East-West J. of Mathematics: Vol. 14, No 1(2012) pp. 28-36

ON SELF-DUAL CONVOLUTIONAL CODES OVER RINGS

Herbert S. Palines and **Virgilio P. Sison**

Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños
College, Laguna 4031, Philippines
e-mail: hspalines@uplb.edu.ph, vpsison@uplb.edu.ph

Abstract

We study the construction of a parity check matrix $H(D) \in R(D)^{(n-k)\times n}$ of a rate-k/n convolutional code $\mathcal{C}$ over a commutative ring R that satisfies the descending chain condition. A $(n-k)\times n$ systematic parity check matrix $H(D)$ is obtained from a standard generator matrix $G(D) \in R(D)^{k\times n}$ of $\mathcal{C}$. If $G(D) = (I_k, A)$ such that $n = 2k$ and $A^{-1} = -A^T$, then $H(D) = (-A^T, I_k)$ is equivalent to $G(D)$, and consequently $\mathcal{C}$ is self-dual. New examples of encoders of rate-4/8 self-dual convolutional codes over the binary field $\mathbb{F}_2$ and the integer ring $\mathbb{Z}_4$ are presented.

1 Introduction

Convolutional codes are used successfully in numerous practical applications in order to achieve reliable data transmission. It includes, but not limited to, digital imaging, radio and mobile communications, and deep space telecommunications. A strong convolutional code or the combination of a convolutional code with a block code are used to achieve power efficient communications. The first error control code developed for deep space application is a rate-1/2 convolutional code of memory 24 for the *Pioneer 9* solar orbiter launched in November 1968. In various radio communication technologies, the *Code Division Multiple Access* (CDMA) digital system is used. This technology increases the capacity up to ten times that of an analog system, improves call quality

Key words: Self-dual convolutional codes over rings, parity check matrix, equivalent convolutional encoders, orthogonal rows
2010 AMS classification:68P30

by producing better and more consistent sound, enhances privacy, and widens network coverage. The IS-95 CDMA cellular standard uses a convolutional code with memory equal to 8. For a detailed discussion of applications of convolutional codes, the reader is referred to [13].

Due to theoretical and practical considerations in coding theory, researchers were motivated to use a bigger class of rings as base structure. Massey and Mittelholzer [6] initiated the theory of convolutional codes over rings when they showed that the most appropriate codes for phase modulation are the linear codes over the residue class ring $\mathbb{Z}_M$. Moreover, Fagnani and Zampieri [3] gave a complete characterization and analysis of the structural properties of generator matrices and convolutional codes over $\mathbb{Z}_{p^r}$. This analysis can be extended to the $\mathbb{Z}_M$ case. The usage of this particular ring is motivated mainly by two reasons: this ring plays a key role for phase-modulated signals and there are some strong results in convolutional codes over this ring which are completely analogous to the classical theory of convolutional codes over fields.

Self-dual block codes stimulated the great interest of many researchers because of its usefulness in practical applications and its rich mathematical theory. To cite, the extended Hamming code of length 8 and the extended Golay code of length 24 are the best known classical self-dual binary linear block codes. These codes, in some sense, are optimal and their construction admits an efficient decoding algorithm. Another one is the self-dual code over the field $\mathbb{F}_{128}$ which is used to encode information for compact discs and digital versatile discs. Until now, researchers are focusing on finding and classifying optimal self-dual block codes of higher dimensions. A survey of self-dual block codes and some open problems are found in [10].

It is rather a different scenario in the theory of self-dual convolutional codes. There are several duality notions and properties for convolutional codes and they are justified by their respective applications [2]. There are two concepts of duality that are most commonly found in literature: the sequence space duality and the natural notion of duality from block codes (for instance, see [2], [14], [5] and [11]).

R. Johannesson, P. Ståhl and E. Wittenmark [4] reported the world's second Type II binary convolutional code. The first was done by A. R. Calderbank, G. D. Forney, Jr. and A. Vardy [1]. We say that a code is of *Type II* if each codeword in the code has a weight divisible by four (*doubly-even*) and the code is self-dual.

We can see that the reported self-dual convolutional codes are classified in terms of their weight properties (*i.e.* of being Type II). Moreover, the duality of these codes are defined with respect to the sequence space duality. In our case, we consider self-duality of convolutional codes in the sense of Definition 2 given in (3). It is quite evident that little is known about this type of self-dual convolutional codes. Nevertheless, Schneider [11], in his doctoral dissertation, generalized some concepts in the theory of self-dual linear block codes over

fields to self-dual convolutional codes over fields. In this paper, we focus on constructing encoders of self-dual convolutional codes over a commutative ring R that satisfies the descending chain condition.

The material is organized as follows. Section 2 introduces the definition of convolutional codes over rings and the notion of self-duality for these codes. Section 3 talks about the algorithm that is used to construct the encoders of self-dual convolutional codes. New examples of minimal-basic and systematic encoders of rate-4/8 self-dual convolutional codes over the binary field $\mathbb{F}_2$ and integer ring $\mathbb{Z}_4$ are presented in Section 4. These examples are constructed using a MAGMA® routine. In Section 5, the summary, conclusion and recommendations are given.

2 Preliminaries and definitions

2.1 Convolutional codes over rings

Let R be a commutative ring with identity $1_R \neq 0$. We let $R[D]$ be the ring of polynomials in the delay operator D with coefficients ring R. Moreover, consider the ring of rational functions $R(D)$ whose elements are of the form

$$\frac{p(D)}{q(D)} \tag{1}$$

where $p(D), q(D) \in R[D]$, and such that the trailing coefficient of $q(D)$ is a unit in R. The trailing coefficient is the coefficient of the smallest power of D with a nonzero coefficient.

We adopt the following definition due to Massey.

Definition 1. *The $R(D)$-submodule of $R(D)^n$ given by*

$$\left\{u(D)G(D) | u(D) \in R(D)^k\right\} \tag{2}$$

where $G(D)$ is a $k \times n$ matrix over $R(D)$ whose rows are free over $R(D)$, is called a rate-k/n convolutional code $\mathcal{C}$ over R. The matrix $G(D)$ is a generator matrix (encoder) for $\mathcal{C}$ if all entries in $G(D)$ are realizable.

Note that the convolutional code $\mathcal{C}$ as defined is completely determined and characterized by the $k \times n$ matrix $G(D)$. Two encoders are *equivalent* if they generate the same code. Moreover, two encoders $G(D)$ and $G'(D)$ of $\mathcal{C}$ are equivalent if and only if there exists a $k \times k$ invertible matrix $T(D)$ over $R(D)$ such that $G'(D) = T(D)G(D)$ [14].

An encoder $G(D)$ is said to be *systematic* if it causes the information symbols to appear unchanged among the code symbols, or equivalently, if some k of its columns form the $k \times k$ identity matrix.

The encoder $G(D)$ is said to be a polynomial generator matrix for $\mathcal{C}$ if its entries are all polynomial. We say that $G(D)$ is *basic* if it is polynomial and has a polynomial right inverse.

Consider a polynomial encoder $G(D)$. The ith *constraint length* of $G(D)$, denoted by ν_i, is defined to be the maximum among the degrees of the component polynomials of the ith row of $G(D)$. The *overall constraint length* of $G(D)$ is given by $\nu = \sum_{i=1}^{k} \nu_i$.

An encoder $G(D)$ is *minimal-basic* if it is basic and the overall constraint length ν is minimal over all equivalent basic encoders.

The reader is referred to [14], [12], [5] and [3] for a complete discussion of structural properties of convolutional encoders.

2.2 Self-dual convolutional codes

The $(n-k)\times n$ matrix $H(D)$ over $R(D)$, of full rank, is a *parity check matrix* of a rate-k/n convolutional code $\mathcal{C}$ generated by a $k\times n$ encoder $G(D)$ if and only if $v(D)H(D)^T = 0$ for all $v(D) \in \mathcal{C}$, or equivalently, if and only if $G(D)H(D)^T = 0$, where $H(D)^T$ is the transpose of $H(D)$. In other words, the rows of $G(D)$ and $H(D)$ are orthogonal.

We simply extend to the ring case the definition of the dual of a convolutional code over fields found in [5].

Definition 2. *If $\mathcal{C}$ is a rate-k/n convolutional code over a ring R, its dual code, denoted by $\mathcal{C}^\perp$ is defined by:*

$$\mathcal{C}^\perp = \{x(D) \in R(D)^n | x(D)\cdot v(D) = 0, \text{ for all } v(D) \in \mathcal{C}\}\,. \tag{3}$$

Since the convolutional code $\mathcal{C}$ can be regarded as a linear block code over $R(D)$, the inner product on $R(D)^n$ can be defined as follows: if $x(D), v(D) \in R(D)$ such that $x(D) = [x_1(D), x_2(D), \ldots, x_n(D)]$ and $v(D) = [v_1(D), v_2(D), \ldots, v_n(D)]$, then $x(D)\cdot v(D)$, or simply $x(D)v(D)$, is given by

$$\sum_{i=1}^{n} x_i(D)v_i(D)\,, \tag{4}$$

where the product $x_i(D)v_i(D)$ is taken over $R(D)$.

If the ring R satisfies the descending chain condition (DCC) on its ideals, the rate-k/n convolutional code $\mathcal{C}$ over R can be characterized by a $(n-k)\times n$ parity check matrix $H(D)$ over $R(D)$ [7]. In this case, the $n-k$ linearly independent rows of $H(D)$ span $\mathcal{C}^\perp$. In other words, $H(D)$ can be considered

as an encoder of $\mathcal{C}^{\perp}$. That is, $\mathcal{C}^{\perp}$ can be seen as a rate-$(n-k)/n$ convolutional code over R generated by $H(D)$.

If $\mathcal{C} = \mathcal{C}^{\perp}$, then we say $\mathcal{C}$ is *self-dual*. It is apparent that a convolutional code $\mathcal{C}$ is self-dual if and only if the encoders of $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are equivalent.Henceforth, we consider the ring R to be a commutative ring with identity $1_R \neq 0$ that satisfies DCC.

3 Obtaining the encoders of self-dual convolutional codes

The second Type II binary convolutional code in [4] was obtained by a computer search. The authors constructed first a huge set of rate-1/8 doubly-even convolutional codes which served as building blocks to create a huge set of rate-2/8 doubly-even convolutional codes. This set was then used to derive the set of rate-4/8 doubly-even convolutional codes. From this, a class of Type II binary convolutional codes can be obtained. See [4] for the thorough analysis of these codes. A specific encoder for this code is given by

$$G(D) = \begin{pmatrix} 0 & 0 & 1 & D & D+1 & D+1 & 1 & D \\ D & 0 & 0 & 1 & 1 & D+1 & D+1 & 1 \\ D & D & D+1 & 0 & 0 & D & D+1 & 1 \\ D+1 & D+1 & 0 & 0 & D & 1 & D & 1 \end{pmatrix}.$$

In our sense, the method discussed in [4] is completely different. Our proposed method is strongly motivated by the following encoders found in [10], [5] and [11], respectively.

$$G_R = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 3 & 2 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 3 & 2 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 3 & 2 \end{pmatrix},$$

$$G_M(D) = \begin{pmatrix} 1 & 0 & \frac{1}{1+D} & \frac{D}{1+D} \\ 0 & 1 & \frac{D}{1+D} & \frac{1}{1+D} \end{pmatrix},$$

and

$$G_S(D) = \begin{pmatrix} 1 & 0 & \frac{2D^2+2D+1}{D^2+2D+2} & \frac{2D^2+2}{D^2+2D+2} \\ 0 & 1 & \frac{D^2+1}{D^2+2D+2} & \frac{2D^2+2D+1}{D^2+2D+2} \end{pmatrix}.$$

The 4×8 matrix G_R over $\mathbb{Z}_4$ is an encoder of the *octacode* which is a self-dual linear block code over $\mathbb{Z}_4$. While the matrices $G_M(D)$ and $G_S(D)$ are encoders of rate-2/4 self-dual convolutional codes over the finite fields $\mathbb{F}_2$ and $\mathbb{F}_3$, respectively. We observe that G_R, $G_M(D)$, and $G_S(D)$ take the form

(I_r, A) where I_r is the $r \times r$ identity matrix and A is an $r \times r$ matrix over $\mathbb{Z}_4$, $\mathbb{F}_2(D)$, and $\mathbb{F}_3(D)$, respectively. Moreover, each matrix satisfies $A^{-1} = -A^T$ and $G_R G_R^T = 0$, $G_M(D)G_M(D)^T = 0$ and $G_S(D)G_S(D)^T = 0$.

The following lemma is used to derive a parity check matrix of a convolutional code from a standard systematic generator matrix of the code. The proof is quite straight forward (see [9]). In fact, this lemma is the convolutional counterpart of the linear block code case. Let $0_{r\times s}$ denote the $r \times s$ zero matrix.

Lemma 1. *Let $G(D)$ be a $k \times n$ matrix over $R(D)$. If $G(D) = (I_k, A)$ is an encoder of a convolutional code $\mathcal{C}$ over R, then a $(n-k) \times n$ parity check matrix $H(D)$ of $\mathcal{C}$ is given by*

$$H(D) = \left(-A^T, I_{n-k}\right) .$$

The following theorem is the main tool in creating the algorithm for constructing the encoders of self-dual convolutional codes over R.

Theorem 1. *If $G(D) = (I_k, A)$ is a $k \times n$ generator matrix of a convolutional code $\mathcal{C}$ over R where $n = 2k$ (i.e. $I, A \in R(D)^{k\times k}$), A is invertible over $R(D)$ and $A^{-1} = -A^T$, then the parity check matrix $H(D) = \left(-A^T, I_{n-k}\right)$ for $\mathcal{C}$ is equivalent to $G(D)$ and consequently, $\mathcal{C}$ is self-dual.*

Proof

$$\begin{aligned} H(D) &= \left(-A^T, I_k\right) \\ &= \left(A^{-1}, I_k\right) \\ &= A^{-1}\left(I_k, A\right) \\ &= A^{-1}G(D). \end{aligned}$$

Note further that A and A^{-1} are invertible over $R(D)$. Indeed, $H(D)$ and $G(D)$ are equivalent. Since $G(D)$ and $H(D)$ generate $\mathcal{C}$ and $\mathcal{C}^\perp$, respectively, therefore $\mathcal{C} = \mathcal{C}^\perp$. Thus, $\mathcal{C}$ is self-dual. □

The Algorithm

Theorem 1 also tells us that $G(D)$ is both a generator matrix and a parity check matrix of $\mathcal{C}$. One can immediately verify by block matrix multiplication that $G(D)G(D)^T = 0_{k\times k}$.

The algorithm for finding $G(D) = (I_k, A)$, that satisfies the conditions of Theorem 1, deals on finding the suitable matrix A such that $A^{-1} = -A^T$. The algorithm is given below.

1. Construct set P of polynomials of degree less than or equal to L.
2. Construct set Q of all possible (distinct) rational functions, such as in (1), from the elements of P.

3. Construct $k \times k$ matrices A_i with entries coming from Q.
4. For each i, test whether matrix A_i is invertible and satisfies $A_i^{-1} = -A_i^T$.
5. Obtain matrix $G(D)$ by augmenting matrix A_i, that completed step 4, to the identity matrix I_k such that $G(D) = (I_k, A_i)$.

Since $G(D) = (I_k, A_i)$ satisfies the conditions of Theorem 1, $G(D)$ will generate a self-dual convolutional code.

4 New examples of encoders of rate-4/8 self-dual convolutional codes over $\mathbb{F}_2$ and $\mathbb{Z}_4$

Since $\mathbb{Z}_{p^r}$ satisfies DCC, a rate-k/n convolutional code over $\mathbb{Z}_{p^r}$ can be characterized by a $(n-k) \times n$ parity check matrix over $\mathbb{Z}_{p^r}(D)$. Consequently, encoders for rate-4/8 self-dual convolutional codes over the binary field $\mathbb{F}_2$ and the integer ring $\mathbb{Z}_4$ are constructed based on the given algorithm. These examples are obtained using a MAGMA® routine.

4.1 A minimal-basic encoder of a rate-4/8 self-dual convolutional code over $\mathbb{F}_2$

Let matrix A_1 be a 4×4 matrix over $\mathbb{F}_2(D)$ given by

$$A_1 = \begin{pmatrix} \frac{1}{D+1} & \frac{1}{D+1} & \frac{1}{D+1} & \frac{D}{D+1} \\ \frac{1}{D+1} & \frac{1}{D+1} & \frac{D}{D+1} & \frac{1}{D+1} \\ \frac{1}{D+1} & \frac{D}{D+1} & \frac{1}{D+1} & \frac{1}{D+1} \\ \frac{D}{D+1} & \frac{1}{D+1} & \frac{1}{D+1} & \frac{1}{D+1} \end{pmatrix}.$$

It can be verified that $A_1^{-1} = -A_1^T$. Since $-1 = 1$ in $\mathbb{F}_2$, we have $-A_1^T = A_1^T = A_1$ and $A_1 A_1^T = I_4$. Now, we augment matrix A_1 to I_4 such that

$$G_1(D) = \begin{pmatrix} 1 & 0 & 0 & 0 & \frac{1}{D+1} & \frac{1}{D+1} & \frac{1}{D+1} & \frac{D}{D+1} \\ 0 & 1 & 0 & 0 & \frac{1}{D+1} & \frac{1}{D+1} & \frac{D}{D+1} & \frac{1}{D+1} \\ 0 & 0 & 1 & 0 & \frac{1}{D+1} & \frac{D}{D+1} & \frac{1}{D+1} & \frac{1}{D+1} \\ 0 & 0 & 0 & 1 & \frac{D}{D+1} & \frac{1}{D+1} & \frac{1}{D+1} & \frac{1}{D+1} \end{pmatrix}.$$

A minimal-basic encoder equivalent to $G_1(D)$ is given by

$$G_1'(D) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ D & 0 & 0 & 1 & 0 & 1 & 1 & D+1 \end{pmatrix}.$$

Their equivalence can be seen via

$$G_1'(D) = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ D & 0 & 0 & 1 \end{pmatrix} G_1(D)\,.$$

Note that $G_1(D)G_1(D)^T = 0_{k\times k} = G_1'(D)G_1'(D)^T$. Hence, $G_1(D)$ or $G_1'(D)$ is an encoder of a self-dual rate-$4/8$ convolutional code over $\mathbb{F}_2$. Moreover, since $G_1'(D)$ is minimal-basic, it is also *minimal* [14].

4.2 A systematic encoder of a rate-$4/8$ self-dual convolutional code over $\mathbb{Z}_4$

An example of a systematic polynomial encoder of a self-dual rate-4/8 convolutional code over $\mathbb{Z}_4$ is given by

$$G_2(D) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 3 & 1 & 2D+1 & 2 \\ 0 & 0 & 1 & 0 & 2 & 2D+3 & 1 & 2D+1 \\ 0 & 0 & 0 & 1 & 3 & 2 & 2D+3 & 1 \end{pmatrix}.$$

One can verify that $G_2(D)G_2(D)^T = \mathbf{0}_{4\times 4}$ and since the first four columns of $G_2(D)$ form the identity matrix, the rows of $G_2(D)$ are free over $\mathbb{Z}_4(D)$. Similarly, if we let

$$A_2 = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 3 & 1 & 2D+1 & 2 \\ 2 & 2D+3 & 1 & 2D+1 \\ 3 & 2 & 2D+3 & 1 \end{pmatrix},$$

then $A_2^{-1} = -A_2^T$ where

$$A_2^{-1} = \begin{pmatrix} 3 & 1 & 2 & 1 \\ 3 & 3 & 2D+1 & 2 \\ 2 & 2D+3 & 3 & 2D+1 \\ 3 & 2 & 2D+3 & 3 \end{pmatrix}.$$

Consequently, since $G_2(D)$ is a polynomial systematic encoder, it is also *minimal* [8].

5 Summary and conclusion

Convolutional codes over rings have been defined. This definition was used to consider the notion of a self-dual convolutional code over a commutative

ring R that satisfies DCC. A method for deriving a parity check matrix of a convolutional code from a standard generator matrix of the code has been given. It was shown that to obtain a $k \times n$ ($n = 2k$) encoder $G(D)$ of a self-dual convolutional code over R, it is enough to find a matrix $A \in R(D)^{k \times k}$ such that $A^{-1} = -A^T$ where $G(D) = (I_k, A) \in R(D)^{k \times 2k}$. In this manner, encoders of a rate-4/8 self-dual convolutional codes over the binary field $\mathbb{F}_2$ and integer ring $\mathbb{Z}_4$ were constucted. It was shown that these encoders are minimal-basic and systematic, respectively.

A good extension of this problem is to consider the doubly-evenness of the constructed codes. It is also interesting to know whether the given algorithm works for any value of $k > 1$.

References

[1] A. R. Calderbank, G. D. Forney, Jr. and A. Vardy, "Minimal tail-biting trellises: The Golay code and more," *IEEE Trans. Inform. Theory*, vol.45, pp. 1435 1455, July 1999.

[2] G.D. Forney and M.D. Trott, "The dynamics of group codes: dual abelian group codes and systems," *IEEE Trans. Inform. Theory*, vol.50, pp. 2935 - 2965, 2004.

[3] F. Fagnani and S. Zampieri, "System-theoretic properties of convolutional codes over rings," *IEEE Trans. Inform. Theory*, vol.47, no. 6, pp. 2256–2274, September 2001.

[4] R. Johannesson, P. Ståhl and E. Wittenmark, "A note on type II Convolutional codes," *IEEE Trans. Inform. Theory*, vol.46, no. 4, pp. 1510 - 1514, July 2000.

[5] R.J. McEliece, "The algebraic theory of convolutional codes,"in Handbook of Coding Theory, V.S. Pless and W.C. Huffman,editors, Amsterdam, The Netherlands: North-Holland, Elsevier, 1998.

[6] J.L. Massey and T. Mittelholzer, "Convolutional codes over rings," *Proc. 4th Joint Swedish-Soviet Int. Workshop on Inform. Th.*, Gotland, Sweden, pp. 14–18, Aug. 27 - Sept. 1, 1989.

[7] T. Mittelholzer, "Convolutional codes over rings and the two chain condition," *Proc. IEEE Int. Symp. Information Theory*, Ulm, Germany, pp. 285, 1997.

[8] T. Mittelholzer, "Minimal encoders for convolutional codes over rings," *Communications Theory and Applications: Systems, Signal Processing and Error Control Coding*, London, U.K.: HW Comm. Ltd., pp. 30 - 36, 1993.

[9] H.S. Palines, "Parity check matrices of convolutional codes over rings," *M.Sc. Thesis*, University of the Philippines Los Baños, Philippines, 2011.

[10] E. M. Rains and N.J.A. Sloane, "Self-Dual Codes," in Handbook of Coding Theory, Information Sciences Research, AT& T Labs-Research, May 19, 1998.

[11] H. Schneider, "On the weight adjacency matrix of convolutional codes," *Ph.D. Dissertation*, Rijksuniversiteit Groningen, 2008.

[12] V. P. Sison, "Convolutional codes from linear block codes over galois rings," *Ph.D. Dissertation*, University of the Philippines Diliman, Philippines, 2005.

[13] M. C. Valenti, "The evolution of error control coding," in author's Ph.D. dissertation: Iterative detection and decoding for wireless communications, Bradley Dept. of Elect. & Comp. Eng., Virginia Tech, July 1999.

[14] E. Wittenmark, "An encounter with convolutional codes over rings," *Ph.D. Dissertation*, Lund University, Sweden, 1998.