ELSEVIER

Discrete Applied Mathematics 111 (2001) 157–175

DISCRETE APPLIED MATHEMATICS

Algebraic structure of quasicyclic codes ☆

Kristine Lally *, Patrick Fitzpatrick

Department of Mathematics, National University of Ireland, Cork, Ireland

Received 3 September 1999; revised 6 March 2000; accepted 13 July 2000

Abstract

We use Gröbner bases of modules as a tool in the construction and classification of quasicyclic codes. Whereas previous studies have been mainly concerned with the 1-generator case, our results elucidate the structure of arbitrary quasicyclic codes and their duals. As an application we provide a complete characterisation of self-dual quasicyclic codes of index 2.

1. Introduction

Quasicyclic codes of index ℓ over a (finite) field F, defined by the property that a cyclic shift of a codeword by ℓ places is another codeword, generalise the class of cyclic codes ($\ell = 1$). Many such codes have been discovered with minimum distance exceeding that previously known for any linear code of the same length and dimension, or, indeed, taking the maximum possible value.

The theory of Gröbner bases of modules (developed in [1,2]) has been applied [6–9] to decoding Reed–Solomon codes, to scalar rational interpolation, and to various other problems, such as Padé approximation, that can be represented as solving systems of polynomial congruences. In [22], the authors use the theory to develop machinery for analysis of Hermitian codes. The essential idea is to use a cyclic group of automorphisms of the code to represent it as a module over the polynomial ring $F[x]$. In this paper we adopt the same approach to provide new insight into the algebraic structure of quasicyclic codes.

Early studies by Chen et al. [3], Karlin [18,19], and Townsend and Weldon [32] established connections between quasicyclic codes, multicirculant, and power residue codes, while [20] showed that quasicyclic codes meet a modified Gilbert–Varshamov bound (see also [23]). The close link between quasicyclic and convolutional codes is

☆ A preliminary version of this paper was presented at the Workshop on Coding and Cryptography, INRIA, Paris, January 1999.

* Corresponding author.

0166-218X/01/$ - see front matter
PII: S0166-218X(00)00350-4

indicated by the obvious similarity between the polynomial form of the generator matrix of a quasicyclic code (see Section 2) and the generator matrix of a convolutional code [24,25,30].

Generally, a quasicyclic code of length ℓm and index ℓ may be represented as the row space of a block matrix, each row of which has the form $(G_1, \ldots, G_\ell)$, where G_i is an $m \times m$ circulant. These rows, or the equivalent polynomial vectors, are conventionally called "generators". A method for constructing 1-generator quasicyclic codes was given by van Tilborg in [33], as well as the results of an exhaustive computer search for such codes over the binary alphabet, for $m = 7, 8$ and length up to 120. Some of these codes meet the best possible values of minimum distance for any linear code. Further developments of van Tilborg's technique were provided by Gulliver and Bhargava [11–15], who carried out non-exhaustive searches, using heuristic combinatorial optimisation techniques and selection algorithms, again resulting in the construction of many new 1-generator quasicyclic codes that improved the known lower bounds. The same authors extended their research to the 2-generator case in [16]. Quasicyclic codes over other fields were studied in [10,13] and many good or optimal codes were constructed. Currently, Zhi Chen maintains a searchable database of quasicyclic codes at http://rimula.hkr.se/∼chen/research/codes/searchqc2.htm.

The structure of quasicyclic codes was explored by Séguin and others [4,26–28], and Tanner [31]. We adopt a new approach based on the construction of a canonical generating set for a quasicyclic code regarded as a submodule of the algebra R^ℓ where $R = F_q[x]/\langle x^m - 1\rangle$. We use the language of Gröbner bases which, although not strictly necessary, leads to concise arguments and has the potential for generalisation to codes over other domains. Our primary aim here is to elucidate structure, so we do not address the important issues of minimum distance, decoding algorithms, and the existence of good quasicyclic codes. Nevertheless, our methods can be used to construct quasicyclic codes of index ℓ and length ℓm for all dimensions permissable by the degrees of the irreducible factors of $x^m - 1$. As a consequence we have constructed many binary quasicyclic codes which are optimal or meet the best known bounds for linear codes, many of which are the first known quasicyclic codes meeting the bounds. Also, using an early version of this paper [21], Siap et al. [29] have constructed many quasicyclic codes over the fields of order 3 and 5 that improved the known bounds.

NB: *Throughout the paper the word* "*code*" *means* "*quasicyclic code*" *unless otherwise specified.*

2. Basic structure

Let $\mathscr{C}$ be a code of length ℓm and index ℓ where ℓ is defined as the smallest power of the cyclic shift operator under which $\mathscr{C}$ is invariant. It is obvious that by a coordinate permutation we may assume that each element of $\mathscr{C}$ can be represented as a vector $c = (c_1(x), \ldots, c_\ell(x))$ of polynomials of degree less than m. In this form the defining property of $\mathscr{C}$ is that it is closed under multiplication by x and reduction modulo $x^m - 1$ in each component, that is, $c \in \mathscr{C}$ implies $xc = (xc_1(x)$

$\bmod x^m-1,\ldots,xc_\ell(x)\bmod x^m-1)\in\mathscr{C}$. If $R=F[x]/\langle x^m-1\rangle$, where F is a finite field, this implies that $\mathscr{C}$ is an R-submodule of R^ℓ, which is the precise generalisation of the structure of a cyclic code. It follows that the preimage $\tilde{\mathscr{C}}$ of $\mathscr{C}$ in $F[x]^\ell$ is an $F[x]$-submodule containing $\tilde{\mathscr{K}}=\langle(x^m-1)e_i,\ i=1,\ldots,\ell\rangle$ where e_i is the standard basis vector with 1 in position i and 0 elsewhere. The tilde will be used conventionally throughout to represent structures over $F[x]$.

Since $\tilde{\mathscr{C}}$ is a submodule of the finitely generated free module over the principal ideal domain $F[x]$ and contains $\tilde{\mathscr{K}}$, it has a generating set of the form $\{r_i,\ i=1,\ldots,t,(x^m-1)e_j,j=1,\ldots,\ell\}$ where $r_i=(r_{i1},\ldots,r_{i\ell})$ (see [17, Chapter 7]). Thus the rows of

$$M=\begin{pmatrix} r_{11} & \cdots & r_{1\ell}\\ r_{21} & \cdots & r_{2\ell}\\ & \cdots & \\ r_{t1} & \cdots & r_{t\ell}\\ x^m-1 & \cdots & 0\\ & \cdots & \\ 0 & \ldots & x^m-1 \end{pmatrix}$$

generate $\tilde{\mathscr{C}}$. Using elementary row operations in $F[x]$ we may triangularise M so that another generating set is given by the *triangular set* of rows $\tilde{\mathscr{G}}=\{g_1,\ldots,g_\ell\}$ of

$$\tilde{G}=\begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1\ell}\\ 0 & g_{22} & \ldots & g_{2\ell}\\ & \cdots & \cdots & \\ 0 & 0 & \ldots & g_{\ell\,\ell} \end{pmatrix} \tag{1}$$

where the *diagonal component* g_{ii} divides x^m-1 for all i. Note that $g_i\neq 0$ for all i. Each non-zero element of $\tilde{\mathscr{C}}$ may be expressed in the form $(0,\ldots,0,c_r,\ldots,c_\ell)$, where $r\geqslant 1$ and $c_r\neq 0$. Writing this as an $F[x]$-linear combination $\sum_{i=1}^{\ell}a_ig_i$, it is immediate that c_r is divisible by the corresponding diagonal component g_{rr}. This implies that $\tilde{\mathscr{G}}$ is a Gröbner basis of $\tilde{\mathscr{C}}$ with respect to the position-over-term (POT) order in $F[x]^\ell$, where $e_1>\cdots>e_\ell$ and the monomials x^i are ordered naturally in each component. Throughout the paper Gröbner bases will be defined with respect to POT order unless otherwise stated. For the theory of Gröbner bases see [1,2,5].

Using further elementary operations we can guarantee that

$$\partial g_{ij}<\partial g_{jj}\quad\text{for } i<j, \tag{2}$$

where ∂ denotes degree and $\partial 0=-1$, and then $\tilde{\mathscr{G}}$ is the reduced Gröbner basis of $\tilde{\mathscr{C}}$. This is uniquely defined up to multiplication by constants, and where appropriate we adopt the natural normalisation in which the diagonal components are monic. We will often make uniqueness statements intending uniqueness up to constant multiples without

explicit mention. If $\tilde{\mathscr{G}}$ is a reduced Gröbner basis and the diagonal component g_{ii} is equal to $x^m - 1$ then $(0,\dots,0,g_{i,i+1},\dots,g_{i\ell}) \in \tilde{\mathscr{C}}$ which means that it is an $F[x]$-linear combination of $\{g_{i+1},\dots,g_\ell\}$. Since $\partial g_{ij} < \partial g_{jj}$ for all $j > i$ this forces $g_{ij} = 0$ for all $j > i$ and hence $g_i = (x^m - 1)e_i$.

The leading term $\mathrm{Lt}(0,\dots,0,v_r,\dots,v_\ell)$, $r \geqslant 1$, $v_r \neq 0$, of an element $v \in F[x]^\ell$ is $x^{\partial v_r} e_r$. Each such v has a uniquely defined normal form $\mathrm{Nf}_{\tilde{\mathscr{G}}}(v) = (0,\dots,0,v'_s,\dots,v'_\ell)$ with respect to $\tilde{\mathscr{G}}$, obtained by successive division of its components by the g_{ii} and satisfying

$$v = (0,\dots,0,v'_s,\dots,v'_\ell) + \sum_{i=1}^{\ell} b_i g_i,$$

where $s \geqslant r$ and $\partial v'_j < \partial g_{jj}$ for $s \leqslant j \leqslant \ell$. (This division algorithm is given in detail in [8,9] and is a straightforward generalisation of that in [5].) Also, $v \in \tilde{\mathscr{C}}$ if and only if $\mathrm{Nf}_{\tilde{\mathscr{G}}}(v) = (0,\dots,0)$. Since the dimension of the quotient $F[x]^\ell/\tilde{\mathscr{K}}$ is finite we may immediately compute the F-dimension of $F[x]^\ell/\tilde{\mathscr{C}}$ as the number of terms $x^i e_j$ which are in normal form modulo $\tilde{\mathscr{G}}$. This is clearly $\sum_{i=1}^{\ell} \partial g_{ii}$.

We summarise in the following theorem.

Theorem 2.1. *Each submodule $\tilde{\mathscr{C}}$ of $F[x]^\ell$ containing $\tilde{\mathscr{K}}$ has a reduced Gröbner basis of the form*

$$\tilde{\mathscr{G}} = \{g_i = (g_{i1}, g_{i2},\dots,g_{i\ell}), i = 1,\dots,\ell\}, \tag{3}$$

where

(i) $g_{ij} = 0$ *for all* $j < i$,
(ii) $\partial g_{ki} < \partial g_{ii}$ *for* $k < i$,
(iii) *if the left-most non-zero component of an element of $\tilde{\mathscr{C}}$ lies in the ith place then it is divisible by g_{ii}; in particular, g_{ii} divides $x^m - 1$,*
(iv) *if* $g_{ii} = x^m - 1$ *then* $g_i = (x^m - 1)e_i$,
(v) *the F-dimension of $F[x]^\ell/\tilde{\mathscr{C}}$ is* $\sum_{i=1}^{\ell} \partial g_{ii}$.

Any triangular set $\tilde{\mathscr{G}}$ is a Gröbner basis of the submodule of $F[x]^\ell$ that it generates. The condition that the submodule should contain $\tilde{\mathscr{K}}$ is equivalent to the existence of a matrix $\tilde{A} \in \mathrm{Mat}_\ell(F[x])$ such that

$$\tilde{A}\tilde{G} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1\ell} \\ a_{21} & a_{22} & \dots & a_{2\ell} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\ell 1} & a_{l2} & \dots & a_{\ell\,\ell} \end{pmatrix} \begin{pmatrix} g_{11} & g_{12} & \dots & g_{1\ell} \\ 0 & g_{22} & \dots & g_{2\ell} \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & g_{\ell\,\ell} \end{pmatrix} = (x^m - 1)I, \tag{4}$$

where I is the identity matrix. It is immediate that $\tilde{A}$ is also upper triangular, and its non-zero entries can be computed recursively from those of $\tilde{G}$. If we consider the equation $\tilde{A}\tilde{G} = (x^m - 1)I$ over the field of fractions of $F[x]$ then the factors are invertible

and therefore also $\tilde{G}\tilde{A} = (x^m - 1)I$ over $F[x]$. It follows that the entries of $\tilde{G}$ satisfy an analogous system of equations in terms of those of $\tilde{A}$.

Theorem 2.2. *The set $\tilde{\mathscr{G}}$ is a Gröbner basis of a submodule $F[x]^\ell$ containing $\tilde{\mathscr{K}}$ if and only if there exist a_{ij} for $1 \leqslant i,\ j \leqslant \ell$ satisfying*

$$a_{ij} = \begin{cases} 0 & \text{if } j < i, \\ \frac{x^m-1}{g_{ii}} & \text{if } j = i, \\ \frac{-1}{g_{jj}}\left(\sum_{k=i}^{j-1} a_{ik} g_{kj}\right) & \text{if } j > i. \end{cases} \tag{5}$$

Moreover the corresponding equations with the roles of g_{ij}, a_{ij} interchanged also hold, and $m - \partial g_{ii} = \partial a_{ii}$ for all i. The Gröbner basis is reduced if and only if $\partial g_{ii} > \partial g_{ji}$ for all $j < i$, if and only if $\partial a_{ii} > \partial a_{ij}$ for all $j > i$.

Proof. This is an easy consequence of the definitions and (4), apart from the degree conditions on the a_{ij}. Suppose that the Gröbner basis is reduced so that $\partial g_{ii} > \partial g_{ji}$ for all $j < i$. The equation $a_{ii}g_{i,i+1} + a_{i,i+1}g_{i+1,i+1} = 0$ implies either $g_{i,i+1} = a_{i,i+1} = 0$ or $\partial a_{ii} - \partial a_{i,i+1} = \partial g_{i+1,i+1} - \partial g_{i,i+1} > 0$. Using an induction argument, if $\partial a_{ii} > \partial a_{ij}$ for $j = i+1, \ldots, k-1$ and $\partial a_{ik} \geqslant \partial a_{ii}$ then the last summand on the left-hand side of the equation

$$a_{ii}g_{ik} + a_{i,i+1}g_{i+1,k} \cdots + a_{i,k-1}g_{k-1,k} + a_{ik}g_{kk} = 0$$

has degree strictly greater than the degrees of the others, which is a contradiction. Hence $\partial a_{ik} < \partial a_{ii}$ and, by induction, the proof in one direction is complete. The converse is true by a symmetrical argument. □

Remark 2.3. Given a triangular set $\tilde{\mathscr{G}}$, verification in practice that it generates a submodule containing $\tilde{\mathscr{K}}$ is carried out as follows. For each i, we check that the diagonal component is a divisor of $x^m - 1$. Then the generator g_i is multiplied by $a_{ii} = (x^m - 1)/g_{ii}$ and subtracted from $(x^m - 1)e_i$. The residual vector must then be reduced to zero by subtracting multiples of $g_{i+1}, \ldots, g_\ell$. This process takes $(\ell - 1)(\ell - i + 1)/2$ polynomial multiplication–subtraction operations, and the total number of such operations required for verification is $(\ell - 1)\ell(\ell + 1)/6$.

The code $\mathscr{C}$ is the image of $\tilde{\mathscr{C}}$ under the natural homomorphism $\varphi\colon F[x]^\ell \to R^\ell, (c_1, \ldots, c_\ell) \mapsto (c_1 + \langle x^m - 1\rangle, \ldots, c_\ell + \langle x^m - 1\rangle)$. Dropping the coset notation we see immediately that $\mathscr{C}$ has an R-generating set $\mathscr{G}$ comprising the elements of a Gröbner basis $\tilde{\mathscr{G}}$ not mapped to zero under φ, that is, those elements not of the form $(x^m - 1)u$ for some $u \in F[x]^\ell$. We refer to this set of generators as a GB *generating set* of $\mathscr{C}$. This is the central structural notion of our theory. Of course, such Gröbner basis generating sets depend on the choice of order (we have used POT order and later will introduce an alternative rPOT order). If the generating set of $\mathscr{C}$ is derived as the set

of images of a reduced Gröbner basis then it will be called an RGB *generating set*. This generating set is uniquely defined with respect to the given order.

Applying part (v) of Theorem 2.1 and subtracting the codimension of $\tilde{\mathscr{C}}$ from that of $\tilde{\mathscr{K}}$, we can immediately assert

Corollary 2.4. *The dimension of the code* $\mathscr{C}$ *with* GB *generating set* $\{\varphi(g_i), i = 1,\ldots,\ell\}$ *is given by*

$$\ell m - \sum_{i=1}^{\ell} \partial g_{ii} = \sum_{i=1}^{\ell} (m - \partial g_{ii}).$$

The possible dimensions of codes can also be enumerated straightforwardly. From now on we fix the notation $x^m - 1 = \prod_{n=1}^{s} f_n^{\varepsilon}$, where $m = (\operatorname{char} F)^t m'$ with $\gcd(m', \operatorname{char} F) = 1$ and $\varepsilon = (\operatorname{char} F)^t$, for the decomposition of $x^m - 1$ into irreducible factors f_n over F. It will be convenient to use the notation $N = \{1, 2, \ldots, s\}$.

Corollary 2.5. *The codes of length* ℓm *and index* ℓ *have dimensions* $\sum_{i=1}^{\ell} \sum_{n=1}^{s} t_{ni} \partial f_n$ *where* $0 \leqslant t_{ni} \leqslant \varepsilon$. *Every such dimension arises in some code* (*for instance, in a code with block diagonal generator matrix*).

Remark 2.6. The most frequently studied codes in the literature are those with one "generator" (in the sense of the Introduction), that is, the cyclic submodules of R^{ℓ}. These are usually referred to as "1-generator" codes. Such codes may well have Gröbner basis generating sets containing more than one element. It is not at all obvious how to determine the dimension of the code from such a generator (but see Corollary 2.14).

We now give two examples $\mathscr{C}_1, \mathscr{C}_2$ which will be used as illustrations.

Example 2.7. Let $\mathscr{C}_1$ be the binary code of index $\ell = 3$ and length $n = \ell m = 21, m = 7$ generated by elements

$$v_1 = (x^5 + x^4 + 1, x^4 + x^3 + x + 1, x^4 + x^3 + x^2)$$
$$v_2 = (x^4 + x^2 + x^3 + 1, x, x^4 + x^3 + x + 1).$$

Let $f_1 = x + 1, f_2 = x^3 + x + 1, f_3 = x^3 + x^2 + 1$ so that $x^7 + 1 = f_1 f_2 f_3$. The reduced Gröbner basis of $\tilde{\mathscr{C}}_1 = \langle v_1, v_2, (x^7 + 1)e_1, (x^7 + 1)e_2, (x^7 + 1)e_3 \rangle$ comprises the rows of

$$\begin{pmatrix} f_2 & f_1^2 & x^2 \\ 0 & f_3 & f_1 f_3 \\ 0 & 0 & x^7 + 1 \end{pmatrix}$$

so the diagonal components are indeed divisors of $x^m - 1$. The corresponding RGB generating set of $\mathscr{C}_1$ consists of the rows of

$$\begin{pmatrix} f_2 & f_1^2 & x^2 \\ 0 & f_3 & f_1 f_3 \end{pmatrix}$$

since the third row is mapped to zero by φ. From the diagonal components we may calculate the dimension of $\mathscr{C}_1$ as $\sum_{i=1}^{l}(m-\partial g_{ii})=4+4+0=8$.

There is no restriction to the semisimple case (corresponding to $\gcd(m,\operatorname{char}F)=1$) in the Gröbner basis formulation, that is, the value of m need not be relatively prime to the characteristic (compare [4,27]). The binary code $\mathscr{C}_2$ of index $\ell=3$ and length $n=\ell m=84, m=28$ whose RGB generating set is given by the rows of

$$\begin{pmatrix} f_1^2 f_2 f_3^3 & f_1^2(x^2+x+1) & 1 \\ 0 & f_1^4 f_2 f_3 & f_2 x \\ 0 & 0 & f_1^3 \end{pmatrix}$$

has dimension $\sum_{i=1}^{l}(m-\partial g_{ii})=14+18+19=51$.

Using the restrictions on the off-diagonal elements of $\tilde{G}$ and $\tilde{A}$ imposed by Theorem 2.2 we can, in principle, construct RGB generating sets for all possible codes of a given index, limited only by the computational effort involved.

Example 2.8. Suppose that we wish to construct RGB generating sets for all binary codes of index $\ell=3$ and length 21 with diagonal components as in $\mathscr{C}_1$. Then we may take

$$\tilde{A}=\begin{pmatrix} f_1 f_3 & p & q \\ 0 & f_1 f_2 & r \\ 0 & 0 & 1 \end{pmatrix}, \quad \tilde{G}=\begin{pmatrix} f_2 & a & b \\ 0 & f_3 & c \\ 0 & 0 & x^7+1 \end{pmatrix}. \tag{6}$$

The equations $\tilde{A}\tilde{G}=\tilde{G}\tilde{A}=(x^7+1)I$ lead to $p=f_1 a, c=f_3 r, b=f_2 q+ar$, while the degree restrictions on the off-diagonal elements of $\tilde{G}$ give $\partial a\leqslant 2, \partial b\leqslant 6, \partial c\leqslant 6, \partial p\leqslant 3$, $\partial q\leqslant 3, \partial r\leqslant 3$. Conversely, any set of polynomials satisfying these constraints is valid. We can choose a,q,r freely and this fixes the code. Hence there are 2^{11} such codes. The same analysis can be carried out for other choices of the diagonal components g_{ii}. In the particular case of $\mathscr{C}_1$ we find the (unique) solution $a=f_1^2,\ b=x^2,\ c=f_1 f_3,\ p=f_1^3,\ q=1,\ r=f_1$.

A generator matrix for the code $\mathscr{C}$, comprising linearly independent rows, can be constructed directly from any GB generating set $\mathscr{G}=\{g_i, i=1,\ldots,\ell\}$ as follows. The diagonal component g_{ii} and its $m-\partial g_{ii}-1$ cyclic shifts $xg_{ii}, x^2 g_{ii},\ldots,x^{m-\partial g_{ii}-1}g_{ii}$ are clearly linearly independent over F (since the leading coefficient of g_{ii} is non-zero). Hence the set of vectors

$$\begin{aligned} g_i &= (0,0,\ldots,0,g_{ii},g_{i,i+1},\ldots,g_{i\ell}) \\ xg_i &= (0,0,\ldots,0,xg_{ii},xg_{i,i+1},\ldots,xg_{i\ell}) \\ &\vdots \\ x^{m-\partial g_{ii}-1}g_i &= (0,0,\ldots,0,x^{m-\partial g_{ii}-1}g_{ii},x^{m-\partial g_{ii}-1}g_{i,i+1},\ldots,x^{m-\partial g_{ii}-1}g_{i\ell}) \end{aligned}$$

is also linearly independent over F for each i. The block upper triangular matrix

$$\begin{pmatrix}
g_{11} & g_{12} & \cdots & g_{1\ell} \\
xg_{11} & xg_{12} & \dots & xg_{1\ell} \\
\vdots & \vdots & & \vdots \\
x^{m-\partial g_{11}-1}g_{11} & x^{m-\partial g_{11}-1}g_{12} & \dots\dots & x^{m-\partial g_{11}-1}g_{1\ell} \\
0 & g_{22} & \cdots & g_{2\ell} \\
0 & xg_{22} & \cdots & xg_{2\ell} \\
\vdots & \vdots & & \vdots \\
0 & x^{m-\partial g_{22}-1}g_{22} & \dots\dots & x^{m-\partial g_{22}-1}g_{2\ell} \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & g_{\ell\,\ell} \\
0 & 0 & \cdots & xg_{\ell\,\ell} \\
\vdots & \vdots & & \vdots \\
0 & 0 & \cdots & x^{m-\partial g_{\ell\,\ell}-1}g_{\ell\,\ell}
\end{pmatrix} \tag{7}$$

is an $\ell \times \ell$ block matrix in which each block is a truncated circulant. Since the diagonal components g_{ii} all lie in different positions, the rows of this matrix are linearly independent and therefore form a basis of $\ell m - \sum_{i=1}^{l} \partial g_{ii}$ vectors in $F^{\ell m}$.

Example 2.9. For $\mathscr{C}_1$ we find the following generator matrix:

$$\begin{pmatrix}
1101000\ 1010000\ 0010000 \\
0110100\ 0101000\ 0001000 \\
0011010\ 0010100\ 0000100 \\
0001101\ 0001010\ 0000010 \\
 \\
0000000\ 1011000\ 1110100 \\
0000000\ 0101100\ 0111010 \\
0000000\ 0010110\ 0011101 \\
0000000\ 0001011\ 1001110
\end{pmatrix}.$$

Previous authors have constructed this form of generator matrix in the 1–generator case (for example [12,26,33]).

Using the RGB generating set $\varphi(\tilde{\mathscr{G}}) = \{\varphi(g_1), \dots, \varphi(g_\ell)\}$ of the code $\mathscr{C}$ we can compute the decomposition of $\mathscr{C}$, regarded as $F[x]$-module, into its primary components (cf. [17, Chapter 8]). These are the submodules $u\mathscr{C}$ generated by the sets of elements $\{u\varphi(g_i),\ i = 1, \dots, \ell\}$ where u is of the form $(x^m - 1)/f_n^{\varepsilon}$ for $n \in N$. In the semisimple case they correspond to the irreducible submodules. However, in order to determine the RGB generating sets of the components, we first carry out the computation in $F[x]^{\ell}$, by reducing the generating sets $\{ug_i, i = 1, \dots, \ell, (x^m - 1)e_j, j = 1, \dots, \ell\}$ to Gröbner basis form, and thus determining the RGB generating sets for the components of $\mathscr{C}$.

Example 2.10. $\tilde{\mathscr{C}}_1$ is the sum of the submodules $f_1f_2\tilde{\mathscr{C}}_1 + \tilde{\mathscr{K}}$, $f_1f_3\tilde{\mathscr{C}}_1 + \tilde{\mathscr{K}}$, and $f_2f_3\tilde{\mathscr{C}}_3 + \tilde{\mathscr{K}}$ which intersect in $\tilde{\mathscr{K}}$. The reduced Gröbner basis generator matrices of the summands are

$$f_1f_2\begin{pmatrix} 1 & f_1 & f_1^2 \\ 0 & f_3 & 0 \\ 0 & 0 & f_3 \end{pmatrix}, \quad f_1f_3\begin{pmatrix} f_2 & 0 & 0 \\ 0 & 1 & f_1 \\ 0 & 0 & f_2 \end{pmatrix}, \quad f_2f_3\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & f_1 \end{pmatrix}$$

respectively. It now follows that the primary components of $\mathscr{C}_1$ have reduced Gröbner bases given by

$$\langle f_1f_2(\,1\;\; f_1\;\; f_1^2\,)\rangle \oplus \langle f_1f_3(\,0\;\; 1\;\; f_1\,)\rangle \oplus \left\langle f_2f_3\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\right\rangle$$

and that the component subcodes have dimensions 3, 3, 2.

Similarly, the component submodules of $\tilde{\mathscr{C}}_2$ are

$$f_1^4f_2^4\begin{pmatrix} f_3^3 & f_1 & 0 \\ 0 & f_3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad f_1^4f_3^4\begin{pmatrix} f_2 & 1 & x^2(x^2+x+1)f_1 \\ 0 & f_2 & (x^4+x+1)f_2 \\ 0 & 0 & f_2^3 \end{pmatrix}, \quad f_2^4f_3^4\begin{pmatrix} f_1^2 & f_1^2 & 0 \\ 0 & f_1^4 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and here the RGB generating set of each of the three primary components of $\mathscr{C}_2$ contains three elements. The dimensions of the primary subcodes are 24, 21, and 6.

The matrix $\tilde{A}$ in (4) may be interpreted as the matrix of $\tilde{\mathscr{K}}$ relative to $\tilde{\mathscr{G}}$, where $\tilde{\mathscr{K}}$ is regarded as the kernel of the surjective homomorphism $\varphi|_{\tilde{\mathscr{C}}} : \tilde{\mathscr{C}} \to \mathscr{C}$, restricting φ to $\tilde{\mathscr{C}}$. By a standard argument ([17, Chapter 7]), the Smith normal form of $\tilde{A}$ is a diagonal matrix $D = X\tilde{A}Y$, and the basis of $\tilde{\mathscr{C}}$ given by the rows of $Y^{-1}\tilde{G}$ provides a direct decomposition of $\mathscr{C}$ as a direct sum of cyclic submodules. We may use this to decompose the primary components of $\mathscr{C}$ into direct sums of submodules of prime power order. In the semisimple case the RGB generating sets of the primary components already give the decomposition, as the following lemma shows.

Lemma 2.11. *If* $\gcd(m, \operatorname{char} F) = 1$ *then each primary component of* $\mathscr{C}$ *decomposes into a direct sum of irreducible cyclic submodules generated by the elements of its RGB generating set.*

Proof. Let f be an irreducible factor of $x^m - 1$ corresponding to the primary component $\mathscr{F}$ of $\mathscr{C}$ and let $x^m - 1 = fh$. Then the matrix of the reduced Gröbner basis of the preimage $\tilde{\mathscr{F}}$ has the form

$$h\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1\ell} \\ 0 & c_{22} & \dots & c_{2\ell} \\ & \dots & \dots & \\ 0 & 0 & \dots & c_{\ell\ell} \end{pmatrix},$$

where the diagonal entries are either 1 or f, and if $c_{jj} = f$ then the corresponding element of the reduced Gröbner basis is $(x^m - 1)e_j$, while if $c_{jj} = 1$ then all entries

Table 1
Irreducible decomposition of $\mathscr{C}_2$

Generator	Order	Dimension
$f_1^4 f_2^4 (f_3^3, f_1, 1)$	f_3^4	12
$f_1^4 f_2^4 (0, 0, 1)$	f_3^4	12
$f_1^4 f_3^4 (0, f_2, (x^4 + x + 1) f_2)$	f_2^3	9
$f_1^4 f_3^4 (f_2, x f_1^2, x^7 + x^3 + 1)$	f_2^4	12
$f_2^4 f_3^4 (f_1^2, f_1^2, 0)$	f_1^2	2
$f_2^4 f_3^4 (f_1^2, f_1^2, 1)$	f_1^4	4

above it are zero. Thus, reducing modulo $x^m - 1$, the RGB generating set $\mathscr{G}$ corresponds to a matrix in reduced row echelon form. It is obvious that no multiple of any element of $\mathscr{G}$ is contained in the submodule generated by the others, and this gives the result.

Example 2.12. The code $\mathscr{C}_1$ decomposes as the direct sum

$$\langle f_1 f_2 (\,1 \;\; f_1 \;\; f_1^2\,)\rangle \oplus \langle f_1 f_3 (\,0 \;\; 1 \;\; f_1\,)\rangle \oplus \langle f_2 f_3 (\,1 \;\; 0 \;\; 1\,)\rangle \oplus \langle f_2 f_3 (\,0 \;\; 1 \;\; 0\,)\rangle,$$

where the orders of the cyclic summands are f_3, f_2, f_1, f_1, respectively, and their orders dimensions are $3, 3, 1, 1$.

The corresponding analysis for $\mathscr{C}_2$ requires the construction of the matrices $\tilde{\mathscr{A}}$ and their decomposition into Smith normal form. Omitting the details, we find that $\mathscr{C}_2$ has a direct decomposition into irreducible cyclic submodules as shown in Table 1.

We end this section with a result describing the diagonal components of a Gröbner basis of a 1-generator code.

Theorem 2.13. *Let $\mathscr{C}$ be the code generated (as R-module) by $(f_1, f_2, \ldots, f_\ell)$. Then the diagonal components of a* Gröbner basis *of the preimage $\tilde{\mathscr{C}}$ are*

$$f_{11} = \gcd(f_1, x^m - 1),$$

$$f_{ii} = \frac{(x^m - 1)\gcd(f_1, f_2, \ldots, f_i, x^m - 1)}{\gcd(f_1, f_2, \ldots, f_{i-1}, x^m - 1)}, \quad i = 2, \ldots, \ell.$$

Proof. A Gröbner basis is constructed by reducing the matrix whose rows are $(f_1, f_2, \ldots, f_\ell), (x^m - 1)\, e_i,\ i = 1, \ldots, \ell$. Consider first the case $\ell = 2$. Let $u f_1 + v(x^m - 1) =$

$d_1 = \gcd(f_1, x^m - 1)$. Then we carry out the following steps:

$$\begin{pmatrix} f_1 & f_2 \\ x^m-1 & 0 \\ 0 & x^m-1 \end{pmatrix} \to \begin{pmatrix} d_1 & Af_2 \\ f_1 & f_2 \\ x^m-1 & 0 \\ 0 & x^m-1 \end{pmatrix} \to \begin{pmatrix} d_1 & uf_2 \\ 0 & f_2 - \dfrac{f_1}{d_1}uf_2 \\ 0 & -\dfrac{x^m-1}{d_1}uf_2 \\ 0 & x^m-1 \end{pmatrix}$$

$$= \begin{pmatrix} d_1 & uf_2 \\ 0 & \dfrac{x^m-1}{d_1}vf_2 \\ 0 & -\dfrac{x^m-1}{d_1}uf_2 \\ 0 & x^m-1 \end{pmatrix} \to \begin{pmatrix} d_1 & uf_2 \\ 0 & \dfrac{x^m-1}{d_1}f_2 \\ 0 & x^m-1 \end{pmatrix},$$

where the last step is carried out using the fact that u, v are relatively prime. In the general case, let the corresponding sequence of operations be defined by the entries in the top left hand 2×2 submatrix. Thus, in this first sequence the $(1,1)$ entry has been replaced by d_1, the $(2,1)$ entry by 0 and the $(2,2)$ entry by $(x^m-1)/d_1 f_2$. By induction, suppose that after $i > 1$ steps the (i,i) entry is $d_i = (x^m - 1)/(d_{i-1})\gcd(d_{i-1}, f_i)$, and the $(i+1,i)$ and $(i+1,i+1)$ entries are 0 and $(x^m-1)/d_i f_{i+1}$, respectively. Then, by an identical sequence of operations, the induction step holds, and this completes the proof. □

Application of Corollary 2.4 gives

Corollary 2.14. *The dimension of the code generated* by $(f_1, f_2, \ldots, f_\ell)$ *is*

$$m - \deg(\gcd(f_1, f_2, \ldots, f_l, x^m - 1)).$$

This formula was given by Séguin and Drolet in [27].

3. Dual codes, parity check matrices

We denote by a_i, $i = 1, \ldots, \ell$ the rows of the matrix $\tilde{A}$ determined in Theorem 2.2. The structure of $\tilde{A}^{\mathrm{T}}$ implies that its rows form a reduced Gröbner basis for the module they generate, but with respect to the *reverse* POT term order (rPOT) in which the basis vectors are ordered $e_1 < \cdots < e_\ell$. (Note that analogous results to those of the previous section hold for rPOT Gröbner bases.) The equation $\tilde{G}^{\mathrm{T}}\tilde{A}^{\mathrm{T}} = (x^m - 1)I$ implies that this module contains $\tilde{\mathscr{K}}$. We define a scalar product on $F[x]^\ell$ by $\langle u, v\rangle = \sum_{i=1}^{\ell} u_i v_i$, and for any submodule $\tilde{\mathscr{C}}$ the *mod-$\tilde{\mathscr{K}}$-dual* of $\tilde{\mathscr{C}}$ by $\tilde{\mathscr{C}}^{\star}_{\tilde{\mathscr{K}}} = \{u \in F[x]^\ell : \langle u, c\rangle \in \tilde{\mathscr{K}} \text{ for all } c \in \tilde{\mathscr{C}}\}$. By projection this gives the usual scalar product on R^ℓ and the image $\varphi(\tilde{\mathscr{C}}^{\star})$ is the algebraic dual $\mathscr{C}^{\star} = \{u \in R^\ell : \langle u, c\rangle = 0 \text{ for all } c \in \mathscr{C}\}$. Note that this is not the usual

dual code $\mathscr{C}^{\perp}$, which will be discussed presently. The algebraic dual is characterised by the following theorem.

Theorem 3.1. *The rows of $\tilde{A}^{\mathrm{T}}$ form an rPOT reduced Gröbner basis for $\tilde{\mathscr{C}}^{\star}_{\tilde{\mathscr{K}}}$.*

Proof. One direction is clear from the equation $\tilde{G}\tilde{A} = (x^m - 1)I$. Now suppose that $u = (u_1, \ldots, u_\ell) \in \tilde{\mathscr{C}}^{\star}$, that is, $\tilde{G}u^{\mathrm{T}} \in \tilde{\mathscr{K}}$. Then $u_\ell g_{\ell\,\ell}$ is divisible by $x^m - 1$ so u_ℓ is a multiple of $a_{\ell\,\ell}$. Thus, there is a v_ℓ such that $u - v_\ell a_\ell^{\mathrm{T}}$ has last component 0 and lies in $\tilde{\mathscr{C}}^{\star}$. Suppose that $u' = u - \sum_{i=\ell}^{\ell-j+1} v_i a_i^{\mathrm{T}} \in \tilde{\mathscr{C}}^{\star}$ has last $j-1$ components 0. Then $u'_{\ell-j} g_{\ell-j,\ell-j}$ is divisible by $x^m - 1$ so $u'_{\ell-j}$ is a multiple of $a_{\ell-j,\ell-j}$. Subtracting a multiple of $a_{\ell-j}^{\mathrm{T}}$ we may remove the $(\ell - j)$th component of u', leaving a residual vector in $\tilde{\mathscr{C}}^{\star}$. By induction, u may be reduced to 0 by $\{a_i^{\mathrm{T}}, i = 1, \ldots, \ell\}$ and the theorem follows. □

As a consequence we have

Corollary 3.2. *The dimension of $\mathscr{C}^{\star}$ is $\sum_{i=1}^{\ell}(m - \partial a_{ii}) = \sum_{i=1}^{\ell}(m - (m - \partial g_{ii})) = \sum_{i=1}^{\ell} \partial g_{ii}$, and this is also the codimension of $\mathscr{C}$. Thus* $\dim \mathscr{C}^{\star} = \ell m - \dim \mathscr{C}$.

Example 3.3. From Example 2.8 the mod-$\tilde{\mathscr{K}}$-dual $(\tilde{\mathscr{C}}_1)^{\star}_{\tilde{\mathscr{K}}}$ has rPOT-reduced Gröbner basis consisting of the rows of

$$\begin{pmatrix} f_1 f_3 & 0 & 0 \\ f_1^3 & f_1 f_2 & 0 \\ 1 & f_1 & 1 \end{pmatrix}.$$

The dimension is $(7-4)+(7-4)+(7-0) = 13$ which is equal to $21-8$ as expected. The primary decomposition of $\mathscr{C}_1^{\star}$ is

$$f_1 f_2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & f_1 & 1 \end{pmatrix} \oplus f_1 f_3 \begin{pmatrix} 1 & 0 & 0 \\ 0 & f_1 & 1 \end{pmatrix} \oplus f_2 f_3 \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}$$

respectively. The component submodules have dimensions $6, 6, 1$.

We now wish to find a generator matrix for the dual code $\mathscr{C}^{\perp}$ and a corresponding GB generating set. It is convenient to adopt the notation $[a]$ for the $m \times m$ circulant matrix whose first row is the sequence of coefficients $\{a_0, \ldots, a_{m-1}\}$ of the polynomial $a(x) \bmod x^m - 1$. The isomorphism between the algebra of circulant matrices and R implies that for two polynomials a, b the congruence $ab \equiv 0 \bmod x^m - 1$ corresponds to the matrix equation $[a][b] = 0$. This means that the rows of $[b]^{\mathrm{T}}$ are orthogonal (for the scalar product over F) to the rows of $[a]$. Now, if $b = \beta_0 + \beta_1 x + \cdots + \beta_{m-1} x^{m-1}$ then $[b]^{\mathrm{T}}$ has first row $(\beta_0, \beta_{m-1}, \ldots, \beta_1)$ so it corresponds to the polynomial $\hat{b} = \beta_0 + \beta_{m-1} x + \cdots + \beta_1 x^{m-1}$, that is, $[b]^{\mathrm{T}} = [\hat{b}]$. Also, using $f \sim g$ to indicate that the polynomial f is a constant multiple of g, $x^{\partial b}\hat{b} \bmod x^m - 1 \sim b^{\star} = x^{\partial b} b(x^{-1})$, the conventional "reciprocal" of b, so that the rows of $[b^{\star}]$ are a cyclic permutation of those of $[\hat{b}]$.

If $\sum_{i=1}^{\ell} a_i b_i \in \tilde{\mathscr{K}}$, for polynomials a_i, b_i, then the corresponding matrix equation is $([a_1]\,[a_2]\,\ldots\,[a_\ell])([b_1]\,[b_2]\,\ldots\,[b_\ell])^{\mathrm{T}} = 0$ and so the rows of $([\hat{b}_1]\,[\hat{b}_2]\,\ldots\,[\hat{b}_\ell])$ are orthogonal to those of $([a_1]\,[a_2]\,\ldots\,[a_\ell])$.

With these preparations, we can now determine a parity check matrix for $\mathscr{C}$. Denote by $[\tilde{A}], [\tilde{G}]$ the matrices over F derived from $\tilde{A}, \tilde{G}$ by replacing each entry by the corresponding circulant, and setting $[x^m - 1] = 0$ where necessary. This gives $[\tilde{A}][\tilde{G}] = [\tilde{G}][\tilde{A}] = 0$ and the rows of

$$[\tilde{A}]^{\mathrm{T}} = \begin{pmatrix} [a_{11}]^{\mathrm{T}} & 0 & \cdots & 0 \\ [a_{12}]^{\mathrm{T}} & [a_{22}]^{\mathrm{T}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ [a_{1\ell}]^{\mathrm{T}} & [a_{2\ell}]^{\mathrm{T}} & \cdots & [a_{\ell\ell}]^{\mathrm{T}} \end{pmatrix} = \begin{pmatrix} [\hat{a}_{11}] & 0 & \cdots & 0 \\ [\hat{a}_{12}] & [\hat{a}_{22}] & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ [\hat{a}_{1\ell}] & [\hat{a}_{2\ell}] & \cdots & [\hat{a}_{\ell\ell}] \end{pmatrix}$$

are in the dual code $\mathscr{C}^{\perp}$. We already know from Corollary 3.2 that the dimension of the code generated by the rows of $\tilde{A}^{\mathrm{T}}$ is $\ell m - \dim(\mathscr{C})$ and, since the rank of $[a_{ij}]$ is equal to that of $[a_{ij}]^{\mathrm{T}}$, it follows that the rank of $[\tilde{A}]^{\mathrm{T}}$ is $\ell m - \dim(\mathscr{C})$. This means that $[\tilde{A}]^{\mathrm{T}}$ is a parity check matrix for $\mathscr{C}$. However, the polynomial vectors corresponding to the rows of $[\tilde{A}]^{\mathrm{T}}$ do not form a Gröbner for $\mathscr{C}^{\perp}$, so instead we define the polynomial matrix $\tilde{H}$ whose (j,i) entry is $h_{ji} = x^{\partial a_{ii}} \hat{a}_{ji} \bmod x^m - 1$. The rows of $[\tilde{H}]$ are a permutation of those of $[\tilde{A}]^{\mathrm{T}}$ and hence $[\tilde{H}]$ also generates $\mathscr{C}^{\perp}$. Let P denote the permutation matrix that carries out this transformation and consider the relation $[\tilde{G}]^{\mathrm{T}} P^{-1} P [\tilde{A}]^{\mathrm{T}} = ([\tilde{G}]^{\mathrm{T}} P^{-1})[\tilde{H}] = 0$. The left-hand factor is derived from $[\tilde{G}]^{\mathrm{T}}$ by permuting its columns in the corresponding manner via P^{-1}. Replacing the circulant matrices in these factors by their polynomial equivalents we obtain

$$\begin{pmatrix} x^{-\partial a_{11}} \hat{g}_{11} & 0 & \cdots & 0 \\ x^{-\partial a_{11}} \hat{g}_{12} & x^{-\partial a_{22}} \hat{g}_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x^{-\partial a_{11}} \hat{g}_{1\ell} & x^{-\partial a_{22}} \hat{g}_{2\ell} & \cdots & x^{-\partial a_{\ell\ell}} \hat{g}_{\ell\ell} \end{pmatrix}, \begin{pmatrix} x^{\partial a_{11}} \hat{a}_{11} & 0 & \cdots & 0 \\ x^{\partial a_{22}} \hat{a}_{12} & x^{\partial a_{22}} \hat{a}_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x^{\partial a_{\ell\ell}} \hat{a}_{1\ell} & x^{\partial a_{\ell\ell}} \hat{a}_{2\ell} & \cdots & x^{\partial a_{\ell\ell}} \hat{a}_{\ell\ell} \end{pmatrix}$$

$$= \begin{pmatrix} g_{11}^{\star} & 0 & \cdots & 0 \\ x^{-\partial a_{11}} \hat{g}_{12} & g_{22}^{\star} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x^{-\partial a_{11}} \hat{g}_{1\ell} & x^{-\partial a_{22}} \hat{g}_{2\ell} & \cdots & g_{\ell\ell}^{\star} \end{pmatrix}, \begin{pmatrix} a_{11}^{\star} & 0 & \cdots & 0 \\ x^{\partial a_{22}} \hat{a}_{12} & a_{22}^{\star} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x^{\partial a_{\ell\ell}} \hat{a}_{1\ell} & x^{\partial a_{\ell\ell}} \hat{a}_{2\ell} & \cdots & a_{\ell\ell}^{\star} \end{pmatrix},$$

$$\equiv 0 \bmod x^m - 1$$

where each entry is interpreted modulo $x^m - 1$. It follows that this product is equal to a lower triangular matrix of the form

$$(x^m - 1) \begin{pmatrix} 1 & 0 & \cdots & 0 \\ m_{21} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ m_{\ell 1} & m_{\ell 2} & \cdots & 1 \end{pmatrix}.$$

This can be reduced to $(x^m - 1)I$ by a sequence of left multiplications by elementary matrices, none of which changes the diagonal entries. Carrying out the same sequence on the left-hand factor above gives a relation $\tilde{G}'\tilde{H} = (x^m - 1)I$ and applying the rPOT analogues of Theorem 2.2 and (7) gives the following result.

Theorem 3.4. *The rows of $\tilde{H}$ form an rPOT Gröbner (usually not reduced) for the preimage $\widetilde{\mathscr{C}^\perp}$ of $\mathscr{C}^\perp$ in $F[x]^\ell$. Redundant rows of the parity check matrix $[\tilde{H}]$ may be removed to form a parity check matrix with linearly independent rows by omitting all but the first $m - \partial a_{ii}$ rows in each block row.*

Example 3.5. The construction of a parity check matrix for $\mathscr{C}_1$ by this theorem begins with the matrix $\tilde{A}$ defined in Example 2.8, namely

$$\begin{pmatrix} (x+1)(x^3+x^2+1) & (x+1)^3 & 1 \\ 0 & (x+1)(x^3+x+1) & x+1 \\ 0 & 0 & 1 \end{pmatrix}$$

from which on transposing and replacing each entry a_{ij} by $\hat{a}_{ij}$ we obtain

$$\begin{pmatrix} x^6+x^5+x^3+1 & 0 & 0 \\ x^6+x^5+x^4+1 & x^5+x^4+x^3+1 & 0 \\ 1 & x^6+1 & 1 \end{pmatrix}.$$

Multiplying each row by the corresponding $x^{\partial a_{ii}}$ gives the rPOT Gröbner matrix

$$\begin{pmatrix} x^4+x^3+x^2+1 & 0 & 0 \\ x^4+x^3+x^2+x & x^4+x^2+x+1 & 0 \\ 1 & x^6+1 & 1 \end{pmatrix}$$

from which, on replacing each polynomial by the corresponding circulant and dropping the redundant rows, we obtain the parity check matrix

$$\begin{pmatrix} 1011100\ 0000000\ 0000000 \\ 0101110\ 0000000\ 0000000 \\ 0010111\ 0000000\ 0000000 \\ \\ 0111100\ 1110100\ 0000000 \\ 0011110\ 0111010\ 0000000 \\ 0001111\ 0011101\ 0000000 \\ \\ 1000000\ 1000001\ 1000000 \\ 0100000\ 1100000\ 0100000 \\ 0010000\ 0110000\ 0010000 \\ 0001000\ 0011000\ 0001000 \\ 0000100\ 0001100\ 0000100 \\ 0000010\ 0000110\ 0000010 \\ 0000001\ 0000011\ 0000001 \end{pmatrix}.$$

For the analysis of self-dual codes of index 2 in the following section it is convenient to have a formula, in the index 2 case, for the POT RGB generating set of the dual code $\mathscr{C}^{\perp}$ in terms of an rPOT GB generating set.

Theorem 3.6. *Let* $\{(a \quad 0),(b \quad c)\}$ *be any rPOT Gröbner of a submodule* $\tilde{\mathscr{D}}$ *of* $F[x]^2$. *Let* $ua + vb = d = \gcd(a,b)$, *where* v *is chosen so that* $\partial v < \partial(a/d)$. *Then* $\{(d \quad vc),(0 \quad a/dc)\}$ *is the POT-reduced Gröbner basis of* $\tilde{\mathscr{D}}$.

Proof. The transformations are as follows:

$$\begin{pmatrix} a & 0 \\ b & c \\ x^m-1 & 0 \\ 0 & x^m-1 \end{pmatrix} \to \begin{pmatrix} a & 0 \\ b & c \\ d & vc \\ 0 & x^m-1 \end{pmatrix} \to \begin{pmatrix} d & vc \\ 0 & c-\frac{b}{d}vc \\ 0 & \frac{a}{d}vc \\ 0 & x^m-1 \end{pmatrix}$$

$$\to \begin{pmatrix} d & vc \\ 0 & \frac{a}{d}uc \\ 0 & \frac{a}{d}vc \\ 0 & x^m-1 \end{pmatrix} \to \begin{pmatrix} d & vc \\ 0 & \frac{a}{d}c \end{pmatrix}.$$

These are straightforward apart from the last step. First, we use the fact that u, v are relatively prime. Second, the equation expressing $\tilde{\mathscr{K}} \subseteq \tilde{\mathscr{D}}$ is

$$\begin{pmatrix} u & 0 \\ v & w \end{pmatrix}\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} x^m-1 & 0 \\ 0 & x^m-1 \end{pmatrix}$$

from which $va + wb = 0, v(a/d) + w(b/d) = 0$ and hence (a/d) divides w. Thus $(a/d)c$ divides $wc = x^m - 1$. □

More generally, an rPOT Gröbner of a submodule of $F[x]^{\ell}$ can be converted into a POT Gröbner basis by a sequence of such transformations defined by 2×2 submatrices. If $\tilde{G}$ is the generator matrix of the rPOT Gröbner basis then we perform in succession the 2×2 transformations defined by the lower triangular submatrices indexed by

$$\begin{pmatrix} 11 & 12 \\ 21 & 22 \end{pmatrix}, \quad \begin{pmatrix} 11 & 13 \\ 31 & 33 \end{pmatrix}, \ldots, \begin{pmatrix} 11 & 1\ell \\ \ell 1 & \ell\ell \end{pmatrix}$$

and making the consequent changes in the corresponding rows and columns of $\tilde{G}$ at each step. The result is a matrix, with zeros in its first column apart from the $(1,1)$ position, such that the submatrix indexed by $(i,j), 2 \leqslant i,j \leqslant \ell$ remains lower triangular. The process continues with this submatrix and eventually gives a generator in upper triangular form.

4. Self-dual codes of index 2

In this section we classify completely the self-dual codes of index 2. We divide the irreducible factors $f_n, n \in N$ of $x^m - 1 = \prod_{n=1}^{s} f_n^{\varepsilon}$ into two types according to whether

or not $f_n^\star \sim f_n$. Let $I \subseteq N$ be the set of indices of irreducible factors having this property. The other irreducible factors then fall into reciprocal pairs. Let $J \subseteq N$ be a set of indices comprising one element of each of these pairs and define the map π from J to the complementary subset $N \setminus (I \cup J)$ by $f_j^\star = f_{\pi(j)}$. Throughout this section the subscripts i, j, n will be assumed to run through the set I, J, N without further comment. The factorisation of $x^m - 1$ may be expressed as

$$x^m - 1 \sim \prod f_i^{\varepsilon} \prod f_j^{\varepsilon} \prod f_{\pi(j)}^{\varepsilon},$$

where $f_i^\star \sim f_i$, $f_j^\star \sim f_{\pi(j)}, f_{\pi(j)}^\star \sim f_j$ and we note that $\partial f_{\pi(n)} = \partial f_n$. For convenience we denote the monic factor $c \prod f_i^{\alpha_i} \prod f_j^{\alpha_j} \prod f_{\pi(j)}^{\alpha_{\pi(j)}}$, where c is an appropriate constant, by the triple $[\alpha_i, \alpha_j, \alpha_{\pi(j)}]$. Throughout the following argument we will freely choose monic representatives without further mention. Now any code $\mathscr{C}$ of index 2 corresponds to a submodule $\tilde{\mathscr{C}} \subseteq F[x]^2$ with minimal Gröbner basis matrix

$$\tilde{G} = \begin{pmatrix} [\alpha_i, \alpha_j, \alpha_{\pi(j)}] & v[\beta_i, \beta_j, \beta_{\pi(j)}] \\ 0 & [\gamma_i, \gamma_j, \gamma_{\pi(j)}] \end{pmatrix}, \tag{8}$$

where v is relatively prime to $x^m - 1$. The divisibility condition derived by multiplying the first row by $(x^m - 1)/[\alpha_i, \alpha_j, \alpha_{\pi(j)}]$ implies

$$\gamma_n \leqslant \varepsilon - \alpha_n + \beta_n. \tag{9}$$

The complementary matrix $\tilde{A}$ is

$$\begin{pmatrix} [\varepsilon - \alpha_i, \varepsilon - \alpha_j, \varepsilon - \alpha_{\pi(j)}] & -v[\varepsilon - \alpha_i + \beta_i - \gamma_i, \varepsilon - \alpha_j + \beta_j - \gamma_j, \varepsilon - \alpha_{\pi(j)} + \beta_{\pi(j)} - \gamma_{\pi(j)}] \\ 0 & [\varepsilon - \gamma_i, \varepsilon - \gamma_j, \varepsilon - \gamma_{\pi(j)}] \end{pmatrix}.$$

Theorem 3.4 may be applied to show that $\widetilde{\mathscr{C}^\perp}$ has rPOT Gröbner matrix $\tilde{H}$ given by

$$\begin{pmatrix} [\varepsilon - \alpha_i, \varepsilon - \alpha_{\pi(j)}, \varepsilon - \alpha_j] & 0 \\ v'[\varepsilon - \alpha_i + \beta_i - \gamma_i, \varepsilon - \alpha_{\pi(j)} + \beta_{\pi(j)} - \gamma_{\pi(j)}, \varepsilon - \alpha_j + \beta_j - \gamma_j] & [\varepsilon - \gamma_i, \varepsilon - \gamma_{\pi(j)}, \varepsilon - \gamma_j] \end{pmatrix}, \tag{10}$$

where $v' = -x^r \hat{v}$ with r defined so as to compensate for the replacement of $\hat{f}_n$ by $f_n^\star$ in the $(2,1)$ entry. Explicitly, $r = \sum \partial f_n (\alpha_n - \beta_n)$ (where, of course, x^r is interpreted modulo $x^m - 1$). Note that v' is relatively prime to $x^m - 1$. Next, by applying Theorem 3.6 to $\tilde{H}$ (and in the notation used there) we obtain a matrix for the POT Gröbner basis of $\widetilde{\mathscr{C}^\perp}$ in the form

$$\tilde{L} = \begin{pmatrix} d & u[\varepsilon - \gamma_i, \varepsilon - \gamma_{\pi(j)}, \varepsilon - \gamma_j] \\ 0 & (a/d)[\varepsilon - \gamma_i, \varepsilon - \gamma_{\pi(j)}, \varepsilon - \gamma_j] \end{pmatrix}, \tag{11}$$

where for the moment we leave a, d unevaluated.

Now suppose that $\mathscr{C}$ is self-dual so that $\tilde{G}, \tilde{H}$ represent bases for the same space $\tilde{\mathscr{C}}$. Then there are (inverse) matrices E, F such that $E\tilde{G} = \tilde{H}, F\tilde{H} = \tilde{G}$. With $E = (e_{ij}), F = (f_{ij})$ we have the following consequences derived from divisibility conditions. From $E\tilde{G} = \tilde{H}$

(i) $2\alpha_i \leqslant \varepsilon, \alpha_j + \alpha_{\pi(j)} \leqslant \varepsilon$, $e_{11} = [\varepsilon - 2\alpha_i, \varepsilon - \alpha_j - \alpha_{\pi(j)}, \varepsilon - \alpha_j - \alpha_{\pi(j)}]$,

(ii) $2\alpha_i \leqslant \varepsilon + \beta_i - \gamma_i, \alpha_j + \alpha_{\pi(j)} \leqslant \varepsilon + \beta_j - \gamma_j, \alpha_j + \alpha_{\pi(j)} \leqslant \varepsilon + \beta_{\pi(j)} - \gamma_{\pi(j)}$, $e_{21} = v'[\varepsilon - 2\alpha_i + \beta_i - \gamma_i, \varepsilon - \alpha_j - \alpha_{\pi(j)} + \beta_{\pi(j)} - \gamma_{\pi(j)}, \varepsilon - \alpha_j - \alpha_{\pi(j)} + \beta_j - \gamma_j]$,

(iii) [using e_{11} from (i)] $e_{12} = -v[\varepsilon - 2\alpha_i + \beta_i - \gamma_i, \varepsilon - \alpha_j - \alpha_{\pi(j)} + \beta_j - \gamma_j, \varepsilon - \alpha_j - \alpha_{\pi(j)} + \beta_{\pi(j)} - \gamma_{\pi(j)}]$,

(iv) [using e_{21} from (ii)] $vv'[\varepsilon - 2\alpha_i + 2\beta_i - \gamma_i, \varepsilon - \alpha_j - \alpha_{\pi(j)} + \beta_j + \beta_{\pi(j)} - \gamma_{\pi(j)}, \varepsilon - \alpha_j - \alpha_{\pi(j)} + \beta_j + \beta_{\pi(j)} - \gamma_j] + e_{22}[\gamma_i, \gamma_j, \gamma_{\pi(j)}] = [\varepsilon - \gamma_i, \varepsilon - \gamma_{\pi(j)}, \varepsilon - \gamma_j]$.

Similarly, from $F\tilde{H} = \tilde{G}$

(v) $\varepsilon \leqslant 2\gamma_i, \varepsilon \leqslant \gamma_j + \gamma_{\pi(j)}$, $f_{22} = [2\gamma_i - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon]$,

(vi) $\varepsilon \leqslant \beta_i + \gamma_i, \varepsilon \leqslant \beta_j + \gamma_{\pi(j)}, \varepsilon \leqslant \beta_{\pi(j)} + \gamma_j$, $f_{12} = v[\beta_i + \gamma_i - \varepsilon, \beta_j + \gamma_{\pi(j)} - \varepsilon, \beta_{\pi(j)} + \gamma_j - \varepsilon]$,

(vii) [using f_{22} from (v)] $f_{21} = -v'[\beta_i + \gamma_i - \varepsilon, \beta_{\pi(j)} + \gamma_j - \varepsilon, \beta_j + \gamma_{\pi(j)} - \varepsilon]$,

(viii) [using f_{12} from (vi)] $f_{11}[\varepsilon - \alpha_i, \varepsilon - \alpha_{\pi(j)}, \varepsilon - \alpha_j] + vv'[2\beta_i - \alpha_i, \beta_j + \beta_{\pi(j)} - \alpha_{\pi(j)}, \beta_j + \beta_{\pi(j)} - \alpha_j] = [\alpha_i, \alpha_j, \alpha_{\pi(j)}]$.

Next, the diagonal entries of $\tilde{L}$ are equal to those of $\tilde{G}$ so

(ix) $d = [\alpha_i, \alpha_j, \alpha_{\pi(j)}]$, $(a/d)[\varepsilon - \gamma_i, \varepsilon - \gamma_{\pi(j)}, \varepsilon - \gamma_j] = [\varepsilon - \alpha_i - \alpha_i + \varepsilon - \gamma_i, \varepsilon - \alpha_{\pi(j)} - \alpha_j + \varepsilon - \gamma_{\pi(j)}, \varepsilon - \alpha_j - \alpha_{\pi(j)} + \varepsilon - \gamma_j] = [\gamma_i, \gamma_j, \gamma_{\pi(j)}]$, hence $\alpha_j + \gamma_i = \varepsilon, \alpha_j + \alpha_{\pi(j)} + \gamma_j + \gamma_{\pi(j)} = 2\varepsilon$.

It now follows that $\mathscr{C}$ has dimension m since

(x) $\dim \mathscr{C} = \sum \partial f_i(\alpha_i + \gamma_i) + \sum \partial f_j(\alpha_j + \alpha_{\pi(j)} + \gamma_j + \gamma_{\pi(j)}) = \sum \partial f_i(\varepsilon) + \sum \partial f_j(2\varepsilon) = m$.

From the conditions thus determined it follows that (iv) and (viii) may be divided through by their right-hand sides, and that the resulting equations are identical apart from the coefficients e_{22}, f_{11}, which are therefore equal. We write w for their common value in

(xi) $vv'[2\beta_i - 2\alpha_i, \beta_j + \beta_{\pi(j)} - \alpha_j - \alpha_{\pi(j)}, \beta_j + \beta_{\pi(j)} - \alpha_j - \alpha_{\pi(j)}] + w[2\gamma_i - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon] = [0, 0, 0]$.

We have now determined a set of necessary conditions on $\alpha_n, \beta_n, \gamma_n, v$ (contained in (i), (ii), (v), (vi), (ix), (xi)) for the structure of a minimal Gröbner basis of a self-dual code of index 2. Their sufficiency follows from the fact that if these conditions hold then the inverse matrices

$$E = \begin{pmatrix} [2\gamma_i - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon] & -v[\beta_i - \alpha_i, \beta_j + \gamma_{\pi(j)} - \varepsilon, \beta_{\pi(j)} + \gamma_j - \varepsilon] \\ v'[\beta_i - \alpha_i, \beta_{\pi(j)} + \gamma_j - \varepsilon, \beta_j + \gamma_{\pi(j)} - \varepsilon] & w \end{pmatrix}$$

$$F = \begin{pmatrix} w & v[\beta_i - \alpha_i, \beta_j + \gamma_{\pi(j)} - \varepsilon, \beta_{\pi(j)} + \gamma_j - \varepsilon] \\ -v'[\beta_i - \alpha_i, \beta_{\pi(j)} + \gamma_j - \varepsilon, \beta_j + \gamma_{\pi(j)} - \varepsilon] & [2\gamma_i - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon] \end{pmatrix}$$

are well defined, have determinant 1, and satisfy $E\tilde{G} = \tilde{H}, F\tilde{H} = \tilde{G}$, which implies that $\tilde{\mathscr{C}} = \tilde{\mathscr{C}}^{\perp}$. We have therefore proved the following characterisation.

Theorem 4.1. *The code $\mathscr{C}$ of index 2 is self-dual if and only if each minimal Gröbner basis of $\tilde{\mathscr{C}}$ has a generator matrix*

$$\begin{pmatrix} [\alpha_i, \alpha_j, \alpha_{\pi(j)}] & v[\beta_i, \beta_j\, \beta_{\pi(j)}] \\ 0 & [\gamma_i, \gamma_j, \gamma_{\pi(j)}] \end{pmatrix},$$

where

(a) $2\alpha_i \leqslant \varepsilon, \alpha_j + \alpha_{\pi(j)} \leqslant \varepsilon$,

(b) $2\alpha_i \leqslant \varepsilon + \beta_i - \gamma_i, \alpha_j + \alpha_{\pi(j)} \leqslant \varepsilon + \beta_j - \gamma_j, \alpha_j + \alpha_{\pi(j)} \leqslant \varepsilon + \beta_{\pi(j)} - \gamma_{\pi(j)}$,

(c) $\varepsilon \leqslant \beta_i + \gamma_i, \varepsilon \leqslant \beta_j + \gamma_{\pi(j)}, \varepsilon \leqslant \beta_{\pi(j)} + \gamma_j$,

(d) $\alpha_i + \gamma_i = \varepsilon, \alpha_j + \alpha_{\pi(j)} + \gamma_j + \gamma_{\pi(j)} = 2\varepsilon$,

(e) $vv'[2\beta_i - 2\alpha_i, \beta_j + \beta_{\pi(j)} - \alpha_j - \alpha_{\pi(j)}, \beta_j + \beta_{\pi(j)} - \alpha_j - \alpha_{\pi(j)}] \equiv 1 \bmod [2\gamma_i - \alpha_i, \gamma_j + \gamma_{\pi(j)} - \varepsilon, \gamma_j + \gamma_{\pi(j)} - \varepsilon]$, *where* $v' = -x^r \hat{v}, r = \sum_i \partial f_i(\alpha_i - \beta_i) + \sum_j \partial f_j(\alpha_j + \alpha_{\pi(j)} - \beta_j - \beta_{\pi(j)})$.

In the special case $[\gamma_i, \gamma_j, \gamma_{\pi(j)}] = x^m - 1$ *the reduced Gröbner basis generating set of* $\mathscr{C}$ *is* $(1\ v)$ *where* $v\hat{v} \equiv -1 \bmod x^m - 1$ *and* $\partial v < m$.

References

[1] W.W. Adams, P. Loustaunau, in: An Introduction to Gröbner Bases, Graduate Studies in Mathematics, Vol. 3, American Mathematical Society, Providence, RI, 1994.

[2] T. Becker, V. Weispfenning, Gröbner Bases: A Computational Approach to Commutative Algebra, Graduate Texts in Mathematics, Springer, New York, 1993.

[3] C.L. Chen, W.W. Peterson, E.J. Weldon Jr., Some results on quasi-cyclic Codes, Inform and Control 15 (1969) 407–423.

[4] J. Conan, G. Séguin, Structural properties and enumeration of quasicyclic codes, Appl. Algebra Eng. Comm. Comput. 4 (1993) 25–39.

[5] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Undergraduate Texts in Mathematics, Springer, New York, 1992.

[6] P. Fitzpatrick, On the key equation, IEEE Trans. Inform. Theory 41 (1995) 1290–1302.

[7] P. Fitzpatrick, On the scalar rational interpolation problem, Math. Control Signals Systems 9 (1996) 352–369.

[8] P. Fitzpatrick, Solving multivariable congruences by change of term order, J. Symbolic Comput. 24 (1997) 575–589.

[9] P. Fitzpatrick, J. Flynn, A Gröbner Basis technique for Padé approximation, J. Symbolic Comput. 13 (1992) 133–138.

[10] P.P. Greenhough, R. Hill, Optimal ternary quasi-cyclic codes, Des. Codes Cryptogr. 2 (1992) 81–91.

[11] T.A. Gulliver, V.K. Bhargava, Some best rate $1/p$ and rate $(1-p)/p$ systematic quasi-cyclic codes, IEEE Trans. Inform. Theory 37 (1991) 552–555.

[12] T.A. Gulliver, V.K. Bhargava, Nine good rate $(m-1)/pm$ quasi-cyclic codes, IEEE Trans. Inform. Theory 38 (1992) 1366–1369.

[13] T.A. Gulliver, V.K. Bhargava, Some best rate $1/p$ and rate $(1-p)/p$ systematic quasi-cyclic codes over GF(3) and GF(4), IEEE Trans. Inform. Theory 38 (1992) 1369–1374.

[14] T.A. Gulliver, V.K. Bhargava, Twelve good rate $(m-r)/pm$ quasi-cyclic codes, IEEE Trans. Inform. Theory 39 (1993) 1750–1751.

[15] T.A. Gulliver, V.K. Bhargava, A (105,10,47) binary quasi-cyclic code, Appl. Math. Lett. 8 (1995) 67–70.

[16] T.A. Gulliver, V.K. Bhargava, New good rate $(m-1)/pm$ ternary and quaternary quasi-cyclic codes, Des. Codes Cryptogr. 7 (1996) 223–234.

[17] B. Hartley, T.O. Hawkes, Rings, Modules and Linear Algebra, Chapman & Hall Mathematics Series, Cambridge University Press, Cambridge, 1970.

[18] M. Karlin, New binary coding results by circulants, IEEE Trans. Inform. Theory 15 (1969) 81–92.

[19] M. Karlin, Decoding of circulant codes, IEEE Trans. Inform. Theory 16 (1970) 797–802.

[20] T. Kasami, A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2, IEEE Trans. Inform. Theory 20 (1974) 679.

[21] K. Lally, P. Fitzpatrick, Construction and classification of quasicyclic codes, Proceedings of the Workshop on Coding and Cryptography, INRIA, Paris, January 1999, pp. 11–20.

[22] J. Little, K. Saints, C. Heegard, On the structure of Hermitian codes, J. Pure Appl. Algebra 121 (1997) 293–314.
[23] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.
[24] W.W. Peterson, E.J. Weldon Jr., Error-Correcting Codes, 2nd Edition, MIT Press, Cambridge, MA, 1972.
[25] J. Rosenthal, J.M. Schumacher, E.V. York, On behaviors and convolutional codes, IEEE Trans. Inform. Theory 42 (1996) 1881–1891.
[26] G.E. Séguin, G. Drolet, The theory of 1-generator quasi-cyclic codes, Dept. of Electrical and Computer Engineering, Royal Military College of Canada, Kingston, Ontario, June 1990.
[27] G.E. Séguin, G. Drolet, The trace description of irreducible quasi-cyclic codes, IEEE Trans. Inform . Theory 36 (1990) 1463–1466.
[28] G.E. Séguin, H.T. Huynh, Quasi-cyclic codes – a study, Report published by Laboratoire de Radiocommunications et de Traitement du Signal, Université Laval, Québec, Canada, 1985.
[29] I. Siap, N. Aydin, D. Ray-Chaudhuri, New ternary QC codes and improvements on minimum distance, preprint 1999.
[30] G. Solomon, H.C.A. van Tilborg, A connection between block and convolutional codes, SIAM J. Appl. Math. 37 (1979) 358–369.
[31] R.M. Tanner, A transform theory for a class of group invariant codes, IEEE Trans. Inform. Theory 34 (1988) 752–775.
[32] R.L. Townsend, E.J. Weldon Jr., Self-orthogonal quasi-cyclic codes, IEEE Trans. Inform. Theory 13 (1967) 183–195.
[33] H.C.A van Tilborg, On quasi-cyclic codes with rate $1/m$, IEEE Trans. Inform. Theory 24 (1978) 628–630.