ELSEVIER

Discrete Mathematics 177 (1997) 273–277

DISCRETE MATHEMATICS

Note

Cyclic codes over finite rings

Marcus Greferath

Department of Mathematics, University of Duisburg, D-47048 Duisburg, Germany

Received 5 October 1995; revised 18 November 1996; accepted 9 December 1996

Dedicated to A.G. Shannon, Technical University of Sydney

Abstract

It is well known that cyclic linear codes of length n over a (finite) field F can be characterized in terms of the factors of the polynomial x^n-1 in $F[x]$. This paper investigates cyclic linear codes over arbitrary (not necessarily commutative) finite rings and proves the above characterization to be true for a large class of such codes over these rings. © 1997 Elsevier Science B.V. All rights reserved

Introduction

Codes over rings have been discussed in a series of papers originating with Blake [2,3], who presented generalized notions of *Hamming codes*, *Reed–Solomon codes*, and *BCH codes* over arbitrary integer residue rings. Spiegel [15,16] continued this work, concentrating on BCH codes involving group algebras over rings of p-adic integers. Both scholars unanimously view cyclic codes of length n over the ring R as ideals in the group algebra RC_n, where C_n is the cyclic group of order n. Shankar [13] considered BCH codes over integer residue rings as well, but started with monic divisors of x^n-1 in $R[x]$ used as generator polynomials for these codes.

Further authors, such as Satyanarayana [12] presented analyses of codes over $\mathbb{Z}_n$ considering their properties under the *Lee metric*. Klemm in the more recent papers [9,10] investigated the *MacWilliams Identity* for codes essentially over $\mathbb{Z}_4$, and gave some invariant theoretic characterization of weight enumerators of self-dual linear codes over this ring. The most exciting development in this direction began with papers by Forney et al. [7] stating that the Nordstrom–Robinson code is the binary image of a well-known $\mathbb{Z}_4$-linear code, namely the Octacode. Hammons et al. [8] continued this line and were able to explain the quasiduality of some notorious nonlinear binary codes (Kerdock, Preparata and related codes) as a proper duality when considered as linear

PII S0012-365X(97)00006-X

codes over $\mathbb{Z}_4$. Since then further papers have been published dealing with linear and cyclic codes over $\mathbb{Z}_4$ and further integer residue rings as well as the ring of p-adic integers (cf. [6,4] and also [14]).

The above papers all coincide mainly in considering linear codes over integer residue rings, while neglecting the general question if the basic class of rings could still be enlarged when generalizing the notion of a linear code.

The present article suggests to investigate codes over arbitrary (not necessarily commutative) finite rings. We propose a notion of a (cyclic) linear code and give a characterization of a large class of cyclic linear codes of length n over such rings by divisors of $x^n - 1$ serving as generator polynomials for the respective codes, thus proving that the classical relation remains valid as well in a more general context.

The following text presupposes all rings to be associative rings possessing a unit element.

1. Linear and cyclic codes over finite rings

Definition 1.1. A *linear left code* C of length n over a finite ring R is a submodule of ${}_RR^n$. We call C *splitting* if it is a direct summand of ${}_RR^n$.

A cyclic code C over R shall be a code where any cyclic shift of the entries in a codeword produces another codeword of C. For linear codes, Blake [2] and Spiegel [16] reflect this fact using the group algebra RG for some cyclic group G. Our investigations will follow a more classical approach where the polynomial ring over R is involved.

Definition 1.2. A *cyclic* linear left code C of length n over a ring R is a left ideal of $R[x]/(x^n - 1)$. C is called *splitting* if it is a direct summand[1] of ${}_R(R[x]/(x^n - 1))$.

It is obvious that for R being a field all the definitions given coincide with the usual ones for linear and cyclic codes; only the notion of a splitting code is a specialization to a proper subclass of linear codes over rings.

Cyclic linear codes of length n over a field F allow a characterization by the divisors of $x^n - 1$ in $F[x]$. This characterization may be stated as follows.

Proposition 1.3. *For a cyclic linear code C over the (finite) field F there exists a unique monic polynomial g of minimal degree such that the following hold:*
(a) *C is generated by g in $F[x]/(x^n - 1)$.*
(b) *g is a divisor of $x^n - 1$ in $F[x]$.*

The proof of the foregoing proposition is straightforward and makes use of the division algorithm in the polynomial ring $F[x]$. In the context of codes over rings

[1] Note that we do not postulate C to be a complemented (left) ideal of $R[x]/(x^n - 1)$.

a statement such as Proposition 1.3 looks rather unlikely, because $R[x]$ is far from possessing a division algorithm in the case of a non-field R. It is surprising, however, that such a result holds for cyclic splitting codes over finite rings. We are going to develop a proof thereof in the following.

2. Divisors of $x^n - 1$ generate splitting codes

Let us first investigate divisors of $x^n - 1$ in the polynomial ring over a finite ring and discover what kind of cyclic codes they generate. The following lemma will be useful.

Lemma 2.1. *Let R be a finite ring, and let $gh = x^n - 1$ for some $g, h \in R[x]$. Then:*
(a) *g and h commute, i.e. $hg = x^n - 1$.*
(b) *${}_R(R[x]h)$ is a free module.*
(c) *$R[x]g$ is a direct summand of ${}_RR[x]$.*

Proof. For the constant coefficients g_0, h_0 of g and h, respectively, we have $g_0 h_0 = -1$ and hence g_0 and h_0 are units of R, since R ist finite. From this we get that $fh = 0$ implies $f = 0$ for all $f \in F[x]$. This leads to the $R[x]$-isomorphy and hence to the R-isomorphy of $R[x]$ and $R[x]h$ which proves this module to be free. Computing $(hg - (x^n - 1))h = hgh - h(x^n - 1) = 0$ we find $hg = x^n - 1$. Let us finally consider the R-linear epimorphism $R[x] \longrightarrow R[x]h/(x^n - 1)$. Its kernel is obviously $R[x]g$, and, since $R[x](x^n - 1)$ is a direct summand of the free module ${}_RR[x]h$, we know $R[x]h/(x^n - 1)$ to be a projective R-module. This shows $R[x]g$ to be a direct summand of ${}_RR[x]$. □

What we have just observed allows the following conclusion:

Corollary 2.2. *For a finite ring R every divisor of $x^n - 1$ in $R[x]$ generates a cyclic splitting code of length n.*

Proof. Let g be a divisor of $x^n - 1$ in $R[x]$, then by Lemma 2.1 we know $R[x]g$ to be a direct summand of ${}_RR[x]$ which contains the submodule $R[x](x^n - 1)$. Hence we obtain $R[x]g/(x^n - 1)$ to be a direct summand in ${}_R(R[x]/(x^n - 1))$ which proves our claim. □

3. Characterization of all cyclic splitting codes

The foregoing section has shown how a large class of cyclic splitting codes of length n may be generated by divisors of $x^n - 1$. This result remains slightly unsatisfactory since it does not imply a characterization of *all* cyclic splitting codes by these divisors

in the sense of Proposition 1.3. Therefore we are going to develop our principal result now and will first recall some important facts concerning finite and semisimple rings. It is well known that if R is a finite ring then $S := R/\mathrm{Rad}(R)$, i.e. the quotient of R by its Jacobson radical is a semisimple ring, and by one of Wedderburn's theorems we know semisimple rings to be direct products of matrix rings over (skew)fields.

Proposition 3.1. (a) *For a semisimple ring S the polynomial ring $S[x]$ is a (left and right) principal ideal ring.*

(b) *If R is a finite ring, then* $\mathrm{Rad}(R)[x]$ *is a small submodule of* ${}_RR[x]$, *i.e. for any submodule U of* ${}_RR[x]$ *with* $\mathrm{Rad}(R)[x] + U = R[x]$ *it follows that* $U = R[x]$.

Proof. (a) Obviously we only have to check our claim for $S = M_k(F)$, the ring of all $k \times k$-matrices over the (skew)field F. It is easily verified that the polynomial ring $M_k(F)[x]$ is isomorphic to the matrix ring $M_k(F[x])$. The latter ring is a matrix ring over a principal ideal domain which refering to [5, Ch. 10.5, Ex. 6] leads to our claim.

(b) Any standard text on (noncommutative) ring theory contains the proof of the fact that for a finite ring R and any module ${}_RM$ the relation $\mathrm{Rad}_R(M) = \mathrm{Rad}(R)M$ holds, the latter clearly being a small submodule of ${}_RM$. Together with $\mathrm{Rad}(R)[x] = \mathrm{Rad}(R)R[x]$ this yields our statement. □

We are now able to state our complete characterization of cyclic splitting codes by divisors of $x^n - 1$.

Theorem 3.2. *For a cyclic linear left code of length n over a finite ring R the following are equivalent:*

(a) *C is a splitting code.*

(b) *There exists a divisor g of $x^n - 1$ in $R[x]$ such that $C = R[x]g/(x^n - 1)$.*

Proof. That (b) implies (a) follows from Corollary 2.2. So let C be a cyclic splitting code of length n over R. For a complement D of C in ${}_R(R[x]/(x^n - 1))$ we have loosely spoken $C + D = R[x]$ and $C \cap D = R[x](x^n - 1)$. Setting $D' := D \cap (\bigoplus_{i=0}^{n-1} Rx^i)$ we easily verify D' to be a complement of C in ${}_RR[x]$. Now consider the natural map $\bar{\cdot} : R \longrightarrow S := R/\mathrm{Rad}(R)$ which induces the (semilinear) epimorphism ${}_RR[x] \longrightarrow {}_SS[x]$. The latter maps C to an ideal $\overline{C}$ of $S[x]$. Applying Proposition 3.1(a) we therefore obtain an element $g \in C$ with $\overline{C} = S[x]\overline{g}$ and define $C_0 := R[x]g$. Then $C_0 \leqslant C$ and $C_0 \cap D' = 0$ whereas $C_0 + D' + \mathrm{Rad}(R)[x] = R[x]$. By Proposition 3.1(b) this yields $C_0 \oplus D' = R[x]$ and thus $C_0 = C$. Hence C is generated by g, and because of $R[x](x^n - 1) \leqslant C$ we obtain a polynomial $h \in R[x]$ such that $hg = x^n - 1$. □

The reader might have noticed that our results are valid for a much larger class of rings. However, because of the more applied context here we have prefered to formulate them for the class of finite rings.

References

[1] F.W. Anderson, K.R. Fuller, Rings and Categories of Modules (Springer, New York, 1974).
[2] I.F. Blake, Codes over certain rings, Information and Control 20 (1972) 396–404.
[3] I.F. Blake, Codes over integer residue rings, Information and Control 29 (1975) 295–300.
[4] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, Designs, Codes and Cryptography 6 (1995) 21–35.
[5] P.M. Cohn, Algebra, Vol. 1, second edition (Wiley, Chichester, 1985).
[6] J.H. Conway, N.J.A. Sloane, Self-dual codes over integers modulo 4, J. Combin. Theory 62 (1993) 30–45.
[7] G.D. Forney, Jr., N.J.A. Sloane, M. Trott, The Nordstrom–Robinson Code is the binary image of the octacode, in: A.R. Calderbank et al., eds., Coding and Quantization: DIMACS/IEEE Workshop 1992, Trans. Amer. Math. Soc. 14 (1993) 19–26.
[8] R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Information Theory 40(2) (1994) 301–319.
[9] M. Klemm, Über die Identität von MacWilliams für die Gewichtsfunktion von Codes, Arch. Math. 49 (1987) 400–406.
[10] M. Klemm, Selbstduale Codes über dem Ring der ganzen Zahlen modulo 4, Arch. Math. 53 (1989) 201–207.
[11] T.Y. Lam, Non-commutative Ring Theory (Springer, New York, 1991).
[12] C. Satyanarayana, Lee metric codes over integer residue rings, IEEE Trans. Information Theory 25(2) (1970) 250–254.
[13] P. Shankar, On BCH codes over arbitrary integer rings, IEEE Trans. Information Theory 25(4) (1970) 480–483.
[14] P. Solé, Open problem 2: cyclic codes over rings and p-adic fields, in: G. Cohen and J. Wolfmann, eds., Coding Theory and Applications (Springer, New York, 1988) 329.
[15] E. Spiegel, Codes over $\mathbb{Z}_m$, Information and Control 35 (1977) 48–51.
[16] E. Spiegel, Codes over $\mathbb{Z}_m$, revisited, Information and Control 37 (1978) 100–104.
[17] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1978).