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. We can represent a codeword of a quasi-cyclic product code as (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 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 as (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 work of Wasan [19] first considers 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. Section V concludes this paper.

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.

I. INTRODUCTION

A linear block code of length ℓm over a finite field $\mathbb{F}_q$ is quasi-cyclic if every cyclic shift of a codeword by $\ell$ positions, for some integer $\ell$ between one and $\ell m$, 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 Grassi’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]. Koshe 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] 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 \(\ell\)-quasi-cyclic code \(C\) of length \(m\ell\), where the components are defined as in (1). Then a codeword in \(C\) represented as one univariate polynomial of degree smaller than \(m\ell\) is
\[
c(X) = \sum_{i=0}^{\ell-1} c_i(X^\ell)X^i.
\]

Proof: Substitute (1) into (2):
\[
c(X) = \sum_{i=0}^{\ell-1} c_i(X^\ell)X^i = \sum_{i=0}^{\ell-1} \sum_{j=0}^{m-1} c_{i,j}X^{j+i}.
\]

Lally and Fitzpatrick [11, 25] showed that this enables us to see a quasi-cyclic code as an \(R\)-submodule of the algebra \(R^\ell\), where \(R = \mathbb{F}_q[X]/(X^m - 1)\). The code \(C\) is the image of the \(\mathbb{F}_q[X]\)-submodule \(\mathcal{C}\) of \(\mathbb{F}_q[X]^\ell\) containing \(K = \langle (X^m - 1)e_j, j \in [\ell] \rangle\) (where \(e_j\) is the standard basis vector with one in position \(j\) and zero elsewhere) under the natural homomorphism
\[
\phi : \mathbb{F}_q[X]^\ell \to R^\ell
\]
\[
(c_0(X) \cdots c_{\ell-1}(X)) \mapsto (c_0(X) + (X^m-1) \cdots c_{\ell-1}(X) + (X^m-1)).
\]

It has a generating set of the form \(\{a_i, i \in [z], (X^m-1)e_j, j \in [\ell]\}\), where \(a_i \in \mathbb{F}_q[X]^\ell\) 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 \(\mathbb{F}_q[X]\):
\[
M(X) = \begin{pmatrix}
a_{0,0}(X) & a_{0,1}(X) & \cdots & a_{0,\ell-1}(X) \\
a_{1,0}(X) & a_{1,1}(X) & \cdots & a_{1,\ell-1}(X) \\
\vdots & \vdots & \ddots & \vdots \\
a_{z-1,0}(X) & a_{z-1,1}(X) & \cdots & a_{z-1,\ell-1}(X) \\
X^m - 1 & \cdots & \cdots & 0 \\
0 & \cdots & \cdots & X^m - 1
\end{pmatrix},
\]

Every matrix \(M(X)\) as in (3) of the preimage \(\mathcal{C}\) 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:
\[
G(X) = \begin{pmatrix}
g_{0,0}(X) & g_{0,1}(X) & \cdots & g_{0,\ell-1}(X) \\
g_{1,0}(X) & g_{1,1}(X) & \cdots & g_{1,\ell-1}(X) \\
\vdots & \vdots & \ddots & \vdots \\
g_{\ell-1,0}(X) & g_{\ell-1,1}(X) & \cdots & g_{\ell-1,\ell-1}(X) \\
0 & \cdots & \cdots & g_{\ell-1,\ell-1}(X)
\end{pmatrix},
\]

where the following conditions must be fulfilled:

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

The rows of \(G(X)\) with \(g_{i,i}(X) \neq X^m - 1\) (i.e., the rows that do not map to zero under \(\phi\)) are called the reduced generating set of the quasi-cyclic code \(C\). A codeword of \(C\) can be represented as \(c(X) = \mathbf{i}(X)G(X)\) 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 \((r\text{-level Quasi-Cyclic Code})\). We call an \(\ell\)-quasi-cyclic code \(C\) of length \(m\ell\) 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 \(g_{r,r}(X) = \cdots = g_{r-1,r-1}(X) = X^m - 1\).

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

Corollary 3 \((1\text{-level Quasi-Cyclic Code})\). The generator matrix in RGB/POT form of a 1-level \(\ell\)-quasi-cyclic code \(C\) of length \(m\ell\) is:
\[
G(X) = \begin{pmatrix}
g(X) & g(X)f_1(X) & \cdots & g(X)f_{\ell-1}(X)
\end{pmatrix},
\]

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

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: \(M_m^{(i)} = \{iq^j \mod m | j \in [a]\}\), where \(a\) is the smallest positive integer such that \(iq^j \equiv 1 \mod m\). The minimal polynomial in \(\mathbb{F}_q[X]\) of the element \(a^i \in \mathbb{F}_{q^r}\) is given by
\[
m_m^{(i)}(X) = \prod_{j \in M_m^{(i)}} (X - a^j).
\]

The following fact is used in Section III.

Fact 4. Let four nonzero integers \(y, a, \ell, m\) be such that
\[
y \equiv a\ell \mod m\ell
\]
holds. Then \(\ell \mid y\) and \(y/\ell \equiv a \mod m\).

III. QUASI-CYCLIC PRODUCT CODE

Throughout this section we consider a linear product code \(A \otimes B\), where \(A\) is the row-code and \(B\) the column-code, respectively. Furthermore, w.l.o.g. let \(A\) be an \([\ell \cdot m_A, k_A, d_A]_q\) \(\ell\)-quasi-cyclic code with reduced Gröbner basis in POT form as defined in (4):
\[
G_A(X) = \begin{pmatrix}
g_{0,0}(X) & g_{0,1}(X) & \cdots & g_{0,\ell-1}(X) \\
g_{1,0}(X) & g_{1,1}(X) & \cdots & g_{1,\ell-1}(X) \\
\vdots & \vdots & \ddots & \vdots \\
g_{\ell-1,0}(X) & g_{\ell-1,1}(X) & \cdots & g_{\ell-1,\ell-1}(X) \\
0 & \cdots & \cdots & 0
\end{pmatrix},
\]

and let \(B\) 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
\[
a\ell m_A + bm_B = 1.
\]

We recall the lemma of Wasan [19], that generalizes the result of Burton–Weldon [22, Theorem 1] for cyclic product codes to
the case of an \( \ell \)-quasi-cyclic product code of an \( \ell \)-quasi-cyclic code \( A \) and a cyclic code \( B \). A codeword of \( A \otimes B \) represented as univariate polynomial \( c(X) \) can then be obtained from the matrix representation \((m_{i,j})_{i \in \{m_A\}}\) as follows:

\[
c(X) = \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j} X^{\mu(i,j)} \mod X^{\ell m_A m_B} - 1, \tag{8}
\]

where

\[
\mu(i,j) \overset{\text{def}}{=} i a \ell m_A + j b m_B \mod \ell m_A m_B. \tag{9}
\]

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

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

A shift by \( \ell \) in each row and a shift by one each column clearly gives a codeword in \( A \otimes B \), because \( A \) is \( \ell \)-quasi-cyclic and \( B \) is cyclic. With

\[
\mu(i+1,j+\ell) \\
\equiv (i+1) a \ell m_A + (j+\ell) b m_B \mod \ell m_A m_B \\
\equiv i a \ell m_A + j b m_B + \ell (a \ell m_A + b m_B) \mod \ell m_A m_B \\
\equiv \mu(i,j) + \ell \mod \ell m_A m_B,
\]

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

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

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

\[
c_h(X) \equiv X^{h(-a m_A)} \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j} X^{\mu(i,j)} \mod X^{\ell m_A m_B} - 1, \quad \forall h \in [\ell], \tag{10}
\]

where

\[
\overline{c}(i,j) \equiv i a \ell m_A + j b m_B \mod m_A m_B. \tag{11}
\]

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

\[
\overline{c}(i,j) + h(-a m_A) \equiv i a \ell m_A + j b m_B \mod m_A m_B \\
\equiv \ell (\overline{c}(i,j) + h(-a m_A)) \mod \ell m_A m_B. \quad \tag{12}
\]

With \(-a \ell m_A = b m_B - 1\), we can rewrite (12):

\[
\ell (\overline{c}(i,j) + h(-a m_A)) = \ell (\overline{c}(i,j) + h(-a m_A)) \\
= \ell (\overline{c}(i,j) + b m_B - h) \\
\equiv \mu(i,j \ell + h) + b m_B - h. \quad \tag{13}
\]

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

\[
c(X) = \sum_{h=0}^{\ell-1} c_h(X^\ell) X^h \\
= \sum_{h=0}^{\ell-1} \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j} X^{\mu(i,j \ell + h)} \\
= \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j} X^{\mu(i,j)}, \quad \tag{14}
\]

which equals (8).

The mapping \( \overline{c}(i,j) \) from (11) of the \( \ell \) submatrices \((m_{i,j \ell})_{i \in \{m_A\}}, (m_{i,j \ell+1})_{i \in \{m_A\}}, \ldots, (m_{i,j \ell+\ell-1})_{i \in \{m_A\}}\) to the \( \ell \) univariate polynomials \( c_0(X), c_1(X), \ldots, c_{\ell-1}(X)\) 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 \( A \) be an \( [\ell \cdot m_A, k_A, d_A]_\ell \)-quasi-cyclic code with generator matrix \( G_A(X) \in F_q[X]^{\ell \times \ell} \) as in (6) and let \( B \) be an \( [m_B, k_B, d_B]_q \)-cyclic code with generator polynomial \( g_B(X) \in F_q[X] \).

Then the \( \ell \)-quasi-cyclic product code \( A \otimes B \) has a generating matrix of the following (reduced) form:

\[
G(X) = \left( G_A^0(X) \ G_A^1(X) \right). \tag{15}
\]
where

\[
G^0(X) = g^0(X^{a_{\ell m A}}),
\]

\[
\begin{pmatrix}
g^0_{A,0}(X^{b_{m B}}) & g^0_{A,1}(X^{b_{m B}}) & \cdots & g^0_{A,1}(X^{b_{m B}}) \\
g^0_{A,1}(X^{b_{m B}}) & g^0_{A,2}(X^{b_{m B}}) & \cdots & g^0_{A,2}(X^{b_{m B}}) \\
\vdots & \vdots & \ddots & \vdots \\
g^0_{A,\ell-1}(X^{b_{m B}}) & g^0_{A,\ell-1}(X^{b_{m B}}) & \cdots & g^0_{A,\ell-1}(X^{b_{m B}}) \\
0 & \cdots & \cdots & 0
\end{pmatrix},
\]

\[
\left. \text{diag}\left(1, X^{-a_{m A}}, X^{-2a_{m A}}, \ldots, X^{-(\ell-1)a_{m A}}\right) \right\}^{(16)}
\]

and

\[
G^1(X) = (X^{m_{A m B}} - 1)I_{\ell}, \quad (17)
\]

where \(I_{\ell}\) 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 \(A \otimes B\) depending on the components of a codeword \((a_0(X) \; a_1(X) \; \cdots \; a_{\ell-1}(X))\) of the row-code \(A\) and depending on the column-code \(B\) based on the expression of Lemma 6. Let the \(m_B \times \ell m_A\) matrix \((m_{i,j})\) be a codeword of the \(\ell\)-quasi-cyclic product code \(A \otimes B\) and let the polynomial

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

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

\[
c_h(X) \equiv X^{h(-a_{m A})} \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j+\ell h} X^{pi(i,j)} \mod X^{m_{A m B}} - 1, \quad \forall h \in [\ell], \quad (20)
\]

and with \(\pi(i,j)\) as in (11) of Lemma 6 we can write (20) explicitly:

\[
c_h(X) \equiv X^{h(-a_{m A})} \sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j+\ell h} X^{ia_{\ell m A} + j b_{m B}} \mod X^{m_{A m B}} - 1, \quad \forall h \in [\ell]. \quad (21)
\]

We define a shifted component:

\[
\bar{c}_h(X) \equiv c_h(X)X^{h(a_{m A})} \mod X^{m_{A m B}} - 1, \quad \forall h \in [\ell]. \quad (22)
\]

Since

\[
\sum_{i=0}^{m_B-1} \sum_{j=0}^{m_A-1} m_{i,j+\ell h} X^{ia_{\ell m A} + j b_{m B}} = \sum_{i=0}^{m_B-1} X^{ia_{\ell m A}} \sum_{j=0}^{m_A-1} m_{i,j+\ell h} X^{j b_{m B}}
\]

\[
= \sum_{i=0}^{m_B-1} X^{ia_{\ell m A}} a_{i,h}(X^{b_{m B}}), \quad \forall h \in [\ell],
\]

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

\[
\bar{c}_h(X) = q_h(X)(X^{m_{A m B}} - 1) + \sum_{i=0}^{m_B-1} X^{ia_{\ell m A}} a_{i,h}(X^{b_{m B}}), \quad \forall h \in [\ell], \quad (23)
\]
for some \( q_h(X) \in \mathbb{F}_q[X] \). Therefore \( \overline{c}_h(X) \) is a multiple of \( \sum_{i=0}^{b} \epsilon_i(X) g_i^A(X^{bm_B}) \) for some \( \epsilon_i(X) \in \mathbb{F}_q[X] \). A codeword \( b_j(X) \) in \( B \) in the \( j \)th column of \( (m_{i,j}) \) is a multiple of \( g(B) \) and we obtain:

\[
\sum_{i=0}^{m_B-1} \sum_{j=0}^{\ell_m - 1} m_{i,j} X^{a_i \ell_m A + j bm_B} = \sum_{j=0}^{\ell_m - 1} X^{bm_B} \sum_{i=0}^{m_B-1} m_{i,j} X^{a_i \ell_m A} \sum_{j=0}^{\ell_m - 1} X^{bm_B} b_j(X^{a_i \ell_m A}),
\]

and therefore \( \overline{c}_h(X) \) is a multiple of \( g(B)(X^{a_i \ell_m A}) \) modulo \( X^{a_i \ell_m A} - 1 \).

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

\[
(c_0(X) c_1(X) \cdots c_{\ell_m - 1}(X)) = (i_0(X) i_1(X) \cdots i_{\ell_m - 1}(X)) G(X),
\]

where \( G(X) \) is as in (15).

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 \( A \) be an \( [\ell, m_A, k_A, d_A]_q \) 1-level \( \ell \)-quasi-cyclic code with generator matrix in RGB/POT form:

\[
G^A(X) = \begin{pmatrix} g_0(X) & g_0^A(X) & \cdots & g_0^A(\ell - 1)(X) \\
g_1(X) & g^A(X) & \cdots & g^A(\ell - 1)(X) \\
g_\ell(X) & g^A(\ell)(X) & \cdots & g^A(\ell - 1)(X) \\
\end{pmatrix} = (g(X), g(X)_{\ell}^A(X^{bm_B}) \cdots g(X)_{\ell - 1}^A(X^{bm_B}))
\]

as shown in Corollary 3. Let \( B \) 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 \( \ell \)-quasi-cyclic product code in RGB/POT form is:

\[
G(X) = (g(X), g(X)_{\ell}^A(X^{bm_B}) \cdots g(X)_{\ell - 1}^A(X^{bm_B})) \cdot \text{diag}(1, X^{-a_{m_A}}, X^{-2a_{m_A}}, \ldots, X^{-(\ell - 1)a_{m_A}}),
\]

where

\[
g(X) = \gcd(X^{m_B} - 1, g(X)) g^A(X^{bm_B}).
\]

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

\[
g(X) = u_0(X) g(X) g^A(X^{bm_B}) g^B(X^{a_{\ell_m A}}) + v_0(X)(X^{a_{\ell_m A}} - 1).
\]

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 \( \text{diag}(1, X^{-a_{m_A}}, X^{-2a_{m_A}}, \ldots, X^{-(\ell - 1)a_{m_A}}) \) and denote by \( Y = X^{bm_B} \) and \( Z = X^{a_{\ell_m A}} \).

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

\[
\begin{pmatrix} g^A(Y) g^B(Z) g^A(Y) f_1^A(Y) g^B(Z) \cdots \\
X^{a_{\ell_m A} m_B} - 1 \\
0 \\
\vdots \end{pmatrix}
\]

\[
\rightarrow R[0] = u_0(X)R[0] + v_0(X)R[1] + v_0(X) f_1^A(Y) R[2] + \cdots + v_0(X) f_{\ell - 1}(Y) R[\ell]
\]

\[
\begin{pmatrix} g(X) g^B(Z) g(X) f_1^A(Y) \cdots \\
X^{a_{\ell_m A} m_B} - 1 \\
0 \\
\vdots \end{pmatrix}
\]

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

\[
\begin{pmatrix} u_0(X) g^A(Y) f_1^A(Y) g^B(Z) + v_0(X) f_1^A(Y) X^{a_{\ell_m A} m_B} - 1 \\
\vdots \end{pmatrix} = f_1^A(Y) (u_0(X) g^A(Y) g^B(Z) + v_0(X) X^{a_{\ell_m A} m_B} - 1),
\]

and with (26) we obtain from (29)

\[
f_1^A(Y) (u_0(X) g^A(Y) g^B(Z) + v_0(X) X^{a_{\ell_m A} m_B} - 1)
\]

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:

\[
\begin{pmatrix} g(X) g(X) f_1^A(X^{bm_B}) \cdots g(X) f_{\ell - 1}^A(X^{bm_B}) \\
\end{pmatrix},
\]

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

Note that (25) is exactly the generator polynomial of a cyclic product code. A 1-level \( \ell \)-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 $G^A(X) = (g^A_{0,0}(X), g^A_{0,1}(X))$ where

$$g^A_{0,0}(X) = m^{(1)}(X) = X^8 + X^7 + X^6 + X^4 + X^2 + X + 1,$$
$$g^A_{0,1}(X) = m^{(1)}(X) = X^{14} + X^{13} + X^{12} + X^{11} + X^8 + 1,$$

and $\mathcal{A}$ is a $[17 \cdot 2, 9, 11]_2$ quasi-cyclic code. Let $\alpha$ be a 17th root of unity in $\mathbb{F}_q[X]$. Thm. 8, we calculate

$$f^A_{\alpha}(X^{-11,3}) \equiv f^A_{\alpha}(X^{18}) = m_0(X^{18}) \cdot (X^{54} + X^{36} + 1) = (X^{18} + 1)^3 \cdot (X^{54} + X^{36} + 1) = X^{108} + X^{54} + X^{18} + 1$$
$$= X^{18} + X^6 + X^3 + 1 \mod (X^{51} + 1),$$

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

$$g_{0,0}(X) = m_0^{(51)}(X)m_1^{(51)}(X)m_3^{(51)}(X)m_5^{(51)}(X)m_9^{(51)}(X)m_{11}^{(51)}(X)m_{13}^{(51)}(X)m_{19}^{(51)}(X)$$
$$= X^{33} + X^{32} + X^{30} + X^{27} + X^{25} + X^{23} + X^{20} + X^{18} + X^{17} + X^{16} + X^{15} + X^{13} + X^{10} + X^8 + X^6 + X^3 + X + 1.$$