Some Small Cyclic Convolutional Codes

Heide Gluesing-Luerssen, Wiland Schmale, Melissa Striha
Department of Mathematics
University of Oldenburg
P.O. Box 2503
26111 Oldenburg
Germany
gluesing@mathematik.uni-oldenburg.de
wiland.schmale@uni-oldenburg.de
Melissa.Striha@mail.uni-oldenburg.de

Abstract

In this note we will construct and investigate some small cyclic convolutional codes. Among other things we will present an infinite series of one-dimensional CCCs over $\mathbb{F}_4$ with length 3 and increasing constraint length (complexity). Our computations show that the first codes in this series have very good free distance.

1 Introduction

In the seventies a short series of papers appeared discussing the notion of cyclic convolutional codes (CCC, for short), see [3, 4, 5, 6]. Thereafter, the topic disappeared from the coding theory stage. However, we think it is worth being brought back into the community of convolutional coding theory. In this short note we want to discuss some phenomena of CCCs and present a few examples of CCCs with small parameters and their respective free distances. One of the main results of the papers above is the fact that there are no CCCs other than cyclic block codes, if cyclicity of a convolutional code is understood as the property where the cyclic shift of each codeword (a vector in $\mathbb{F}((D))^n$) is a codeword itself. This insight has led to a more general notion of cyclicity for convolutional codes. Just like in the case of block codes, a CCC is best described as an ideal in a suitable quotient ring. However, in contrast to block codes, the quotient ring now is a noncommutative polynomial ring whose multiplication is based on a nontrivial automorphism of the constants.

This concept of CCCs raises the question as to what the smallest length of a binary CCC or a CCC over $\mathbb{F}_3$ or $\mathbb{F}_4$ is. While this question is answered in [6] for the binary case, we will discuss the two other cases. The examples will show that the class of CCCs contain some codes with fairly good free distances.

2 Cyclic Convolutional Codes

In this section we recall the fundamental notions and results for cyclic convolutional codes; for the details the reader is asked to consult the papers [5, 6].

Recall that an (n,k)-convolutional code over a finite field $\mathbb{F}$ is a k-dimensional $\mathbb{F}((D))$-subspace $\mathcal{C}$ of $\mathbb{F}((D))^n$ of the form

$$\mathcal{C} = \operatorname{im} G := \{uG \mid u \in \mathbb{F}((D))^k\} \subseteq \mathbb{F}((D))^n \text{ with } G \in \mathbb{F}[D]^{k\times n},\ \operatorname{rk} G = k,$$

where

$$\mathbb{F}[D] = \Big\{ \sum_{j=0}^{N} D^j f_j \,\Big|\, N \in \mathbb{N},\ f_j \in \mathbb{F} \Big\} \text{ and } \mathbb{F}((D)) = \Big\{ \sum_{j=l}^{\infty} D^j f_j \,\Big|\, l \in \mathbb{Z},\ f_j \in \mathbb{F} \Big\}$$

are the polynomial ring and the field of formal Laurent series over $\mathbb{F}$ in the delay-operator D, respectively. (Due to a left-module structure to be introduced later in this section it is advantageous to put the coefficients to the right of the indeterminate D.) The matrix G is called a generator matrix of the code $\mathcal{C}$. Without loss of generality it can be assumed *basic*, i. e. the k-minors $\gamma_1, \ldots, \gamma_N \in \mathbb{F}[D]$ of G (where $N = \binom{n}{k}$) are coprime polynomials. In other words, the encoder is non-catastrophic. In that case the number

$$\delta(\mathcal{C}) := \max\{\deg \gamma_i \mid i = 1, \ldots, N\}$$

does not depend on the choice of G and is called the complexity of the code. It is also well-known [1] that we can assume $G = (g_{ij})$ to be *minimal*, i. e. the complexity equals the sum of the row degrees: $\delta = \sum_{i=1}^{k} \max_{j=1,\ldots,n} \deg g_{ij}$. If $\delta = 0$, the code can be regarded as a block code since it has a constant minimal generator matrix.

In the following we will assume that the length n and the characteristic of the field $\mathbb{F}$ are coprime. As in the case of cyclic block codes, we introduce the quotient ring

$$R_n := \mathbb{F}[x]/_{\langle x^n - 1\rangle},$$

which, as an $\mathbb{F}$-vector space, is isomorphic to $\mathbb{F}^n$. Then we have the identification

$$\left.\begin{array}{rcl} \psi: \quad \mathbb{F}((D))^n & \longrightarrow & R_n((D)) = \Big\{ \sum_{j=l}^{\infty} D^j v_j \,\Big|\, l \in \mathbb{Z},\ v_j \in R_n \Big\} \\ \Big(\sum_{j=l}^{\infty} D^j v_{0j}, \ldots, \sum_{j=l}^{\infty} D^j v_{n-1,j} \Big) & \longmapsto & \sum_{j=l}^{\infty} \sum_{i=0}^{n-1} D^j v_{ij} x^i. \end{array}\right\} \tag{2.1}$$

The set $R_n((D))$ carries a natural left R_n-module structure (coefficientwise multiplication). Just like in the case of block codes, left-multiplication of $v \in R_n((D))$ by $x \in R_n$ corresponds to the cyclic shift of the associated vector $\psi^{-1}(v) \in \mathbb{F}((D))^n$. In the following we will not distinguish between $\mathbb{F}((D))^n$ and $R_n((D))$. The following result, which has been proven in [6, Thm. 6] (see also [4, Thm. 6.4] for the binary case), shows that there are no convolutional codes (other than block codes) that are cyclic in the usual sense. More precisely, we have

Theorem 2.1
Let $\mathcal{C} \subseteq R_n((D))$ be a convolutional code (i. e. an $\mathbb{F}((D))$-subspace of $R_n((D))$) satisfying the condition

$$v \in \mathcal{C} \Longrightarrow xv \in \mathcal{C}.$$

Then $\delta(\mathcal{C}) = 0$, i. e. $\mathcal{C}$ is a block code.

This negative result has led to the following generalized concept of cyclic shifts and CCCs, see [5, 6].

Definition 2.2
Let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(R_n)$, the group of $\mathbb{F}$-algebra-automorphisms of R_n.

(a) The multiplication

$$R_n \times R_n((D)) \longrightarrow R_n((D)), \quad \Big(a, \sum_{j=l}^{\infty} D^j v_j\Big) \longmapsto a * \sum_{j=l}^{\infty} D^j v_j := \sum_{j=l}^{\infty} D^j \sigma^j(a) v_j$$

turns $R_n((D))$ into a left R_n-module. To be precise, we will call this the (R_n, σ)-module structure on $R_n((D))$. Extending this multiplication in the obvious way

$$\begin{gathered} R_n((D)) \times R_n((D)) \longrightarrow R_n((D)) \\ \Big(\sum_{\mu=m}^{\infty} D^\mu w_\mu, \sum_{j=l}^{\infty} D^j v_j\Big) \longmapsto \sum_{\mu=m}^{\infty} D^\mu w_\mu * \sum_{j=l}^{\infty} D^j v_j := \sum_{i=m+l}^{\infty} D^i \sum_{\mu+j=i} \sigma^j(w_\mu) v_j \end{gathered}$$

we obtain a non-commutative ring, denoted by $(R_n((D)), \sigma)$.

(b) A subset $\mathcal{C} \subseteq R_n((D))$ is called a convolutional code, if $\mathcal{C}$ is an $\mathbb{F}((D))$-subspace. It is called a σ-cyclic convolutional code (for short, σ-CCC), if it is additionally a left (R_n, σ)-submodule of $R_n((D))$, hence if it also satisfies

$$v \in \mathcal{C} \Longrightarrow x * v \in \mathcal{C}. \tag{2.2}$$

Hence the σ-CCCs are the left-ideals in the non-commutative ring $(R_n((D)), \sigma)$.

(c) A σ-cyclic convolutional code is called proper if it has complexity $\delta > 0$. Hence an improper σ-CCC has a constant generator matrix and therefore is the same as a block code.

Remark 2.3

(a) Of course, for $\sigma = \mathrm{id}_{R_n}$ the above defined multiplication $*$ is just the usual multiplication. In this case σ-cyclicity corresponds to the usual cyclic shift of the associated vectors and Theorem 2.1 applies.

(b) Piret [5] chooses the automorphism σ more restrictively than in the definition above. Only monomial automorphisms, i. e. $\sigma(x) = x^{\pi}$ for some $\pi \in \mathbb{Z}$ relatively prime to n, were considered.

(c) It is easy to see from the multiplication $*$, that if $G = \sum_{i=0}^{m} D^i G_i \in \mathbb{F}[D]^{k\times n}$ is the generator matrix of a σ-CCC for some automorphism σ, then G_0 generates a cyclic block code.

3 Some Small Cyclic Convolutional Codes

In this section we will present some CCCs with small parameters and their respective free distances. The main tool for the construction is a theorem by Piret [5] concerning the structure of CCCs. Recall that Piret only considers monomial automorphisms, see Rem. 2.3(b). However, it turns out that his (quite sophisticated) considerations work just as well for any automorphism on R_n and lead, among other things, to the following result.

Theorem 3.1
Let n, $q \in \mathbb{N}$ with q being a prime power and $(n, q) = 1$. Let $\mathbb{F}$ be a field with q elements and let $\sigma \in \mathrm{Aut}_{\mathbb{F}}(R_n)$ be any automorphism. Choose an idempotent $e \in R_n$ generating an irreducible cyclic block code $\langle e\rangle \subseteq R_n$. Let $k := \dim_{\mathbb{F}} \langle e\rangle$ and $h \in \mathbb{F}[x]$ be the parity check polynomial of $\langle e\rangle$. Finally, pick an element $f \in R_n$ sucht that $f \bmod h$ is a primitive element of the field $\mathbb{F}[x]/_{\langle h\rangle}$ and a sequence $(b_i)_{i\in\mathbb{N}_0}$ in $\mathbb{N}_0$. Then for every $m \in \mathbb{N}$ the polynomial

$$g := \sum_{i=0}^{m} D^i \sigma^i(e)\big(\sigma^i(f)\big)^{b_i}$$

generates an irreducible (n, k)-CCC in $R_n((D))$.

Remark 3.2

(a) Notice, that the set $\{g,\ x{*}g,\ \ldots,\ x^{k-1}{*}g\}$ is an $\mathbb{F}((D))$-basis of the code, hence a generator matrix is given by

$$G = \begin{bmatrix} \psi^{-1}(g) \\ \psi^{-1}(x * g) \\ \vdots \\ \psi^{-1}(x^{k-1} * g) \end{bmatrix} \in \mathbb{F}[D]^{k\times n}. \tag{3.1}$$

Thus the codewords $(u_0, \ldots, u_{k-1})G \in \mathbb{F}((D))^n$, $u_i \in \mathbb{F}((D))$, correspond, via the isomorphism ψ in (2.1), to the product $\sum_{i=0}^{k-1} u_i x^i * g$. Since the parity check polynomial h of the ideal $\langle e\rangle$ has degree k, this indeed leads to *all* elements of the left ideal generated by g, i. e. we have

$$\Big\{\sum_{i=0}^{k-1} u_i x^i * g \mid u_0, \ldots, u_{k-1} \in \mathbb{F}((D))\Big\} = \big\{u * g \mid u \in R_n((D))\big\}.$$

Unfortunately, it is not clear how the complexity of the CCC can be determined directly from the given data. In general the construction might lead to non-basic generator matrices and in the extreme case to cyclic block codes.

(b) In [5] and also in [6] it is shown that each CCC is the direct sum of CCCs of the form as in Theorem 3.1. The direct summands are determined by the decomposition of the associated cyclic block code (given by the constant terms) into irreducible block codes. In the theorem above, the irreducibility guarantees that the CCC has the same dimension as the cyclic block code one starts with.

We will illustrate the construction of Theorem 3.1 for some small parameters. In [6] the case of binary CCCs was considered. It has been shown that a proper binary CCC over $\mathbb{F}_2$ has length at least 7. In the following we will see that there are proper CCCs of length 2 (resp. 3) over $\mathbb{F}_3$ (resp. $\mathbb{F}_4$).

Example 3.3
In this example we show the existence of a $(2,1)$-CCC over the field $\mathbb{F}_3$. In order to do so we need a nontrivial automorphism of $R_2 := \mathbb{F}_3[x]/_{\langle x^2-1\rangle}$. Using the isomorphism $R_2 \cong \mathbb{F}_3[x]/_{\langle x-1\rangle} \oplus \mathbb{F}_3[x]/_{\langle x+1\rangle}$ it is easily seen that $\sigma(x) := 2x$ defines the only nontrivial element of $\mathrm{Aut}_{\mathbb{F}_3}(R_2)$. Moreover, there are two nontrivial $(2,1)$-cyclic block codes over $\mathbb{F}_3$, having generating idempotents $e_1 := 2 + x$ and $e_2 := 2 + 2x$ respectively. Let us pick e_1. Since $\sigma^j(e_1) = e_2$ for odd j and $\sigma^j(e_1) = e_1$ for even j, we obtain a σ-CCC for every $\delta > 0$ via the generator polynomial

$$g_\delta := \sum_{i=0}^{\delta} D^i \sigma^i(e_1) = \sum_{i=0}^{\delta} D^i(2 + 2^i x).$$

Using the isomorphism (2.1) this leads to the generator matrices

$$G^{(\delta)} := [2 + 2D + 2D^2 + \ldots + 2D^\delta,\ 1 + 2D + D^2 + \ldots + 2^\delta D^\delta] \in \mathbb{F}_3[D]^{1\times 2}$$

of $(2,1)$-CCCs over $\mathbb{F}_3$ (note that in a generator matrix it doesn't matter if the coefficients are put to the left or to the right of D since σ is the identity on $\mathbb{F}_3$). It is easy to see that $G^{(\delta)}$ is basic iff δ is even or $\delta = 1$. If δ is odd, then $G^{(\delta)} = \sum_{i=0}^{(\delta-1)/2} D^{2i} G^{(1)}$, hence generates the same code as $G^{(1)}$. It is obvious that $d_{\text{free}}(\operatorname{im} G^{(1)}) = 4$ and $d_{\text{free}}(\operatorname{im} G^{(2)}) = 6$. Moreover, one can easily verify that

$$d_{\text{free}}(\operatorname{im} G^{(\delta)}) = \text{weight}\left((1 + 2D^2)G^{(\delta)}\right) = 8 \text{ for all even } \delta \geq 4.$$

But we can do better. Theorem 3.1 allows for some additional factors in the coefficients of g_δ. Using $f = 2$ and $b_2 = 1$ we get the CCC with generator matrix

$$\hat{G}^{(6)} := [2 + 2D + D^2 + 2D^3 + D^4 + 2D^5 + D^6,\ 1 + 2D + 2D^2 + 2D^3 + 2D^4 + 2D^5 + 2D^6].$$

The matrix is basic, hence the complexity of the code is $\delta = 6$ and using a computer algebra program one can check that its free distance is 10. In a similar way we obtain basic generator matrices

$$\hat{G}^{(5)} := \begin{bmatrix} 2 + 2D + 2D^2 + 2D^3 + 2D^4 + D^5 \\ 1 + 2D + D^2 + 2D^3 + D^4 + D^5 \end{bmatrix}^{\mathsf{T}}$$

and

$$\hat{G}^{(7)} := \begin{bmatrix} 2 + D + 2D^2 + 2D^3 + D^4 + 2D^5 + 2D^6 + D^7 \\ 1 + D + D^2 + 2D^3 + 2D^4 + 2D^5 + D^6 + D^7 \end{bmatrix}^{\mathsf{T}}$$

which lead to CCCs with distances 9 and 11, respectively.

Using the generalized Heller bound

$$d_{\text{free}} \leq \min \left\{ \left\lfloor \frac{n(m+i)q^{k(m+i)-\delta-1}(q-1)}{q^{k(m+i)-\delta} - 1} \right\rfloor \,\middle|\, i \in \mathbb{N} \right\} \tag{3.2}$$

for the free distance of an (n, k)-convolutional code over $\mathbb{F}_q$ with complexity δ and memory m (see [2, p. 132] for the binary case), one can check that the code $\operatorname{im} G''$ above is just one less than the Heller bound.

Example 3.4
Now we construct some small CCCs over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where $\alpha^2 + \alpha + 1 = 0$.

(a) We will restrict ourselves to length $n = 3$ first. We proceed as in Example 3.3. Let $R_3 := \mathbb{F}_4[x]/_{\langle x^3 - 1\rangle}$. Using the isomorphism $R_3 \cong \mathbb{F}_4[x]/_{\langle x - 1\rangle} \oplus \mathbb{F}_4[x]/_{\langle x - \alpha\rangle} \oplus \mathbb{F}_4[x]/_{\langle x - \alpha^2\rangle}$, one can see that the $\mathbb{F}_4$-algebra R_3 has 6 automorphisms. One of them is given by $\sigma(x) = \alpha^2 x$. Proceeding as in Theorem 3.1, we begin with a generating idempotent of an irreducible cyclic block code. We choose the idempotent $e_0 := 1 + \alpha x + \alpha^2 x^2 \in R_3$, which generates the 1-dimensional cyclic block code with generator polynomial $(x - 1)(x - \alpha)$. One easily calculates

$$\sigma(e_0) = 1 + x + x^2 =: e_1,\ \sigma^2(e_0) = 1 + \alpha^2 x + \alpha x^2 =: e_2,\ \sigma^3(e_0) = e_0.$$

Hence we get σ-CCCs of length $n = 3$ and dimension $k = 1$ via the the generating polynomials

$$\begin{aligned} g_\delta &:= \sum_{i=0}^{\delta} D^i e_{i \bmod 3} \\ &= (1 + \alpha x + \alpha^2 x^2) + D(1 + x + x^2) + D^2(1 + \alpha^2 x + \alpha x^2) + D^3(1 + \alpha x + \alpha^2 x^2) \\ &\quad + D^4(1 + x + x^2) + D^5(1 + \alpha^2 x + \alpha x^2) + D^6(1 + \alpha x + \alpha^2 x^2) + \ldots \end{aligned}$$

and with the generator matrices

$$G^{(\delta)} := \sum_{i=0}^{\delta} D^i G_{i \bmod 3}, \quad \text{where } G_0 = [1,\ \alpha,\ \alpha^2],\ G_1 = [1,\ 1,\ 1],\ G_2 = [1,\ \alpha^2,\ \alpha].$$

Obviously, the matrices are not basic if $\delta > 2$ and $\delta \equiv 2 \bmod 3$. In the other cases, i. e. $\delta = 2$ or $\delta \not\equiv 2 \bmod 3$, the matrices $G^{(\delta)}$ are basic. (One can even show that in these cases the first two entries of $G^{(\delta)}$ are coprime.) Hence we get two series of basic generator matrices with constant sizes and increasing complexities (for $\delta \equiv 0 \bmod 3$ and for $\delta \equiv 1 \bmod 3$). We tested some of the first codes in these series and obtained free distances as follows.

$$d_{\text{free}}\left(\operatorname{im}[1 + D + D^2,\ \alpha + D + D^2\alpha^2,\ \alpha^2 + D + D^2\alpha]\right) = 9,$$
$$d_{\text{free}}\left(\operatorname{im}[1 + D + D^2 + D^3,\ \alpha + D + D^2\alpha^2 + D^3\alpha,\ \alpha^2 + D + D^2\alpha + D^3\alpha^2]\right) = 12,$$
$$d_{\text{free}}\left(\operatorname{im}\begin{bmatrix} 1 + D + D^2 + D^3 + D^4 \\ \alpha + D + D^2\alpha^2 + D^3\alpha + D^4 \\ \alpha^2 + D + D^2\alpha + D^3\alpha^2 + D^4 \end{bmatrix}^{\mathsf{T}}\right) = 13$$

and

$$d_{\text{free}}\left(\operatorname{im}\begin{bmatrix} 1 + D + D^2 + D^3 + D^4 + D^5 + D^6 \\ \alpha + D + D^2\alpha^2 + D^3\alpha + D^4 + D^5\alpha^2 + D^6\alpha \\ \alpha^2 + D + D^2\alpha + D^3\alpha^2 + D^4 + D^5\alpha + D^6\alpha^2 \end{bmatrix}^{\mathsf{T}}\right) = 15.$$

Notice that the free distances of $\operatorname{im} G^{(2)}$ and $\operatorname{im} G^{(3)}$ are optimal for codes with parameters $(3, 1)$ and complexity 2 and 3, respectively. Hence these codes are MDS-convolutional codes in the sense of [7]. The free distance of the code $\operatorname{im} G^{(4)}$ is just one less than the Heller bound (3.2).

(b) Let us now switch to length $n = 5$. In this case the $\mathbb{F}_4$-algebra

$$R_5 := \mathbb{F}_4[x]/_{\langle x^5 - 1\rangle} \cong \mathbb{F}_4[x]_{\langle x - 1\rangle} \oplus \mathbb{F}_4[x]/_{\langle x^2 + \alpha^2 x + 1\rangle} \oplus \mathbb{F}_4[x]/_{\langle x^2 + \alpha x + 1\rangle}$$

has 8 automorphisms one of which is given by $\sigma(x) = x^4 + \alpha x^3 + \alpha^2 x^2 + x$. Choosing the idempotent $e := \alpha x + \alpha^2 x^2 + \alpha^2 x^3 + \alpha x^4$, which generates the 2-dimensional block code $\langle (x - 1)(x^2 + \alpha^2 x + 1)\rangle$, we obtain for instance for $\delta = 1$ the polynomial

$$g := (\alpha x + \alpha^2 x^2 + \alpha^2 x^3 + \alpha x^4) + D(\alpha^2 x + \alpha x^2 + \alpha x^3 + \alpha^2 x^4).$$

Calculating $x * g$ leads to the generator matrix (see (3.1))

$$G = \begin{bmatrix} 0 & \alpha + D\alpha^2 & \alpha^2 + D\alpha & \alpha^2 + D\alpha & \alpha + D\alpha^2 \\ \alpha + D\alpha & D\alpha^2 & \alpha & \alpha^2 + D\alpha^2 & \alpha^2 + D\alpha \end{bmatrix}.$$

It is easy to see that the matrix G is basic and that $d_{\text{free}}(\operatorname{im} G) = 8$, since both cyclic block codes, $\langle e\rangle$ and $\langle \sigma(e)\rangle$, have distance 4. The Heller bound shows that this code is optimal among all $(5, 2)$-codes over $\mathbb{F}_4$ with complexity $\delta = 2$.

The examples presented above show that some of the constructions lead to quite good convolutional codes. We think that it is worthwhile resuming the investigation of CCCs as it was initiated in the seventies by Piret and Roos. In particular, the examples above give rise to the question whether one can explicitly construct a family of (n, k, δ)-CCCs with fixed parameters (n, k), increasing δ, and good free distances. Example 3.4 (a) looks very promising to us in this regard.

References

[1] G. D. Forney Jr. Convolutional codes I: Algebraic structure. *IEEE Trans. Inform. Theory*, 16:720–738, 1970. (see also corrections in IEEE Trans. Inf. Theory, vol. 17,1971, p. 360).

[2] R. Johannesson and K. S. Zigangirov. *Fundamentals of Convolutional Coding.* IEEE Press, New York, 1999.

[3] P. Piret. Convolutional codes and irreducible ideals. *Philips Res. Report*, 27:257–271, 1972.

[4] P. Piret. On a class of alternating cyclic convolutional codes. *IEEE Trans. Inform. Theory*, 12:64–69, 1975.

[5] P. Piret. Structure and constructions of cyclic convolutional codes. *IEEE Trans. Inform. Theory*, 22:147–155, 1976.

[6] C. Roos. On the structure of convolutional and cyclic convolutional codes. *IEEE Trans. Inform. Theory*, 25:676–683, 1979.

[7] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, 10:15–32, 1999.