



Construction of Quasi-Cyclic Product Codes

Alexander Zeh, San Ling

► **To cite this version:**

Alexander Zeh, San Ling. Construction of Quasi-Cyclic Product Codes. 10th International ITG Conference on Systems, Communications and Coding (SCC), Feb 2015, Hamburg, Germany. <hal-01109353v2>

HAL Id: hal-01109353

<https://hal.inria.fr/hal-01109353v2>

Submitted on 26 Jan 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Construction of Quasi-Cyclic Product Codes

Alexander Zeh

Computer Science Department
Technion—Israel Institute of Technology
Haifa, Israel
alex@codingtheory.eu

San Ling

Division of Mathematical Sciences, School of Physical &
Mathematical Sciences, Nanyang Technological University
Singapore, Republic of Singapore
lingsan@ntu.edu.sg

Abstract—Linear quasi-cyclic product codes over finite fields are investigated. Given the generating set in the form of a reduced Gröbner basis of a quasi-cyclic component code and the generator polynomial of a second cyclic component code, an explicit expression of the basis of the generating set of the quasi-cyclic product code is given. Furthermore, the reduced Gröbner basis of a one-level quasi-cyclic product code is derived.

Index Terms—Cyclic code, Gröbner basis, module minimization, product code, quasi-cyclic code, submodule

I. INTRODUCTION

A linear block code of length ℓm over a finite field \mathbb{F}_q is a quasi-cyclic code if every cyclic shift of a codeword by ℓ positions, for some integer ℓ between one and ℓm , results in another codeword. Quasi-cyclic codes are a natural generalization of cyclic codes (where $\ell = 1$), and have a closely linked algebraic structure. In contrast to cyclic codes, quasi-cyclic codes are known to be asymptotically good (see Chen–Peterson–Weldon [1]). Several such codes have been discovered with the highest minimum distance for a given length and dimension (see Gulliver–Bhargava [2] as well as Chen’s and Grassl’s databases [3], [4]). Several good LDPC codes are quasi-cyclic (see e.g. [5]) and the connection to convolutional codes was investigated among others in [6]–[8].

Recent papers of Barbier *et al.* [9], [10], Lally–Fitzpatrick [8], [11], [12], Ling–Solé [13]–[15], Semenov–Trifonov [16], Güneri–Özbudak [17] and ours [18] discuss different aspects of the algebraic structure of quasi-cyclic codes including lower bounds on the minimum Hamming distance and efficient decoding algorithms.

The focus of this paper is on a simple method to combine two given quasi-cyclic codes into a product code. More specifically, we give a description of a quasi-cyclic product code when one component code is quasi-cyclic and the second one is cyclic.

The work of Wasan [19] first considers quasi-cyclic product codes while investigating the mathematical properties of the wider class of quasi-abelian codes. Some more results were published in a short note by Wasan and Dass [20]. Koshy proposed a so-called “circle” quasi-cyclic product codes in [21].

Our work considers quasi-cyclic product codes that generalize the results of Burton–Weldon [22] and Lin–Weldon [23]

(see also [24, Chapter 18]) based on the reduced Gröbner basis representation of Lally–Fitzpatrick [11] of the quasi-cyclic component code. We derive a representation of the generating set of a quasi-cyclic product code, where one component code is quasi-cyclic and the other is cyclic (in Thm. 7) and we give a reduced Gröbner basis for the special class of one-level quasi-cyclic product codes (in Thm. 8).

The paper is structured as follows. In Section II, we give necessary preliminaries on quasi-cyclic codes over finite fields. We outline relevant basics of the reduced Gröbner basis representation of Lally–Fitzpatrick [11]. Furthermore, the special class of r -level quasi-cyclic codes is defined in this section. Section III contains the main result on quasi-cyclic product codes, where the row-code is quasi-cyclic and the column-code is cyclic. Moreover, an explicit expression of the basis of a 1-level quasi-cyclic product code is derived in Section III. For illustration, we explicitly give an example of a binary 2-quasi-cyclic product code in Section IV. Section V concludes this paper.

II. PRELIMINARIES

Let \mathbb{F}_q denote the finite field of order q and $\mathbb{F}_q[X]$ the polynomial ring over \mathbb{F}_q with indeterminate X . Let a, b with $b > a$ be two positive integers and denote by $[a, b)$ the set of integers $\{a, a + 1, \dots, b - 1\}$ and by $[b) = [0, b)$. A vector of length n is denoted by a lowercase bold letter as $\mathbf{v} = (v_0 \ v_1 \ \dots \ v_{n-1})$ and an $m \times n$ matrix is denoted by a capital bold letter as $\mathbf{M} = (m_{i,j})_{i \in [m], j \in [n]}$.

A linear $[\ell \cdot m, k, d]_q$ code \mathcal{C} of length ℓm , dimension k and minimum Hamming distance d over \mathbb{F}_q is ℓ -quasi-cyclic if every cyclic shift by ℓ of a codeword is again a codeword of \mathcal{C} , more explicitly if:

$$\begin{aligned} (c_{0,0} \cdots c_{\ell-1,0} \quad c_{0,1} \cdots c_{\ell-1,1} \quad \dots \quad c_{\ell-1,m-1}) &\in \mathcal{C} \\ \Rightarrow \\ (c_{0,m-1} \cdots c_{\ell-1,m-1} \quad c_{0,0} \cdots c_{\ell-1,0} \quad \dots \quad c_{\ell-1,m-2}) &\in \mathcal{C}. \end{aligned}$$

We can represent a codeword of an $[\ell \cdot m, k, d]_q$ ℓ -quasi-cyclic code as $\mathbf{c}(X) = (c_0(X) \ c_1(X) \ \dots \ c_{\ell-1}(X)) \in \mathbb{F}_q[X]^\ell$, where

$$c_i(X) \stackrel{\text{def}}{=} \sum_{j=0}^{m-1} c_{i,j} X^j, \quad \forall i \in [\ell]. \quad (1)$$

Then, the defining property of \mathcal{C} is that each component $c_i(X)$ of $\mathbf{c}(X)$ is closed under multiplication by X and reduction modulo $X^m - 1$.

A. Zeh has been supported by the German research council (Deutsche Forschungsgemeinschaft, DFG) under grant Ze1016/1-1. S. Ling has been supported by NTU Research Grant M4080456.

Lemma 1. Let $(c_0(X) \ c_1(X) \ \cdots \ c_{\ell-1}(X))$ be a codeword of an ℓ -quasi-cyclic code \mathcal{C} of length $m\ell$, where the components are defined as in (1). Then a codeword in \mathcal{C} represented as one univariate polynomial of degree smaller than $m\ell$ is

$$c(X) = \sum_{i=0}^{\ell-1} c_i(X^\ell)X^i. \quad (2)$$

Proof. Substitute (1) into (2):

$$c(X) = \sum_{i=0}^{\ell-1} c_i(X^\ell)X^i = \sum_{i=0}^{\ell-1} \sum_{j=0}^{m-1} c_{i,j}X^{j\ell+i}.$$

□

Lally and Fitzpatrick [11], [25] showed that this enables us to see a quasi-cyclic code as an R -submodule of the algebra R^ℓ , where $R = \mathbb{F}_q[X]/\langle X^m - 1 \rangle$. The code \mathcal{C} is the image of an $\mathbb{F}_q[X]$ -submodule $\tilde{\mathcal{C}}$ of $\mathbb{F}_q[X]^\ell$ containing $\tilde{K} = \langle (X^m - 1)\mathbf{e}_j, j \in [\ell] \rangle$ (where \mathbf{e}_j is the standard basis vector with one in position j and zero elsewhere) under the natural homomorphism

$$\begin{aligned} \phi: \mathbb{F}_q[X]^\ell &\rightarrow R^\ell \\ (c_0(X) \ \cdots \ c_{\ell-1}(X)) &\mapsto (c_0(X) + \langle X^m - 1 \rangle \ \cdots \\ &\quad c_{\ell-1}(X) + \langle X^m - 1 \rangle). \end{aligned}$$

It has a generating set of the form $\{\mathbf{a}_i, i \in [z], (X^m - 1)\mathbf{e}_j, j \in [\ell]\}$, where $\mathbf{a}_i \in \mathbb{F}_q[X]^\ell$ and $z \leq \ell$ (see e.g. [26, Chapter 5] for further information). Therefore, its generating set can be represented as a matrix with entries in $\mathbb{F}_q[X]$:

$$\mathbf{M}(X) = \begin{pmatrix} a_{0,0}(X) & a_{0,1}(X) & \cdots & a_{0,\ell-1}(X) \\ a_{1,0}(X) & a_{1,1}(X) & \cdots & a_{1,\ell-1}(X) \\ \vdots & \vdots & \ddots & \vdots \\ a_{z-1,0}(X) & a_{z-1,1}(X) & \cdots & a_{z-1,\ell-1}(X) \\ X^m - 1 & & & \mathbf{0} \\ & X^m - 1 & & \mathbf{0} \\ & \mathbf{0} & \ddots & \\ & & & X^m - 1 \end{pmatrix}. \quad (3)$$

Every matrix $\mathbf{M}(X)$ as in (3) of the preimage $\tilde{\mathcal{C}}$ can be transformed into a reduced Gröbner basis (RGB) with respect to the position-over-term order (POT) in $\mathbb{F}_q[X]^\ell$ (see [11], [25]). This basis can be represented in the form of an upper-triangular $\ell \times \ell$ matrix with entries in $\mathbb{F}_q[X]$ as follows:

$$\mathbf{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) & \cdots & g_{0,\ell-1}(X) \\ & g_{1,1}(X) & \cdots & g_{1,\ell-1}(X) \\ & \mathbf{0} & \ddots & \vdots \\ & & & g_{\ell-1,\ell-1}(X) \end{pmatrix}, \quad (4)$$

where the following conditions must be fulfilled:

- 1) $g_{i,j}(X) = 0, \quad \forall 0 \leq j < i < \ell,$
- 2) $\deg g_{j,i}(X) < \deg g_{i,i}(X), \quad \forall j < i, i \in [\ell],$
- 3) $g_{i,i}(X) \mid (X^m - 1), \quad \forall i \in [\ell],$
- 4) if $g_{i,i}(X) = X^m - 1$ then $g_{i,j}(X) = 0, \quad \forall j \in [i + 1, \ell].$

The rows of $\mathbf{G}(X)$ with $g_{i,i}(X) \neq X^m - 1$ (i.e., the rows that do not map to zero under ϕ) are called the reduced generating set of the quasi-cyclic code \mathcal{C} . A codeword of \mathcal{C} can be represented as $\mathbf{c}(X) = \mathbf{i}(X)\mathbf{G}(X)$ and it follows that $k = m\ell - \sum_{i=0}^{\ell-1} \deg g_{i,i}(X)$. Let us recall the following definition (see also [25, Thm. 3.2]).

Definition 2 (*r*-level Quasi-Cyclic Code). We call an ℓ -quasi-cyclic code \mathcal{C} of length ℓm an *r*-level quasi-cyclic code if there is an index $r \in [\ell]$ for which the RGB/POT matrix as defined in (4) is such that $g_{r-1,r-1}(X) \neq X^m - 1$ and $g_{r,r}(X) = \cdots = g_{\ell-1,\ell-1}(X) = X^m - 1$.

We recall [25, Corollary 3.3] for the case of a 1-level quasi-cyclic code in the following.

Corollary 3 (1-level Quasi-Cyclic Code). The generator matrix in RGB/POT form of a 1-level ℓ -quasi-cyclic code \mathcal{C} of length ℓm is:

$$\mathbf{G}(X) = (g(X) \ g(X)f_1(X) \ \cdots \ g(X)f_{\ell-1}(X)),$$

where $g(X) \mid (X^m - 1)$ and $f_1(X), \dots, f_{\ell-1}(X) \in \mathbb{F}_q[X]$.

To describe quasi-cyclic codes explicitly, we need to recall the following facts of cyclic codes. A q -cyclotomic coset $M_m^{(i)}$ is defined as: $M_m^{(i)} \stackrel{\text{def}}{=} \{iq^j \bmod m \mid j \in [a]\}$, where a is the smallest positive integer such that $iq^a \equiv i \pmod{m}$. The minimal polynomial in $\mathbb{F}_q[X]$ of the element $\alpha^i \in \mathbb{F}_{q^r}$ is given by

$$m_m^{(i)}(X) = \prod_{j \in M_m^{(i)}} (X - \alpha^j). \quad (5)$$

The following fact is used in Section III.

Fact 4. Let four nonzero integers y, a, ℓ, m be such that

$$y \equiv a\ell \pmod{m\ell}$$

holds. Then $\ell \mid y$ and $y/\ell \equiv a \pmod{m}$.

III. QUASI-CYCLIC PRODUCT CODE

Throughout this section we consider a linear product code $\mathcal{A} \otimes \mathcal{B}$, where \mathcal{A} is the row-code and \mathcal{B} the column-code, respectively. Furthermore, w.l.o.g. let \mathcal{A} be an $[\ell \cdot m_A, k_A, d_A]_q$ ℓ -quasi-cyclic code with reduced Gröbner basis in POT form as defined in (4):

$$\mathbf{G}^A(X) = \begin{pmatrix} g_{0,0}^A(X) & g_{0,1}^A(X) & \cdots & g_{0,\ell-1}^A(X) \\ & g_{1,1}^A(X) & \cdots & g_{1,\ell-1}^A(X) \\ & \mathbf{0} & \ddots & \vdots \\ & & & g_{\ell-1,\ell-1}^A(X) \end{pmatrix}, \quad (6)$$

and let \mathcal{B} be an $[m_B, k_B, d_B]_q$ cyclic code with generator polynomial $g^B(X)$ of degree $m_B - k_B$.

Throughout the paper, we assume that $\gcd(\ell m_A, m_B) = 1$ and we furthermore assume that the two integers a and b are such that

$$a\ell m_A + b m_B = 1. \quad (7)$$

We recall the lemma of Wasan [19], that generalizes the result of Burton–Weldon [22, Theorem I] for cyclic product codes to

the case of an ℓ -quasi-cyclic product code of an ℓ -quasi-cyclic code \mathcal{A} and a cyclic code \mathcal{B} . A codeword of $\mathcal{A} \otimes \mathcal{B}$ represented as univariate polynomial $c(X)$ can then be obtained from the matrix representation $(m_{i,j})_{\substack{j \in [\ell m_A] \\ i \in [m_B]}}$ as follows:

$$c(X) \equiv \sum_{i=0}^{m_B-1} \sum_{j=0}^{\ell m_A-1} m_{i,j} X^{\mu(i,j)} \pmod{X^{\ell m_A m_B} - 1}, \quad (8)$$

where

$$\mu(i,j) \stackrel{\text{def}}{=} ialm_A + jbm_B \pmod{\ell m_A m_B}. \quad (9)$$

Lemma 5 (Mapping to a Univariate Polynomial [19]). *Let \mathcal{A} be an ℓ -quasi-cyclic code of length ℓm_A and let \mathcal{B} be a cyclic code of length m_B . The product code $\mathcal{A} \otimes \mathcal{B}$ is an ℓ -quasi-cyclic code of length $\ell m_A m_B$ if $\gcd(\ell m_A, m_B) = 1$.*

Proof. Let $(m_{i,j})_{\substack{j \in [\ell m_A] \\ i \in [m_B]}}$ be a codeword of the product code $\mathcal{A} \otimes \mathcal{B}$, where each row is a codeword of \mathcal{A} and each column is a codeword of \mathcal{B} . The entry $m_{i,j}$ is the coefficient $c_{\mu(i,j)}$ of the codeword $\sum_i c_i X^i$ as in (8). In order to prove that $\mathcal{A} \otimes \mathcal{B}$ is ℓ -quasi-cyclic it is sufficient to show that a shift by ℓ positions of a codeword serialized to a univariate polynomial by (9) of $\mathcal{A} \otimes \mathcal{B}$ is again a codeword of $\mathcal{A} \otimes \mathcal{B}$.

A shift by ℓ in each row and a shift by one each column clearly gives a codeword in $\mathcal{A} \otimes \mathcal{B}$, because \mathcal{A} is ℓ -quasi-cyclic and \mathcal{B} is cyclic. With

$$\begin{aligned} \mu(i+1, j+\ell) &\equiv (i+1)alm_A + (j+\ell)bm_B \pmod{\ell m_A m_B} \\ &\equiv ialm_A + jbm_B + \ell(alm_A + bm_B) \pmod{\ell m_A m_B} \\ &\equiv \mu(i, j) + \ell \pmod{\ell m_A m_B}, \end{aligned}$$

we obtain an ℓ -quasi-cyclic shift of the univariate codeword obtained by (8) and (9). \square

Instead of representing a codeword of $\mathcal{A} \otimes \mathcal{B}$ as one univariate polynomial as in (8), we want to represent it as ℓ univariate polynomials as defined in (1).

Lemma 6 (Mapping to ℓ Univariate Polynomials). *Let \mathcal{A} be an ℓ -quasi-cyclic code of length ℓm_A and let \mathcal{B} be a cyclic code of length m_B . Let the matrix $(m_{i,j})_{\substack{j \in [\ell m_A] \\ i \in [m_B]}}$ be a codeword of $\mathcal{A} \otimes \mathcal{B}$, where each row is in \mathcal{A} and each column is in \mathcal{B} . The ℓ univariate polynomials of the corresponding codeword $(c_0(X) \ c_1(X) \ \cdots \ c_{\ell-1}(X))$, where each component is defined as in (1), are given by:*

$$c_h(X) \equiv X^{h(-am_A)} \cdot \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j\ell+h} X^{\bar{\mu}(i,j)} \pmod{X^{\ell m_A m_B} - 1}, \quad \forall h \in [\ell], \quad (10)$$

where

$$\bar{\mu}(i,j) \equiv ialm_A + jbm_B \pmod{m_A m_B}. \quad (11)$$

Proof. From Fact 4 we have for the exponents in (10):

$$\begin{aligned} \bar{\mu}(i,j) + h(-am_A) &\equiv ialm_A + jbm_B \pmod{m_A m_B} \\ &\Leftrightarrow \\ &\ell(\bar{\mu}(i,j) + h(-am_A)) \\ &\equiv \ell(ialm_A + jbm_B + h(-am_A)) \pmod{\ell m_A m_B}. \end{aligned} \quad (12)$$

With $-alm_A = bm_B - 1$, we can rewrite (12):

$$\begin{aligned} \ell(\bar{\mu}(i,j) + h(-am_A)) &= \ell\bar{\mu}(i,j) + \ell h(-am_A) \\ &= \ell\bar{\mu}(i,j) + hbm_B - h, \end{aligned}$$

and this gives with $\bar{\mu}(i,j)$ as in (11) and $\mu(i,j)$ as in (9):

$$\begin{aligned} \ell\bar{\mu}(i,j) + hbm_B - h &\equiv \ell(ialm_A + jbm_B) + hbm_B - h \\ &\equiv \ell ialm_A + (j\ell + h)bm_B - h \pmod{\ell m_A m_B} \\ &= \mu(i, j\ell + h) - h. \end{aligned} \quad (13)$$

Inserting (13) in (2) of Lemma 1 leads to:

$$\begin{aligned} c(X) &= \sum_{h=0}^{\ell-1} c_h(X^\ell) X^h \\ &= \sum_{h=0}^{\ell-1} \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j\ell+h} X^{\mu(i,j\ell+h)} \\ &= \sum_{i=0}^{m_B-1} \sum_{j=0}^{\ell m_A-1} m_{i,j} X^{\mu(i,j)}, \end{aligned} \quad (14)$$

which equals (8). \square

The mapping $\bar{\mu}(i,j)$ from (11) of the ℓ submatrices $(m_{i,j\ell})_{\substack{j \in [m_A] \\ i \in [m_B]}}$, $(m_{i,j\ell+1})_{\substack{j \in [m_A] \\ i \in [m_B]}}$, \dots , $(m_{i,j\ell+\ell-1})_{\substack{j \in [m_A] \\ i \in [m_B]}}$ to the ℓ univariate polynomials $c_0(X), c_1(X), \dots, c_{\ell-1}(X)$ is the same as the one used to map the codeword of a cyclic product code from its matrix representation to a polynomial representation (see [22, Thm. 1]).

In Fig. III, we illustrate the $\mu(i,j)$ as in (9) for $a = 1$, $\ell = 2$, $m_A = 17$ and $b = -11$, $m_B = 3$. Subfigure 1(a) shows the values of $\mu(i,j)$. The two submatrices (m_{i,j_2}) and (m_{i,j_2+1}) for $i \in [3]$ and $j \in [17]$ are shown in Subfigure 1(b). Subfigure 1(c) contains the coefficients of the two univariate polynomials $c_0(X)$ and $c_1(X)$, where $(c_0(X) \ c_1(X))$ is a codeword of the 2-quasi-cyclic product code of length 102.

The following theorem gives the basis representation of a quasi-cyclic product code, where the row-code is quasi-cyclic and the column-code is cyclic.

Theorem 7 (Quasi-Cyclic Product Code). *Let \mathcal{A} be an $[\ell \cdot m_A, k_A, d_A]_q$ ℓ -quasi-cyclic code with generator matrix $\mathbf{G}^A(X) \in \mathbb{F}_q[X]^{\ell \times \ell}$ as in (6) and let \mathcal{B} be an $[m_B, k_B, d_B]_q$ cyclic code with generator polynomial $g^B(X) \in \mathbb{F}_q[X]$.*

Then the ℓ -quasi-cyclic product code $\mathcal{A} \otimes \mathcal{B}$ has a generating matrix of the following (unreduced) form:

$$\mathbf{G}(X) = \begin{pmatrix} \mathbf{G}^0(X) \\ \mathbf{G}^1(X) \end{pmatrix}, \quad (15)$$

0	69	36	3	72	39	6	75	42	9	78	45	12	81	48	15	84	51	18	87	54	21	90	57	24	93	60	27	96	63	30	99	66	33
68	35	2	71	38	5	74	41	8	77	44	11	80	47	14	83	50	17	86	53	20	89	56	23	92	59	26	95	62	29	98	65	32	101
34	1	70	37	4	73	40	7	76	43	10	79	46	13	82	49	16	85	52	19	88	55	22	91	58	25	94	61	28	97	64	31	100	67

(a) The $3 \times (2 \cdot 17)$ codeword matrix $(m_{i,j})$ of the 2-quasi-cyclic product code $\mathcal{A} \otimes \mathcal{B}$. Each entry contains the index of the coefficient c_i of the univariate polynomial $c(X) = \sum_{i=0}^{101} c_i X^i \in \mathcal{A} \otimes \mathcal{B}$.

0	36	72	6	42	78	12	48	84	18	54	90	24	60	96	30	66
68	2	38	74	8	44	80	14	50	86	20	56	92	26	62	98	32
34	70	4	40	76	10	46	82	16	52	88	22	58	94	28	64	100

69	3	39	75	9	45	81	15	51	87	21	57	93	27	63	99	33
35	71	5	41	77	11	47	83	17	53	89	23	59	95	29	65	101
1	37	73	7	43	79	13	49	85	19	55	91	25	61	97	31	67

(b) The two submatrices $(m_{i,2j})_{i \in [3]}^{j \in [17]}$ and $(m_{i,2j+1})_{i \in [3]}^{j \in [17]}$ with entries that are the coefficients of $c_0(X^2)$ and $Xc_1(X^2)$.

0	18	36	3	21	39	6	24	42	9	27	45	12	30	48	15	33
34	1	19	37	4	22	40	7	25	43	10	28	46	13	31	49	16
17	35	2	20	38	5	23	41	8	26	44	11	29	47	14	32	50

34	1	19	37	4	22	40	7	25	43	10	28	46	13	31	49	16
17	35	2	20	38	5	23	41	8	26	44	11	29	47	14	32	50
0	18	36	3	21	39	6	24	42	9	27	45	12	30	48	15	33

(c) The left submatrix contains the coefficients $c_{0,i}$ of the univariate polynomials $c_0(X)$ (the right one contains $c_{1,i}$ of $c_1(X)$, respectively).

Figure 1. Illustration of the mapping $\mu(i, j)$ (as defined in (9)) from a codeword of a quasi-cyclic product code represented as matrix to a polynomial representation. The product code $\mathcal{A} \otimes \mathcal{B}$ is 2-quasi-cyclic. The row-code \mathcal{A} is 2-quasi-cyclic and has length $\ell m_A = 2 \cdot 17$ and the column-code \mathcal{B} is cyclic and has length $m_B = 3$ (Subfigure 1(a), here $a = 1$ and $b = -11$). The mapping $\bar{\mu}(i, j)$ (as in (11)) to two univariate polynomials is illustrated in Subfigure 1(b) and Subfigure 1(c).

where

$$\mathbf{G}^0(X) = g^B(X^{a\ell m_A}).$$

$$\begin{pmatrix} g_{0,0}^A(X^{bm_B}) & g_{0,1}^A(X^{bm_B}) & \cdots & g_{0,\ell-1}^A(X^{bm_B}) \\ & g_{1,1}^A(X^{bm_B}) & \cdots & g_{1,\ell-1}^A(X^{bm_B}) \\ & & \ddots & \vdots \\ & & & g_{\ell-1,\ell-1}^A(X^{bm_B}) \end{pmatrix},$$

$$\cdot \text{diag}(1, X^{-am_A}, X^{-2am_A}, \dots, X^{-(\ell-1)am_A}) \quad (16)$$

and

$$\mathbf{G}^1(X) = (X^{m_A m_B} - 1) \mathbf{I}_\ell, \quad (17)$$

where \mathbf{I}_ℓ is the $\ell \times \ell$ identity matrix.

Proof. We first give an explicit expression for each component of a codeword $(c_0(X) \ c_1(X) \ \cdots \ c_{\ell-1}(X))$ in $\mathcal{A} \otimes \mathcal{B}$ depending on the components of a codeword $(a_0(X) \ a_1(X) \ \cdots \ a_{\ell-1}(X))$ of the row-code \mathcal{A} and depending the column-code \mathcal{B} based on the expression of Lemma 6. Let the $m_B \times \ell m_A$ matrix $(m_{i,j})$ be a codeword of the ℓ -quasi-cyclic product code $\mathcal{A} \otimes \mathcal{B}$ and let the polynomial

$$a_{i,h}(X) \stackrel{\text{def}}{=} \sum_{j=0}^{m_A-1} m_{i,j\ell+h} X^j, \quad \forall h \in [\ell], i \in [m_B] \quad (18)$$

denote the h th component of a codeword $(a_{i,0}(X) \ a_{i,1}(X) \ \cdots \ a_{i,\ell-1}(X))$ in \mathcal{A} in the i th row of the matrix $(m_{i,j})$. Denote a codeword $b_j(X)$ of \mathcal{B} in the j th column by

$$b_j(X) = \sum_{i=0}^{m_B-1} m_{i,j} X^i, \quad \forall j \in [\ell m_A], \quad (19)$$

respectively. From (10), we have for the h th component of a codeword of the product code $\mathcal{A} \otimes \mathcal{B}$:

$$c_h(X) \equiv X^{h(-am_A)} \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j\ell+h} X^{\bar{\mu}(i,j)} \pmod{X^{m_A m_B} - 1}, \quad \forall h \in [\ell], \quad (20)$$

and with $\bar{\mu}(i, j)$ as in (11) of Lemma 6 we can write (20) explicitly:

$$c_h(X) \equiv X^{h(-am_A)} \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j\ell+h} X^{ia\ell m_A + jbm_B} \pmod{X^{m_A m_B} - 1}, \quad \forall h \in [\ell]. \quad (21)$$

We define a shifted component:

$$\tilde{c}_h(X) \equiv c_h(X) X^{h(am_A)} \pmod{X^{m_A m_B} - 1}, \quad \forall h \in [\ell]. \quad (22)$$

Since

$$\begin{aligned} & \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j\ell+h} X^{ia\ell m_A + jbm_B} \\ &= \sum_{i=0}^{m_B-1} X^{ia\ell m_A} \sum_{j=0}^{m_A-1} m_{i,j\ell+h} X^{jbm_B} \\ &= \sum_{i=0}^{m_B-1} X^{ia\ell m_A} a_{i,h}(X^{bm_B}), \quad \forall h \in [\ell], \end{aligned}$$

and from (22) and in terms of the components of the row-code as defined in (18), we obtain:

$$\tilde{c}_h(X) = q_h(X) (X^{m_A m_B} - 1) + \sum_{i=0}^{m_B-1} X^{ia\ell m_A} a_{i,h}(X^{bm_B}), \quad \forall h \in [\ell], \quad (23)$$

for some $q_h(X) \in \mathbb{F}_q[X]$. Therefore $\tilde{c}_h(X)$ is a multiple of $\sum_{i=0}^h \epsilon_i(X) g_{i,h}^A(X^{bm_B})$ for some $\epsilon_i(X) \in \mathbb{F}_q[X]$. A codeword $b_j(X)$ in \mathcal{B} in the j th column of $(m_{i,j})$ is a multiple of $g^B(X)$ and we obtain:

$$\begin{aligned} & \sum_{i=0}^{m_B-1} \sum_{j=0}^{\ell m_A-1} m_{i,j} X^{ialm_A+jbm_B} \\ &= \sum_{j=0}^{\ell m_A-1} X^{jbm_B} \sum_{i=0}^{m_B-1} m_{i,j} X^{ialm_A} \\ &= \sum_{j=0}^{\ell m_A-1} X^{jbm_B} b_j(X^{al m_A}), \end{aligned}$$

and therefore $\tilde{c}_h(X)$ is a multiple of $g^B(X^{al m_A})$ modulo $X^{m_A m_B} - 1$.

Similar to the proof of [22, Thm. III], it can be shown that every shifted component $\tilde{c}_h(X)$ is a multiple of the product of $g^B(X^{al m_A})$ and $\sum_{i=0}^h \epsilon_i g_{i,h}^A(X^{bm_B})$ modulo $(X^{m_A m_B} - 1)$. Therefore, we can represent each codeword in $\mathcal{A} \otimes \mathcal{B}$ as:

$$\begin{aligned} & (c_0(X) \ c_1(X) \ \cdots \ c_{\ell-1}(X)) \\ &= (i_0(X) \ i_1(X) \ \cdots \ i_{\ell-1}(X)) \mathbf{G}(X), \end{aligned}$$

where $\mathbf{G}(X)$ is as in (15). \square

The following theorem gives the reduced Gröbner basis (as defined in (4)) representation of the quasi-cyclic product code from Thm. 7, where the row-code is a 1-level quasi-cyclic code.

Theorem 8 (1-Level Quasi-Cyclic Product Code). *Let \mathcal{A} be an $[\ell \cdot m_A, k_A, d_A]_q$ 1-level ℓ -quasi-cyclic code with generator matrix in RGB/POT form:*

$$\begin{aligned} & \mathbf{G}^A(X) \\ &= (g_{0,0}^A(X) \ g_{0,1}^A(X) \ \cdots \ g_{0,\ell-1}^A(X)) \\ &= (g^A(X) \ g^A(X) f_1^A(X) \ \cdots \ g^A(X) f_{\ell-1}^A(X)) \end{aligned} \quad (24)$$

as shown in Corollary 3. Let \mathcal{B} be an $[m_B, k_B, d_B]_q$ cyclic code with generator polynomial $g^B(X) \in \mathbb{F}_q[X]$.

Then a generator matrix of the 1-level ℓ -quasi-cyclic product code in RGB/POT form is:

$$\begin{aligned} \mathbf{G}(X) &= (g(X) \ g(X) f_1^A(X^{bm_B}) \ \cdots \ g(X) f_{\ell-1}^A(X^{bm_B})) \\ &\quad \cdot \text{diag}(1, X^{-am_A}, X^{-2am_A}, \dots, X^{-(\ell-1)am_A}), \end{aligned}$$

where

$$g(X) = \gcd(X^{m_A m_B} - 1, g^A(X^{bm_B}) g^B(X^{al m_A})). \quad (25)$$

Proof. Let two polynomials $u_0(X), v_0(X) \in \mathbb{F}_q[X]$ be such that:

$$\begin{aligned} g(X) &= u_0(X) g^A(X^{bm_B}) g^B(X^{al m_A}) \\ &\quad + v_0(X) (X^{m_A m_B} - 1). \end{aligned} \quad (26)$$

We show now how to reduce the basis representation to the RGB/POT form. We denote a new Row i by $R[i]'$. For ease of notation, we omit the term $\text{diag}(1, X^{-am_A}, X^{-2am_A}, \dots, X^{-(\ell-1)am_A})$ and denote by $Y = X^{bm_B}$ and $Z = X^{al m_A}$.

We write the basis of the submodule in unreduced form (as in (15)):

$$\begin{pmatrix} g^A(Y) g^B(Z) & g^A(Y) f_1^A(Y) g^B(Z) & \cdots \\ X^{m_A m_B} - 1 & & \\ & X^{m_A m_B} - 1 & \\ \mathbf{0} & & \ddots \end{pmatrix} \quad (27)$$

$$\begin{aligned} \rightarrow R[0]' &= u_0(X) R[0] + v_0(X) R[1] + v_0(X) f_1^A(Y) R[2] \\ &\quad + \cdots + v_0(X) f_{\ell-1}^A(Y) R[\ell] \end{aligned}$$

$$\begin{pmatrix} g(X) & g(X) f_1^A(Y) & \cdots \\ g^A(Y) g^B(Z) & g^A(Y) f_1^A(Y) g^B(Z) & \cdots \\ X^{m_A m_B} - 1 & & \\ & X^{m_A m_B} - 1 & \\ \mathbf{0} & & \ddots \end{pmatrix}, \quad (28)$$

where the i th entry in new row 0 was obtained using:

$$\begin{aligned} & u_0(X) g^A(Y) f_i^A(Y) g^B(Z) + v_0(X) f_i^A(Y) (X^{m_A m_B} - 1) \\ &= f_i^A(Y) (u_0(X) g^A(Y) g^B(Z) \\ &\quad + v_0(X) (X^{m_A m_B} - 1)), \end{aligned} \quad (29)$$

and with (26) we obtain from (29)

$$\begin{aligned} & f_i^A(Y) (u_0(X) g^A(Y) g^B(Z) + v_0(X) (X^{m_A m_B} - 1)) \\ &= f_i^A(Y) g(X). \end{aligned}$$

Clearly, $g(X)$ divides $g^A(Y) g^B(Z)$ and it is easy to check that Row 1 of the matrix in (28) can be obtained from Row 0 by multiplying by $g^A(Y) g^B(Z) / g(X)$. Therefore, we can omit the linearly dependent Row 1 in (28) and write the reduced basis as:

$$(g(X) \ g(X) f_1^A(X^{bm_B}) \ \cdots \ g(X) f_{\ell-1}^A(X^{bm_B})),$$

where we omitted the matrix $\text{diag}(1, X^{-am_A}, X^{-2am_A}, \dots, X^{-(\ell-1)am_A})$ for the first row during the proof, but it will only influence the row-operations by a factor. \square

Note that (25) is exactly the generator polynomial of a cyclic product code. A 1-level ℓ -quasi-cyclic product has rate greater than $(\ell - 1)/\ell$ and is therefore of high practical relevance. The explicit RGB/POT form of the 1-level quasi-cyclic product code as in Thm. 8 allows statements on the minimum distance and to develop decoding algorithms.

IV. EXAMPLE

We consider a 2-quasi-cyclic product code with the same parameters as the one illustrated in Fig. III. In this section we investigate a more explicit example to be able to calculate the basis as given in Thm. 8.

Let \mathcal{A} be a binary 2-quasi-cyclic code of length $\ell m_A = 2 \cdot 17 = 34$ and let \mathcal{B} be a cyclic code of length $m_B = 3$. We have $X^{17} - 1 = m_0^{(17)}(X) m_1^{(17)}(X) m_3^{(17)}(X)$, where the minimal polynomials are as defined in (5). Let the generator

matrix of \mathcal{A} in RGB/POT form as in (4) be $\mathbf{G}^A(X) = (g_{0,0}^A(X) \ g_{0,1}^A(X))$ where

$$\begin{aligned} g_{0,0}^A(X) &= m_1^{\langle 17 \rangle}(X) \\ &= X^8 + X^7 + X^6 + X^4 + X^2 + X + 1, \\ g_{0,1}^A(X) &= m_1^{\langle 17 \rangle}(X) \cdot m_0(X)^3 \cdot (X^3 + X^2 + 1) \\ &= X^{14} + X^{13} + X^{12} + X^{11} + X^8 + 1, \end{aligned}$$

and \mathcal{A} is a $[17 \cdot 2, 9, 11]_2$ 2-quasi-cyclic code. Let α be a 17th root of unity in $\mathbb{F}_{2^8}[X] \cong \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X^2 + 1)$. Let $g^B(X) = m_0^{\langle 3 \rangle}(X) = X + 1$ be the generator polynomial of the $[3, 2, 2]_2$ cyclic code \mathcal{B} and let $a = 1$ and $b = -11$ be such that (7) holds. We have

$$\begin{aligned} X^{51} - 1 &= m_0^{\langle 51 \rangle}(X) m_1^{\langle 51 \rangle}(X) m_3^{\langle 51 \rangle}(X) m_5^{\langle 51 \rangle}(X) m_9^{\langle 51 \rangle}(X) \\ &\quad m_{11}^{\langle 51 \rangle}(X) m_{17}^{\langle 51 \rangle}(X) m_{19}^{\langle 51 \rangle}(X). \end{aligned}$$

According to Thm. 8, we calculate

$$\begin{aligned} f_1^A(X^{-11 \cdot 3}) &\equiv f_{0,1}^A(X^{18}) = m_0(X^{18})^3 \cdot (X^{54} + X^{36} + 1) \\ &= (X^{18} + 1)^3 \cdot (X^{54} + X^{36} + 1) \\ &= X^{108} + X^{54} + X^{18} + 1 \\ &\equiv X^{18} + X^6 + X^3 + 1 \pmod{(X^{51} + 1)}, \end{aligned}$$

and we obtain the generator matrix $\mathbf{G}(X) = (g_{0,0}(X) \ g_{0,1}(X))$ of $\mathcal{A} \otimes \mathcal{B}$, where:

$$\begin{aligned} g_{0,0}(X) &= m_0^{\langle 51 \rangle}(X) m_1^{\langle 51 \rangle}(X) m_3^{\langle 51 \rangle}(X) m_9^{\langle 51 \rangle}(X) m_{19}^{\langle 51 \rangle}(X) \\ &= X^{33} + X^{32} + X^{30} + X^{27} + X^{25} + X^{23} + X^{20} \\ &\quad + X^{18} + X^{17} + X^{16} + X^{15} + X^{13} + X^{10} + X^8 \\ &\quad + X^6 + X^3 + X + 1. \end{aligned}$$

With Thm. 8, we obtain:

$$\begin{aligned} g_{0,1}(X) &\equiv a_1^A(X^{-11 \cdot 3}) g_{0,0}(X) \\ &\equiv X^{50} + X^{48} + X^{45} + X^{43} + X^{41} + X^{39} + X^{36} \\ &\quad + X^{34} + X^{32} + X^{29} + X^{27} + X^{26} + X^{25} + X^{23} \\ &\quad + X^{22} + X^{21} + X^{19} + X^{18} + X^{17} + X^{16} + X^{15} \\ &\quad + X^{14} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^6 \\ &\quad + X^4 + X \pmod{(X^{51} + 1)}. \end{aligned}$$

V. CONCLUSION AND OUTLOOK

Based on the RGB/POT representation of an ℓ -quasi-cyclic code \mathcal{A} and the generator polynomial of a cyclic code \mathcal{B} , a basis representation of the ℓ -quasi-cyclic product code $\mathcal{A} \otimes \mathcal{B}$ was proven. The reduced basis representation of the special case of a 1-generator quasi-cyclic product code was derived.

The general case of the basis representation of an $\ell_A \ell_B$ -quasi cyclic product code from an ℓ_A -quasi-cyclic code \mathcal{A} and an ℓ_B -quasi-cyclic code \mathcal{B} as well as the reduction of the basis remains an open future work. Furthermore, a technique to bound the minimum distance of a given quasi-cyclic code by embedding it into a product code similar to [27] seems to be realizable.

REFERENCES

- [1] C. L. Chen, W. W. Peterson, and E. J. Weldon Jr., "Some results on quasi-cyclic codes", *Inf. Control*, vol. 15, no. 5, pp. 407–423, 1969.
- [2] T. Gulliver and V. Bhargava, "Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes", *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 552–555, 1991.
- [3] E. Z. Chen, *A database on binary quasi-cyclic codes*, Online available at <http://moodle.tec.hkr.se/~chen/research/codes/qc.htm>, 2014.
- [4] M. Grassl, *Bounds on the Minimum Distance of Linear Codes and Quantum Codes*, Online available at <http://www.codetables.de>, 2014.
- [5] B. K. Butler and P. H. Siegel, "Bounds on the minimum distance of punctured quasi-cyclic LDPC codes", *IEEE Trans. Inform. Theory*, vol. 59, no. 7, pp. 4584–4597, 2013.
- [6] G. Solomon and H. C. A. v. Tilborg, "A connection between block and convolutional codes", *SIAM J. Appl. Math.*, vol. 37, no. 2, pp. 358–369, 1979.
- [7] M. Esmaeili, T. A. Gulliver, N. P. Secord, and S. A. Mahmoud, "A link between quasi-cyclic codes and convolutional codes", *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 431–435, 1998.
- [8] K. Lally, "Algebraic lower bounds on the free distance of convolutional codes", *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2101–2110, 2006.
- [9] M. Barbier, C. Chabot, and G. Quintin, "On quasi-cyclic codes as a generalization of cyclic codes", *Finite Fields Th. App.*, vol. 18, no. 5, pp. 904–919, 2012.
- [10] M. Barbier, G. Quintin, and C. Pernet, "On the decoding of quasi-BCH codes", *Intern. Workshop on Coding and Cryptography (WCC)*, Bergen, Norway, 2013.
- [11] K. Lally and P. Fitzpatrick, "Algebraic structure of quasicyclic codes", *Discrete Appl. Math.*, vol. 111, no. 1-2, pp. 157–175, 2001.
- [12] K. Lally, "Quasicyclic Codes of Index ℓ over F_q Viewed as $F_q[x]$ -Submodules of $F_q[x]/(x^m - 1)$ ", *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. Lecture Notes in Computer Science 2643, Springer Berlin Heidelberg, 2003, pp. 244–253.
- [13] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes i: finite fields", *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2751–2760, 2001.
- [14] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes II: chain rings", *Des. Codes Cryptogr.*, vol. 30, no. 1, pp. 113–130, 2003.
- [15] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes III: generator theory", *IEEE Trans. Inform. Theory*, vol. 51, no. 7, pp. 2692–2700, 2005.
- [16] P. Semenov and P. Trifonov, "Spectral method for quasi-cyclic code analysis", *IEEE Comm. Letters*, vol. 16, no. 11, pp. 1840–1843, 2012.
- [17] C. Güneri and F. Özbudak, "A bound on the minimum distance of quasi-cyclic codes", *SIAM J. Discrete Math.*, vol. 26, no. 4, pp. 1781–1796, 2012.
- [18] A. Zeh and S. Ling, "Decoding of quasi-cyclic codes up to a new lower bound on the minimum distance", *Intern. Symp. on Inf. Theory (ISIT)*, Honolulu, USA, 2014, pp. 2584–2588.
- [19] S. K. Wasan, "Quasi abelian codes", *Publications de l'Institut Mathématique*, no. 41, pp. 201–206, 1977.
- [20] B. K. Dass and S. K. Wasan, "A note on quasi-cyclic codes", *International Journal of Electronics*, vol. 54, no. 1, pp. 91–94, 1983.
- [21] T. Koshy, "Quasi-cyclic product codes", *Bulletin of Cal. Math. Soc.*, vol. 64, no. 2, pp. 83–90, 1972.
- [22] H. Burton and E. J. Weldon, "Cyclic product codes", *IEEE Trans. Inform. Theory*, vol. 11, no. 3, pp. 433–439, 1965.
- [23] S. Lin and E. J. Weldon, "Further results on cyclic product codes", *IEEE Trans. Inform. Theory*, vol. 16, no. 4, pp. 452–459, 1970.
- [24] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*. North Holland Publishing Co., 1988.
- [25] K. Lally and P. Fitzpatrick, "Construction and classification of quasi-cyclic codes", *Intern. Workshop on Coding and Cryptography (WCC)*, Paris, France, 1999, pp. 11–20.
- [26] D. A. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, Springer, 1998.
- [27] A. Zeh, A. Wachter-Zeh, and S. V. Bezzateev, "Decoding cyclic codes up to a new bound on the minimum distance", *IEEE Trans. Inform. Theory*, vol. 58, no. 6, pp. 3951–3960, 2012.