(h),$$

where ψ_F denotes the standard additive character of F defined by $\psi(x) = \omega^{Tr(x)}$, with ω a complex primitive root of unity of order p, the characteristic of F.

Lemma 2. *Assume $f(0) \neq 0$. If C is an ideal of R_f, then, for any function ϕ with domain R_f we have the summation formula*

$$\sum_{c \in C^0} \phi(c) = \frac{1}{|C|} \sum_{c \in C} \widehat{\phi}(c).$$

Proof. We expand the right hand side of the summation formula as follows.

$$\sum_{c \in C} \widehat{\phi}(c) = \sum_{d \in C^0} \phi(d) \sum_{c \in C} \psi_F(\langle c, d\rangle_f) + \sum_{d \notin C^0} \phi(d) \sum_{c \in C} \psi_F(\langle c, d\rangle_f)$$

Now, by Lemma 1 and the orthogonality of group characters, the second sum vanishes. The result follows. □

We are ready for the main result of this section, an anlogue of the MacWilliams formula.

Theorem 1. *Assume $f(0) \neq 0$. If C is an ideal of R_f, we have*

$$W_{C^0}(x, y) = \frac{1}{|C|} \sum_{c \in C} \sum_{d \in R_f} \psi_F(\langle c, d\rangle_f) x^{n-w(d)} y^{w(d)}.$$

Proof. Follows by the preceding lemma applied to $\phi : d \mapsto x^{n-w(d)} y^{w(d)}$. □

4. Formally self-dual codes

In this section, we assume $F = GF(2)$. We begin with a classic Lemma. Recall that a code is homogeneous if sets of words of any fixed weight hold a 1-design. We denote by C/i and $C - i$ the shortened and punctured codes of C at coordinate i.

Lemma 3. *If C is homogeneous, then for any coordinate i the weight enumerators of its punctured and shortened codes are, respectively*

$$W_{C-i} = \frac{\partial W_C}{\partial x} + \frac{\partial W_C}{\partial y}$$

and

$$W_{C/i} = \frac{\partial W_C}{\partial x}.$$

Proof. This is a restatement of Prange's theorem [4, Th. 7.6.1] in terms of weight enumerators. □

Theorem 2. *If C is an homogeneous code of distance > 1, obtained by puncturing from a fsd homogeneous code of distance > 1, then any of its shortened codes is fsd.*

Proof. Let E denote the homogeneous code from which C is obtained and let $W = W_E, S = W_C$ and $T = W_{C/1}$. Since E is fsd we get

$$W(x, y) = W\left(\frac{x + y}{\sqrt{2}}, \frac{x - y}{\sqrt{2}}\right).$$

Applying Lemma 3 twice we get

$$S = \frac{\partial W}{\partial x} + \frac{\partial W}{\partial y}, \, T = \frac{\partial S}{\partial x},$$

and, from the right hand side of the transformation law for W, eventually

$$T(x,y) = \frac{\partial^2 W}{\partial x^2}(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}) + \frac{\partial^2 W}{\partial x \partial y}(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}).$$

By substitution in that equality we obtain

$$T(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}) = \frac{\partial^2 W_C}{\partial x^2}(x,y) + \frac{\partial^2 W_C}{\partial x \partial y}(x,y).$$

Applying Lemma 3 again to the definition of W, S, T we identify the right hand side of the last equality as $T(x,y)$. The result follows. □

There is a fsd code with distance 2, length 6, obtained for $g = x^3 + x + 1$, the generator polynomial of the $[7,4,3]$ Hamming code. This example is generalized in the two following corollaries.

Corollary 1. *Let $QR(p)$ denote the binary quadratic residue code attached to the prime p. The shortening of $QR(p)$ at any place is a self-annihilating code which is formally self-dual.*

Proof. The generator polynomial $g(x)$ of $QR(p)$ as a cyclic code of length p is also the generator polynomial of its shortening modulo g^2. Homogeneity properties come from the fact that the automorphism group of the extended quadratic residue code $XQR(p)$ contains $PSL(2,p)$ a group that is two-transitive. The fsd property of $XQR(p)$ is well known, since this code is either self-dual or isodual depending on the congruence class of p modulo 4 [8]. The result follows then by the preceding theorem applied to $C = QR(p)$. The minimum distance of $QR(p)$ is trivially > 1 by the BCH bound, and so is, as a consequence, that of $XQR(p)$. □

Corollary 2. *Let $RM(\frac{m-1}{2}, m)$ denote the binary Reed Muller code of order $\frac{m-1}{2}$ and length $2^m \geq 8$. Let C_m denote this code punctured in one coordinate. The shortening of C_m at any place is a self-annihilating code which is formally self-dual.*

Proof. It is well-known that Reed-Muller codes are extended cyclic and, moreover, that $RM(\frac{m-1}{2}, m)$ is self-dual with automorphism group the affine group acting on 2^m points, a 2-transitive group. The minimum distance of $RM(\frac{m-1}{2}, m)$ is $2^{\frac{m+1}{2}} > 2$ for $m \geq 3$. The result follows. □

Remarks:

- The shortened cyclic codes constructed by the above theorem cannot be self-dual; they contain odd weight vectors, being obtained by shortening and puncturing from an even weight code.
- There are shortened cyclic codes of rate one half that are not isodual. For instance shortening the binary cyclic code of length 31 and generator polynomial $x^{15} + x^7 + x^3 + x + 1$ on its first coordinate yields a $[30,15,5]$ code that is neither self-dual nor isodual. In fact, it is not even formally self-dual, as it contains 26 codewords of weight 5, and its dual only 6.

If C is a polycyclic code with $C = C^0$ we say that C is a *self-annihilator*.

Theorem 3. *A polycyclic code $\langle g\rangle$ in $F[x]/\langle f\rangle$ is a self-annihilator if and only if $f = g^2$.*

Proof. If $g^2 = 0$ then it is immediate that $C \subseteq C^0$. Then we have that the $deg(g) = \frac{deg(f)}{2}$. Hence the dimension of C is precisely half the dimension of the ambient space. Therefore $C = C^0$. □

A code over a field is said to be isodual if C and $C^\perp$ are equivalent codes. It is self-dual if $C = C^\perp$.

Proposition 2. *If C is self-annihilator and cyclic then C is isodual.*

Proof. If C is cyclic then the generator polynomial of the annihilator and the generator polynomial of the dual are related by taking the reciprocal polynomial. □

A polycyclic code over a field is said to be *annihilating isodual* if C and C^0 are equivalent codes.

Proposition 3. *If C is a self-dual cyclic code then C is annihilating isodual.*

Proof. The proof is identical to the proof of Proposition 2. □

5. Polycyclic codes

In this section (Theorem 4) we provide a new proof of Theorem 2.4 in [7]. We do so to serve our purpose of determining the non-existence of self-dual left-right polycyclic codes (Theorem 6). That proof requires an explicit description of the associate vector $\mathbf{d}$ when a right polycyclic code is viewed as left-polycyclic. Such explicit description was not given in the original proof of Theorem 2.4 in [7].

We say that a linear code C over a field F is right 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

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

Similarly, we say that a linear code C over a field F is left 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

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

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

Associate $\mathbf{c}$ with 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 [7] that right polycyclic codes are ideals in $F[x]/\langle f(x)\rangle$ with the usual correspondence between vectors and polynomials and left polycyclic codes are ideals in $F[x]/\langle f(x)\rangle$ with the reciprocal correspondence that associates $\mathbf{c}$ with the polynomial $c(x) = c_{n-1} + c_{n-2}x + c_{n-3}x^2 + \cdots + c_0x^{n-1}$. Hence both of these types of codes are polycyclic codes in terms of our original definition.

It is shown in [7], that a right polycyclic code with associate vector $\mathbf{c}$ is held invariant by right multiplication of the matrix D of the form:

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

It is also shown in [7], that a left polycyclic code with associate vector $\mathbf{d}$ is held invariant by right multiplication of the matrix E of the form:

$$E = \begin{pmatrix} d_0 & d_1 & d_2 & \dots & d_{n-1} \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}. \tag{2}$$

Lemma 4. *Let D be a matrix with entries from the finite field F. If D is of the form given in Equation (1) with $c_0 \neq 0$, then it is invertible, and its inverse is* $D^{-1} = \begin{pmatrix} d_0 & d_1 & d_2 & \dots & d_{n-1} \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$ *where* $d_j = \frac{-c_{j+1}}{c_0}$ *for* $j < n-1$ *and* $d_{n-1} = \frac{1}{c_0}$.

Proof. Multiply the two matrices together and get

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 1 & 0 \\ c_0 d_0 + c_1 & c_0 d_1 + c_2 & \dots & c_0 d_{n-2} + c_{n-1} & c_0 d_{n-1} \end{pmatrix}.$$

Then by making the last row equal to $(0, 0, \dots, 0, 1)$ we have the result. □

Theorem 4. *Let C be a code over the finite field F. If C is a right polycyclic code for the polynomial $c(x) = c_0 + c_1 x + \dots + c_{n-1}x^{n-1}$ with $c_0 \neq 0$, then C is a left polycyclic code for the polynomial $d(x) = d_0 + d_1 x + \dots + d_{n-1}x^{n-1}$ where $d_j = \frac{-c_{j+1}}{c_0}$ for $j < n-1$ and $d_{n-1} = \frac{1}{c_0}$.*

Proof. Let C be a right polycyclic code for the polynomial $c(x) = c_0 + c_1 x + \dots + c_{n-1}x^{n-1}$ then $CD = C$, where D is the matrix given in Equation 1. Then multiplying on the right by D^{-1} we have $CDD^{-1} = CD^{-1}$ which implies $C = CD^{-1}$ and then C is a left polycyclic code since by Lemma 4, D^{-1} is of the form for the invariant of a right polycyclic code. □

Remark: The proof of Theorem 4 requires an explicit description of the associate vector $\mathbf{d}$ when a right polycyclic code is viewed as left-polycyclic and such an explicit description was not given in the original proof of Theorem 2.4 in [7]. It follows from Lemma 4 that

$$d(x) = \frac{x^{n-1}}{c_0} - \frac{(c(x) - c_0)}{c_0}. \tag{3}$$

Namely, the first part gives d_{n-1} and the second part gives the rest.

We say that a code is *left-right* polycyclic, if it is both left polycyclic and right polycyclic for the same polynomial $c(x)$. The next result characterizes such codes by their associate polynomial.

Theorem 5. *If C is left-right polycyclic for the polynomial $c(x)$ then $c(x) = \frac{x^n+c_0}{1+c_0x}$ where $c_0^{n+1} = (-1)^{n+1}$.*

Proof. In this case we have $c(x) = d(x)$. Then by Equation 3, we have

$$\begin{aligned} c(x) &= \frac{x^{n-1}}{c_0} - \frac{(c(x)-c_0)}{c_0} \\ c_0xc(x) &= x^n - c(x) + c_0 \\ c(x) &= \frac{x^n + c_0}{1+c_0x}. \end{aligned}$$

We need this expression to be a polynomial, hence we need the denominator to divide the numerator. The root of the denominator is $\frac{-1}{c_0}$. We need this to also be a root of the numerator. That is we need $(\frac{-1}{c_0})^n + c_0 = 0$. This simplifies to $(-1)^{n+1} = c_0^{n+1}$. Then multiplying both sides by -1 gives the result. □

Theorem 6. *There are no self-dual left-right polycyclic codes.*

Proof. If $C = C^\perp$ then C and $C^\perp$ are left polycyclic codes which implies C is constacyclic by Theorem 3.5 in [7]. However, our polynomial $c(x)$ for left-right polycyclic codes is never the polynomial for constacyclic codes. □

6. Sequential codes

Let C be a linear code in F^n, F a field. The code C is right sequential if there is a function $\phi : F^n \to F$ such that for every $(a_0, a_1, \ldots, a_{n-1}) \in C$ we have that $(a_1, a_2, \ldots, a_{n-1}, b) \in C$ where $b = \phi((a_0, a_1, \ldots, a_{n-1}))$. The code C is left sequential if there is a function $\psi : F^n \to F$ such that for every $(a_0, a_1, \ldots, a_{n-1}) \in C$ we have that $(d, a_0, a_1, a_2, \ldots, a_{n-2}) \in C$ where $d = \psi((a_0, a_1, \ldots, a_{n-1}))$. The code C is bisequential if it is both right and left sequential. The functions ϕ and ψ are, as a rule, linear functions. Each one of them is associated with any vector that realizes them. This vector is known as the associate vector of the code.

It is shown in [7], that a right sequential code with associate vector $\mathbf{c}$ is held invariant by right multiplication of the matrix D^T of the form:

$$D^T = \begin{pmatrix} 0 & 0 & 0 & \ldots & c_0 \\ 1 & 0 & 0 & \ldots & c_1 \\ 0 & 1 & 0 & \ldots & c_2 \\ \vdots & & & & \\ 0 & 0 & \ldots & 1 & c_{n-1} \end{pmatrix}. \tag{4}$$

It is also shown in [7], that a left sequential code with associate vector $\mathbf{d}$ is held invariant by right multiplication of the matrix E^T of the form:

$$E^T = \begin{pmatrix} d_0 & 1 & 0 & \ldots & 0 \\ d_1 & 0 & 1 & \ldots & 0 \\ \vdots & & & & \\ d_{n-2} & 0 & 0 & \ldots & 1 \\ d_{n-1} & 0 & & \ldots & 0 \end{pmatrix}. \tag{5}$$

Theorem 7. *Let C be a code over the finite field F. If C is a right sequential code for the polynomial $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ with $c_0 \neq 0$, then C is a left sequential code for the polynomial $d(x) = d_0 + d_1x + \cdots + d_{n-1}x^{n-1}$ where $d_j = \frac{-c_{j+1}}{c_0}$ for $j < n-1$ and $d_{n-1} = \frac{1}{c_0}$.*

Proof. If the code C is right sequential then we have that $CD^T = C$ where D^T is given in Equation 4. Then by multiplying on the right $(D^T)^{-1}$ we have $C = C(D^T)^{-1}$.

We note that $(D^T)^{-1} = (D^{-1})^T$. Then the computation follows exactly as in Theorem 4. □

We say that a code is *left-right* sequential, if it is both left polycyclic and right polycyclic for the same polynomial $c(x)$.

Theorem 8. *If C is left-right sequential for the polynomial $c(x)$ then $c(x) = \frac{x^n+c_0}{1+c_0x}$ where $c_0^{n+1} = (-1)^{n+1}$.*

Proof. Follows exactly as in Theorem 5. □

Let C be a code with parity check matrix H. Then $0 = CH^T$. If C is right sequential then $0 = CD^TH^T = C(HD)^T$. Therefore the dual of C is invariant by multiplication by D on the right and hence is right polycyclic. Notice, however, that they have the same associate vector. It is easy to see that the same is true for left sequential and left polycyclic. Since it is the same associate vector we have the following theorem.

Theorem 9. *A code C over a field is left-right polycyclic if and only if $C^\perp$ is left-right sequential.*

7. Conclusion and open problems

We have introduced the notion of the annihilator code of a polycyclic code which behaves like the dual of a standard cyclic code in many ways. For example, we derive MacWilliams relations which relate the weight enumerator of the code with the weight enumerator of its annihilator. The class of self annihilator codes deserves more attention. We have shown that right polycyclic codes are left polycyclic for different associate polynomials and characterized the case when they are equal. We conducted a similar study for sequential codes. Extension of these results to skew polynomial rings warrants further study.

Acknowledgments

The authors thanks the anonymous referees for their helpful remarks that greatly improved the presentation of the material.

References

[1] K. Betsumiya and M. Harada, Binary optimal odd formally self-dual codes, *Des. Codes Crypt.*, **23** (2001), 11–22.

[2] J. Fields, P. Gaborit, V. Pless and W. C. Huffman, On the classification of extremal even formally self-dual codes of lengths 20 and 22, *Discrete Appl. Math.*, **111** (2001), 75–86.

[3] M. Grassl, Bounds on the minimum distance of linear codes, available online at http://www.codetables.de

[4] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge Univ. Press, 2003.

[5] T. T. Kasami, Optimum shortened cyclic codes for burst-error correction, *IEEE Trans. Inform. Theory*, **9** (1963), 105–109.

[6] J.-L. Kim and V. Pless, A note on formally self-dual even codes of length divisible by 8, *Finite Fields Appl.*, **13** (2007), 224–229.

[7] S. R. Lopez-Permouth, B. R. Parra-Avila and S. Szabo, Dual generalizations of the concept of cyclicity of codes, *Adv. Math. Commun.*, **3** (2009), 227–234.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[9] M. Matsuoka, θ-polycyclic codes and θ-sequential codes over finite fields, *Int. J. Algebra*, **5** (2011), 65–70.

[10] W. W. Peterson and E. J. Weldon, *Error Correcting Codes*, MIT Press, 1972.

[11] E. M. Rains and N. J. A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, Elsevier, Amsterdam, 1998.

[12] J. Wood, Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.*, **121** (1999), 555–575.

Received for publication March 2015.

E-mail address: adelnife2@yahoo.com
E-mail address: doughertys1@scranton.edu
E-mail address: andre.leroy@univ-artois.fr
E-mail address: patrick.sole@telecom-paristech.fr