On doubly-cyclic convolutional codes

Heide Gluesing-Luerssen[*] and Wiland Schmale[†]

February 17, 2006

Abstract

Cyclicity of a convolutional code (CC) is relying on a nontrivial automorphism of the algebra $\mathbb{F}[x]/(x^n - 1)$, where $\mathbb{F}$ is a finite field. A particular choice of the data leads to the class of doubly-cyclic CC's. Within this large class Reed-Solomon and BCH convolutional codes can be defined. After constructing doubly-cyclic CC's, basic properties are derived on the basis of which distance properties of Reed-Solomon convolutional codes are investigated. This shows that some of them are optimal or near optimal with respect to distance and performance.

Keywords: Convolutional coding theory, cyclic codes, skew polynomial rings.

MSC (2000): 94B10, 94B15, 16S36

1 Introduction

Despite the fact that convolutional codes are as important for applications as block codes, their mathematical description is much less developed, and there has been growing activity to fill this gap during the last decade, see, e. g., [18, 19, 1, 9, 7, 8, 5, 6, 4].

The gap in the mathematical theory of block and convolutional codes is particularly big when it comes to the notion of cyclicity. Cyclic convolutional codes (shortly, cyclic CC's or just CCC's) have been introduced and investigated by Piret and Roos in [15, 17]; for definitions see below. Their approach has much later been extended in [8] to a theoretical framework which exhibits many features in close analogy to the well known theory of cyclic linear block codes. It turned out that the class of CCC's contains plenty of codes with very good performance and distance properties, see also [7, 5].

In this article we construct a specific subclass of CCC's where the generating polynomial has an additional cyclic structure, see Section 3. Among these are Reed-Solomon type doubly-cyclic CC's, for which distance properties are derived in Section 4. More general results, leading to BCH convolutional codes, are indicated in Section 5. The algebraic prerequisites can be found in Section 2.

One standard way of defining CC's is as follows.

---

[*]University of Groningen, Department of Mathematics, P. O. Box 800, 9700 AV Groningen, The Netherlands; gluesing@math.rug.nl

[†]Department of Mathematics, University of Oldenburg, 26 111 Oldenburg, Germany; schmale@mathematik.uni-oldenburg.de

Definition 1.1 Let $\mathbb{F}$ be any finite field. A *convolutional code* $\mathcal{C} \subseteq \mathbb{F}[\boldsymbol{z}]^n$ with (algebraic) parameters (n, k, δ) is a submodule of the form $\mathcal{C} = \operatorname{im} G$, where $G \in \mathbb{F}[\boldsymbol{z}]^{k \times n}$ is a right-invertible matrix such that $\delta = \max\{\deg \gamma \mid \gamma \text{ is a } k\text{-minor of } G\}$. We call G a *generator matrix* of the code. The number n is called the *length*, k is the *dimension*, and δ is called the *overall constraint length* of the code.

By elementary matrix and module theory over $\mathbb{F}[\boldsymbol{z}]$ one realizes that a CC with parameters (n, k, δ) is just a direct summand of $\mathbb{F}[\boldsymbol{z}]^n$ of rank k and that the overall contraint length δ does not depend on the choice of the generating matrix G for $\mathcal{C}$. Details can be found for instance in [2, 13, 8]. In the coding literature a right invertible matrix is often called *basic* [2, p. 730] or *delay-free and non-catastrophic*, see [13, p. 1102].

It is well-known that each submodule of $\mathbb{F}[\boldsymbol{z}]^n$ has a minimal generator matrix in the sense of the next definition [2, Thm. 5] or [3, p. 495]. In the same paper [3, Sec. 4] it has been shown how to derive such a matrix from a given generator matrix in a constructive way. For a row vector $v \in \mathbb{F}[\boldsymbol{z}]^n$ we will denote by $\deg v$ the maximum degree of its components. The zero vector has degree $-\infty$.

Definition 1.2 Let $G \in \mathbb{F}[\boldsymbol{z}]^{k \times n}$ be a matrix with rank k and overall constraint length δ and let $\nu_1, \ldots, \nu_k$ be the degrees of the rows of G. We say that G is *minimal* if $\delta = \sum_{i=1}^{k} \nu_i$. In this case the row degrees of G are uniquely determined by the submodule $\mathcal{S} := \operatorname{im} G$. They are called the *Forney indices* of $\mathcal{S}$. The largest Forney index is called the *memory* of $\mathcal{S}$.

The notion "minimal" stems from the (simple) fact that for an arbitrary generator matrix G one has $\delta \leq \sum_{i=1}^{k} \nu_i$. Thus, in a minimal generator matrix the rows degrees have been reduced to their minimal values. Using such a generator matrix it is easily seen that a code with overall constraint length zero can be regarded as a block code.

An important quality characteristic of a code is its so-called distance. It measures the error-correcting capability. For a polynomial vector $v = \sum_{j=0}^{N} v_j \boldsymbol{z}^j \in \mathbb{F}[\boldsymbol{z}]^n$, where $v_j \in \mathbb{F}^n$, the *weight* is defined as $\operatorname{wt}(v) = \sum_{j=0}^{N} \operatorname{wt}(v_j)$ where the weight of $v_j \in \mathbb{F}^n$ denotes the usual Hamming weight. Then the *(free) distance* of a code $\mathcal{C} \subseteq \mathbb{F}[\boldsymbol{z}]^n$ is, just like for block codes, defined as $\operatorname{dist}(\mathcal{C}) := \min\{\operatorname{wt}(v) \mid v \in \mathcal{C},\ v \neq 0\}$.

2 Preliminaries for cyclic convolutional codes

As usual a cyclic block code of length n and dimension k over the field $\mathbb{F}$ will be described as a principal ideal in the algebra $A := \mathbb{F}[x]/\langle x^n - 1 \rangle$. We always assume that $\operatorname{char}(\mathbb{F})$ does not divide n. We have the natural vector space isomorphism

$$\mathfrak{p} : \mathbb{F}^n \to A, \ (v_0, \ldots, v_{n-1}) \mapsto \sum_{i=0}^{n-1} v_i x^i.$$

The weight function on A is defined such that $\mathfrak{p}$ is an isometry between A and $\mathbb{F}^n$ endowed with the usual Hamming metric, i. e., $\operatorname{wt}(a) := \operatorname{wt}\big(\mathfrak{p}^{-1}(a)\big)$ for all $a \in A$. Let

$$x^n - 1 = \prod_{i=0}^{r-1} \pi_i \tag{2.1}$$

be the prime factorization over $\mathbb{F}[x]$. Since we assume char$(\mathbb{F})$ and n to be coprime, the normed prime polynomials π_i are all different. According to this factorization the algebra A decomposes into a direct sum of minimal cyclic block codes, which can be generated by the (primitive) idempotents $\varepsilon^{(i)}, 0 \leq i \leq r-1$. We have

$$\varepsilon^{(i)} \bmod \pi_j = \delta_{ij} \text{ for all } i,j = 0,\ldots,r-1, \tag{2.2}$$

and their existence is guaranteed by the Chinese Remainder Theorem. The idempotents are uniquely determined by A and (2.2) implies

$$\varepsilon^{(i)} = \beta_i \prod_{j \neq i} \pi_j \text{ for some units } \beta_i \in A, \ i = 0,\ldots,r-1. \tag{2.3}$$

The cyclic code $\langle \varepsilon^{(i)} \rangle$ is minimal and also isomorphic to $\mathbb{F}[x]/\langle \pi_i \rangle$ and in addition one has

$$\dim_{\mathbb{F}} \langle \varepsilon^{(i)} \rangle = \deg \pi_i. \tag{2.4}$$

Moreover, any cyclic block code of length n over $\mathbb{F}$ is generated by a sum of idempotents, which is unique up to ordering of the summands.

In the convolutional setting, the vector space $\mathbb{F}^n$ has to be replaced by $\mathbb{F}[\boldsymbol{z}]^n := \{\sum_{j=0}^N \boldsymbol{z}^j v_j \mid N \in \mathbb{N}_0, \ v_j \in \mathbb{F}^n\}$ and, consequently, the ring A by the polynomial ring

$$A[\boldsymbol{z}] := \Big\{ \sum_{j=0}^N \boldsymbol{z}^j a_j \,\Big|\, N \in \mathbb{N}_0, \ a_j \in A \Big\}$$

over A. The natural extension of the map $\mathfrak{p}$ is given by

$$\mathfrak{p}\Big(\sum_{j=0}^N \boldsymbol{z}^j v_j \Big) = \sum_{j=0}^N \boldsymbol{z}^j \mathfrak{p}(v_j) \tag{2.5}$$

where, of course, $v_j \in \mathbb{F}^n$ and thus $\mathfrak{p}(v_j) \in A$ for all j. This map is an isomorphism of $\mathbb{F}[\boldsymbol{z}]$-modules, and we put

$$\mathfrak{v} := \mathfrak{p}^{-1}. \tag{2.6}$$

Note that $\mathfrak{p}$ and $\mathfrak{v}$ are isometries if we define $\text{wt}(g) := \text{wt}(\mathfrak{v}(g))$ for all $g \in A[\boldsymbol{z}]$.

It is now tempting to define a cyclic convolutional code (CCC) to be an ideal in $A[\boldsymbol{z}]$ or, more precisely, to declare a code $\mathcal{C} \subseteq \mathbb{F}[\boldsymbol{z}]^n$ as cyclic if $\mathfrak{p}(\mathcal{C})$ is an ideal in $A[\boldsymbol{z}]$. It has been shown in [15, Thm. 3.12] and [17, Thm. 6] that this does not result in any codes other than block codes, see also [8, Prop. 2.7]. Led by this negative result, a more general notion of cyclicity has been introduced for convolutional codes [15, 17, 8]. It makes use of an automorphism of the $\mathbb{F}$-algebra A. Thus, let $\text{Aut}_{\mathbb{F}}(A)$ be the group of all $\mathbb{F}$-automorphisms on A. Detailed information on this group can be found in [8, Sec. 3]. In particular, it is shown that in general there are quite a lot of automorphisms and how to determine them. For later use we wish to mention that, since the $\mathbb{F}$-algebra A is generated by x, each automorphism $\sigma \in \text{Aut}_{\mathbb{F}}(A)$ is uniquely determined by the value of $\sigma(x)$. It is obvious that the assignment $\sigma(x) = b$ determines an automorphism σ if and only if $b^n = 1$ and b generates the $\mathbb{F}$-algebra A. A particular class of automorphisms is given by defining $\sigma(x) = a^k x$ where $a \in \mathbb{F}\backslash\{0\}$ is such that $\text{ord}(a) \mid n$ and $k \in \{0,\ldots,n-1\}$. Notice that these automorphisms are even weight preserving. In Section 4, where we will compute the distance of certain

3

codes, we will specialize to such automorphisms. The rest of this section as well as Section 3, however, will be based on arbitrary automorphisms.

Picking an automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$, a new multiplication in the $\mathbb{F}[\boldsymbol{z}]$-module $A[\boldsymbol{z}]$ is defined via

$$a\boldsymbol{z} = \boldsymbol{z}\sigma(a) \text{ for all } a \in A \tag{2.7}$$

along with associativity and distributivity. This turns $A[\boldsymbol{z}]$ into a non-commutative $\mathbb{F}[\boldsymbol{z}]$-algebra which will be denoted by $A[\boldsymbol{z}; \sigma]$. We call $A[\boldsymbol{z}; \sigma]$ the *Piret algebra* (over A and with respect to the automorphism σ). Note that it coincides with the commutative ring $A[\boldsymbol{z}]$ if σ is the identity. In all other cases it is a non-commutative ring. In particular, it is important to distinguish between left and right coefficients of $\boldsymbol{z}$. The coefficients can be moved to either side by applying the rule (2.7) since σ is invertible. Multiplication inside A remains the same as before. Hence A is a commutative subring of $A[\boldsymbol{z}; \sigma]$. Due to this very specific non-commutativity the ring $A[\boldsymbol{z}; \sigma]$ is also called a *skew-polynomial ring*. Since $\sigma|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$, the ordinary commutative polynomial ring $\mathbb{F}[\boldsymbol{z}]$ is a subring of $A[\boldsymbol{z}; \sigma]$, too. As a consequence, $A[\boldsymbol{z}; \sigma]$ inherits the (left and right) $\mathbb{F}[\boldsymbol{z}]$-module structure from $A[\boldsymbol{z}]$. For us, only the left module structure will be important. In particular, the map $\mathfrak{p}$ from (2.5) is an isomorphism between the left $\mathbb{F}[\boldsymbol{z}]$-modules $\mathbb{F}[\boldsymbol{z}]^n$ and $A[\boldsymbol{z}; \sigma]$ (notice that in $\mathfrak{p}$ the coefficients are on the right of $\boldsymbol{z}$).

Now we declare a submodule $\mathcal{C} \subseteq \mathbb{F}[\boldsymbol{z}]^n$ to be σ-*cyclic* if $\mathfrak{p}(\mathcal{C})$ is a left ideal in $A[\boldsymbol{z}; \sigma]$. Cyclic CC's have been investigated in detail in the papers [15, 17, 8, 7] and it turned out that there are many good CCC's that are not block codes. See [8] for more details. In the same paper an algebraic theory of CCC's has been developed where in the context of Piret algebras notions like non-catastrophicity, dimension of a code, and overall constraint length could be handled successfully. In the next section multiple use of these results will be made.

3   Construction of doubly-cyclic codes

In this section we will give a construction of CCC's with parameters (n, k, km) where m is the memory. It is based on cyclic block codes as discussed in the previous section. The distances of a subclass of these codes will be computed in Section 4.

Consider an automorphism $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$. It is easy to see that σ induces a permutation on the set

$$E = \{\varepsilon^{(0)}, \dots, \varepsilon^{(r-1)}\}$$

of primitive idempotents. Remember that according to (2.2) the ith idempotent corresponds to the ith prime factor of $x^n - 1$. Indeed, one can easily show that $\sigma(\varepsilon^{(i)}) = \varepsilon^{(j)}$ implies $\deg \pi_i = \deg \pi_j$ [8, Sec. 3]. As a consequence, the automorphism σ induces the trivial permutation on E if the degrees of the prime factors of $x^n - 1$ are all pairwise different. From [8, Prop. 3.4] it is known that in this case each σ-cyclic CC is a block code.

Therefore, we will assume from now on that the degrees of the prime factors of $x^n - 1$ are not all pairwise different and that σ does not induce the identity permutation on E (the existence of such σ is then guaranteed by [8, Thm. 3.1]). In this case there exists a subset $S \subset E$ such that $S \cap \sigma(S) = \varnothing$. Furthermore, we define $b \in \mathbb{N}$ such that

$$S \cap \sigma^j(S) = \varnothing \text{ for all } 1 \le j \le b. \tag{3.1}$$

4

Note that this implies $\sigma^i(S) \cap \sigma^j(S) = \varnothing$ for all $0 \le i < j$ such that $j - i \le b$. Let $s := |S|$. Then $(b+1)s \le r$ and $(b+1)s = r \Longleftrightarrow E = \bigcup_{i=0}^{b} \sigma^i(S)$.

Consider now the cyclic block code generated by

$$c := \sum_{\varepsilon^{(i)} \in S} \varepsilon^{(i)}. \tag{3.2}$$

It is the direct sum of the minimal block codes $\langle \varepsilon^{(i)} \rangle$ and based on (2.3) and (2.4) one obtains

$$k := \dim_{\mathbb{F}} \langle c \rangle = \sum_{\varepsilon^{(i)} \in S} \deg \pi_i. \tag{3.3}$$

A basis is, for instance, given by the elements $c, xc, \ldots, x^{k-1}c$. Equation (3.1) can now also be expressed via the orthogonality

$$\sigma^i(c)\sigma^j(c) = 0 \text{ for all } 0 \le i < j \text{ such that } j - i \le b. \tag{3.4}$$

Example 3.1 (a) Let $\mathbb{F} = \mathbb{F}_4$, $n = 15$, and α be a primitive element for $\mathbb{F}$. We compute

$$x^{15} - 1 = (x+1)(x+\alpha^2)(x+\alpha)(x^2+\alpha^2 x + 1)(x^2+\alpha x + \alpha)(x^2+x+\alpha^2)$$
$$(x^2+\alpha^2 x + \alpha^2)(x^2+\alpha x + 1)(x^2+x+\alpha)$$

and order the idempotents $\varepsilon^{(0)}, \ldots, \varepsilon^{(8)}$ according to the ordering of the factors. For the automorphism we consider σ defined by $\sigma(x) = \alpha x$. Then one can show that the permutation $\sigma|_E : E \longrightarrow E$ has the cycles

$$\left(\varepsilon^{(0)}, \varepsilon^{(1)}, \varepsilon^{(2)}\right)\left(\varepsilon^{(3)}, \varepsilon^{(4)}, \varepsilon^{(5)}\right)\left(\varepsilon^{(6)}, \varepsilon^{(7)}, \varepsilon^{(8)}\right).$$

Let now, for instance, $S = \{\varepsilon^{(0)}, \varepsilon^{(3)}, \varepsilon^{(6)}\}$ then $S \cup \sigma(S) \cup \sigma^2(S)$ is a disjoint union and is equal to $E = \{\varepsilon^{(0)}, \ldots, \varepsilon^{(8)}\}$, the full set of idempotents.

(b) Let $\mathbb{F} = \mathbb{F}_2$ and $n = 31$. One computes

$$x^n - 1 = (x+1)(x^5+x^4+x^3+x^2+1)(x^5+x^2+1)(x^5+x^4+x^3+x+1)$$
$$(x^5+x^3+x^2+x+1)(x^5+x^3+1)(x^5+x^4+x^2+x+1)\ .$$

Let the idempotents $\varepsilon^{(0)}, \ldots, \varepsilon^{(6)}$ be numbered accordingly. In this situation the assignment $\sigma(x) := x^3$ leads to an automorphism with $\sigma(\varepsilon^{(0)}) = \varepsilon^{(0)}$ and $\sigma(\varepsilon^{(k)}) = \varepsilon^{(k+1)}$ for $1 \le k \le 5$. Now, for instance, defining $S = \{\varepsilon^{(1)}, \varepsilon^{(4)}\}$ one has $|S| = 2$ and

$$\{\varepsilon^{(1)}, \ldots, \varepsilon^{(6)}\} = S \cup \sigma(S) \cup \sigma^2(S)$$

as a disjoint union. This example is typical in some sense, since $x - 1$ is always one of the prime factors of $x^n - 1$. Thus, if $x^n - 1$ has no further linear factors, then S can only contain idempotents different from $\varepsilon^{(0)}$.

The following example introduces CCC's of Reed-Solomon type which will be further investigated in later sections.

Example 3.2 Let $\mathbb{F} = \mathbb{F}_q$ be a field of size q and let $n := q - 1$. Furthermore let $\alpha \in \mathbb{F}$ be a primitive element, thus $\mathrm{ord}(\alpha) = n$. Then the prime factor decomposition of $x^n - 1$ is given by $x^n - 1 = \prod_{i=0}^{n-1} \pi_i$, where $\pi_i = x - \alpha^i$. We pick $k \in \mathbb{N}$ such that $1 \leq k \leq \frac{n}{2}$ and choose $\sigma \in \mathrm{Aut}_{\mathbb{F}}(A)$ such that

$$\sigma(x) = \alpha^k x .$$

Since $\mathrm{ord}(\alpha^k) \mid n$ this does indeed define an automorphism on A. Since $\varepsilon^{(j)} = \beta_j \prod_{i \neq j}(x - \alpha^i)$ for $0 \leq j \leq n - 1$ and some $\beta_j \in \mathbb{F}^*$, the automorphism σ acts on the idempotents as follows:

$$\sigma(\varepsilon^{(j)}) = \varepsilon^{(j-k \bmod n)}, \text{ for } j = 0, \ldots, n-1.$$

Define

$$S := \{\varepsilon^{(n-k)}, \ldots, \varepsilon^{(n-1)}\} \text{ and } b := \lfloor \tfrac{n}{k} \rfloor - 1.$$

Then Equation (3.1) is satisfied and due to the restriction $k \leq \frac{n}{2}$ we have $b \geq 1$. Let now c be as in (3.2). Then $\langle c \rangle$ is a k-dimensional cyclic block code with generator polynomial

$$f := \prod_{l=0}^{n-k-1} (x - \alpha^l) \in \mathbb{F}[x],$$

and k is as in (3.3). This shows that $\langle c \rangle$ is a Reed-Solomon code of length n. It is well-known, see e. g. [12, Thm. 6.6.2], that

$$\mathrm{dist}\langle c \rangle = n - k + 1.$$

We return now to the general situation and introduce what will be called a *doubly-cyclic convolutional code*. Using the ingredients from (3.1) – (3.3) along with the automorphism σ and the isomorphism from (2.6) we define the matrix

$$G := \sum_{\nu=0}^{m} \boldsymbol{z}^\nu G_\nu \in \mathbb{F}[\boldsymbol{z}]^{k \times n} \text{ where } G_\nu := \begin{pmatrix} \mathfrak{v}(\sigma^\nu(c)) \\ \mathfrak{v}(\sigma^\nu(xc)) \\ \vdots \\ \mathfrak{v}(\sigma^\nu(x^{k-1}c)) \end{pmatrix} \in \mathbb{F}^{k \times n}, \qquad (3.5)$$

and where

$$1 \leq m \leq b. \qquad (3.6)$$

The matrix G above might look artificial. However, it becomes quite natural once considered over the Piret algebra $A[\boldsymbol{z}; \sigma]$. Recall that $\mathbb{F}[\boldsymbol{z}]^n \cong A[\boldsymbol{z}; \sigma]$ as left $\mathbb{F}[\boldsymbol{z}]$-modules via the isomorphisms $\mathfrak{p}$ and $\mathfrak{v}$ in (2.5) and (2.6), and also recall the skew multiplication defined via (2.7). Define

$$g := c \sum_{\nu=0}^{m} \boldsymbol{z}^\nu = \sum_{\nu=0}^{m} \boldsymbol{z}^\nu \sigma^\nu(c) \in A[\boldsymbol{z}; \sigma]. \qquad (3.7)$$

Then we obtain $x^i g = \sum_{\nu=0}^{m} \boldsymbol{z}^\nu \sigma^\nu(x^i c)$ for all $i \in \mathbb{N}_0$ and, due to left $\mathbb{F}[\boldsymbol{z}]$-linearity of $\mathfrak{v}$,

$$G = \begin{pmatrix} \mathfrak{v}(g) \\ \mathfrak{v}(xg) \\ \vdots \\ \mathfrak{v}(x^{k-1}g) \end{pmatrix}.$$

In Theorem 3.3 we will show that $\operatorname{im} G = \mathfrak{v}(^{\bullet}\langle g \rangle)$ where $^{\bullet}\langle g \rangle := \{fg \mid f \in A[\boldsymbol{z}; \sigma]\}$ is the left ideal generated by g. Moreover, we will see that G is right invertible and thus defines a CCC. Dimension and overall constraint length of this code are also derived. For a subclass of doubly-cyclic CC's we will compute distances and extended row distances in the next section.

Theorem 3.3 *Let the data be as in* (3.1) – (3.7). *Then*

(a) $g = c(1 + \boldsymbol{z}\sigma(c))(1 + \boldsymbol{z}\sigma^2(c)) \cdot \ldots \cdot (1 + \boldsymbol{z}\sigma^m(c))$.

(b) *We have* $gu = c$ *where* $u = (1 - \boldsymbol{z}\sigma^m(c))(1 - \boldsymbol{z}\sigma^{m-1}(c)) \cdot \ldots \cdot (1 - \boldsymbol{z}\sigma(c))$. *Furthermore,* u *is a unit in* $A[\boldsymbol{z}; \sigma]$ *and* $u = 1 - \boldsymbol{z}(\sigma(c) + \ldots + \sigma^m(c))$.

(c) *Define* $\mathcal{C} := \operatorname{im} G$. *Then* $\mathcal{C} = \mathfrak{v}(^{\bullet}\langle g \rangle)$. *Thus,* $\mathcal{C}$ *is a cyclic submodule of* $\mathbb{F}[\boldsymbol{z}]^n$. *Moreover,* $\operatorname{rank} \mathcal{C} = k$.

(d) $\mathcal{C}$ *is a cyclic convolutional code, hence in particular a direct summand of* $\mathbb{F}[\boldsymbol{z}]^n$. *Equivalently, the matrix* G *is right invertible.*

(e) *The matrix* G *is minimal in the sense of Definition 1.2.*

(f) $\mathcal{C}$ *is a code with parameters* (n, k, km) *and memory* m. *In particular, all Forney indices of the code* $\mathcal{C}$ *are equal to* m.

The convolutional code $\mathcal{C}$ *will be called a doubly-cyclic code.*

The qualifier "doubly-cyclic" refers to the fact that these codes are cyclic CC's where the coefficient block codes are all obtained as iterated images of a single cyclic block code under a fixed automorphism. In particular, doubly cyclic CC's are completely determined by a single cyclic block code along with the degree m and the automorphism. In Proposition 3.4 we will encounter another cyclic-type property, induced by the coefficient matrices G_ν of the encoder matrix G.

PROOF: (a) We proceed by induction. For $m = 1$ we have, since $\sigma(c)$ is idempotent,
$$g = c + \boldsymbol{z}\sigma(c) = c + \boldsymbol{z}(\sigma(c))^2 = c + c\boldsymbol{z}\sigma(c) = c(1 + \boldsymbol{z}\sigma(c)).$$

Let now $\sum_{\nu=0}^{m-1} \boldsymbol{z}^\nu \sigma^\nu(c) = c(1 + \boldsymbol{z}\sigma(c))(1 + \boldsymbol{z}\sigma^2(c)) \cdot \ldots \cdot (1 + \boldsymbol{z}\sigma^{m-1}(c))$. Then

$$\sum_{\nu=0}^{m-1} \boldsymbol{z}^\nu \sigma^\nu(c)(1 + \boldsymbol{z}\sigma^m(c)) = \sum_{\nu=0}^{m-1} \boldsymbol{z}^\nu \sigma^\nu(c) + \sum_{\nu=0}^{m-1} \boldsymbol{z}^\nu \sigma^\nu(c)\boldsymbol{z}\sigma^m(c) = \sum_{\nu=0}^{m} \boldsymbol{z}^\nu \sigma^\nu(c).$$

The last identity follows from the fact that

$$\boldsymbol{z}^\nu \sigma^\nu(c)\boldsymbol{z}\sigma^m(c) = \boldsymbol{z}^{\nu+1}\sigma^{\nu+1}(c)\sigma^m(c) = \begin{cases} 0, & \text{if } \nu < m - 1 \\ \boldsymbol{z}^m \sigma^m(c), & \text{if } \nu = m - 1 \end{cases}$$

due to $m \le b$ and (3.4).

(b) The equation $gu = c$ as well as the fact that u is a unit follow from (a) along with
$$(1 - \boldsymbol{z}\sigma^\nu(c))(1 + \boldsymbol{z}\sigma^\nu(c)) = (1 + \boldsymbol{z}\sigma^\nu(c))(1 - \boldsymbol{z}\sigma^\nu(c)) = 1,$$

which in turn is a consequence of $\sigma^{\nu+1}(c)\sigma^\nu(c) = 0$, see (3.4). The last part of (b) can easily be shown as in (a).

For the assertions (c) – (f) we first have to show that the polynomial g is reduced in the sense of [8, Def. 4.9(b)]. We have

$$\varepsilon^{(i)} g = \begin{cases} 0 & \text{if } \varepsilon^{(i)} \notin S \\ \sum_{\nu=0}^{m} \boldsymbol{z}^\nu \sigma^\nu(\varepsilon^{(i)}) & \text{if } \varepsilon^{(i)} \in S. \end{cases}$$

7

This shows that the polynomials $\varepsilon^{(i)}g$, $\varepsilon^{(i)} \in S$, all have degree m and their highest coefficients do not divide each other in A proving the reducedness of g in the above mentioned sense. Now, application of [8, Thm. 7.8] yields (c) while (d) follows from [8, Prop. 7.10] along with part (b) above.

(e) To see minimality of G, observe that the leading coefficient matrix is given by

$$
\begin{pmatrix}
\mathfrak{v}\big(\sigma^m(c)\big) \\
\mathfrak{v}\big(\sigma^m(xc)\big) \\
\vdots \\
\mathfrak{v}\big(\sigma^m(x^{k-1}c)\big)
\end{pmatrix}.
$$

This matrix has full row rank since, by choice of c, the polynomials $c, xc, \ldots, x^{k-1}c$ are linearly independent in the $\mathbb{F}$-vector space A. Hence G is a minimal matrix due to [3, p. 495].

(f) is a consequence of the previous results. $\qquad\square$

Notice that by construction doubly-cyclic codes are always proper convolutional codes, i. e., codes with nonzero memory. They are determined by the cyclic block code $\langle c \rangle$ and the cyclic behavior of the automorphism σ.

Note that part (a) and the first statement of (b) in Theorem 3.3 still remain true for $m = b + 1$. For the statements in (c) to (f) no restriction for m is necessary. Later on, however, (3.6) will be an essential assumption in order to obtain precise information on the distance of doubly-cyclic codes. We will also need the following information on various block codes appearing in our construction.

Proposition 3.4 Let G and G_ν be as in (3.5) and (3.6). For $0 \le \mu \le \nu \le m$ define the matrix

$$
G_{\mu,\nu} := \begin{pmatrix}
G_\mu \\
G_{\mu+1} \\
\vdots \\
G_\nu
\end{pmatrix} \in \mathbb{F}^{(\nu-\mu+1)k \times n}.
$$

and put $\mathcal{C}_{\mu,\nu} := \operatorname{im} G_{\mu,\nu}$. Then $\mathcal{C}_{\mu,\nu}$ is a cyclic block code given by

$$
\mathcal{C}_{\mu,\nu} = \mathfrak{v}\Big(\langle \sigma^\mu(c) \rangle + \ldots + \langle \sigma^\nu(c) \rangle\Big) = \mathfrak{v}\Big(\langle \sigma^\mu(c) \rangle \oplus \ldots \oplus \langle \sigma^\nu(c) \rangle\Big).
$$

Moreover, $\dim \mathcal{C}_{\mu,\nu} = (\nu - \mu + 1)k$ and $\mathfrak{p}\big(\mathcal{C}_{\mu,\nu}\big)$ has the idempotent generator

$$
\sigma^\mu(c) + \ldots + \sigma^\nu(c) = \sum_{\varepsilon \in \sigma^\mu(S) \cup \ldots \cup \sigma^\nu(S)} \varepsilon .
$$

PROOF: As for the first identity, observe that each code $\langle \sigma^i(c) \rangle$ has dimension k and is generated by the elements $\sigma^i(c), \sigma^i(xc), \ldots, \sigma^i(x^{k-1}c)$. This follows easily from the case $i = 0$ and the fact that σ is an automorphism. Therefore,

$$
\begin{aligned}
\mathfrak{p}\big(\mathcal{C}_{\mu,\nu}\big) &= \operatorname{span}_{\mathbb{F}}\{\sigma^\mu(c), \sigma^\mu(xc), \ldots, \sigma^\mu(x^{k-1}c), \ldots, \sigma^\nu(c), \sigma^\nu(xc), \ldots, \sigma^\nu(x^{k-1}c)\} \\
&= \langle \sigma^\mu(c) \rangle + \ldots + \langle \sigma^\nu(c) \rangle.
\end{aligned}
$$

The second identity follows from (3.4) along with the inequalities $\mu \le \nu \le m \le b$, see also [12, Thm. 6.4.3]. As a consequence we obtain $\dim \mathcal{C}_{\mu,\nu} = (\nu - \mu + 1)k$. The form of the

idempotent generator is a consequence of the fact that each $\sigma^i(c)$ is the idempotent generator of the corresponding code. Hence the direct sum is generated by the sum of these generators, see again [12, Thm. 6.4.3]. $\qquad\square$

In special cases one can even obtain simple formulas for the distances of the codes $\mathcal{C}_{\mu,\nu}$. As we will see next this is, for instance, the case in the situation of Example 3.2.

Lemma 3.5 *Let $\mathbb{F}$ and n, the automorphism σ, and the set S be as in Example 3.2. Define the matrix G as in (3.5), (3.6) and let the code $\mathcal{C}_{\mu,\nu}$ be as in Proposition 3.4. Then*

$$\mathrm{dist}(\mathcal{C}_{\mu,\nu}) = n - (\nu - \mu + 1)k + 1.$$

for all $0 \leq \mu \leq \nu \leq m$. Hence all these codes are MDS block codes.

PROOF: First notice that σ is an isometry, i.e., $\mathrm{wt}(a) = \mathrm{wt}(\sigma(a))$ for all $a \in A$. Thus it suffices to show the result for $\mu = 0$, see also Proposition 3.4. In the case under consideration we have $\sigma^i(S) = \{\varepsilon^{(n-(i+1)k)}, \varepsilon^{(n-(i+1)k+1)}, \ldots, \varepsilon^{(n-ik-1)}\}$. Thus

$$S \cup \sigma(S) \cup \ldots \cup \sigma^\nu(S) = \{\varepsilon^{(i)} \mid i = n - (\nu+1)k, \ldots, n-1\}.$$

Thus, Proposition 3.4 shows that

$$\mathcal{C}_{0,\nu} = \mathfrak{v}\left(\left\langle \sum_{i=n-(\nu+1)k}^{n-1} \varepsilon^{(i)} \right\rangle\right) = \mathfrak{v}\left(\left\langle \prod_{i=0}^{n-(\nu+1)k-1} \pi_i \right\rangle\right).$$

Since $\pi_i = x - \alpha^i$, the generator polynomial has exactly $n - (\nu+1)k$ consecutive powers of α as zeros, proving that $\mathrm{dist}(\mathcal{C}_{0,\nu}) \geq n - (\nu+1)k + 1$. Using $\dim(\mathcal{C}_{0,\nu}) = (\nu+1)k$ from Proposition 3.4 together with the Singleton bound completes the proof. $\qquad\square$

4 Distance parameters for Reed-Solomon convolutional codes

In this section we will consider only the situation of Example 3.2. We will compute the distances of the codes of this type and also derive lower bounds for the extended row distances.

We begin with presenting the following upper bound on the distance of convolutional codes with given algebraic parameters. It will later provide us with some insight into the quality of the codes constructed in the foregoing sections. For one-dimensional codes we will see that our codes attain the generalized Singleton bound [18, Thm. 2.2]

$$\mathrm{dist}(\mathcal{C}) \leq n(m+1) \text{ for any code } \mathcal{C} \text{ with parameters } (n, 1, m). \tag{4.1}$$

For codes of bigger dimension we will compare the distance with the upper bound given next.

Proposition 4.1 *Let $\mathbb{F} = \mathbb{F}_q$ and $n = q - 1$. Let $\mathcal{C} \subseteq \mathbb{F}[\mathbf{z}]^n$ be a code with parameters (n, k, km) and memory m. Suppose $k > 1$ and $m \leq \frac{n}{k} - 1$. Then the distance satisfies $\mathrm{dist}(\mathcal{C}) \leq (m+1)(n-k+1) + (k-2)m$.*

PROOF: This follows easily by using the Griesmer bound, see [7, Thm. 3.4]. Indeed, the case $i = 1$ in the Griesmer bound shows that the distance d of $\mathcal{C}$ satisfies $\sum_{l=0}^{k-1} \lceil \frac{d}{(n+1)^l} \rceil \leq n(m+1)$.

9

Suppose now that $d \geq (m+1)(n-k+1) + (k-2)m + 1 = (m+1)(n+1) - k - 2m + 1$. Then the above implies

$$(m+1)(n+1) - k - 2m + 1 + \frac{(m+1)(n+1) - k - 2m + 1}{n+1}$$
$$+ \sum_{l=2}^{k-1} \left\lceil \frac{(m+1)(n-k+1) - k - 2m + 1}{(n+1)^l} \right\rceil \leq n(m+1),$$

and, using that the upper floors in the sum are all at least 1, we obtain $\frac{(m+1)(n+1) - k - 2m + 1}{n+1} \leq m$. Hence $\frac{k+2m-1}{n+1} \geq 1$. But this implies $m > \frac{n-k}{2}$, contradicting $m \leq \frac{n-k}{k}$ since $k \geq 2$. $\quad\square$

We will see below that in the 2-dimensional case our codes attain this bound, hence are optimal. It is not clear to us whether the bound can actually be realized by a suitable code for arbitrary dimension $k \geq 2$ and memory $m \leq \frac{n}{k} - 1$.

Let us repeat the situation of Example 3.2. Thus

$$n := q - 1, \ 1 \leq k \leq \frac{n}{2}, \ \text{and } \alpha \in \mathbb{F} := \mathbb{F}_q \text{ such that ord}(\alpha) = n. \qquad (4.2)$$

Then the prime factor decomposition of $x^n - 1$ is given by $x^n - 1 = \prod_{i=0}^{n-1} \pi_i$, where $\pi_i = x - \alpha^i$. Choose $\sigma \in \text{Aut}_{\mathbb{F}}(A)$ such that

$$\sigma(x) = \alpha^k x. \qquad (4.3)$$

This assignment does indeed define an automorphism on A. It has been shown in Example 3.2 that $S := \{\varepsilon^{(n-k)}, \ldots, \varepsilon^{(n-1)}\}$ and $b := \lfloor \frac{n}{k} \rfloor - 1$ satisfy (3.1). Thus let

$$c := \varepsilon^{(n-k)} + \ldots + \varepsilon^{(n-1)}. \qquad (4.4)$$

As shown in Example 3.2, $\langle c \rangle$ is a Reed-Solomon block code. Therefore, we call the code $\mathcal{C} = \text{im } G$ where G is in (3.5) and (3.6) in this situation a *Reed-Solomon convolutional code.*

Below we will not only compute the distance of the associated codes but also the extended row distances. They have been introduced in [20, p. 639] and [11, p. 541] and are most closely related to the performance of the code.[1] The jth extended row distance amounts to the minimum weight of all paths through the state diagram starting at the zero state and which reach the zero state after exactly j steps for the first time. In other words, it is the minimum weight of all atomic codewords of degree $j - 1$ (i. e., length j) in the sense of [14]. The details are also explained in [10, Sec. 3.10] and [4, Sec. 3]. In our case where all row degrees of the matrix G are equal to m (see Theorem 3.3(f)), the atomic codewords are easily described. We will confine ourselves to the following property. It follows easily from the fact that the last m coefficient vectors of the message $u \in \mathbb{F}[\mathbf{z}]^k$ make up the current state in the state diagram.

Remark 4.2 Let $G \in \mathbb{F}[\mathbf{z}]^{k \times n}$ be a minimal right-invertible generator matrix with all row degrees equal to m and let $u \in \mathbb{F}[\mathbf{z}]^k$. Then the following are equivalent.
(i) The codeword uG is atomic (i. e., the associated path through the state diagram does not pass through the zero state except for its starting and end point).
(ii) The polynomial $u \in \mathbb{F}[\mathbf{z}]^k$ does not have m consecutive zero coefficients in $\mathbb{F}^k$.

---
[1]The row distances, as defined in [10, p. 114] do not give any further information. They are all equal to the distance $n(\delta + 1)$.

Having this in mind, the jth extended row distance of the code $\mathcal{C} = \mathrm{im}\, G$ is given by

$$\hat{d}_j^r := \min\left\{\mathrm{wt}(uG) \;\middle|\; \begin{array}{l} u \in \mathbb{F}[\boldsymbol{z}]^k,\ u_0 \neq 0,\ \deg u = j - m - 1,\ \text{and} \\ \text{no } m \text{ consecutive coefficients of } u \text{ are zero} \end{array}\right\} \text{ for all } j \geq m + 1.$$

Notice that $\deg(u) = j - m - 1$ implies $\deg(uG) = j - 1$ and thus the associated path has length j. The shortest length occurring is, of course, $m + 1$. It should also be observed that in our case the extended row distances do not depend on the choice of the minimal generator matrix G. This follows easily from the fact that, since all Forney indices are equal to m, two minimal generator matrices are related via left multiplication by some constant regular matrix.[2] Finally, one easily shows that $\mathrm{dist}(\mathcal{C}) = \min_{j \geq m+1} \hat{d}_j^r$.

Now we can formulate the result about the distance and the extended row distances of the cyclic code under consideration.

Theorem 4.3 *Let the data be as in (4.2) – (4.4). Let $\mathcal{C} = \mathrm{im}\, G \subseteq \mathbb{F}[\boldsymbol{z}]^n$ be the code with generator matrix G defined in (3.5) and (3.6) where $b = \left\lfloor \frac{n}{k} \right\rfloor - 1$. Then*
(1) $\mathrm{dist}(\mathcal{C}) = (m+1)(n-k+1)$.
(2) $\hat{d}_j^r \geq (m+1)(n-k+1) + (j-1-m)(n-k(m+1)+1)$ for all $j \geq m+1$.
In other words, the extended row distances are bounded from below by a linear function with slope $n - k(m+1) + 1$.

Notice that in the case $m = 0$ the first part reduces to the classical result for k-dimensional Reed-Solomon block codes. Moreover, we see that for $k = 1$ the codes thus constructed attain the generalized Singleton bound (4.1), thus are MDS codes in the sense of [18, Def. 2.5] and that for $k = 2$ the codes are optimal among all codes over the same field and with the same parameters, according to Proposition 4.1. For bigger k the distance stays linearly below the upper bound given in Proposition 4.1. Part (2) shows in particular that all codewords of weight $(m+1)(n-k+1)$ are associated with constant messages, i. e., messages of length 1. It is worth mentioning that the slope $n - k(m+1) + 1$ for the extended row distances is optimal. Indeed, as we will see below in (4.6) for large degree the "middle coefficients" of a codeword are contained in the block code generated by $G_{0,m}$. In our case this matrix has full row rank (thus no cancellation $uG_{0,m} = 0$ can arise) and the code is MDS, hence has the best distance possible. Thus the weight of the codewords must increase by the amount $n - k(m+1) + 1$ in each step of the degree. However, it is theoretically possible that certain constellations of the entries of G even allow a bigger growth rate.

PROOF: We will first prove that the distance cannot be bigger than $(m+1)(n-k+1)$. For this remember from Example 3.2 that $f = \prod_{l=0}^{n-k-1}(x - \alpha^l)$ is in the code generated by c. Thus $f = ac$ for some $a \in A$. Define $\hat{g} := f \sum_{\nu=0}^m \boldsymbol{z}^\nu = \sum_{\nu=0}^m \boldsymbol{z}^\nu \sigma^\nu(f) \in A[\boldsymbol{z}; \sigma]$. Then $\hat{g} = ag$, hence $\hat{g} \in {}^\bullet\langle g \rangle$. Using Theorem 3.3(c) we derive $\mathfrak{v}(\hat{g}) \in \mathcal{C}$. Now observe that f has weight exactly $n - k + 1$ and the same is true for $\sigma^\nu(f)$ since σ is weight preserving. Thus we derive at $\mathrm{wt}(\mathfrak{v}(\hat{g})) = (m+1)(n-k+1)$ showing that the distance is at most this number.

As for the rest of the theorem it suffices to prove part (2). Indeed, the assumption $m \leq \frac{n-k}{k}$ guarantees that $n + 1 - k(m+1) > 0$ and thus the lower bound in (2) is always at least $(m+1)(n-k+1)$. As for proving (2), we will make use of the matrices $G_{\mu,\nu}$ from Proposition 3.4. Remember from Lemma 3.5 that $\mathrm{dist}(\mathrm{im}\, G_{\mu,\nu}) = n - (\nu - \mu + 1)k + 1$.

---

[2] If the Forney indices are not all identical, then the extended row distances need to be defined via atomic codewords in order to make them independent of the choice of the minimal generator matrix.

Let $u = \sum_{j=0}^{t} u_j \boldsymbol{z}^j \in \mathbb{F}[\boldsymbol{z}]^k$ be a message with $u_0 \neq 0 \neq u_t$ and no m consecutive zero coefficients. Then the associated codeword $v := uG$ has degree $t + m$ and length $t + m + 1$. In the case $t < m$ the codeword v reads as

$$
\begin{aligned}
v \;=\; & \sum_{\nu=0}^{t} (u_\nu, u_{\nu-1}, \ldots, u_0) G_{0,\nu} \boldsymbol{z}^\nu + \sum_{\nu=t+1}^{m} (u_t, u_{t-1}, \ldots, u_0) G_{\nu-t,\nu} \boldsymbol{z}^\nu \\
& + \sum_{\nu=m+1}^{m+t} (u_t, u_{t-1}, \ldots, u_{\nu-m}) G_{\nu-t,m} \boldsymbol{z}^\nu.
\end{aligned}
\tag{4.5}
$$

From Proposition 3.4 and the fact that $u_0 \neq 0 \neq u_t$ we know that each coefficient of v is nonzero. Using Lemma 3.5 we therefore obtain for the weight of v

$$
\begin{aligned}
\mathrm{wt}(v) &\geq \sum_{\nu=0}^{t} (n+1-k(\nu+1)) + \sum_{\nu=t+1}^{m} (n+1-k(t+1)) + \sum_{\nu=m+1}^{m+t} (n+1-k(m+t-\nu+1)) \\
&= (m+t+1)(n+1) - k \sum_{\nu=0}^{t}(\nu+1) - (m-t)k(t+1) - k \sum_{\nu=1}^{t} \nu \\
&= (m+1)(n+1) + t(n+1-mk-k) - mk - k \\
&= (m+1)(n-k+1) + t(n+1-k(m+1)).
\end{aligned}
$$

If $t \geq m$ one has

$$
\begin{aligned}
v \;=\; & \sum_{\nu=0}^{m-1} (u_\nu, u_{\nu-1}, \ldots, u_0) G_{0,\nu} \boldsymbol{z}^\nu + \sum_{\nu=m}^{t} (u_\nu, u_{\nu-1}, \ldots, u_{\nu-m}) G_{0,m} \boldsymbol{z}^\nu \\
& + \sum_{\nu=t+1}^{t+m} (u_t, u_{t-1}, \ldots, u_{\nu-m}) G_{\nu-t,m} \boldsymbol{z}^\nu.
\end{aligned}
\tag{4.6}
$$

Using that $u_0 \neq 0 \neq u_t$ and that no m consecutive coefficients of u are zero, one obtains like in the previous case

$$
\begin{aligned}
\mathrm{wt}(v) &\geq \sum_{\nu=0}^{m-1} (n+1-k(\nu+1)) + \sum_{\nu=m}^{t} (n+1-k(m+1)) + \sum_{\nu=t+1}^{t+m} (n+1-k(m+t-\nu+1)) \\
&= (m+t+1)(n+1) - k \sum_{\nu=0}^{m-1}(\nu+1) - (t-m+1)k(m+1) - k \sum_{\nu=1}^{m} \nu \\
&= (m+1)(n-k+1) + t(n+1-k(m+1)).
\end{aligned}
$$

This proves the assertions. $\qquad\square$

As the proof shows the lower bound for the extended row distances does not rely on the cyclicity of these codes, but solely on the facts that, firstly, the matrices $G_{\mu,\nu}$ have full row rank (Proposition 3.4) and, secondly, the codes $\mathcal{C}_{\mu,\nu} = \operatorname{im} G_{\mu,\nu}$ are MDS block codes (Lemma 3.5). As a result Theorem 4.3(2) is true for any code $\mathcal{C} = \operatorname{im} G$, where $G = \sum_{\nu=0}^{m} z^\nu G_\nu \in \mathbb{F}[z]^{k \times n}$ satisfies the two properties just mentioned. In particular, the distance of $\mathcal{C}$ is at least $(m+1)(n-k+1)$. It has to remain open for future research whether a different choice of the matrices G_ν can be made such that it results in a code $\mathcal{C}$ with parameters (n, k, km) and even larger distance.

Remark 4.4 The results of Theorem 4.3 are also true if we choose the field size q such that $n|(q-1)$ rather than $n = q - 1$. In this case there exists an element of order n in $\mathbb{F}$ and this is all what is needed for the construction to work. However, that construction does not give us a better distance and thus the constructed codes might be farther away from the corresponding Griesmer bound for codes with parameters (n, k, km) and memory m over $\mathbb{F}_q$.

The following examples illustrate these results.

Example 4.5 We choose $\mathbb{F} = \mathbb{F}_8$ with primitive element α satisfying $\alpha^3 + \alpha + 1 = 0$. Thus $n = 7$.

(a) If we pick $k = 2$, then the automorphism is given by $\sigma(x) = \alpha^2 x$. The set $S := \{\varepsilon^{(5)}, \varepsilon^{(6)}\}$, see (4.4), satisfies $\sigma(S) = \{\varepsilon^{(3)}, \varepsilon^{(4)}\}$, $\sigma^2(S) = \{\varepsilon^{(1)}, \varepsilon^{(2)}\}$, $\sigma^3(S) = \{\varepsilon^{(6)}, \varepsilon^{(0)}\}$. This shows that $b = \lfloor \frac{n}{k} \rfloor - 1 = 2$ is the maximum value satisfying (3.1). We obtain

$$c := \varepsilon^{(5)} + \varepsilon^{(6)} = \alpha x^6 + \alpha^2 x^5 + \alpha^2 x^4 + \alpha^4 x^3 + \alpha x^2 + \alpha^4 x.$$

Choosing $m = 2$ and applying (3.5) we derive

$$G = \begin{pmatrix} 0 & \alpha + \alpha z + \alpha z^2 \\ \alpha^4 + \alpha^6 z + \alpha z^2 & 0 \\ \alpha + \alpha^5 z + \alpha^2 z^2 & \alpha^4 + \alpha z + \alpha^5 z^2 \\ \alpha^4 + \alpha^3 z + \alpha^2 z^2 & \alpha + z + \alpha^6 z^2 \\ \alpha^2 + \alpha^3 z + \alpha^4 z^2 & \alpha^4 + \alpha^5 z + \alpha^6 z^2 \\ \alpha^2 + \alpha^5 z + \alpha z^2 & \alpha^2 + \alpha^5 z + \alpha z^2 \\ \alpha + \alpha^6 z + \alpha^4 z^2 & \alpha^2 + z + \alpha^5 z^2 \end{pmatrix}^{\mathsf{T}} \in \mathbb{F}[z]^{2\times 7}.$$

According to Theorem 4.3 the code $\operatorname{im} G$ has distance 18. Its extended row distances satisfy $\hat{d}_j^r \geq 2j + 12$ for $j \geq 3$.

(b) If we choose $k = 3$, then the automorphism is given by $\sigma(x) = \alpha^3 x$ and we get $S = \{\varepsilon^{(4)}, \varepsilon^{(5)}, \varepsilon^{(6)}\}$, $\sigma(S) = \{\varepsilon^{(1)}, \varepsilon^{(2)}, \varepsilon^{(3)}\}$ and $b = 1$. In this case

$$c = \varepsilon^{(4)} + \varepsilon^{(5)} + \varepsilon^{(6)} = \alpha^2 x^6 + \alpha^4 x^5 + \alpha^3 x^4 + \alpha x^3 + \alpha^5 x^2 + \alpha^6 x + 1$$

and picking $m = 1$ we have

$$G = \begin{pmatrix} 1 + z & \alpha^6 + \alpha^2 z & \alpha^5 + \alpha^4 z & \alpha + \alpha^3 z & \alpha^3 + \alpha z & \alpha^4 + \alpha^5 z & \alpha^2 + \alpha^6 z \\ \alpha^2 + \alpha^2 z & 1 + \alpha^3 z & \alpha^6 + \alpha^5 z & \alpha^5 + z & \alpha + \alpha^6 z & \alpha^3 + \alpha^4 z & \alpha^4 + \alpha z \\ \alpha^4 + \alpha^4 z & \alpha^2 + \alpha^5 z & 1 + \alpha^6 z & \alpha^6 + \alpha z & \alpha^5 + \alpha^3 z & \alpha + \alpha^2 z & \alpha^3 + z \end{pmatrix}$$

The code $\operatorname{im} G$ has distance 10 and the extended row distances satisfy $\hat{d}_j^r \geq 2j + 6$ for $j \geq 2$.

As can be seen from the second example the rows of the generator matrices G do not necessarily have minimal weight $(m+1)(n-k+1)$. Indeed, since multiplication by x as well as σ are weight preserving maps, each row of G has weight $(m+1)\mathrm{wt}(c)$ and the weight of the idempotent generator c is in general bigger than the distance $n - k + 1$ of the code $\langle c \rangle$. This is also the reason why we have used a different element in the first paragraph of the proof above. Using the same idea we can actually present a generator matrix of our Reed-Solomon convolutional codes where each row has weight $(m + 1)(n - k + 1)$. Indeed, as we have seen in the first part of the proof of Theorem 4.3, the polynomial $\hat{g} = f \sum_{\nu=0}^{m} z^{\nu}$ is in the left

ideal $^\bullet\langle g\rangle$. Since actually $f = ac$ for some unit $a \in A$ we even have $^\bullet\langle \hat{g}\rangle = {}^\bullet\langle g\rangle$ in $A[z; \sigma]$. Furthermore, $\varepsilon^{(i)}\hat{g} = 0$ for $i = 0, \ldots, n - k - 1$ and $\deg \varepsilon^{(i)}\hat{g} = m$ for $i = n - k, \ldots, n - 1$. Therefore, just like in the proof of Theorem 3.3(c) the polynomial $\hat{g}$ is reduced in the sense of [8, Def. 4.9(b)]. Using [8, Thm. 7.8] we obtain $\mathcal{C} = \operatorname{im}\hat{G}$ with

$$
\hat{G} = \begin{pmatrix} \mathfrak{v}(\hat{g}) \\ \mathfrak{v}(x\hat{g}) \\ \vdots \\ \mathfrak{v}(x^{k-1}\hat{g}) \end{pmatrix} = \sum_{\nu=0}^{m} z^\nu \hat{G}_\nu \text{ where } \hat{G}_\nu = \begin{pmatrix} \mathfrak{v}(\sigma^\nu(f)) \\ \mathfrak{v}(\sigma^\nu(xf)) \\ \vdots \\ \mathfrak{v}(\sigma^\nu(x^{k-1}f)) \end{pmatrix} \in \mathbb{F}^{k\times n}.
$$

Since $\operatorname{wt}(f) = n - k + 1$ we now have that each row of $\hat{G}$ has weight $(m+1)(n-k+1)$. In Example 4.5(b) above we obtain $f = \alpha^6 + \alpha^5 x + \alpha^5 x^2 + \alpha^2 x^3 + x^4$ and

$$
\hat{G} = \begin{pmatrix} \alpha^6 + \alpha^6 z & \alpha^5 + \alpha z & \alpha^5 + \alpha^4 z & \alpha^2 + \alpha^4 z & 1 + \alpha^5 z & 0 & 0 \\ 0 & \alpha^6 + \alpha^2 z & \alpha^5 + \alpha^4 z & \alpha^5 + z & \alpha^2 + z & 1 + \alpha z & 0 \\ 0 & 0 & \alpha^6 + \alpha^5 z & \alpha^5 + z & \alpha^5 + \alpha^3 z & \alpha^2 + \alpha^3 z & 1 + \alpha^4 z \end{pmatrix}.
$$

As discussed above each row of $\hat{G}$ has weight 10.

We close this section with a comparison of our codes to another construction of cyclic convolutional codes known in the literature.

Remark 4.6 In [16, p. 445] Piret presents a class of cyclic convolutional codes by constructing a suitable parity check matrix $H := H_0 + z H_1 \in \mathbb{F}[z]^{n\times(n-k)}$ where $\mathbb{F} = \mathbb{F}_{2^m}$ for some m such that $n \mid (2^m - 1)$ and where $k \geq \frac{n+1}{2}$. As one can show by some straightforward computations, the resulting codes are always cyclic with respect to the automorphism given by $\sigma(x) = x^{n-1}$ and they have dimension k. Moreover, these codes have overall constraint length $n - k$ and unit memory, that is, all row degrees of a minimal generator matrix are at most 1. Finally, it has been shown in [16, p. 446] that the distance is $2(n - k) + 1$, which is basically due to the fact that the block code with parity check matrix (H_0, H_1) has distance $2(n - k) + 1$. Notice also that, since $k \geq n - k$, each minimal generator matrix of the code $\ker H$ contains $2k - n$ constant rows, therefore the code contains an $(n, 2k - n)$-block code, explaining once more that its distance cannot be bigger than $2(n - k) + 1 \leq n$. These codes are best if $n - k$ is big and the optimum is reached by taking $k = \frac{n+1}{2}$ in which case the distance is n. In contrast to that, the codes we constructed above exist only for $k \leq \frac{n}{2}$; they are best if k is small and even optimal for $k \leq 2$. Moreover, our codes never contain constant codewords.

5 A generalization to BCH codes

In this short section we will briefly sketch how the previous ideas can be generalized to BCH codes. It is clear that, in principle, the computations in the proof of Theorem 4.3 can be generalized to all codes of Theorem 3.3. However, the resulting formulas look much more complicated. We restrict ourselves to presenting the following case.

Proposition 5.1 *Let the data be as in* (3.1) − (3.5) *and let the codes* $\mathcal{C}_{\mu,\nu}$ *be as in Proposi-*

tion 3.4. Assume $\mathrm{dist}(\mathcal{C}_{\mu,\mu+\nu}) = d_\nu$ for all $0 \leq \mu \leq \mu + \nu \leq b$. Define

$$
D(t) := \begin{cases} 2\sum_{\nu=0}^{t-1} d_\nu + (m-t+1)d_t, & \text{if } t = 0, \ldots, m, \\ 2\sum_{\nu=0}^{m-1} d_\nu + (t-m+1)d_m, & \text{if } t \geq m+1. \end{cases}
$$

Then $\hat{d}_j^r \geq D(j - m - 1)$ for all $j \geq m+1$ and $\mathrm{dist}(\mathcal{C}) \geq \min\{D(0), D(1), \ldots, D(m)\}$.

The assumption that all codes $\mathcal{C}_{\mu,\mu+\nu}$ have the same distance independent of μ is satisfied whenever the automorphism σ is weight-preserving. This can be seen directly from the form of $\mathcal{C}_{\mu,\mu+\nu}$ given in Proposition 3.4. A special case was given in Lemma 3.5.

PROOF: We argue as in the proof of Theorem 4.3. The codewords of length $m + t + 1$ look again like in (4.5) and (4.6). That gives us in the case $t < m$

$$
\mathrm{wt}(v) \geq \sum_{\nu=0}^{t} d_\nu + \sum_{\nu=t+1}^{m} d_t + \sum_{\nu=m+1}^{m+t} d_{m+t-\nu} = 2\sum_{\nu=0}^{t-1} d_\nu + (m-t+1)d_t
$$

and in the case where $t \geq m$ we obtain

$$
\mathrm{wt}(v) \geq \sum_{\nu=0}^{m-1} d_\nu + \sum_{\nu=m}^{t} d_m + \sum_{t+1}^{t+m} d_{m+t-\nu} = 2\sum_{\nu=0}^{m-1} d_\nu + (t-m+1)d_m.
$$

This proves the first part of the proposition. The second part follows from

$$
\mathrm{dist}(\mathcal{C}) \geq \min\{D(t) \mid t \in \mathbb{N}_0\} = \min\{D(t) \mid t = 0, \ldots, m\}. \qquad \square
$$

In the following example we will use a BCH block code and a weight preserving automorphism σ. The distances of the resulting convolutional codes will be estimated according to the previous proposition and compared to the Griesmer bound known for the distance of convolutional codes.

Example 5.2 We choose $\mathbb{F} = \mathbb{F}_2$ and $n = 31$ along with the weight preserving automorphism given by $\sigma(x) = x^{13}$. Then $x^{31} - 1 = (x-1)\prod_{i=1}^{6} \pi_i$ where

$$
\pi_1 = x^5 + x^2 + 1, \quad \pi_2 = x^5 + x^4 + x^3 + x^2 + 1, \quad \pi_3 = x^5 + x^4 + x^2 + x + 1,
$$
$$
\pi_4 = x^5 + x^3 + 1, \quad \pi_5 = x^5 + x^3 + x^2 + x + 1, \quad \pi_6 = x^5 + x^4 + x^3 + x + 1.
$$

The automorphism induces the permutation $\sigma|_E : E \longrightarrow E$ with cycles

$$
\left(\varepsilon^{(0)}\right)\left(\varepsilon^{(1)}, \varepsilon^{(2)}, \varepsilon^{(3)}, \varepsilon^{(4)}, \varepsilon^{(5)}, \varepsilon^{(6)}\right).
$$

We pick the set $S := \{\varepsilon^{(1)}\}$ and $b := 5$. We will consider the codes generated by $g := \varepsilon^{(1)} \sum_{i=0}^{m} \boldsymbol{z}^i$ for all $1 \leq m \leq b$. According to Theorem 3.3(c) they all have dimension 5. We will compute the lower bounds for the distances using Proposition 5.1. Since σ is weight-preserving, the codes $\mathcal{C}_{\mu,\mu+\nu}$ have the same distance as $\mathcal{C}_{0,\nu} = \langle \varepsilon^{(1)} + \ldots + \sigma^\nu(\varepsilon^{(1)}) \rangle$. Moreover, according to Proposition 3.4 they are all cyclic block codes of dimension $5(\nu+1)$, $0 \leq \nu \leq b$. We can find a lower bound of their distances by counting the number of consecutive

15

zeros of these codes. In order to do so, we notice that over $\mathbb{F}_{32}$ with primitive element α satisfying $\alpha^5 + \alpha^2 + 1 = 0$ we have

$$
\begin{aligned}
\pi_1 &= (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)(x - \alpha^{16}), \\
\pi_2 &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^{24})(x - \alpha^{17}), \\
\pi_3 &= (x - \alpha^5)(x - \alpha^{10})(x - \alpha^{20})(x - \alpha^9)(x - \alpha^{18}), \\
\pi_4 &= (x - \alpha^{15})(x - \alpha^{30})(x - \alpha^{29})(x - \alpha^{27})(x - \alpha^{23}), \\
\pi_5 &= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{28})(x - \alpha^{25})(x - \alpha^{19}), \\
\pi_6 &= (x - \alpha^{11})(x - \alpha^{22})(x - \alpha^{13})(x - \alpha^{26})(x - \alpha^{21}).
\end{aligned}
\tag{5.1}
$$

It is worth mentioning that this implies

$$
\varepsilon^{(1)} = \beta(x - 1) \prod_{i=2}^{6} \pi_i = \gcd\left(\mathrm{MiPo}(\alpha^i, \mathbb{F}_2) \,\middle|\, i = 17, \ldots, 31\right) \in \mathbb{F}_2[x],
$$

thus $\langle \varepsilon^{(1)} \rangle$ is a BCH block code. Therefore we call the codes generated by g above *BCH convolutional codes*. Counting successive powers of α we obtain from (5.1) for the distances $d_\nu = \mathrm{dist}(\mathcal{C}_{0,\nu})$

$$
d_0 \geq 16, \; d_1 \geq 8, \; d_2 \geq 8, \; d_3 \geq 3, \; d_4 \geq 3, \; d_5 \geq 2.
$$

Using now Proposition 5.1 we can derive lower bounds for the distances of the codes $\mathcal{C} = \mathrm{im}\, G$ where G is as in (3.5). We also compare the results with the Griesmer bound known for codes with parameters $(31, 5, 5m)$ and memory m [7, Thm. 3.4].

m	lower bound for the distance	Griesmer bound
1	$\mathrm{dist}(\mathcal{C}) \geq \min\{32, 40\} = 32$	32
2	$\mathrm{dist}(\mathcal{C}) \geq \min\{48, 48, 56\} = 48$	48
3	$\mathrm{dist}(\mathcal{C}) \geq \min\{64, 56, 64, 67\} = 56$	64
4	$\mathrm{dist}(\mathcal{C}) \geq \min\{80, 64, 72, 70, 73\} = 64$	80
5	$\mathrm{dist}(\mathcal{C}) \geq \min\{96, 72, 80, 73, 76, 78\} = 72$	96

By computing the distances d_0 and d_1 of the two smaller block codes $\mathcal{C}_{0,0}$ and $\mathcal{C}_{0,1}$ exactly (for instance, using Maple), one obtains $d_0 = 16$, $d_1 = 12$, showing that these two codes attain the Griesmer bound for block codes, see [12, Thm. 5.2.6]. Computing the Gauss-Jordan form of the generator matrix of the code $\mathcal{C}_{0,2}$ one can see that $d_2 = 8$. The actual value of d_1 improves the lower bounds in the table above. Indeed, for $m = 3$ we obtain $\mathrm{dist}(\mathcal{C}) \geq 64$, showing that the code is optimal with respect to its distance, and for $m = 4$ we obtain $\mathrm{dist}(\mathcal{C}) \geq 78$ which is actually pretty close to the Griesmer bound. For $m = 5$ we get $\mathrm{dist}(\mathcal{C}) \geq 81$ which still is relatively far below the Griesmer bound.

Using the same ideas as in the proof of Theorem 4.3 (see also the paragraph right after that theorem) one also obtains a lower bound for the extended row distances of these codes. For the code with memory m this slope is given by $d_m = \mathrm{dist}(\mathcal{C}_{0,m})$. For instance, for memory $m = 1$ this slope is at least 12. In this case we also computed the weight distribution of the code explicitly (see also [14, Sec. 3] or [4, Def. 3.3]) and obtained, using Maple,

$$
\begin{aligned}
\Omega(L, W) &= \frac{31 L^2 W^{32}}{1 - 6LW^{20} - 15LW^{16} - 10LW^2} \\
&= 31\left(W^{32}L^2 + W^{44}(10 + 15W^4 + 6W^8)L^3 + W^{56}(10 + 15W^4 + 6W^8)^2 L^4 + O(L^5)\right)
\end{aligned}
$$

16

showing that the least weight of atomic codewords of length 2 is 32, the least weight of atomic codewords of length 3 is 44 etc. Thus the slope of the extended row distances is exactly 12.

The numbers $D(t)$ in Proposition 5.1 can also be generalized to the case where $\text{dist}(\mathcal{C}_{\mu,\mu+\nu})$ does depend on μ and ν. However, we omit this rather technical case.

6 Concluding remarks

In this paper we defined, as a special case of doubly-cyclic codes, the class of Reed-Solomon convolutional codes, and we determined their distance and extended row distances. This shows that these codes possess, at least theoretically, a good performance. We also showed an example of how to extend these results to BCH convolutional codes. We did not discuss the issue of decoding for these codes. Up to now we can only come up with an iterative decoding scheme for Reed-Solomon convolutional codes that does not outperform the algebraic decoding of the Reed-Solomon block code $\langle c \rangle$. This certainly needs to be investigated further.

Acknowledgement

References

[1] J. A. Domínguez Pérez, J. M. Muñoz Porras, and G. Serrano Sotelo. Convolutional codes of Goppa type. *Appl. Algebra Engrg. Comm. and Comput.*, 15:51–61, 2004.

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

[3] G. D. Forney Jr. Minimal bases of rational vector spaces, with applications to multivariable linear systems. *SIAM J. on Contr.*, 13:493–520, 1975.

[4] H. Gluesing-Luerssen. On the weight distribution of convolutional codes. *Linear Algebra and its Applications*, 408:298–326, 2005.

[5] H. Gluesing-Luerssen and B. Langfeld. On the algebraic parameters of convolutional codes with cyclic structure. Preprint 2003. Accepted for publication in Journal of Algebra and its Applications. Available at http://arxiv.org/pdf/math.RA/0312092.

[6] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52:584–598, 2006.

[7] H. Gluesing-Luerssen and W. Schmale. Distance bounds for convolutional codes and some optimal codes. Preprint 2003. Available at http://arxiv.org/pdf/math.RA/0305135.

[8] H. Gluesing-Luerssen and W. Schmale. On cyclic convolutional codes. *Acta Applicandae Mathematicae*, 82:183–237, 2004.

[9] R. Hutchinson, J. Rosenthal, and R. Smarandache. Convolutional codes with maximum distance profile. *Syst. Contr. Lett.*, 54:53–63, 2005.

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

[11] J. Justesen, E. Paaske, and M. Ballan. Quasi-cyclic unit memory convolutional codes. *IEEE Trans. Inform. Theory*, IT-36:540–547, 1990.

[12] J. H. v. Lint. *Introduction to Coding Theory.* Springer, 3. edition, 1999.

[13] R. J. McEliece. The algebraic theory of convolutional codes. In V. Pless and W. Huffman, editors, *Handbook of Coding Theory, Vol. 1*, pages 1065–1138. Elsevier, Amsterdam, 1998.

[14] R. J. McEliece. How to compute weight enumerators for convolutional codes. In M. Darnell and B. Honory, editors, *Communications and Coding (P. G. Farrell 60th birthday celebration)*, pages 121–141. Wiley, New York, 1998.

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

[16] P. Piret. A convolutional equivalent to Reed-Solomon codes. *Philips J. Res.*, 43:441–458, 1988.

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

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

[19] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, IT-47:2045–2049, 2001.

[20] C. Thommesen and J. Justesen. Bounds on distances and error exponents of unit memory codes. *IEEE Trans. Inform. Theory*, IT-29:637–649, 1983.