On the algebraic structure of quasi-cyclic codes I : finite fields

Ling, San; Sole, Patrick

2001

Ling, S., & Solé, P. (2001). On the algebraic structure of quasi-cyclic codes I: Finite fields. IEEE Transactions on Information Theory, 47(7), 2751-2760.

https://hdl.handle.net/10356/96416

https://doi.org/10.1109/18.959257

On the Algebraic Structure of Quasi-Cyclic Codes I: Finite Fields

San Ling and Patrick Solé, *Member, IEEE*

***Abstract*—A new algebraic approach to quasi-cyclic codes is introduced. The key idea is to regard a quasi-cyclic code over a field as a linear code over an auxiliary ring. By the use of the Chinese Remainder Theorem (CRT), or of the Discrete Fourier Transform (DFT), that ring can be decomposed into a direct product of fields. That ring decomposition in turn yields a code construction from codes of lower lengths which turns out to be in some cases the celebrated squaring and cubing constructions and in other cases the recent $(u+v|u-v)$ and Vandermonde constructions. All binary extended quadratic residue codes of length a multiple of three are shown to be attainable by the cubing construction. Quinting and septing constructions are introduced. Other results made possible by the ring decomposition are a characterization of self-dual quasi-cyclic codes, and a trace representation that generalizes that of cyclic codes.**

***Index Terms*—$(a+x|b+x|a+b+x)$ construction, Chinese remainder theorem (CRT), discrete Fourier transform (DFT), quasi-cyclic codes, self-dual codes, $(u|u+v)$ construction, $(u+v|u-v)$ construction.**

I. Introduction

QUASI-CYCLIC codes have been around for more than 35 years. They constitute a remarkable generalization of cyclic codes. First, they are asymptotically good [16], [30] due to their abundant population. Second, they have produced many record breakers in short lengths [9]–[12]. Finally, they are closely linked to convolutional codes [6], [27]. (More references can be found in [3].) In spite of their respectable age, their algebraic structure has not been satisfactorily elucidated so far. One approach uses a module structure over an infinite ring [4]; another, more recent, employs Gröbner bases [18].

In this work, we propose to view quasi-cyclic codes of length ℓm and index ℓ over a field F as codes over the polynomial ring

$$R(F, m) := F[Y]/(Y^m - 1).$$

When m is coprime with the characteristic of F, the latter ring can be decomposed into a direct sum of fields.

This decomposition can be achieved by either the Chinese Remainder Theorem (CRT) or the discrete Fourier transform (DFT) (exactly the Mattson–Solomon transform for cyclic codes of length m over F). The benefits of this approach are twofold. First, we can investigate self-dual quasi-cyclic codes in a systematic way. Second, we can decompose quasi-cyclic codes into codes of lower lengths. The composition products that occur are very well known [29] in the area of trellis decoding: twisted squaring [1], cubing [8], ternary cubing [17], $(\boldsymbol{u}+\boldsymbol{v}|\boldsymbol{u}-\boldsymbol{v})$ [14], Vandermonde [15]. As the main example, we give a motivation for the existence of the Turyn construction for the Golay code and generalize it to all binary extended quadratic residue codes of length a multiple of three. New constructions (quinting, septing) are introduced as well.

We hope that a future impact of this work will be more efficient trellises for more block codes and more lattices.

The paper is organized in the following way. Section II contains some basic notations and definitions. Section III discusses the correspondence between quasi-cyclic codes over a field F with linear codes over the auxiliary ring $R(F, m)$. Section IV develops the alphabet decomposition using the CRT. Section V tackles the same problem with the DFT which results in a trace representation for quasi-cyclic codes that generalizes nicely the trace representation of cyclic codes and linearly recurring sequences. Section VI develops applications of the above theory, first for small lengths of the composition codes (e.g., double circulant codes), then, for large lengths. In Section VII, we include a discussion on self-dual binary quasi-cyclic codes. An appendix collects the necessary material on permutation groups of codes. In particular, we give as examples affine-invariant and extended quadratic residue codes.

II. Facts and Notations

A. Codes Over Fields

Let F denote a finite field. When its cardinality q needs to be specified, we will write $F = \boldsymbol{F}_q$. If L is an extension of degree s of F, then the trace of $x \in L$ down to F is

$$\mathrm{Tr}_{L/F}(x) := x + x^q + x^{q^2} + \cdots + x^{q^{s-1}}.$$

A linear code of length n over F is an F-vector subspace of F^n. The dual $C^\perp$ of a code C is understood with respect to the standard inner product. A code C is *self-dual* if $C = C^\perp$. We denote by T the standard shift operator on F^n. A (linear) code is said to be *quasi-cyclic* of index ℓ or ℓ-quasi-cyclic if and only if it is invariant under T^ℓ. If $\ell = 1$, it is just a cyclic code. Throughout the paper, we shall assume that the index ℓ divides the length n. For instance, if $\ell = 2$ and the first circulant block is the identity matrix, such a code is equivalent to a so-called pure *double circulant* code [21]. More generally, up to equivalence,

This work was performed while S. Ling was visiting CNRS-I3S, ESSI, Sophia Antipolis, France.

S. Ling is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: lings@math.nus.edu.sg).

P. Solé is with CNRS, I3S, ESSI, BP 145, 06 903 Sophia Antipolis, France (e-mail: ps@essi.fr).

Communicated by R. Koetter, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)08965-9.

the generator matrix of such a code consists of $m \times m$ circulant matrices. This point will be elaborated upon in Lemma 3.1.

B. Codes Over Rings

For a commutative ring A with identity, a linear code C of length n over A is an A-submodule of A^n. If C is a subset of A^n, checking linearity is equivalent to checking the two conditions

- $x, y \in C \Longrightarrow x + y \in C$;
- $\forall \lambda \in A, x \in C \Longrightarrow \lambda x \in C$,

with addition and scalar multiplication as per the laws of the ring A.

III. Quasi-Cyclic Codes

Let F be a finite field and let m be a positive integer coprime with the characteristic of F. Let $F[Y]$ denote the polynomials in the indeterminate Y with coefficients in F. Let $R := R(F, m) = F[Y]/(Y^m - 1)$. This is the same ring which is instrumental in the polynomial representation of cyclic codes of length m over F. Namely, cyclic codes of length m over F are essentially ideals of $R(F, m)$.

Let C be a quasi-cyclic code over F of length ℓm and index ℓ. Let

$$\boldsymbol{c} = (c_{00}, c_{01}, \ldots, c_{0,\ell-1}, c_{10}, \ldots, c_{1,\ell-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,\ell-1})$$

denote a codeword in C.

Define a map ϕ: $F^{\ell m} \to R^\ell$ by

$$\phi(\boldsymbol{c}) = (\boldsymbol{c}_0(Y), \boldsymbol{c}_1(Y), \ldots, \boldsymbol{c}_{\ell-1}(Y)) \in R^\ell$$

where

$$\boldsymbol{c}_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in R.$$

Let $\phi(C)$ denote the image of C under ϕ. The following lemma is well-known (cf. [18] for instance).

Lemma 3.1: The map ϕ induces a one-to-one correspondence between quasi-cyclic codes over F of index ℓ and length ℓm and linear codes over R of length ℓ.

Proof: Since C is a linear code over F, $\phi(C)$ is closed under scalar multiplication by elements of F. Since $Y^m = 1$ in R,

$$Y\boldsymbol{c}_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^{i+1} = \sum_{i=0}^{m-1} c_{i-1,j} Y^i$$

where the subscript $i-1$ is considered to be in $\{0, 1, \ldots, m-1\}$ by taking modulo m. The word

$$(Y\boldsymbol{c}_0(Y), Y\boldsymbol{c}_1(Y), \ldots, Y\boldsymbol{c}_{\ell-1}(Y)) \in R^\ell$$

corresponds to the word

$$(c_{m-1,0}, c_{m-1,1}, \ldots, c_{m-1,\ell-1}, c_{00}, c_{01}, \ldots, c_{0,\ell-1}, \ldots, c_{m-2,0}, \ldots, c_{m-2,\ell-1}) \in F^{\ell m}$$

which is in C since C is quasi-cyclic of index ℓ. Therefore, $\phi(C)$ is closed under multiplication by Y, and hence $\phi(C)$ is an R-submodule of R^ℓ.

By reversing the above argument, one sees immediately that every linear code over R of length ℓ comes from a quasi-cyclic code of index ℓ and length ℓm over F. $\square$

We now proceed to the study of duality for linear codes over R, in relation with the duality of codes over F. We define a "conjugation" map $^-$ on R as one that acts as the identity on the elements of F and that sends Y to $Y^{-1} = Y^{m-1}$, and is extended F-linearly.

We define on $F^{\ell m}$ the usual Euclidean inner product: for

$$\boldsymbol{a} = (a_{00}, a_{01}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1})$$

and

$$\boldsymbol{b} = (b_{00}, b_{01}, \ldots, b_{0,\ell-1}, b_{10}, \ldots, b_{1,\ell-1}, \ldots, b_{m-1,0}, \ldots, b_{m-1,\ell-1})$$

we define

$$\boldsymbol{a} \cdot \boldsymbol{b} = \sum_{i=0}^{m-1} \sum_{j=0}^{\ell-1} a_{ij} b_{ij}.$$

On R^ℓ, we define the Hermitian inner product: for $\boldsymbol{x} = (x_0, \ldots, x_{\ell-1})$ and $\boldsymbol{y} = (y_0, \ldots, y_{\ell-1})$

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{j=0}^{\ell-1} x_j \overline{y_j}.$$

Proposition 3.2: Let $\boldsymbol{a}, \boldsymbol{b} \in F^{\ell m}$. Then $(T^{\ell k}(\boldsymbol{a})) \cdot \boldsymbol{b} = 0$ for all $0 \le k \le m-1$ if and only if $\langle \phi(\boldsymbol{a}), \phi(\boldsymbol{b}) \rangle = 0$.

Proof: The condition $\langle \phi(\boldsymbol{a}), \phi(\boldsymbol{b}) \rangle = 0$ is equivalent to

$$0 = \sum_{j=0}^{\ell-1} a_j \overline{b_j} = \sum_{j=0}^{\ell-1} \left(\sum_{i=0}^{m-1} a_{ij} Y^i \right) \left(\sum_{k=0}^{m-1} b_{kj} Y^{-k} \right). \quad (1)$$

Comparing the coefficients of Y^h on both sides, (1) is equivalent to

$$\sum_{j=0}^{\ell-1} \sum_{i=0}^{m-1} a_{i+h,j} b_{ij} = 0, \qquad \text{for all } 0 \le h \le m-1 \quad (2)$$

where the subscripts $i+h$ are taken modulo m. Equation (2) means precisely that $(T^{-\ell h}(\boldsymbol{a})) \cdot \boldsymbol{b} = 0$. Since $T^{-\ell h} = T^{\ell(m-h)}$, it follows that (2), and hence $\langle \phi(\boldsymbol{a}), \phi(\boldsymbol{b}) \rangle = 0$, is equivalent to $(T^{\ell k}(\boldsymbol{a})) \cdot \boldsymbol{b} = 0$ for all $0 \le k \le m-1$. $\square$

By applying Proposition 3.2 with $\boldsymbol{a}$ belonging to an ℓ-quasi-cyclic codes C of length ℓm over F, we obtain the following.

Corollary 3.3: Let C be a quasi-cyclic code over F of length ℓm and of index ℓ and let $\phi(C)$ be its image in R^ℓ under ϕ. Then $\phi(C)^\perp = \phi(C^\perp)$, where the dual in $F^{\ell m}$ is taken with respect to the Euclidean inner product, while the dual in R^ℓ is taken with respect to the Hermitian inner product. In particular, a quasi-cyclic code C over F is self-dual with respect to the Euclidean inner product if and only if $\phi(C)$ is self-dual over R with respect to the Hermitian inner product.

IV. The Ring $R(F, m)$

When $m > 1$, the ring $R = R(F, m) = F[Y]/(Y^m - 1)$ is never a finite field. However, the CRT tells us that, if m is coprime with the characteristic of F, then the ring is a direct product of finite fields.

Under the latter assumption, the polynomial $Y^m - 1$ factors completely into distinct irreducible factors in $F[Y]$, so we may write $Y^m - 1 \in F[Y]$ as

$$Y^m - 1 = f_1 f_2 \cdots f_r$$

where f_j are distinct irreducible polynomials. This product is unique in the sense that, if $Y^m - 1 = f_1' f_2' \cdots f_s'$ is another decomposition into irreducible polynomials, then $r = s$ and, after suitable renumbering of the f_j''s, we have that f_j is an associate of f_j' for each $1 \le j \le r$.

For a polynomial f, let f^* denote its reciprocal polynomial. Note that $(f^*)^* = f$. We have, therefore,

$$Y^m - 1 = -f_1^* f_2^* \cdots f_r^*.$$

If f is an irreducible polynomial, so is f^*. By the uniqueness of the decomposition of a polynomial into irreducible factors, we can now write

$$Y^m - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*$$

where δ is nonzero in F, $g_1, \ldots, g_s$ are those f_j's that are associates to their own reciprocals, and $h_1, h_1^*, \ldots, h_t, h_t^*$ are the remaining f_j's grouped in pairs.

Consequently, we may now write

$$R = \frac{F[Y]}{(Y^m - 1)} = \left(\bigoplus_{i=1}^{s} \frac{F[Y]}{(g_i)} \right) \oplus \left(\bigoplus_{j=1}^{t} \left(\frac{F[Y]}{(h_j)} \oplus \frac{F[Y]}{(h_j^*)} \right) \right). \quad (3)$$

The direct sum on the right-hand side is endowed with the coordinate-wise addition and multiplication.

For simplicity of notation, whenever m is fixed, we denote $F[Y]/(g_i)$ by G_i, $F[Y]/(h_j)$ by H_j', and $F[Y]/(h_j^*)$ by H_j''.

It follows from (3) that

$$R^\ell = \left(\bigoplus_{i=1}^{s} G_i^\ell \right) \oplus \left(\bigoplus_{j=1}^{t} \left({H_j'}^\ell \oplus {H_j''}^\ell \right) \right).$$

In particular, every R-linear code C of length ℓ can be decomposed as the direct sum

$$C = \left(\bigoplus_{i=1}^{s} C_i \right) \oplus \left(\bigoplus_{j=1}^{t} (C_j' \oplus C_j'') \right)$$

where, for each $1 \le i \le s$, C_i is a linear code over G_i of length ℓ and, for each $1 \le j \le t$, C_j' is a linear code over H_j' of length ℓ and C_j'' is a linear code over H_j'' of length ℓ.

Every element of R may be written as $\boldsymbol{c}(Y)$ for some polynomial $\boldsymbol{c} \in F[Y]$. The decomposition (3) shows that $\boldsymbol{c}(Y)$ may also be written as an $(s + 2t)$-tuple

$$(c_1(Y), \ldots, c_s(Y), c_1'(Y), c_1''(Y), \ldots, c_t'(Y), c_t''(Y)) \quad (4)$$

where

$$c_i(Y) \in G_i \ (1 \le i \le s), \ c_j'(Y) \in H_j', \quad \text{and } c_j''(Y) \in H_j'' \ (1 \le j \le t).$$

Of course, the c_i, c_j', and c_j'' may also be considered as polynomials in $F[Y]$.

For any element $\boldsymbol{r} \in R$, we have earlier defined its "conjugate" $\overline{\boldsymbol{r}}$, induced by the map $Y \mapsto Y^{-1}$ in R. Suppose that $\boldsymbol{r}$, expressed in terms of the decomposition (3), is given by

$$\boldsymbol{r} = (r_1, \ldots, r_s, r_1', r_1'', \ldots, r_t', r_t''),$$

where

$$r_i \in G_i \ (1 \le i \le s), \ r_j' \in H_j', \text{ and } r_j'' \in H_j'' \ (1 \le j \le t).$$

We shall now describe $\overline{\boldsymbol{r}}$ in terms of the decomposition (3).

We note that, for a polynomial $f \in F[Y]$ that divides $Y^m - 1$, the quotients $F[Y]/(f)$ and $F[Y]/(f^*)$ are isomorphic as rings. The isomorphism is given by

$$\frac{F[Y]}{(f)} \longrightarrow \frac{F[Y]}{(f^*)}$$
$$c(Y) + (f) \longmapsto c\left(Y^{-1}\right) + (f^*). \quad (5)$$

(Here, the symbol Y^{-1} makes sense. It can, in fact, be considered as Y^{m-1}, since f and hence f^* divide $Y^m - 1$ implies that $Y^m = 1$ in both of these rings.)

In the case where f and f^* are associates, we see from (5) that the map $Y \mapsto Y^{-1}$ induces an automorphism of $F[Y]/(f)$. For $r \in F[Y]/(f)$, we denote by $\overline{r}$ its image under this induced map. When the degree of f is 1, note that the induced map is the identity map, so $\overline{r} = r$.

Therefore, the element $\overline{\boldsymbol{r}}$ can now be expressed as

$$(\overline{r_1}, \ldots, \overline{r_s}, r_1'', r_1', \ldots, r_t'', r_t').$$

When f and f^* are associates, for vectors $\boldsymbol{c} = (c_1, \ldots, c_\ell)$, $\boldsymbol{c}' = (c_1', \ldots, c_\ell') \in (F[Y]/(f))^\ell$, we define the Hermitian inner product on $(F[Y]/(f))^\ell$ to be

$$\langle \boldsymbol{c}, \boldsymbol{c}' \rangle = \sum_{i=1}^{\ell} c_i \overline{c_i'}. \quad (6)$$

Remarks:

1) In the case where the degree of f is 1, since the map $r \mapsto \overline{r}$ is the identity, the Hermitian inner product (6) is none other than the usual Euclidean inner product on F. Note that, when $F = \boldsymbol{F}_q$, where q is a perfect square, the Hermitian inner product (6) is therefore *different* from what is usually referred to as the Hermitian inner product in the literature. When the Hermitian inner product is used in the rest of this paper, we shall also mean the Hermitian inner product as defined in (6).

2) When $F = \boldsymbol{F}_q$ is a finite field and when $\deg(f) \ne 1$, it is easy to see that f and f^* are associates implies that the degree e of f is even. In this case, $F[Y]/(f)$ is isomorphic to $\boldsymbol{F}_{q^e}$ and the map $Y \mapsto Y^{-1}$ is, in fact, the map $Y \mapsto Y^{q^{e/2}}$. Hence the map $r \mapsto \overline{r}$ is the map $r \mapsto r^{q^{e/2}}$. In this

case, the Hermitian inner product (6) coincides with the usual Hermitian inner product defined on $\boldsymbol{F}_{q^e}$.

The following proposition is now an immediate consequence of the above discussion.

Proposition 4.1: Let $\boldsymbol{a}, \boldsymbol{b} \in R^\ell$ and write

$$\boldsymbol{a} = (\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_{\ell-1})$$

and

$$\boldsymbol{b} = (\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{\ell-1}).$$

Decomposing each $\boldsymbol{a}_i$, $\boldsymbol{b}_i$ using (4), we write

$$\boldsymbol{a}_i = (a_{i1}, \ldots, a_{is}, a'_{i1}, a''_{i1}, \ldots, a'_{it}, a''_{it})$$

and

$$\boldsymbol{b}_i = (b_{i1}, \ldots, b_{is}, b'_{i1}, b''_{i1}, \ldots, b'_{it}, b''_{it})$$

where $a_{ij}, b_{ij} \in G_j$, $a'_{ij}, b'_{ij}, a''_{ij}, b''_{ij} \in H'_j$ (with H'_j and H''_j identified). Then

$$\begin{aligned}\langle \boldsymbol{a}, \boldsymbol{b} \rangle &= \sum_{i=0}^{\ell-1} \boldsymbol{a}_i \overline{\boldsymbol{b}_i} \\ &= \left(\sum_i a_{i1}\, \overline{b_{i1}}, \ldots, \sum_i a_{is}\, \overline{b_{is}}, \sum_i a'_{i1} b''_{i1}, \right. \\ &\qquad \left. \sum_i a''_{i1} b'_{i1}, \ldots, \sum_i a'_{it} b''_{it}, \sum_i a''_{it} b'_{it} \right).\end{aligned}$$

In particular, $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = 0$ if and only if

$$\sum_i a_{ij} \overline{b_{ij}} = 0 \qquad (1 \le j \le s)$$

and

$$\sum_i a'_{ik} b''_{ik} = 0 = \sum_i a''_{ik} b'_{ik} \qquad (1 \le k \le t).$$

An immediate consequence is the following characterization of self-dual codes over R.

Theorem 4.2: A linear code C over $R(F, m)$ of length ℓ is self-dual with respect to the Hermitian inner product, or equivalently, an ℓ-quasi-cyclic code of length ℓm over F is self-dual with respect to the Euclidean inner product, if and only if

$$C = \left(\bigoplus_{i=1}^{s} C_i \right) \oplus \left(\bigoplus_{j=1}^{t} \left(C'_j \oplus (C'_j)^\perp\right) \right)$$

where, for $1 \le i \le s$, C_i is a self-dual code over G_i of length ℓ (with respect to the Hermitian inner product) and, for $1 \le j \le t$, C'_j is a linear code of length ℓ over H'_j and $C'^{\perp}_j$ is its dual with respect to the Euclidean inner product.

V. Trace Formula

Let $F = \boldsymbol{F}_q$ and assume $(m, q) = 1$. In that case, $m \in F^\times := F - \{0\}$, and the isomorphism (3) can, in fact, be described in a more explicit way via the DFT or, in the language of cyclic codes, the Mattson–Solomon transform.

In (3), the direct factors on the right-hand side correspond to the irreducible factors of $Y^m - 1$ in $F[Y]$.

There is a one-to-one correspondence between these factors and the q-cyclotomic cosets of $\boldsymbol{Z}/m\boldsymbol{Z}$. Denote by U_i $(1 \le i \le s)$ the q-cyclotomic coset corresponding to g_i, V_j, and W_j $(1 \le j \le t)$ the cyclotomic cosets corresponding to h_j and h_j^*, respectively.

For

$$\boldsymbol{c} = \sum_{g \in \boldsymbol{Z}/m\boldsymbol{Z}} c_g Y^g \in F[Y]/(Y^m - 1)$$

its Fourier transform is $\hat{\boldsymbol{c}} = \sum_{h \in \boldsymbol{Z}/m\boldsymbol{Z}} \hat{c}_h Y^h$, where the Fourier coefficient $\hat{c}_h$ is defined as

$$\hat{c}_h = \sum_{g \in \boldsymbol{Z}/m\boldsymbol{Z}} c_g \zeta^{gh}$$

where ζ is a primitive mth root of 1 in some (sufficiently large) Galois extension of F. The inverse transform is given by

$$c_g = m^{-1} \sum_{h \in \boldsymbol{Z}/m\boldsymbol{Z}} \hat{c}_h \zeta^{-gh}.$$

It is well known that $\hat{c}_{qh} = \hat{c}_h^q$ and, for $h \in U_i$, $\hat{c}_h \in G_i$, while for $h \in V_j$ (resp., W_j), $\hat{c}_h \in H'_j$ (resp., H''_j). In fact, the Fourier transform gives rise to the isomorphism (3). The inverse is given by the inverse transform, which can be expressed as follows. Let G_i, H'_j, and H''_j denote the Galois extensions of F corresponding to the polynomials g_i, h_j, and h_j^*, with corresponding cyclotomic cosets U_i, V_j and W_j. For each i, choose and fix some $u_i \in U_i$. For each j, choose and fix some $v_j \in V_j$ and $w_j \in W_j$. Let $\hat{c}_i \in G_i$, $\hat{c}'_j \in H'_j$, and $\hat{c}''_j \in H''_j$. To the $(s+2t)$-tuple $(\hat{c}_1, \ldots, \hat{c}_s, \hat{c}'_1, \hat{c}''_1, \ldots, \hat{c}'_t, \hat{c}''_t)$, we associate the element

$$\sum_{g \in \boldsymbol{Z}/m\boldsymbol{Z}} c_g Y^g \in F[Y]/(Y^m - 1)$$

where

$$\begin{aligned} m c_g = \sum_{i=1}^{s} \mathrm{Tr}_{G_i/F}(\hat{c}_i \zeta^{-g u_i}) + \sum_{j=1}^{t} \big(&\mathrm{Tr}_{H'_j/F}(\hat{c}'_j \zeta^{-g v_j}) \\ &+ \mathrm{Tr}_{H''_j/F}(\hat{c}''_j \zeta^{-g w_j}) \big) \end{aligned}$$

where, for any extension L of F, $\mathrm{Tr}_{L/F}$ denotes the trace from L to F. For a vector $\boldsymbol{x}$, by its Fourier transform, we simply mean the vector whose ith entry is the Fourier transform of the ith entry of $\boldsymbol{x}$. By the trace of $\boldsymbol{x}$ we mean the vector whose coordinates are the traces of the coordinates of $\boldsymbol{x}$.

This description gives the following trace parametrization for quasi-cyclic codes over finite fields, analogous to the trace description of cyclic codes.

Theorem 5.1: Let $F = \boldsymbol{F}_q$ and $(m, q) = 1$. Then, for any ℓ, the quasi-cyclic codes over F of length ℓm and of index ℓ are precisely given by the following construction: write $Y^m - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*$, where δ is a nonzero element of F, g_i are irreducible factors that are associates to their own reciprocals, and h_j are irreducible factors whose reciprocals are h_j^*. Write $F[Y]/(g_i) = G_i$, $F[Y]/(h_j) = H'_j$, and $F[Y]/(h_j^*) = H''_j$. Let U_i (resp., V_j and W_j) denote the cyclotomic coset of $\boldsymbol{Z}/m\boldsymbol{Z}$ corresponding to G_i (resp., H'_j and H''_j) and fix $u_i \in U_i$, $v_j \in V_j$, and $w_j \in W_j$. For each i, let C_i be a code of length ℓ

over G_i, and for each j, let C'_j be a code of length ℓ over H'_j and let C''_j be a code of length ℓ over H''_j. For $\boldsymbol{x}_i \in C_i$, $\boldsymbol{y}'_j \in C'_j$, and $\boldsymbol{y}''_j \in C''_j$, and for each $0 \le g \le m-1$, let

$$\begin{aligned}\boldsymbol{c}_g((\boldsymbol{x}_i), (\boldsymbol{y}'_j), (\boldsymbol{y}''_j)) = &\sum_{i=1}^{s} \mathrm{Tr}_{G_i/F}(\boldsymbol{x}_i \zeta^{-gu_i}) \\ &+ \sum_{j=1}^{t} (\mathrm{Tr}_{H'_j/F}(\boldsymbol{y}'_j \zeta^{-gv_j}) \\ &+ \mathrm{Tr}_{H''_j/F}(\boldsymbol{y}''_j \zeta^{-gw_j})).\end{aligned}$$

Then the code

$$\begin{aligned}C = \{(\boldsymbol{c}_0((\boldsymbol{x}_i), (\boldsymbol{y}'_j), (\boldsymbol{y}''_j)), \ldots, \boldsymbol{c}_{m-1}((\boldsymbol{x}_i), (\boldsymbol{y}'_j), (\boldsymbol{y}''_j))) \mid \\ \forall \boldsymbol{x}_i \in C_i, \forall \boldsymbol{y}'_j \in C'_j \text{ and } \forall \boldsymbol{y}''_j \in C''_j\}\end{aligned}$$

is a quasi-cyclic code over F of length ℓm and of index ℓ. Conversely, every quasi-cyclic code over F of length ℓm and of index ℓ is obtained through this construction.

Moreover, C is self-dual with respect to the Euclidean inner product if and only if the C_i are self-dual with respect to the Hermitian inner product and $C''_j = (C'_j)^{\perp}$ for each j with respect to the Euclidean inner product.

Remark: In the definition of $\boldsymbol{c}_g((\boldsymbol{x}_i), (\boldsymbol{y}'_j), (\boldsymbol{y}''_j))$ in Theorem 5.1, the m has been suppressed. Note that m is nonzero in F, so $mC = C$.

VI. Applications

We now apply our earlier discussions to several situations. We can either start with a (small) fixed ℓ or a (small) fixed m. The former case contains the popular case of double circulant codes. The latter case is relevant to the squaring and cubing constructions. We give explicit examples of both cases. Due to the arithmetic nature of the factorization of $Y^m - 1$ (cyclotomy), it is hopeless to expect a unified treatment at this level of concreteness.

A. *Quasi-Cyclic Codes of Index* 2

Let $\ell = 2$ and let $\boldsymbol{F}_q$ be any finite field. Suppose first that m is relatively prime to q. The decomposition (3) shows that R is the direct sum of finite extensions of $\boldsymbol{F}_q$.

Self-dual codes (with respect to the Euclidean inner product) of length 2 over a finite field $\boldsymbol{F}_q$ exist if and only if -1 is a square in $\boldsymbol{F}_q$, which is the case when one of the following is true:

1) q is a power of 2;
2) $q = p^b$, where p is a prime congruent to $1 \bmod 4$; or
3) $q = p^{2b}$, where p is a prime congruent to $3 \bmod 4$.

In this case, up to equivalence, there is a unique self-dual code of length 2 over $\boldsymbol{F}_q$, viz., the one with generator matrix $(1, i)$, where i denotes a square root of -1 in $\boldsymbol{F}_q$.

This enables one to characterize the self-dual quasi-cyclic codes over $\boldsymbol{F}_q$ of length $2m$ and of index 2, where m is relatively prime to q, once the irreducible factors of $Y^m - 1$ are known.

Proposition 6.1: Let m be relatively prime to q. Then self-dual 2-quasi-cyclic codes over $\boldsymbol{F}_q$ of length $2m$ exist if and only if exactly one of the following conditions is satisfied:

1) q is a power of 2;
2) $q = p^b$, where p is a prime congruent to $1 \bmod 4$; or
3) $q = p^{2b}$, where p is a prime congruent to $3 \bmod 4$.

Proof: If a self-dual 2-quasi-cyclic code over $\boldsymbol{F}_q$ of length $2m$ exists, then the decomposition (3) shows that there is a self-dual code of length 2 over $G_1 = \boldsymbol{F}_q$. Hence the conditions in the proposition are certainly necessary.

Conversely, if any one of the conditions in the proposition is satisfied, then there exists $i \in \boldsymbol{F}_q$ such that $i^2 + 1 = 0$. Consequently, every finite extension of $\boldsymbol{F}_q$ also contains such an i. Hence, the code generated by $(1, i)$ over any extension of $\boldsymbol{F}_q$ is self-dual (with respect to both the Euclidean and Hermitian inner products) of length 2. Hence, Theorem 4.2 ensures the existence of a self-dual 2-quasi-cyclic code of length $2m$ over $\boldsymbol{F}_q$. □

Let $N(\ell, q)$ denote the number of distinct linear codes of length ℓ over $\boldsymbol{F}_q$. It is well known that

$$\begin{aligned}N(\ell, q) &= \sum_{k=0}^{\ell} \begin{bmatrix} \ell \\ k \end{bmatrix}_q \\ &= 1 + \sum_{k=1}^{\ell} \frac{(q^\ell - 1)(q^\ell - q)\cdots(q^\ell - q^{k-1})}{(q^k - 1)(q^k - q)\cdots(q^k - q^{k-1})}.\end{aligned}$$

Proposition 6.2: Let q be a prime power satisfying one of the conditions in Proposition 6.1 and let m be an integer relatively prime to q. Suppose that $Y^m - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*$ in $\boldsymbol{F}_q[Y]$, where δ is a nonzero element of $\boldsymbol{F}_q$, $g_1, \ldots, g_s$, $h_1, h_1^*, \ldots, h_t, h_t^*$ are monic irreducible polynomials such that g_i are self-reciprocal, and h_j and h_j^* are reciprocals. Suppose further that $g_1 = Y - 1$ and, if m is even, $g_2 = Y + 1$. Let the degree of g_i be $2d_i$, and let the degree of h_j (hence also h_j^*) be e_j. Then the number of distinct self-dual 2-quasi-cyclic codes of length $2m$ over $\boldsymbol{F}_q$ is given by

$$\begin{cases} 4\prod_{i=3}^{s}(q^{d_i}+1)\prod_{j=1}^{t} N(2, q^{e_j}), & \text{if } m \text{ is even and } q \text{ is odd} \\ 2\prod_{i=2}^{s}(q^{d_i}+1)\prod_{j=1}^{t} N(2, q^{e_j}), & \text{if } m \text{ is odd and } q \text{ is odd} \\ \prod_{i=2}^{s}(q^{d_i}+1)\prod_{j=1}^{t} N(2, q^{e_j}), & \text{if } m \text{ is odd and } q \text{ is even.} \end{cases}$$

Proof: This follows from the well-known formulas for the number of the distinct self-dual codes of length 2 over $\boldsymbol{F}_q$ with respect to the Euclidean and Hermitian inner products, respectively. □

Proposition 6.3: Let m be relatively prime to q and let ℓ be odd. Then no self-dual ℓ-quasi-cyclic codes over $\boldsymbol{F}_q$ of length ℓm exist. Moreover, when $q \equiv 3 \bmod 4$, self-dual ℓ-quasi-cyclic codes over $\boldsymbol{F}_q$ of length ℓm exist only if $\ell \equiv 0 \bmod 4$.

Proof: Since $Y - 1$ is a factor of $Y^m - 1$, $\boldsymbol{F}_q$ is always a direct factor of R in the decomposition (3). Since ℓ is odd, no self-dual code of length ℓ exists over $\boldsymbol{F}_q$. The last statement follows from the fact that, when $q \equiv 3 \bmod 4$, a self-dual code of length ℓ exists only when ℓ is divisible by 4 [23]. $\square$

When m is divisible by p, where p is a prime such that $q = p^b$, writing $m = p^a m'$ as before, the factors on the right-hand side of (3) are no longer finite fields. They are, however, finite chain rings of depth p^a [20]. Therefore, to classify the self-dual quasi-cyclic codes over $\boldsymbol{F}_q$ of index 2 and of length $2m$, we would first need a classification of self-dual codes of length 2 over finite chain rings of depth p^a.

B. $m = 2$ and the $(u+v|u-v)$ Construction

In this subsection, we consider ℓ-quasi-cyclic codes of length 2ℓ over the finite field $\boldsymbol{F}_q$.

1) When q Is Odd: Let $m = 2$ and suppose that q is odd. Then $Y^2 - 1$ factors into distinct linear factors $(Y-1)(Y+1)$, each of which is self-reciprocal. Hence, R decomposes into a direct sum $\boldsymbol{F}_q \oplus \boldsymbol{F}_q$, and an ℓ-quasi-cyclic code C of length 2ℓ over $\boldsymbol{F}_q$ can be expressed as $C_1 \oplus C_2$, where C_1 and C_2 are codes over $\boldsymbol{F}_q$ of length ℓ. Moreover, C is self-dual if and only if C_1 and C_2 are self-dual with respect to the Euclidean inner product. It follows from the DFT (cf. Theorem 5.1) that the correspondence $C \leftrightarrow C_1 \oplus C_2$ is equivalent to the $(\boldsymbol{u}+\boldsymbol{v}|\boldsymbol{u}-\boldsymbol{v})$ construction. Therefore, we have the following proposition.

Proposition 6.4: Let q be odd. If C_1 and C_2 are codes of length ℓ over $\boldsymbol{F}_q$, then

$$C := \{(\boldsymbol{u}+\boldsymbol{v}|\boldsymbol{u}-\boldsymbol{v}) \,|\, \boldsymbol{u} \in C_1, \, \boldsymbol{v} \in C_2\}$$

is an ℓ-quasi-cyclic code of length 2ℓ over $\boldsymbol{F}_q$. All ℓ-quasi-cyclic codes of length 2ℓ over $\boldsymbol{F}_q$ are constructed this way. Moreover, C is self-dual if and only if C_1 and C_2 are self-dual.

We will see in Section VI-G that this construction is a special case of the Vandermonde construction where $m = 2$.

Corollary 6.5: Let w be an odd prime power with $w \equiv -1 \bmod 12$. Then the $[2w+2, \, w+1]$ self-dual Pless symmetry code over $\boldsymbol{F}_3$ can be obtained from the $(\boldsymbol{u}+\boldsymbol{v}|\boldsymbol{u}-\boldsymbol{v})$ construction and is $(w+1)$-quasi-cyclic.

Proof: From [13, Example 9.17], this code admits an automorphism that is a product of $w+1$ 2-cycles. This corresponds to the situation of $m = 2$ and $\ell = w+1$. $\square$

Proposition 6.6: Suppose $q \equiv 1 \bmod 4$ and ℓ is even, or $q \equiv 3 \bmod 4$ and $\ell \equiv 0 \bmod 4$. The number of distinct self-dual ℓ-quasi-cyclic codes of length 2ℓ over $\boldsymbol{F}_q$ is

$$4 \prod_{i=1}^{\frac{\ell}{2}-1} (q^i + 1)^2.$$

Proof: This follows from the well-known fact that the number of distinct self-dual codes over $\boldsymbol{F}_q$ (with respect to the Euclidean inner product) is

$$2 \prod_{i=1}^{\frac{\ell}{2}-1} (q^i + 1). \qquad \square$$

2) When q Is Even: If q is a power of 2, then $Y^2 - 1 = (Y-1)^2$, so R is the ring $\boldsymbol{F}_q + u\boldsymbol{F}_q$, where $u^2 = 0$. Therefore, every ℓ-quasi-cyclic code of length 2ℓ over $\boldsymbol{F}_q$ (q even) can be realized as a code of length ℓ over $\boldsymbol{F}_q + u\boldsymbol{F}_q$. See [20] for more discussion in the case $q = 2$.

C. $m = 3$ and Turyn's Construction

In this subsection, we assume that $m = 3$ and that q is not a power of 3. We study the ℓ-quasi-cyclic codes of length 3ℓ over $\boldsymbol{F}_q$.

1) $q \equiv 2 \bmod 3$ and Turyn's Construction: When $q \equiv 2 \bmod 3$, Y^2+Y+1 is irreducible in $\boldsymbol{F}_q[Y]$, so

$$Y^3 - 1 = (Y-1)(Y^2+Y+1)$$

as a product of irreducible factors. The decomposition (3) then yields

$$R = \frac{\boldsymbol{F}_q[Y]}{(Y^3-1)} = \boldsymbol{F}_q \oplus \boldsymbol{F}_{q^2}.$$

This isomorphism gives a correspondence between the ℓ-quasi-cyclic codes C of length 3ℓ over $\boldsymbol{F}_q$ and a pair $(C_1, \, C_2)$, where C_1 is a linear code over $\boldsymbol{F}_q$ of length ℓ (with respect to the Euclidean inner product) and C_2 is a linear code over $\boldsymbol{F}_{q^2}$ of length ℓ (with respect to the Hermitian inner product). Using the DFT (cf. Theorem 5.1), we have

$$C = \{(\boldsymbol{x}+2\boldsymbol{a}-\boldsymbol{b}|\boldsymbol{x}-\boldsymbol{a}+2\boldsymbol{b}|\boldsymbol{x}-\boldsymbol{a}-\boldsymbol{b}) \,|\, \boldsymbol{x} \in C_1, \; \boldsymbol{a}+\zeta\boldsymbol{b} \in C_2\}$$

where $\zeta^2 + \zeta + 1 = 0$.

In particular, when $q = 2^t$ (t odd) and for any ℓ

$$C = \{(\boldsymbol{x}+\boldsymbol{b}|\boldsymbol{x}+\boldsymbol{a}|\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b}) \,|\, \boldsymbol{x} \in C_1, \; \boldsymbol{a}+\zeta\boldsymbol{b} \in C_2\}. \quad (7)$$

It is easy to verify that, if $\boldsymbol{a}, \, \boldsymbol{b} \in C_2'$ for some linear code C_2' over $\boldsymbol{F}_q$, then $C_2 := \{\boldsymbol{a}+\boldsymbol{b}\zeta \,|\, \boldsymbol{a}, \, \boldsymbol{b} \in C_2'\}$ is a linear code over $\boldsymbol{F}_{q^2}$.

Therefore, if we begin with two $\boldsymbol{F}_q$-linear codes C_2' and C_1, the construction in (7) in fact yields Turyn's $(\boldsymbol{a}+\boldsymbol{x}|\boldsymbol{b}+\boldsymbol{x}|\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{x})$-construction. In particular, we obtain

Theorem 6.7: The $(\boldsymbol{a}+\boldsymbol{x}|\boldsymbol{b}+\boldsymbol{x}|\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{x})$-construction, applied to two linear codes over $\boldsymbol{F}_{2^t}$ (t odd) of length ℓ, yields an $\boldsymbol{F}_{2^t}$-linear code of length 3ℓ that is quasi-cyclic of index ℓ.

Examples:

1) Since the binary extended Golay code may be obtained from Turyn's construction, by choosing C_2' and C_1 to be, respectively, the binary extended Hamming code and its equivalent code by reversing the order of the coordinates of the words, we get the following.

Corollary 6.8: The binary extended Golay code is quasi-cyclic of index 8.

2) In [25], Turyn's construction is used to construct a family of linear binary codes of parameters $(3 \cdot 2^m, \, 2^{3m+3}, \, 2^m)$ with $m = 3, 4, 5, \ldots$, starting from two first-order Reed–Muller codes. It follows that these codes are also quasi-cyclic of index 2^m.

3) Consider the binary extended quadratic residue code of length $p+1$, where p is an odd prime. Corollary A.2 shows that it is 2ℓ-quasi-cyclic for every divisor 2ℓ of $p+1$. If $p+1$ is

divisible by 3, the code is quasi-cyclic of index $(p+1)/3$, so it is obtained from the cubing construction of Theorem 6.7.

Proposition 6.9: Suppose that q and ℓ satisfy one of the following:

i) $q \equiv 11 \bmod 12$ and $\ell \equiv 0 \bmod 4$; or

ii) $q \equiv 2 \bmod 3$ but $q \not\equiv 11 \bmod 12$, and ℓ is even.

Then the number of distinct self-dual ℓ-quasi-cyclic codes over $\boldsymbol{F}_q$ of length 3ℓ is given by

$$b(q+1)\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)(q^{2i+1}+1)$$

where $b=1$ if q is even, 2 if q is odd.

Proof: This follows from the well-known facts that the number of distinct self-dual codes of length ℓ over $\boldsymbol{F}_q$ (with respect to the Euclidean inner product) is

$$b\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)$$

and the number of distinct self-dual codes of length ℓ over $\boldsymbol{F}_{q^2}$ (with respect to the Hermitian inner product) is

$$\prod_{i=0}^{\frac{\ell}{2}-1}(q^{2i+1}+1). \qquad \square$$

2) When $q \equiv 1 \bmod 3$: In this case, Y^3-1 factors completely into $(Y-1)(Y-\zeta)(Y-\zeta^2)$, where $\zeta^2+\zeta+1=0$ and $\zeta \in \boldsymbol{F}_q$. An ℓ-quasi-cyclic code C over $\boldsymbol{F}_q$ of length ℓ, therefore, decomposes into $C_1 \oplus C_2 \oplus C_3$, where C_1, C_2, and C_3 are codes over $\boldsymbol{F}_q$ of length ℓ. Moreover, C is self-dual if and only if C_1 is self-dual (with respect to the Euclidean inner product) and $C_3 = C_2^{\perp}$ with respect to the Euclidean inner product.

Proposition 6.10: Let q and ℓ satisfy one of the following:

i) $q \equiv 7 \bmod 12$ and $\ell \equiv 0 \bmod 4$; or

ii) $q \equiv 1 \bmod 3$ but $q \not\equiv 7 \bmod 12$, and ℓ is even.

Then the number of distinct self-dual ℓ-quasi-cyclic codes of length 3ℓ over $\boldsymbol{F}_q$ is given by

$$b\left(\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)\right)N(\ell,\,q),$$

where $b=1$ if q is even, 2 if q is odd.

We will see in Section VI-G that the case in this subsection is a special case of the Vandermonde construction when $m=3$.

D. $m = 4$

We now discuss the case where $m=4$ and q is odd.

1) When -1 Is Not a Square in $\boldsymbol{F}_q$: Suppose first that -1 is not a square in $\boldsymbol{F}_q$. In this case, the decomposition (3) of R is isomorphic to $\boldsymbol{F}_q \oplus \boldsymbol{F}_q \oplus \boldsymbol{F}_{q^2}$.

Theorem 6.11: Suppose $m=4$ and -1 is not a square in $\boldsymbol{F}_q$ with q odd. Let i denote an element of $\boldsymbol{F}_{q^2}$ such that $i^2+1=0$. If C_1 and C_2 are codes of length ℓ over $\boldsymbol{F}_q$ and C_3 is a code of length ℓ over $\boldsymbol{F}_{q^2}$, then the code

$$C = \{(\boldsymbol{c}_0,\,\boldsymbol{c}_1,\,\boldsymbol{c}_2,\,\boldsymbol{c}_3) \mid \boldsymbol{c}_g = \boldsymbol{x} + (-1)^g\boldsymbol{y} + \mathrm{Tr}(\boldsymbol{z}i^g),\ \boldsymbol{x}\in C_1,\,\boldsymbol{y}\in C_2,\,\boldsymbol{z}\in C_3\}$$

is an ℓ-quasi-cyclic code over $\boldsymbol{F}_q$ of length 4ℓ. (Here, Tr denotes the trace from $\boldsymbol{F}_{q^2}$ to $\boldsymbol{F}_q$.) Every ℓ-quasi-cyclic code over $\boldsymbol{F}_q$ of length 4ℓ is constructed this way.

Moreover, C is self-dual if and only if C_1 and C_2 are self-dual with respect to the Euclidean inner product and C_3 is self-dual with respect to the Hermitian inner product.

Example: When $q=3$, writing $\boldsymbol{z}=\boldsymbol{a}+i\boldsymbol{b}$, this construction is the construction $(\boldsymbol{x}+\boldsymbol{y}-\boldsymbol{a}|\boldsymbol{x}-\boldsymbol{y}-\boldsymbol{b}|\boldsymbol{x}+\boldsymbol{y}+\boldsymbol{a}|\boldsymbol{x}-\boldsymbol{y}+\boldsymbol{b})$, where $\boldsymbol{x}\in C_1$, $\boldsymbol{y}\in C_2$ and $\boldsymbol{a}+i\boldsymbol{b}\in C_3$.

Proposition 6.12: Let q be an odd prime power such that -1 is not a square in $\boldsymbol{F}_q$ and let $\ell \equiv 0 \bmod 4$. Then the number of distinct self-dual ℓ-quasi-cyclic codes over $\boldsymbol{F}_q$ of length 4ℓ is

$$4(q+1)\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)^2(q^{2i+1}+1).$$

2) When -1 Is a Square in $\boldsymbol{F}_q$: In this case, R decomposes completely into the direct sum of four copies of $\boldsymbol{F}_q$. Two of these copies correspond to the self-reciprocal polynomials $Y-1$ and $Y+1$, while the other two copies correspond to $Y-i$, where i is a square root of -1, and its reciprocal $Y+i$. Therefore, we get the following.

Proposition 6.13: Let ℓ be even and let q be an odd prime power such that -1 is a square in $\boldsymbol{F}_q$. Then, the number of distinct self-dual ℓ-quasi-cyclic codes over $\boldsymbol{F}_q$ of length 4ℓ is

$$\left(4\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)^2\right)N(\ell,\,q).$$

We will see in Section VI-G that this construction is a special case of the Vandermonde construction when $m=4$.

E. When $m = 5$

Theorem 6.14: Suppose that $m=5$ and q is such that $Y^4+Y^3+Y^2+Y+1$ is irreducible in $\boldsymbol{F}_q[Y]$. Let $\zeta\in\boldsymbol{F}_{q^4}$ be such that $\zeta^4+\zeta^3+\zeta^2+\zeta+1=0$ and let Tr denote the trace from $\boldsymbol{F}_{q^4}$ to $\boldsymbol{F}_q$. Then, for C_1 a code of length ℓ over $\boldsymbol{F}_q$ and C_2 a code of length ℓ over $\boldsymbol{F}_{q^4}$, the code

$$C = \{(\boldsymbol{x}+\mathrm{Tr}(\boldsymbol{y})|\boldsymbol{x}+\mathrm{Tr}(\boldsymbol{y}\zeta^{-1})|\boldsymbol{x}+\mathrm{Tr}(\boldsymbol{y}\zeta^{-2})|\boldsymbol{x} +\mathrm{Tr}(\boldsymbol{y}\zeta^{-3})|\boldsymbol{x}+\mathrm{Tr}(\boldsymbol{y}\zeta^{-4})) \mid \boldsymbol{x}\in C_1,\ \boldsymbol{y}\in C_2\}$$

is an ℓ-quasi-cyclic code of length 5ℓ over $\boldsymbol{F}_q$. Every ℓ-quasi-cyclic code of length 5ℓ over $\boldsymbol{F}_q$ is constructed this way.

Moreover, C is self-dual if and only if C_1 is self-dual with respect to the Euclidean inner product and C_2 is self-dual with respect to the Hermitian inner product.

Remark: When $q=2^t$, the above construction is equivalent to the construction $(\boldsymbol{x}+\boldsymbol{a}|\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b}|\boldsymbol{x}+\boldsymbol{b}+\boldsymbol{c}|\boldsymbol{x}+\boldsymbol{c}+\boldsymbol{d}|\boldsymbol{x}+\boldsymbol{d})$, where $\boldsymbol{x}\in C_1$ and $\boldsymbol{a}+\boldsymbol{b}\zeta+\boldsymbol{c}\zeta^2+\boldsymbol{d}\zeta^3\in C_2$.

Example: Taking C_1 and C_2 as in the Turyn construction of the Golay code yields an extremal binary $[40, 20, 8]$ Type II code (see Section VII for a definition of Type II).

Proposition 6.15: Let ℓ be even and let q be such that $Y^4+Y^3+Y^2+Y+1$ is irreducible in $\boldsymbol{F}_q[Y]$. If $q \equiv 3 \bmod 4$, suppose further that $\ell \equiv 0 \bmod 4$. Then, the number of distinct self-dual ℓ-quasi-cyclic codes over $\boldsymbol{F}_q$ of length 5ℓ is

$$b(q^2+1)\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)(q^{4i+2}+1)$$

where $b = 1$ if q is even, 2 if q is odd.

F. When $m = 7$

Let $m = 7$ and suppose that $q = 2^t$ is such that $Y^7 - 1$ factors into $(Y-1)(Y^3+Y+1)(Y^3+Y^2+1)$ as a product of irreducible factors. Let ζ be a root of Y^3+Y+1 in $\boldsymbol{F}_{q^3}$. Let C_1 be a code of length ℓ over $\boldsymbol{F}_q$ and let C_2, C_3 be codes of length ℓ over $\boldsymbol{F}_{q^3}$. Let Tr denote the trace from $\boldsymbol{F}_{q^3}$ to $\boldsymbol{F}_q$. Then the code

$$C = \{(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_6) \mid \boldsymbol{c}_i = \boldsymbol{x} + \mathrm{Tr}(\boldsymbol{y}\zeta^{-i}) + \mathrm{Tr}(\boldsymbol{z}\zeta^{i}), \quad \boldsymbol{x} \in C_1,\ \boldsymbol{y} \in C_2,\ \boldsymbol{z} \in C_3\}$$

is an ℓ-quasi-cyclic code over $\boldsymbol{F}_q$ of length 7ℓ. Conversely, all ℓ-quasi-cyclic codes over $\boldsymbol{F}_q$ of length 7ℓ are constructed this way. Moreover, C is self-dual if and only if C_1 is self-dual and $C_3 = C_2^{\perp}$.

Explicitly, it is an easy, albeit somewhat tedious, exercise to verify that, if we set

$$\begin{aligned}
\boldsymbol{c}_0 &= \boldsymbol{x}+\boldsymbol{a}+\boldsymbol{d}\\
\boldsymbol{c}_1 &= \boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{e}\\
\boldsymbol{c}_2 &= \boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}+\boldsymbol{d}+\boldsymbol{f}\\
\boldsymbol{c}_3 &= \boldsymbol{x}+\boldsymbol{b}+\boldsymbol{c}+\boldsymbol{d}+\boldsymbol{e}\\
\boldsymbol{c}_4 &= \boldsymbol{x}+\boldsymbol{a}+\boldsymbol{c}+\boldsymbol{d}+\boldsymbol{e}+\boldsymbol{f}\\
\boldsymbol{c}_5 &= \boldsymbol{x}+\boldsymbol{b}+\boldsymbol{e}+\boldsymbol{f}\\
\boldsymbol{c}_6 &= \boldsymbol{x}+\boldsymbol{c}+\boldsymbol{f}
\end{aligned}$$

where $\boldsymbol{x} \in C_1$, $\boldsymbol{a}+\boldsymbol{b}\zeta+\boldsymbol{c}\zeta^2 \in C_2$ and $\boldsymbol{d}+\boldsymbol{e}\zeta^{-1}+\boldsymbol{f}\zeta^{-2} \in C_3$, then

$$C = \{(\boldsymbol{c}_0, \ldots, \boldsymbol{c}_6)\}.$$

Example: There is an extremal Type I code of length 42 which is cyclic [26], hence 6-quasi-cyclic. Its binary component C_1 has to be equivalent to the unique [6, 3, 2] self-dual code.

G. The Vandermonde Construction

Let F be, as before, a finite field and m an integer coprime with the characteristic of F. Assume for this section only that $F^{\times}$ contains an element ζ of order m. Then the polynomial $Y^m - 1$ splits completely into linear factors

$$Y^m - 1 = (Y-1)(Y-\zeta)\cdots(Y-\zeta^{m-1}).$$

From the Fourier transform of Section V, we see that if we write

$$f = f_0 + f_1Y + \cdots + f_{m-1}Y^{m-1} \in F[Y]/(Y^m-1)$$

where $f_i \in F$ for $0 \le i \le m-1$, then

$$\begin{pmatrix} f_0\\ f_1\\ \vdots\\ f_{m-1}\end{pmatrix} = V^{-1}\begin{pmatrix} \hat{f}_0\\ \hat{f}_1\\ \vdots\\ \hat{f}_{m-1}\end{pmatrix}$$

where $\hat{f}_i$ are the Fourier coefficients and $V = (\zeta^{ij})_{0\le i,\, j\le m-1}$ is the $m \times m$ Vandermonde matrix.

For a given positive integer ℓ, let $\boldsymbol{a}_0, \ldots, \boldsymbol{a}_{m-1} \in F^{\ell}$ be m vectors. The construction

$$V^{-1}\begin{pmatrix} \boldsymbol{a}_0\\ \vdots\\ \boldsymbol{a}_i\\ \vdots\end{pmatrix}$$

gives an element of R^{ℓ}. If C_i $(0 \le i \le m-1)$ are linear codes over F of length ℓ, and $\boldsymbol{a}_i \in C_i$ for $0 \le i \le m-1$, then we obtain a linear code over R of length ℓ, which then corresponds to a quasi-cyclic code over F of length ℓm and of index ℓ.

One sees readily that the above construction gives exactly the Vandermonde product defined in [14, Ch. 8]. We, therefore, obtain the following theorem.

Theorem 6.16: Let F be a finite field and m an integer coprime with the characteristic of F. Assume that $F^{\times}$ contains an element ζ of order m. Let $C_0, \ldots, C_{m-1}$ be linear codes of length ℓ over F. Then the Vandermonde product of $C_0, \ldots, C_{m-1}$ is a quasi-cyclic code over F of length ℓm and of index ℓ. Moreover, when F and m are as above, every ℓ-quasi-cyclic code of length ℓm over F is obtained via the Vandermonde construction.

Proposition 6.17: When ℓ is even, m is an integer and q is a prime power relatively prime to m such that $Y^m - 1$ factors completely into linear factors over $\boldsymbol{F}_q$, with the additional constraint that $\ell \equiv 0 \bmod 4$ in the case $q \equiv 3 \bmod 4$, the number of distinct self-dual ℓ-quasi-cyclic codes over $\boldsymbol{F}_q$ of length ℓm is equal to

$$\begin{cases}
\left(\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)\right)N(\ell,q)^{(m-1)/2} & \text{if } q \text{ is even}\\
\left(2\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)\right)N(\ell,q)^{(m-1)/2} & \text{if } q \text{ is odd and } m \text{ is odd}\\
\left(2\prod_{i=1}^{\frac{\ell}{2}-1}(q^i+1)\right)^2 N(\ell,q)^{(m-2)/2} & \text{if } q \text{ is odd and } m \text{ is even.}
\end{cases}$$

Proof: This follows easily from the well-known formulas for the number of distinct self-dual codes of length ℓ over $\boldsymbol{F}_q$ with respect to the Euclidean and Hermitian inner products. ☐

VII. Self-Dual Binary Codes

Recall that a binary code is said to be of Type II if and only if it is self-dual and all its codewords have Hamming weights divisible by 4. For a binary ℓ-quasi-cyclic code of length 3ℓ, i.e., $m = 3$, by its binary component C_1, we mean the component in the decomposition (3) corresponding to the polynomial $Y - 1$. We also call the component corresponding to the polynomial Y^2+Y+1 the quaternary component C_2 of the code.

Proposition 7.1: A self-dual binary code C is a Type II ℓ-quasi-cyclic code of length 3ℓ if and only if its binary component C_1 is of Type II.

Proof: Taking $\boldsymbol{a}=\boldsymbol{b}=\boldsymbol{0}$ in the $(\boldsymbol{x}+\boldsymbol{a}|\boldsymbol{x}+\boldsymbol{b}|\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})$ construction, we see that C contains $(\boldsymbol{x}, \boldsymbol{x}, \boldsymbol{x})$ for all $\boldsymbol{x} \in C_1$. Thus, C_1 is Type II. To derive the other direction, observe that the weight of $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{a}+\boldsymbol{b})$ is twice the Hamming weight of $(\boldsymbol{a}+\zeta\boldsymbol{b})$, where $\zeta^2+\zeta+1=0$. From the Hermitian self-duality of C_2, it follows that the Hamming weight of $(\boldsymbol{a}+\zeta\boldsymbol{b})$ is even, hence the weight of $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{a}+\boldsymbol{b})$ is a multiple of 4. □

Example: The Feit code [7] admits for C_1 the (extremal) $[32, 16, 8]$ quadratic residue code.

Corollary 7.2: If there is a binary 24-quasi-cyclic $[72, 36, 16]$ Type II code, then its binary component is equivalent to the extended Golay code and its quaternary component is a Hermitian self-dual quaternary $[24, 12, 8]$.

Proof: By the same argument as in the proof of Proposition 7.1, we see that C_1 has to be of Type II of distance 8, hence equivalent to the Golay code. Similarly, we see that C_2 is a $[24, 12, 8]$ Hermitian self-dual code. □

Proposition 7.3: For $m=5$ or 7, a self-dual binary code C is a Type II ℓ-quasi-cyclic code of length ℓm if and only if its binary component C_1 is of Type II.

Proof: If C is of Type II, the same proof as for Proposition 7.1 shows that C_1 is of Type II. To show the other direction, we observe first that C is spanned by $(\boldsymbol{x}, \boldsymbol{x}, \ldots, \boldsymbol{x})$, for $\boldsymbol{x} \in C_1$ and

1) for $m=5$, $(\boldsymbol{a}, \boldsymbol{a}+\boldsymbol{b}, \boldsymbol{b}+\boldsymbol{c}, \boldsymbol{c}+\boldsymbol{d}, \boldsymbol{d})$, where $\boldsymbol{a}+\boldsymbol{b}\zeta+\boldsymbol{c}\zeta^2+\boldsymbol{d}\zeta^3 \in C_2$ with C_2 Hermitian self-dual over $\boldsymbol{F}_{16}$,
2) for $m=7$

$$(\boldsymbol{a}, \boldsymbol{a}+\boldsymbol{b}, \boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}, \boldsymbol{b}+\boldsymbol{c}, \boldsymbol{a}+\boldsymbol{c}, \boldsymbol{b}, \boldsymbol{c})$$

and

$$(\boldsymbol{d}, \boldsymbol{e}, \boldsymbol{d}+\boldsymbol{f}, \boldsymbol{d}+\boldsymbol{e}, \boldsymbol{d}+\boldsymbol{e}+\boldsymbol{f}, \boldsymbol{e}+\boldsymbol{f}, \boldsymbol{f})$$

where $\boldsymbol{a}+\boldsymbol{b}\zeta+\boldsymbol{c}\zeta^2 \in C_2$ and $\boldsymbol{d}+\boldsymbol{e}\zeta^{-1}+\boldsymbol{f}\zeta^{-2} \in C_3$, with C_2 and C_3 defined over $\boldsymbol{F}_8$.

Since C_1 is of Type II, $\boldsymbol{x}$ has weight divisible by 4. Therefore, the weight of $(\boldsymbol{x}, \boldsymbol{x}, \ldots, \boldsymbol{x})$ is divisible by 4.

When $m=5$, observe that the weight of $(\boldsymbol{a}, \boldsymbol{a}+\boldsymbol{b}, \boldsymbol{b}+\boldsymbol{c}, \boldsymbol{c}+\boldsymbol{d}, \boldsymbol{d})$ is

$$2(\mathrm{wt}(\boldsymbol{a})+\mathrm{wt}(\boldsymbol{b})+\mathrm{wt}(\boldsymbol{c})+\mathrm{wt}(\boldsymbol{d})-\mathrm{wt}(\boldsymbol{a}\otimes\boldsymbol{b}) -\mathrm{wt}(\boldsymbol{b}\otimes\boldsymbol{c})-\mathrm{wt}(\boldsymbol{c}\otimes\boldsymbol{d}))$$

where wt denotes the Hamming weight and $\otimes$ denotes the coordinatewise multiplication.

Since C_2 is Hermitian self-dual, it follows that

$$\begin{aligned}&\mathrm{wt}(\boldsymbol{a})+\mathrm{wt}(\boldsymbol{b})+\mathrm{wt}(\boldsymbol{c})+\mathrm{wt}(\boldsymbol{d})-\mathrm{wt}(\boldsymbol{a}\otimes\boldsymbol{b})\\ &\quad-\mathrm{wt}(\boldsymbol{b}\otimes\boldsymbol{c})-\mathrm{wt}(\boldsymbol{c}\otimes\boldsymbol{d})\\ &\quad\equiv \boldsymbol{a}\cdot\boldsymbol{a}+\boldsymbol{b}\cdot\boldsymbol{b}+\boldsymbol{c}\cdot\boldsymbol{c}+\boldsymbol{d}\cdot\boldsymbol{d}+\boldsymbol{a}\cdot\boldsymbol{b}+\boldsymbol{b}\cdot\boldsymbol{c}+\boldsymbol{c}\cdot\boldsymbol{d}\\ &\quad\equiv 0 \bmod 2.\end{aligned}$$

Hence, it follows that the weight of $(\boldsymbol{a}, \boldsymbol{a}+\boldsymbol{b}, \boldsymbol{b}+\boldsymbol{c}, \boldsymbol{c}+\boldsymbol{d}, \boldsymbol{d})$ is divisible by 4. It also follows that C is spanned by a set of vectors whose weights are divisible by 4, hence C is of Type II.

Using the Pless power moment identity of the first order (cf. [21, p. 131, eq. (19)]), we see that, in the case $m=7$, the weights of

$$(\boldsymbol{a}, \boldsymbol{a}+\boldsymbol{b}, \boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}, \boldsymbol{b}+\boldsymbol{c}, \boldsymbol{a}+\boldsymbol{c}, \boldsymbol{b}, \boldsymbol{c})$$

and

$$(\boldsymbol{d}, \boldsymbol{e}, \boldsymbol{d}+\boldsymbol{f}, \boldsymbol{d}+\boldsymbol{e}, \boldsymbol{d}+\boldsymbol{e}+\boldsymbol{f}, \boldsymbol{e}+\boldsymbol{f}, \boldsymbol{f})$$

are four times those of $\boldsymbol{a}+\boldsymbol{b}\zeta+\boldsymbol{c}\zeta^2$ and $\boldsymbol{d}+\boldsymbol{e}\zeta^{-1}+\boldsymbol{f}\zeta^{-2}$, respectively. It follows that C is spanned by a set of vectors whose weights are all divisible by 4, hence C is of Type II. □

Remark: When $m=7$, it also follows from the above proof that, if the minimal distance of C is d, then the minimal distances of C_2 and C_3 are at least $d/4$.

VIII. Conclusion

In this work, we have shown that all quasi-cyclic codes admitted a combinatorial construction from codes of lower lengths. Conversely, some codes constructed in that way are shown to have a quasi-cyclic structure [25]. The following table summarizes the results we know regarding classical families of codes over finite fields. More families appear in [20].

Code	q	m	Construction	Reference
S_p	3	2	$(\boldsymbol{u}+\boldsymbol{v}\|\boldsymbol{u}-\boldsymbol{v})$	Cor. 6.5
SRC	2	3	$(\boldsymbol{a}+\boldsymbol{x}\|\boldsymbol{b}+\boldsymbol{x}\|\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{x})$	[25]
QR_p	2	3	$(\boldsymbol{a}+\boldsymbol{x}\|\boldsymbol{b}+\boldsymbol{x}\|\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{x})$	Theo. 6.7

Appendix
Algebraic Characterization

In this appendix, we describe a group-theoretic approach to quasi-cyclic codes. Throughout this section, the code C is defined over any field F. Recall that the permutation group $\mathrm{Perm}(C)$ of a code C of length n is the subgroup of S_n, the group of all permutations on n letters, that fixes C under coordinate permutations. We begin with a characterization of quasi-cyclic codes in terms of permutation groups.

Proposition A.1: A code C of length $n=\ell m$ is ℓ-quasi-cyclic if and only if $\mathrm{Perm}(C)$ contains a fixed-point free (fpf) permutation consisting of ℓ disjoint m-cycles. In particular, if p denotes a prime, C of length $n=\ell p$ is ℓ-quasi-cyclic if and only if $\mathrm{Perm}(C)$ contains an fpf permutation of order p.

Proof: If C is ℓ-quasi-cyclic then T^ℓ is the permutation sought for, where T denotes the cyclic shift. Conversely, if $\mathrm{Perm}(C)$ contains such a permutation σ, then up to coordinate labeling, we can assume that $\sigma=T^\ell$. □

Corollary A.2: Let C be a code of length $p+1$ invariant under $PSL(2, p)$, where p is a prime. Then C is 2ℓ-quasi-cyclic for every divisor 2ℓ of $(p+1)$.

Proof: By [21, Ch. 16, Lemma 14] $\mathrm{Perm}(C)$ contains an fpf permutation made of two disjoint cycles of length $(p+1)/2$. Therefore, its $\ell =: (p+1)/2d$th power is also fpf but of order d. By the characterization in Proposition A.1, the result follows. □

ACKNOWLEDGMENT

P. Solé wishes to thank Ms. Desideri-Bracco for careful proofreading. Both authors wish to thank R. Koetter for helpful editing advice and an anonymous referee for useful comments. S. Ling wishes to thank CNRS-I3S, ESSI for hospitality.

REFERENCES

[1] Y. Berger and Y. Béery, "The twisted squaring construction trellis complexity, and generalized weights of BCH and QR codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1817–1827, Nov. 1996.

[2] A. Bonnecaze, P. Solé, and A. R. Calderbank, "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory*, vol. 41, pp. 366–377, Mar. 1995.

[3] Z. Chen. Report. [Online] Available: http://www.tec.hkr.se/~chen/research/codes/

[4] J. Conan and G. Séguin, "Structural properties and enumeration of quasi-cyclic codes," *AAECC*, vol. 4, pp. 25–39, 1993.

[5] S. T. Dougherty, P. Gaborit, M. Harada, and P. Solé, "Type II codes over $\boldsymbol{F}_2 + u\boldsymbol{F}_2$," *IEEE Trans. Inform. Theory*, vol. 45, pp. 32–45, Jan. 1999.

[6] 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, pp. 431–435, Jan. 1998.

[7] W. Feit, "A self-dual even (96, 48, 16) code," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 136–138, Jan. 1974.

[8] G. D. Forney, "Coset codes II: Binary lattices," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.

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

[10] ——, "Nine good $(m-1)/pm$ quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1366–1369, July 1992.

[11] ——, "Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over GF(3) and GF(4)," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1369–1374, July 1992.

[12] ——, "Twelve good rate $(m-r)/pm$ binary quasi-cyclic codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1750–1751, Sept. 1993.

[13] W. C. Huffman, "Codes and groups," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, vol. II, pp. 1345–1440.

[14] G. Hughes, "Codes and arrays from cocycles," Ph.D. dissertation, Royal Melbourne Inst. Technol., Melbourne, Australia, 2000.

[15] ——, "Constacyclic codes, cocycles and a $u+v|u-v$ construction," *IEEE Trans. Inform. Theory*, vol. 46, pp. 674–680, Mar. 2000.

[16] T. Kasami, "A Gilbert–Varshamov bound for quasi-cyclic codes of rate 1/2," *IEEE Trans. Inform. Theory*, vol. IT-20, p. 679, Sept. 1974.

[17] F. K. Kschichang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inform. Theory*, vol. 38, pp. 227–246, Mar. 1992.

[18] K. Lally and P. Fitzpatrick, "Algebraic structure of quasi-cyclic codes," *Discr. Appl. Math.*, vol. 111, pp. 157–175, 2001.

[19] S. Ling and P. Solé, "Type II codes over $\boldsymbol{F}_4 + u\boldsymbol{F}_4$," *European J. Comb.*, to be published.

[20] ——, "On the algebraic structure of quasi-cyclic codes II: Chain rings," preprint, 2001.

[21] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[22] B. R. McDonald, *Finite Rings With Identity*. New York: Marcel Dekker, 1974.

[23] V. Pless, "On the uniqueness of the Golay codes," *J. Comb. Theory*, vol. 5, pp. 215–228, 1968.

[24] ——, "Symmetry codes over $GF(3)$ and new 5-designs," *J. Comb. Theory*, vol. 12, pp. 119–142, 1972.

[25] N. J. A. Sloane, S. M. Reddy, and C.-L. Chen, "New binary codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 503–510, July 1972.

[26] N. J. A. Sloane and J. G. Thompson, "Cyclic self-dual codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 364–366, May 1983.

[27] G. Solomon and H. C. A. van Tilborg, "A connection between block codes and convolutional codes," *SIAM J. Appl. Math.*, vol. 37, pp. 358–369, 1979.

[28] R. M. Tanner, "A transform theory for a class of group-invariant codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 752–775, July 1988.

[29] A. Vardy, "Trellis structure of codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier Science, 1998, vol. II, pp. 1989–2118.

[30] E. J. Weldon, Jr., "Long quasi-cyclic codes are good," *IEEE Trans. Inform. Theory*, vol. IT-16, p. 130, Jan. 1970.