Self-orthogonality of q-ary Images of q^m-ary Codes

Sundeep Balaji and Andrew Thangaraj, *Member, IEEE*

Abstract

A code over GF(q^m) can be imaged or expanded into a code over GF(q) using a basis for the extension field over the base field. The properties of such an image depend on the original code and the basis chosen for imaging. Problems relating the properties of a code and its image with respect to a basis have been of great interest in the field of coding theory. In this work, a generalized version of the problem of self-orthogonality of the q-ary image of a q^m-ary code has been considered. Given an inner product (more generally, a biadditive form), necessary and sufficient conditions have been derived for a code over a field extension and an expansion basis so that an image of that code is self-orthogonal. The conditions require that the original code be self-orthogonal with respect to several related biadditive forms whenever certain power sums of the dual basis elements do not vanish. Numerous interesting corollaries have been derived by specializing the general conditions. An interesting result for the canonical or regular inner product in fields of characteristic two is that only self-orthogonal codes result in self-orthogonal images. Another result is that image of a code is self-orthogonal for all bases if and only if trace of the code is self-orthogonal, except for the case of binary images of 4-ary codes. The conditions are particularly simple to state and apply for cyclic codes. To illustrate a possible application, new quantum error-correcting codes have been constructed with larger minimum distance than previously known.

Index Terms

Self-orthogonality, images of codes, trace of codes, quantum codes.

Sundeep B. and A. Thangaraj are with the Department of Electrical Engineering in the Indian Institute of Technology Madras, Chennai, India.

Self-orthogonality of q-ary Images of q^m-ary Codes

I. Introduction

Linear codes are subspaces of vector spaces over a finite field. To find efficient codes over a particular field, it is often-times beneficial to look for codes over an extension field. Since the extension field is a vector space over the base field, any vector in a vector space over the extension field can be *imaged* into a vector over the base field by expanding each coordinate with respect to a basis for the extension field. Reed-Solomon (RS) codes, one of the most successful codes in practice, form a popular example of a code construction over extension fields. The binary image of RS codes is used in many applications such as magnetic hard disk drives, optical drives and deep space communications. Codes formed as images of a code over an extension field turn out to have some useful properties and advantages such as protection against burst errors and ease of encoding and decoding.

While images of codes have been successfully used in practice, a precise description of their algebraic properties has been a challenge in the field of coding theory for a long time. Problems related to codes over extension fields and their images continue to remain unsolved today [1, Chapter 10]. A few problems have attracted some attention in the past. The problem of determining when the q-ary image of a cyclic code over GF(q^m) is cyclic was solved in [5] by using a module structure for images. Perhaps the most interesting problem related to images is the determination of minimum distance of the image of a code. Many versions of this problem have been studied in works such as [6], [7]. Properties of the images of codes have also been studied with respect to soft-decision decoding [8], [9].

In this paper, we study the problem of self-orthogonality of q-ary images of q^m-ary codes ($q = p^r$, p prime). We derive necessary and sufficient conditions on the original code and the basis such that the image is self-orthogonal with respect to a given product. Our primary result is that self-orthogonality of the image with respect to a particular product (such as $\sum xy$) depends on self-orthogonality of the original code with respect to several conjugate products (such as $\sum xy^{p^i}$) whenever suitable power sums of the dual basis elements do not vanish. The manner in which the condition on the basis separates from the condition on the code and controls self-orthogonality is an illustration of the strong structure of images of codes. We derive several corollaries and consider special cases to expand on the main result. One interesting corollary is that only self-orthogonal codes result in self-orthogonal images in characteristic-2 fields under the canonical inner product ($\sum xy$). An important application for self-orthogonal codes is in the construction of quantum codes [4]. We expand on the codes provided in [3] and provide constructions for a larger set of quantum codes from self-orthogonal GF(4)-images of codes over GF(4^m).

In our most general results, self-orthogonality is studied with respect to a given biadditive form in vector spaces over finite fields. The structure of general biadditive forms over finite fields is exploited in deriving the necessary and sufficient conditions for self-orthogonality. The special cases of canonical inner products and Hermitian-type products have also been studied in detail.

Since the image of a code is a concatenation of codewords from the trace of the code, the trace of the code plays an important role in determining the orthogonality properties of the image [3], [6]. Self-orthogonality of the trace can be determined as a corollary to many of our results concerning images. In particular, we have shown that the trace is self-orthogonal if and only if all images are self-orthogonal with only a single exception of images of codes from GF(4) to GF(2).

The problem of determining self-orthogonality of binary images of Reed-Solomon codes with respect to the canonical inner product has been previously studied in [2]. The relationship between self-orthogonality and power sums of dual basis elements was first derived in [2] for the special case of cyclic codes in extension fields of characteristic two. In this work, we have generalized the results of [2]. Our general conditions for self-orthogonality of images of scalable codes over an arbitrary finite field with respect to a biadditive form can be shown to reduce to the conditions presented in [2].

The rest of the paper is organized as follows. We introduce notation and some basic definitions in Section II. Our main results are presented in the form of two theorems in Section III. Numerous special cases and interesting results are derived and studied in Section IV. The simple case of quadratic extension (GF(q^2) over GF(q)) is explored in detail in Section V. Several examples of self-orthogonal images and construction of new quantum codes is presented in Section VI. We conclude in Section VII with some discussion of results and remarks.

II. Definitions and Notation

We begin by introducing our notation and stating a few relevant preliminary results. See [1] as a reference for further details. Let p be a prime number and q a power of p - i.e., $q = p^r$ for some $r > 0$. Let GF(q) denote the finite field with q elements. The finite field GF(q^m) is a field extension of degree m of the field GF(q). The trace map Tr : GF$(q^m) \to$ GF(q) is defined as Tr$(a) = a + a^q + \ldots + a^{q^{m-1}}$ for $a \in$ GF(q^m). Let $\mathscr{B} = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a basis of GF(q^m) when seen as a vector space over GF(q). Then there exists a unique basis $\mathscr{B}' = \{\beta'_1, \beta'_2, \ldots, \beta'_m\}$ such that Tr$(\beta_i\beta'_j) = \delta_{ij}$ for $1 \leq i, j \leq m$. $\mathscr{B}'$ is said to be the *dual basis* of $\mathscr{B}$ and vice versa. $\mathscr{B}$ is said to be a *self-dual basis* if $\mathscr{B}' = \mathscr{B}$. Clearly, $a =$Tr$(\beta'_1 a)\beta_1$+Tr$(\beta'_2 a)\beta_2 + \ldots +Tr(\beta'_m a)\beta_m$ for all $a \in$ GF(q^m). Hence, (Tr$(\beta'_1 a)$, Tr$(\beta'_2 a), \ldots,$ Tr$(\beta'_m a))$ are the coordinates of $a \in$ GF(q^m) with respect to (w.r.t) the basis $\mathscr{B}$.

A *code* $\mathscr{C}$ over GF(q^m) of length n is a subset of GF$(q^m)^n$. A *scalable code* is a code $\mathscr{C}$ such that $x \in \mathscr{C} \Rightarrow \alpha x \in \mathscr{C}\ \forall \alpha \in$ GF(q^m). In other words, a scalable code of length n over GF(q^m) is a subset of GF$(q^m)^n$ consisting of straight lines through the origin. A *linear code* $\mathscr{C}$ is a subspace of GF$(q^m)^n$ and hence is scalable.

Let $\mathscr{B}$ and $\mathscr{B}'$ be as defined above. Define Im$_{\mathscr{B}}$: GF$(q^m)^n \to$ GF$(q)^{nm}$ and Tr : GF$(q^m)^n \to$ GF$(q)^n$ by

$$\begin{aligned} \text{Im}_{\mathscr{B}}((\alpha_1, \alpha_2, \ldots, \alpha_n)) &= (\text{Tr}(\beta'_1\alpha_1), \ldots, \text{Tr}(\beta'_1\alpha_n), \ldots, \text{Tr}(\beta'_m\alpha_1), \ldots, \text{Tr}(\beta'_m\alpha_n)) \\ \text{Tr}((\alpha_1, \alpha_2, \ldots, \alpha_n)) &= (\text{Tr}(\alpha_1), \text{Tr}(\alpha_2), \ldots, \text{Tr}(\alpha_n)). \end{aligned}$$

In other words, Im$_{\mathscr{B}}$ replaces every coordinate of a vector in GF$(q^m)^n$ with its coordinates w.r.t the basis $\mathscr{B}$ and arranges these coordinates in a specific order and Tr replaces every coordinate of a vector in GF$(q^m)^n$ with its trace. Im$_{\mathscr{B}}(\mathscr{C})$ is called the *Image of* $\mathscr{C}$ w.r.t the basis $\mathscr{B}$ and Tr$(\mathscr{C})$ is called the *Trace of* $\mathscr{C}$. Clearly, Im$_{\mathscr{B}}(\mathscr{C})$

and Tr$(\mathscr{C})$ are codes over GF(q) of lengths nm and n respectively. Additionally, these codes are scalable (linear) if $\mathscr{C}$ is scalable (linear). Notice that if we set $\mathscr{B}' = \{1\}$ (though not a basis) we will get Tr$(\mathscr{C})$ as the *image*.

A function f : GF$(q^m)^n \times$ GF$(q^m)^n \rightarrow$ GF(q^m) is said to be a *biadditive form* if $f(x+y,z) = f(x,z)+f(y,z)$ and $f(z,x+y) = f(z,x) + f(z,y)$ for all $x,y,z \in$ GF$(q^m)^n$. When studying self-orthogonality of traces and images of codes over GF(q^m), it is useful to consider two other related biadditive forms. The first form is the natural restriction f : GF$(q)^n \times$ GF$(q)^n \rightarrow$ GF(q^m). The restricted form is easily seen to be biadditive. The second induced biadditive form $\tilde{f}$: GF$(q)^{nm} \times$ GF$(q)^{nm} \rightarrow$ GF(q^m) is defined as

$$\tilde{f}(x,y) = \sum_{i=0}^{m-1} f((x_{in+1}, x_{in+2}, \ldots, x_{in+n}), (y_{in+1}, y_{in+2}, \ldots, y_{in+n})),$$

where $x = (x_1, x_2, \ldots, x_{nm}), y = (y_1, y_2, \ldots, y_{nm})$ are vectors in GF$(q)^{mn}$. We say that a code $\mathscr{C}$ over GF(q^m) is *self-orthogonal* w.r.t a biadditive form f if $f(x,y) = 0$ for all $x, y \in \mathscr{C}$. In this work, we consider the problem of determining when Im$_{\mathscr{B}}(\mathscr{C})$ and Tr$(\mathscr{C})$ are self-orthogonal w.r.t the induced and restricted biadditive forms $\tilde{f}$ and f, respectively, when $\mathscr{C}$ is a scalable code.

Two particular cases of biadditive forms are important: if f is defined as $f(x,y) = \sum_{i=1}^{n} x_i y_i$ then f is called the *canonical inner product* and if f is defined as $f(x,y) = \sum_{i=1}^{n} x_i y_i^{q^k p^l}$, where $0 \leq k \leq m-1$ and $0 \leq l \leq r-1$, then it is called a *Hermitian-type product* and is denoted by f_{kl}. We note that the induced and restricted forms obtained from the canonical inner product are also canonical inner products. Additionally, the Hermitian-type product defined by $\tilde{h}_l((x_1, \ldots, x_{mn}), (y_1, \ldots, y_{mn})) = \sum_{i=1}^{mn} x_i y_i^{p^l}$ is the form induced by f_{kl} and the Hermitian-type product defined by $h_l((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sum_{i=1}^{n} x_i y_i^{p^l}$ is the form obtained by restricting the domain of f. We consider these special cases and derive results specific to them.

III. Self-orthogonality w.r.t Biadditive Forms

In this section, we consider self-orthogonality of images and trace of a scalable code w.r.t biadditive forms. We derive the necessary and sufficient condition for self-orthogonality of images and trace and prove that self-orthogonality of image for all bases is equivalent to self-orthogonality of trace. We need two lemmas. The first one concerns the structure of general biadditive forms over finite fields and the forms induced by them.

Lemma 1: Let $q = p^r$, where p is a prime, and f : GF$(q^m)^n \times$ GF$(q^m)^n \rightarrow$ GF(q^m) be a biadditive form and $\tilde{f}$: GF$(q)^{nm} \times$ GF$(q)^{nm} \rightarrow$ GF(q^m) be the biadditive form induced by f. Then

$$f((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sum_{1 \leq i,j \leq n} \sum_{0 \leq k,l \leq rm-1} a_{ijkl} x_i^{p^k} y_j^{p^l},$$

$$\tilde{f}((x_1, \ldots, x_{nm}), (y_1, \ldots, y_{nm})) = \sum_{1 \leq i,j \leq n} \sum_{0 \leq k,l \leq r-1} \sum_{s=0}^{m-1} b_{ijkl} x_{sn+i}^{p^k} y_{sn+j}^{p^l},$$

where $a_{ijkl} \in$ GF(q^m) and $b_{ijkl} = \sum_{0 \leq u,v \leq m-1} a_{ij(k+ur)(l+vr)}$.

Proof: Since f is biadditive, $f(ax, by) = ab(x,y)$ for all $a, b \in$ GF(p) and $x, y \in$ GF$(q^m)^n$. Let $\{\beta_1, \ldots, \beta_{rm}\}$ be a basis of GF(q^m) over GF(p) and $\{\beta_1', \ldots, \beta_{rm}'\}$ be its dual basis. Let $\{e_1, \ldots, e_n\}$ be the standard basis of

GF$(q^m)^n$ over GF(q^m). Then $(x_1,\ldots,x_n) = \sum_{i=1}^n x_i e_i$ and $a = \sum_{s=1}^{rm} \text{Tr}(\beta_s' a)\beta_s$ (here the trace map is from GF(q^m) to GF(p)) for all $(x_1,\ldots,x_n) \in \text{GF}(q^m)^n$ and $a \in \text{GF}(q^m)$. Hence,

$$\begin{aligned} f((x_1,\ldots,x_n),(y_1,\ldots,y_n)) &= f(\sum_{i=1}^{n}\sum_{s=1}^{rm}\text{Tr}(\beta_s' x_i)\beta_s e_i, \sum_{j=1}^{n}\sum_{t=1}^{rm}\text{Tr}(\beta_t' y_j)\beta_t e_j) \\ &= \sum_{1\le i,j\le n}\sum_{1\le s,t\le rm}\text{Tr}(\beta_s' x_i)\text{Tr}(\beta_t' y_j) f(\beta_s e_i,\beta_t e_j). \end{aligned}$$

Since $\text{Tr}(\beta_s' x_i) = \beta_s' x_i + (\beta_s' x_i)^p + \ldots + (\beta_s' x_i)^{p^{rm-1}}$ and $\text{Tr}(\beta_t' y_j) = \beta_t' y_j + (\beta_t' y_j)^p + \ldots + (\beta_t' y_j)^{p^{rm-1}}$, we have

$$\begin{aligned} f((x_1,\ldots,x_n),(y_1,\ldots,y_n)) &= \sum_{1\le i,j\le n}\sum_{1\le s,t\le rm}\sum_{0\le k,l\le rm-1}(\beta_s' x_i)^{p^k}(\beta_t' y_j)^{p^l} f(\beta_s e_i,\beta_t e_j) \\ &= \sum_{1\le i,j\le n}\sum_{0\le k,l\le rm-1} a_{ijkl} x_i^{p^k} y_j^{p^l}, \end{aligned}$$

where $a_{ijkl} = \sum_{1\le s,t\le rm} \beta_s'^{p^k}\beta_t'^{p^l} f(\beta_s e_i,\beta_t e_j)$. By definition,

$$\tilde{f}((x_1,\ldots,x_{nm}),(y_1,\ldots,y_{nm})) = \sum_{s=0}^{m-1}\sum_{1\le i,j\le n}\sum_{0\le k,l\le rm-1} a_{ijkl} x_{sn+i}^{p^k} y_{sn+j}^{p^l}.$$

Since the coordinates satisfy $X^q = X^{p^r} = X$, we have

$$\tilde{f}((x_1,\ldots,x_{nm}),(y_1,\ldots,y_{nm})) = \sum_{s=0}^{m-1}\sum_{1\le i,j\le n}\sum_{0\le k,l\le r-1} b_{ijkl} x_{sn+i}^{p^k} y_{sn+j}^{p^l},$$

where $b_{ijkl} = \sum_{0\le u,v\le m-1} a_{ij(k+ur)(l+vr)}$. ∎

The second lemma is a property of the trace map.

Lemma 2: Let $\text{Tr}: \text{GF}(q^m) \to \text{GF}(q)$ be the trace map and $a_0,\ldots,a_{q-1}$ be elements of GF(q^m). Then $\text{Tr}(a_0 + \lambda a_1 + \lambda^2 a_2 + \ldots + \lambda^{q-1}a_{q-1}) = 0$ for all $\lambda \in \text{GF}(q^m)$ if and only if $\text{Tr}(a_0), a_1,\ldots,a_{q-1}$ are all zero.

Proof:

$$\begin{aligned} &\text{Tr}(a_0 + \lambda a_1 + \lambda^2 a_2 + \ldots + \lambda^{q-1}a_{q-1}) = \\ &a_0 + \lambda a_1 + \lambda^2 a_2 + \ldots + \lambda^{q-1}a_{q-1} + \\ &a_0^q + \lambda^q a_1^q + \lambda^{2q}a_2^q + \ldots + \lambda^{q(q-1)}a_{q-1}^q + \ldots \\ &a_0^{q^{m-1}} + \lambda^{q^{m-1}}a_1^{q^{m-1}} + \lambda^{2q^{m-1}}a_2^{q^{m-1}} + \ldots + \lambda^{q^{m-1}(q-1)}a_{q-1}^{q^{m-1}} \end{aligned}$$

Hence, we have q^m zeros for a polynomial of degree at most $q^{m-1}(q-1)$ with coefficients in GF(q^m). This is possible if and only if all the coefficients are zero - i.e., if and only if $\text{Tr}(a_0), a_1,\ldots,a_{q-1}$ are all zero. ∎

A. Self-orthogonality of images and traces of codes

We now state our main result concerning the self-orthogonality of images of codes in the following theorem.

Theorem 3 (Self-orthogonality of Im$_{\mathscr{B}}(\mathscr{C})$): Let $\mathscr{C}$ be a scalable code over GF(q^m) of length n. Let $q = p^r$, where p is a prime number. Let $\mathscr{B}$ be a basis of GF(q^m) over GF(q) and $\mathscr{B}' = \{\beta_1,\ldots,\beta_m\}$ be its dual basis.

Let $f : \mathrm{GF}(q^m)^n \times \mathrm{GF}(q^m)^n \rightarrow \mathrm{GF}(q^m)$ be given by

$$f((x_1,\dots,x_n),(y_1,\dots,y_n)) = \sum_{1\leq i,j\leq n}\sum_{0\leq k,l\leq rm-1} a_{ijkl} x_i^{p^k} y_j^{p^l}$$

for some $a_{ijkl} \in \mathrm{GF}(q^m)$. Let $\tilde{f} : \mathrm{GF}(q)^{mn} \times \mathrm{GF}(q)^{mn} \rightarrow \mathrm{GF}(q^m)$ be the biadditive form induced by f. Let $b_{ijkl} = \sum_{0\leq u,v\leq m-1} a_{ij(k+ur)(l+vr)}$. Then $\mathrm{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ if and only if

$$(\sum_{1\leq i,j\leq n} b_{ijkl} x_i y_j^{p^{l-k}q^w})(\sum_{s=1}^{m} \beta_s^{1+p^{l-k}q^w}) = 0$$

for all $(x_1,\dots,x_n),(y_1,\dots,y_n) \in \mathscr{C}, 0 \leq k,l \leq r-1$ and $0 \leq w \leq m-1$

Proof: From Lemma 1, $\mathrm{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ if and only if

$$\sum_{1\leq i,j\leq n}\sum_{0\leq k,l\leq r-1}\sum_{s=1}^{m} b_{ijkl}\mathrm{Tr}(\beta_s x_i)^{p^k}\mathrm{Tr}(\beta_s y_j)^{p^l} = 0 \quad \forall x=(x_1,\dots,x_n), y=(y_1,\dots,y_n) \in \mathscr{C}.$$

Since $\mathscr{C}$ is a scalable code, the above condition is equivalent to

$$\sum_{1\leq i,j\leq n}\sum_{0\leq k,l\leq r-1}\sum_{s=1}^{m} b_{ijkl}\mathrm{Tr}(\beta_s\lambda_1 x_i)^{p^k}\mathrm{Tr}(\beta_s\lambda_2 y_j)^{p^l} = 0 \quad \forall x,y \in \mathscr{C}, \lambda_1,\lambda_2 \in \mathrm{GF}(q^m).$$

Let $\{c_{ijklt}\}_{1\leq t\leq m}$ be the coordinates of b_{ijkl} w.r.t some basis $\{\gamma_1,\gamma_2,\dots,\gamma_m\}$ of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. Writing b_{ijkl} as $\sum_{t=1}^{m} c_{ijklt}\gamma_t$ we get that the above condition is equivalent to

$$\sum_{t=1}^{m}\left\{\sum_{\substack{1\leq i,j\leq n\\0\leq k,l\leq r-1\\1\leq s\leq m}} c_{ijklt}\mathrm{Tr}(\beta_s\lambda_1 x_i)^{p^k}\mathrm{Tr}(\beta_s\lambda_2 y_j)^{p^l}\right\}\gamma_t = 0 \quad \forall x,y \in \mathscr{C}, \lambda_1,\lambda_2 \in \mathrm{GF}(q^m).$$

Each term in the parenthesis is an element of $\mathrm{GF}(q)$ and $\{\gamma_1,\gamma_2,\dots,\gamma_m\}$ is a basis of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. Hence, the above sum vanishes if and only if each term in the parenthesis vanishes. In other words, the above condition is equivalent to

$$\sum_{\substack{1\leq i,j\leq n\\0\leq k,l\leq r-1\\1\leq s\leq m}} c_{ijklt}\mathrm{Tr}(\beta_s\lambda_1 x_i)^{p^k}\mathrm{Tr}(\beta_s\lambda_2 y_j)^{p^l} = 0 \quad \forall x,y \in \mathscr{C}, 1 \leq t \leq m, \lambda_1,\lambda_2 \in \mathrm{GF}(q^m).$$

Using the definition of Tr and the fact that it is a linear functional from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$ we have

$$\sum_{\substack{1\leq i,j\leq n\\0\leq k,l\leq r-1\\1\leq s\leq m}} c_{ijklt}\mathrm{Tr}(\beta_s\lambda_1 x_i)^{p^k}\mathrm{Tr}(\beta_s\lambda_2 y_j)^{p^l} = \mathrm{Tr}(\sum_{\substack{1\leq i,j\leq n\\0\leq k,l\leq r-1\\1\leq s\leq m\\0\leq w\leq m-1}} c_{ijklt}(\beta_s\lambda_1 x_i)^{p^k}(\beta_s\lambda_2 y_j)^{p^{l+wr}}).$$

Hence, we need trace of a polynomial in λ_1 of degree at most p^{r-1} to be identically zero for all $\lambda_1 \in \mathrm{GF}(q^m)$. By Lemma 2, this is possible if and only if each coefficient of the polynomial is zero. Hence, $\mathrm{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ if and only if

$$\sum_{\substack{1\leq i,j\leq n\\0\leq l\leq r-1\\1\leq s\leq m\\0\leq w\leq m-1}} c_{ijklt}(\beta_s x_i)^{p^k}(\beta_s\lambda_2 y_j)^{p^{l+wr}} = 0 \quad \forall x,y \in \mathscr{C}, 0 \leq k \leq r-1, 1 \leq t \leq m, \lambda_2 \in \mathrm{GF}(q^m).$$

Since $b_{ijkl} = \sum_{t=1}^{m} c_{ijklt}\gamma_t$, the above condition is equivalent to

$$\sum_{\substack{1\le i,j\le n\\ 0\le l\le r-1\\ 1\le s\le m\\ 0\le w\le m-1}} b_{ijkl}(\beta_s x_i)^{p^k}(\beta_s \lambda_2 y_j)^{p^{l+wr}} = 0 \quad \forall x, y \in \mathscr{C}, 0 \le k \le r-1, \lambda_2 \in \text{GF}(q^m).$$

Hence, we need p^{rm} zeros for a polynomial in λ_2 of degree at most p^{rm-1} with coefficients in GF(p^{rm}). This is possible if and only if all the coefficients are zero - i.e., if and only if

$$\sum_{1\le i,j\le n}\sum_{s=1}^{m} b_{ijkl}(\beta_s x_i)^{p^k}(\beta_s y_j)^{p^{l+wr}} = 0 \quad \forall x, y \in \mathscr{C}, 0 \le k, l \le r-1, 0 \le w \le m-1.$$

Hence, Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t f if and only if

$$(\sum_{1\le i,j\le n} b_{ijkl} x_i^{p^k} y_j^{p^l q^w})(\sum_{s=1}^{m}\beta_s^{p^k+p^l q^w}) = 0 \quad \forall x, y \in \mathscr{C}, 0 \le k, l \le r-1 \text{ and } 0 \le w \le m-1.$$

Since, every element in GF(q^m) has a pth root and GF(q^m) is of characteristic p, Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t f if and only if

$$(\sum_{1\le i,j\le n} b_{ijkl} x_i y_j^{p^{l-k} q^w})(\sum_{s=1}^{m}\beta_s^{1+p^{l-k} q^w}) = 0$$

for all $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathscr{C}, 0 \le k, l \le r-1$ and $0 \le w \le m-1$ ■

Notice that in the above proof, the fact that $\mathscr{B}'$ is a basis is never used. Hence, setting $\mathscr{B}' = \{1\}$ we get our most general result concerning self-orthogonality of traces of codes.

Theorem 4 (Self-orthogonality of Tr($\mathscr{C}$)): Let $\mathscr{C}$ be a code over GF(q^m). Let $q = p^r$, where p is a prime number. Let f : GF$(q^m)^n \times$ GF$(q^m)^n \to$ GF(q^m) be given by

$$f((x_1, \dots, x_n), (y_1, \dots, y_n)) = \sum_{1\le i,j\le n}\sum_{0\le k,l\le rm-1} a_{ijkl} x_i^{p^k} y_j^{p^l}$$

for some $a_{ijkl} \in$ GF$(q^m))$ and $b_{ijkl} = \sum_{0\le u,v\le m-1} a_{ij(k+ur)(l+vr)}$. Then Tr$(\mathscr{C})$ is self-orthogonal w.r.t f if and only if

$$\sum_{1\le i,j\le n} b_{ijkl} x_i y_j^{p^{l-k} q^w} = 0$$

for all $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathscr{C}, 0 \le k, l \le r-1$ and $0 \le w \le m-1$

The above two results say the following: given a basis for GF(p^{rm}) over GF(p^r) and a biadditive form f, we have r^2m related conjugate biadditive forms and r^2m power sums of the dual basis elements corresponding to each value of k, l and w. Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal if and only if $\mathscr{C}$ is self-orthogonal w.r.t all those biadditive forms for which the corresponding power sum of the dual basis elements is non-zero and Tr$(\mathscr{C})$ is self-orthogonal if and only if $\mathscr{C}$ is self-orthogonal w.r.t all the r^2m biadditive forms. We note that for a fixed k and l, all the m power sums $\sum_{s=1}^{m}\beta_s^{1+p^{l-k}q^w}, 0 \le w \le m-1$ cannot be zero. ($\sum_{w=0}^{m-1}\sum_{s=1}^{m}\beta_s^{1+p^{l-k}q^w} = \sum_{s=1}^{m}\mathrm{Tr}(\beta_\mathrm{s})^{\mathrm{p}^{\mathrm{l-k}}}\beta_\mathrm{s} \neq 0$, since $\mathscr{B}'$ is a basis for GF(q^m) over GF(q) and Tr is a non-zero linear functional from GF(q^m) to GF(q).) Hence, Im$_{\mathscr{B}}(\mathscr{C})$ being self-orthogonal forces $\mathscr{C}$ to be self-orthogonal w.r.t at least r^2 biadditive forms. We note that some or all of these forms might be identically zero depending on f. For example, let q be even and f be given by $f(x, y) = \sum_{i=1}^{n} x_i y_i + x_i y_i^q$. Then $\tilde{f}$ is the zero map.

B. *Self-orthogonality of images w.r.t. all bases*

We now prove the equivalence of self-orthogonality of image for all bases and self-orthogonality of trace. By definition, each codeword of Im$_{\mathscr{B}}(\mathscr{C})$ is got by concatenating certain codewords of Tr$(\mathscr{C})$. As observed in [3], if Tr$(\mathscr{C})$ is self-orthogonal w.r.t f then Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ for every basis $\mathscr{B}$. The following two results show that the converse is also true except for the case $q = m = 2$. We give an example to show that the converse need not hold when $q = m = 2$. Later, we examine why this happens.

Theorem 5: Let $\mathscr{C}$ be a scalable code of length n over GF(q^m). Let f : GF$(q^m)^n$ × GF$(q^m)^n$ → GF(q^m) be a biadditive form and $\tilde{f}$: GF$(q)^{mn}$ × GF$(q)^{mn}$ → GF(q^m) be the biadditive form induced by f. Suppose $q > 2$ and Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ for three bases $\mathscr{B}_1, \mathscr{B}_2, \mathscr{B}_3$ of GF(q^m) over GF(q) such that $\mathscr{B}_1' = \{\beta_1, \dots, \beta_m\}, \mathscr{B}_2' = \{\beta_1 + \alpha\beta_2, \beta_2, \dots, \beta_m\}$ and $\mathscr{B}_3' = \{\beta_1 + \gamma\beta_2, \beta_2, \dots, \beta_m\}$, where α and γ are distinct non-zero elements of GF(q). Then Tr$(\mathscr{C})$ is self-orthogonal w.r.t f and Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ for all bases $\mathscr{B}$.

Proof: From Theorems 3 and 4, to prove that Tr$(\mathscr{C})$ is self-orthogonal w.r.t. f it is enough to show that for all $0 \le k, l \le r-1$ and $0 \le w \le m-1$ one of the following equations is false:

$$\sum_{s=1}^{m} \beta_s^{1+p^{l-k}q^w} = 0 \tag{1}$$

$$(\beta_1 + \alpha\beta_2)^{1+p^{l-k}q^w} + \sum_{s=2}^{m} \beta_s^{1+p^{l-k}q^w} = 0 \tag{2}$$

$$(\beta_1 + \gamma\beta_2)^{1+p^{l-k}q^w} + \sum_{s=2}^{m} \beta_s^{1+p^{l-k}q^w} = 0. \tag{3}$$

Suppose all the above three equations are true for some k, l and w. Using the fact that GF(q^m) is of characteristic p and comparing (1) and (2) and (1) and (3) we have,

$$\alpha\beta_2\beta_1^{p^{l-k}q^w} + \alpha^{p^{l-k}q^w}\beta_1\beta_2^{p^{l-k}q^w} + (\alpha\beta_2)^{1+p^{l-k}q^w} = 0. \tag{4}$$

$$\gamma\beta_2\beta_1^{p^{l-k}q^w} + \gamma^{p^{l-k}q^w}\beta_1\beta_2^{p^{l-k}q^w} + (\gamma\beta_2)^{1+p^{l-k}q^w} = 0. \tag{5}$$

Multiplying (4) by γ and (5) by α, subtracting one from the other and dividing the resulting equation by $\beta_2^{p^{l-k}q^w}$ we get

$$(\gamma\alpha^{p^{l-k}q^w} - \alpha\gamma^{p^{l-k}q^w})\beta_1 + (\gamma\alpha^{1+p^{l-k}q^w} - \alpha\gamma^{1+p^{l-k}q^w})\beta_2 = 0.$$

Since β_1 and β_2 are linearly independent over GF(q) we have $\gamma\alpha^{p^{l-k}q^w} = \alpha\gamma^{p^{l-k}q^w}$ and $\gamma\alpha^{1+p^{l-k}q^w} = \alpha\gamma^{1+p^{l-k}q^w}$. Since α and γ are distinct and non-zero these equations lead to a contradiction. It follows that Tr$(\mathscr{C})$ is self-orthogonal w.r.t f, hence Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ for all bases $\mathscr{B}$. ■

Notice that the condition $q > 2$ is vital for the above theorem as two distinct nonzero elements are assumed to be available in the field. We next prove a similar result for the case $m > 2$.

Theorem 6: Let $\mathscr{C}$ be a scalable code of length n over GF(q^m). Let f : GF$(q^m)^n$ × GF$(q^m)^n$ → GF(q^m) be a biadditive form and $\tilde{f}$: GF$(q)^{mn}$ × GF$(q)^{mn}$ → GF(q^m) be the biadditive form induced by f. Suppose $m > 2$ and Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ for five bases $\mathscr{B}_1, \mathscr{B}_2, \mathscr{B}_3, \mathscr{B}_4, \mathscr{B}_5$ of GF(q^m) over GF(q) such that $\mathscr{B}_1' =$

$\{\beta_1,\dots,\beta_m\}$, $\mathscr{B}'_2=\{\beta_1+\alpha\beta_2,\beta_2,\dots,\beta_m\}$, $\mathscr{B}'_3=\{\beta_1+\gamma\beta_3,\beta_2,\dots,\beta_m\}$, $\mathscr{B}'_4=\{\beta_1,\beta_2+\delta\beta_3,\beta_3,\dots,\beta_m\}$, and $\mathscr{B}'_5=\{\beta_1+\alpha\beta_2+\gamma\beta_3,\beta_2,\dots,\beta_m\}$, where α,γ,δ are non-zero not necessarily distinct elements of GF(q). Then Tr$(\mathscr{C})$ is self-orthogonal w.r.t f and Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ for all bases.

Proof: From Theorems 3 and 4, to prove that Tr$(\mathscr{C})$ is self-orthogonal w.r.t. f it is enough to show that for all $0\le k,l\le r-1$ and $0\le w\le m-1$ one of the following equations is false:

$$\sum_{s=1}^{m}\beta_s^{1+p^{l-k}q^w} = 0 \tag{6}$$

$$(\beta_1+\alpha\beta_2)^{1+p^{l-k}q^w}+\sum_{s=2}^{m}\beta_s^{1+p^{l-k}q^w} = 0 \tag{7}$$

$$(\beta_1+\gamma\beta_3)^{1+p^{l-k}q^w}+\sum_{s=2}^{m}\beta_s^{1+p^{l-k}q^w} = 0 \tag{8}$$

$$\beta_1^{1+p^{l-k}q^w}+(\beta_2+\delta\beta_3)^{1+p^{l-k}q^w}+\sum_{s=3}^{m}\beta_s^{1+p^{l-k}q^w} = 0 \tag{9}$$

$$(\beta_1+\alpha\beta_2+\gamma\beta_3)^{1+p^{l-k}q^w}+\sum_{s=2}^{m}\beta_s^{1+p^{l-k}q^w} = 0. \tag{10}$$

Suppose all the above five equations are true for some k, l and w. Using the fact that GF(q^m) is of characteristic p and comparing (6) with each of (7), (8), (9) and (10) we have,

$$\alpha\beta_2\beta_1^{p^{l-k}q^w}+\alpha^{p^{l-k}q^w}\beta_1\beta_2^{p^{l-k}q^w}+(\alpha\beta_2)^{1+p^{l-k}q^w} = 0, \tag{11}$$

$$\gamma\beta_3\beta_1^{p^{l-k}q^w}+\gamma^{p^{l-k}q^w}\beta_1\beta_3^{p^{l-k}q^w}+(\gamma\beta_3)^{1+p^{l-k}q^w} = 0, \tag{12}$$

$$\delta\beta_3\beta_2^{p^{l-k}q^w}+\delta^{p^{l-k}q^w}\beta_2\beta_3^{p^{l-k}q^w}+(\delta\beta_3)^{1+p^{l-k}q^w} = 0, \tag{13}$$

$$\begin{aligned}&\alpha^{p^{l-k}q^w}\beta_1\beta_2^{p^{l-k}q^w}+\gamma^{p^{l-k}q^w}\beta_1\beta_3^{p^{l-k}q^w}+\alpha\beta_2\beta_1^{p^{l-k}q^w}+(\alpha\beta_2)^{1+p^{l-k}q^w}+\\&\alpha\gamma^{p^{l-k}q^w}\beta_2\beta_3^{p^{l-k}q^w}+\gamma\beta_3\beta_1^{p^{l-k}q^w}+\gamma\alpha^{p^{l-k}q^w}\beta_3\beta_2^{p^{l-k}q^w}+(\gamma\beta_3)^{1+p^{l-k}q^w} = 0.\end{aligned} \tag{14}$$

From (11), (12) and (14) above we have

$$\alpha\gamma^{p^{l-k}q^w}\beta_2\beta_3^{p^{l-k}q^w}+\gamma\alpha^{p^{l-k}q^w}\beta_3\beta_2^{p^{l-k}q^w}=0. \tag{15}$$

Multiplying (15) by δ and (13) by $\gamma\alpha^{p^{l-k}q^w}$, subtracting one from the other and dividing the resulting equation by $\beta_3^{p^{l-k}q^w}$ we get

$$(\gamma(\alpha\delta)^{p^{l-k}q^w}-\alpha\delta\gamma^{p^{l-k}q^w})\beta_2+\gamma\alpha^{p^{l-k}q^w}\delta^{1+p^{l-k}q^w}\beta_3=0.$$

Since β_2 and β_3 are linearly independent over GF(q) we have $\gamma\alpha^{p^{l-k}q^w}\delta^{1+p^{l-k}q^w}=0$ which is a contradiction to the fact that α,γ and δ are non-zero. It follows that Tr$(\mathscr{C})$ is self-orthogonal w.r.t f, hence Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{f}$ for all bases $\mathscr{B}$. ■

Notice that the condition $m>2$ has been used in the above theorem through the implicit assumption that a basis contains at least three elements β_1, β_2 and β_3. We now see that if either $q>2$ or $m>2$, all images being self-orthogonal implies that trace is self-orthogonal. The only remaining case is that of images of codes over the field with $q=2$ and $m=2$, namely GF(4) over GF(2).

When $q = 2$ and $m = 2$, Tr$(\mathscr{C})$ need not be self-orthogonal even if Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal for all bases. Consider $\mathscr{C} = \{(0,0,0),(1,\omega,\omega^2),(\omega,\omega^2,1),(\omega^2,1,\omega)\}$, where ω is a primitive element of GF(4). The three bases for GF(4) over GF(2) are $\mathscr{B}_1 = \{1,\omega\}, \mathscr{B}_2 = \{\omega,\omega^2\}, \mathscr{B}_3 = \{1,\omega^2\}$. It is easily seen that

$$\begin{aligned}
\text{Im}_{\mathscr{B}_1}(\mathscr{C}) &= \{(0,0,0,0,0,0),(1,0,0,1,1,1),(0,1,1,1,1,0),(1,1,1,0,0,1)\},\\
\text{Im}_{\mathscr{B}_2}(\mathscr{C}) &= \{(0,0,0,0,0,0),(1,1,1,0,0,1),(1,0,0,1,1,1),(0,1,1,1,1,0)\},\\
\text{Im}_{\mathscr{B}_3}(\mathscr{C}) &= \{(0,0,0,0,0,0),(1,0,1,1,0,1),(1,1,0,1,1,0),(0,1,1,0,1,1)\}.
\end{aligned}$$

Hence, all the three images are self-orthogonal w.r.t the canonical inner product but

$$\text{Tr}(\mathscr{C}) = \{(0,0,0),(0,1,1),(1,1,0),(1,0,1)\}$$

and it is not self-orthogonal w.r.t the canonical inner product.

IV. Some Special Cases

In this section, we apply our main results to various specific situations to derive some results of interest.

A. Self-orthogonality w.r.t Hermitian-type products

We begin by considering self-orthogonality of images and trace of a scalable code w.r.t Hermitian-type products due to their importance. Let $q = p^r$, where p is a prime number. For $0 \le k \le m-1$ and $0 \le l \le r-1$, a Hermitian-type product f_{kl} : GF$(q^m)^n \times$ GF$(q^m)^n \to$ GF(q^m) is defined as $f_{kl}(x,y) = \sum_{i=1}^{n} x_i y_i^{p^l q^k}$, where $x = (x_1,\ldots,x_n), y = (y_1,\ldots,y_n)$. Then the map $\tilde{h}_l$: GF$(q)^{mn} \times$ GF$(q)^{mn} \to$ GF(q) given by $\tilde{h}_l(x,y) = \sum_{i=1}^{mn} x_i y_i^{p^l}$ is the map induced by f_{kl} and the restricted map h_l : GF$(q)^n \times$GF$(q)^n \to$ GF(q) is given by $h_l(x,y) = \sum_{i=1}^{n} x_i y_i^{p^l}$. Notice that the form f_{00} is the canonical inner product $\sum_{i=1}^{n} x_i y_i$, which results in both the restricted and induced maps being canonical as well.

We now restate our main results for the case of Hermitian-type products in the following two theorems for ease of reference and clarity.

Theorem 7 (Self-orthogonality of Im$_{\mathscr{B}}(\mathscr{C})$): Let $\mathscr{C}$ be a scalable code of length n over GF(q^m), $\mathscr{B}$ be a basis of GF(q^m) over GF(q) and $\mathscr{B}' = \{\beta_1,\ldots,\beta_m\}$ be the dual basis of $\mathscr{B}$. Then Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the Hermitian-type product, $\sum_{i=1}^{mn} x_i y_i^{p^l}$ if and only if

$$(\sum_{i=1}^{n} x_i y_i^{p^l q^k})(\sum_{j=1}^{m} \beta_j^{1+p^l q^k}) = 0$$

for all $x = (x_1,\ldots,x_n), y = (y_1,\ldots,y_n) \in \mathscr{C}$ and $0 \le k \le m-1$.

Theorem 8 (Self-orthogonality of Tr$(\mathscr{C})$): Let $\mathscr{C}$ be a scalable code of length n over GF(q^m). Then Tr$(\mathscr{C})$ is self-orthogonal w.r.t the Hermitian-type product, $\sum_{i=1}^{n} x_i y_i^{p^l}$ if and only if

$$\sum_{i=1}^{n} x_i y_i^{p^l q^k} = 0$$

for all $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathscr{C}$ and $0 \le k \le m-1$ - i.e., if and only if $\mathscr{C}$ is self-orthogonal w.r.t f_{kl} for $0 \le k \le m-1$.

The above two main results say the following: given a basis for GF(q^m) over GF(q) and the Hermitian-type product $\sum_{i=1}^{mn} x_i y_i^{p^l}$ over GF(q), we have m related Hermitian-type products $\sum_{i=1}^{n} x_i y_i^{p^l q^k}$ over GF(q^m) and m power sums of the elements of the dual basis $\sum_{j=1}^{m} \beta_j^{1+p^l q^k}$ corresponding to each value of $k = 0, 1, \ldots, m-1$. Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal if and only if $\mathscr{C}$ is self-orthogonal w.r.t all those Hermitian-type products for which the corresponding power sum of the dual basis elements is non-zero and Tr$(\mathscr{C})$ is self-orthogonal if and only if $\mathscr{C}$ is self-orthogonal w.r.t all the m Hermitian-type products. For a fixed l, all the m power sums $\sum_{j=1}^{m} \beta_j^{1+p^l q^k}, 0 \le k \le m-1$ cannot be zero. Hence, Im$_{\mathscr{B}}(\mathscr{C})$ being self-orthogonal forces $\mathscr{C}$ to be self-orthogonal w.r.t at least one Hermitian-type product.

B. *Self-orthogonality w.r.t canonical inner product*

We now derive some interesting results for the case of the canonical inner product. Our interest is in finding non-self-orthogonal codes whose images are self-orthogonal w.r.t the canonical inner product. Most of our results are negative in this context.

1) GF(4) over GF(2): We have seen that images from GF(4) to GF(2) make an important counterexample for the situation where self-orthogonality w.r.t all bases does not imply self-orthogonality of the trace.

Proposition 9: Let $\mathscr{C}$ be a scalable code over GF(4). Then the following are equivalent:

(i) Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product for some basis $\mathscr{B}$.

(ii) Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product for all bases $\mathscr{B}$.

(iii) $\mathscr{C}$ is self-orthogonal w.r.t the canonical inner product.

Proof: The only bases for GF(4) over GF(2) are $\mathscr{B}_1 = \{1, \omega\}, \mathscr{B}_2 = \{1, \omega^2\}$, and $\mathscr{B}_3 = \{\omega, \omega^2\}$, where ω is a primitive element of GF(4). By simple computation, it is seen that $\beta_1^{1+2^k} + \beta_2^{1+2^k}$ is non-zero for $k = 0$ and zero for $k = 1$ for the above three bases. It follows from this and Theorem 7 that for any basis $\mathscr{B}$, Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product if and only if $\mathscr{C}$ is self-orthogonal w.r.t the canonical inner product. It follows that the proposition is true.

Alternate Proof (without using our results). From the definition of the trace map, it is seen that Tr(0)=0, Tr(1)=1, Tr(ω)=1, and Tr(ω^2)=1. Additionally, the trace map is given by Tr$(a) = a + a^2$ and $a^4 = a$ for all a in GF(4). Hence, if x and y are two elements of GF(4),

$$\begin{aligned}
\text{Tr}(x)\text{Tr}(y) + \text{Tr}(\omega^2 x)\text{Tr}(\omega^2 y) &= \text{Tr}(\omega^2 xy), \\
\text{Tr}(\omega^2 x)\text{Tr}(\omega^2 y) + \text{Tr}(\omega x)\text{Tr}(\omega y) &= \text{Tr}(xy), \\
\text{Tr}(\omega x)\text{Tr}(\omega y) + \text{Tr}(x)\text{Tr}(y) &= \text{Tr}(\omega xy).
\end{aligned}$$

Suppose $\mathscr{B} = \mathscr{B}_1$. Then $\mathscr{B}' = \{\omega^2, 1\}$. Hence, Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product if and only if $\sum_{i=1}^{n}$ Tr(a_i)Tr$(b_i)+$Tr$(\omega^2 a_i)$Tr$(\omega^2 b_i) = 0$ for all $(a_i), (b_i) \in \mathscr{C}$. This is equivalent to Tr$(\sum_{i=1}^{n} \omega^2 a_i b_i) = 0$ for all $(a_i), (b_i) \in \mathscr{C}$. This is true if and only if $\sum_{i=1}^{n} a_i b_i = \omega$ or 0 for all $(a_i), (b_i) \in \mathscr{C}$. Suppose $\sum_{i=1}^{n} a_i b_i = \omega$

for some $(a_i), (b_i) \in \mathscr{C}$. Since $\mathscr{C}$ is scalable, $(a_i) \in \mathscr{C}$ implies $(\omega a_i) \in \mathscr{C}$. In that case, $\sum_{i=1}^{n} (\omega a_i) b_i = \omega^2$, which is not possible. Hence, $\text{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product if and only if $\sum_{i=1}^{n} a_i b_i = 0$ for all $(a_i), (b_i) \in \mathscr{C}$ - i.e., if and only if $\mathscr{C}$ is self-orthogonal w.r.t the canonical inner product. Similarly, if $\mathscr{B} = \mathscr{B}_2$ and $\mathscr{B}_3$ respectively, then $\mathscr{B}' = \{\omega, 1\}$ and $\mathscr{B}_3$ respectively and $\text{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product if and only if $\mathscr{C}$ is self-orthogonal w.r.t to the canonical inner product. Hence, (i) is equivalent to (iii). From this it follows that (ii) and (iii) are equivalent and we are done. ■

Let us examine the counterexample more closely. From Theorem 8, Tr($\mathscr{C}$) is self-orthogonal w.r.t the canonical inner product if and only if $\mathscr{C}$ is self-orthogonal w.r.t the canonical and the Hermitian inner products given by $\sum x_i y_i$ and $\sum x_i y_i^2$, respectively. From Proposition 9, $\text{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product for all bases $\mathscr{B}$ if and only if $\mathscr{C}$ is self-orthogonal w.r.t the canonical inner product. Hence, we see that Tr($\mathscr{C}$) being self-orthogonal is a more stringent condition than $\text{Im}_{\mathscr{B}}(\mathscr{C})$ being self-orthogonal for all bases. Hence, for $q = m = 2$, we can say Tr($\mathscr{C}$) is self-orthogonal w.r.t the canonical inner product if and only if $\text{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product for some basis and $\mathscr{C}$ is self-orthogonal w.r.t the Hermitian inner product.

2) GF(2^m) over GF(2): An interesting result for fields of even characteristic is that self-orthogonality of any image w.r.t the canonical inner product implies self-orthogonality of the original code.

Proposition 10: Let $\mathscr{C}$ be a scalable code over GF(q^m) for some even q and $\mathscr{B}$ be a basis of GF(q^m) over GF(q). If $\text{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product, then so is $\mathscr{C}$.

Proof: Let $\mathscr{B}' = \{\beta_1, \ldots, \beta_m\}$. From Theorem 7, it is enough to show that $\sum_{i=1}^{m} \beta_i^{1+q^0}$ is nonzero. Since q is even, the characteristic of GF(q^m) is 2. Hence, $\sum_{i=1}^{m} \beta_i^{1+q^0} = \sum_{i=1}^{m} \beta_i^2 = (\sum_{i=1}^{m} \beta_i)^2 \neq 0$. Hence, if any q-ary image is self-orthogonal w.r.t the canonical inner product, then $\mathscr{C}$ is self-orthogonal w.r.t the canonical inner product. ■

3) Self-dual basis: Below is a well-known result. We give a novel proof using the ideas we have developed.

Proposition 11: Let $\mathscr{C}$ be a scalable code over GF(q^m), $\mathscr{B} = \{\beta_1, \ldots, \beta_m\}$ be a basis of GF(q^m) over GF(q) such that $\mathscr{B}' = \mathscr{B}$. $\text{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product if and only if $\mathscr{C}$ is self-orthogonal w.r.t the canonical inner product.

Proof: Let A be a matrix defined by

$$A = \begin{pmatrix} \beta_1 & \beta_1^q & \ldots & \beta_1^{q^{m-1}} \\ \beta_2 & \beta_2^q & \ldots & \beta_2^{q^{m-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_m & \beta_m^q & \ldots & \beta_m^{q^{m-1}} \end{pmatrix}.$$

Since $\mathscr{B}' = \mathscr{B}$, we have $\text{Tr}(\beta_i \beta_j) = \delta_{ij}$ for $1 \leq i, j \leq m$. Hence, $A \times A^T = I$, where I is the $m \times m$ identity matrix and A^T is the transpose of A. Hence, $A^T \times A = I$. The first row of $A^T \times A$ is $[\sum \beta_i^2, \ldots, \sum \beta_i^{1+q^{m-1}}]$. Hence, $\sum_{i=i}^{m} \beta_i^{1+q^k} = \delta_{0k}$ for $0 \leq k \leq m-1$. From Theorem 7, it follows that $\text{Im}_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product if and only if $\mathscr{C}$ is self-orthogonal w.r.t the canonical inner product. ■

4) GF(q^2) over GF(q), $4|(q-1)$:

Proposition 12: Let $\mathscr{C}$ be a scalable code over GF(q^2), where $4|(q-1)$ and $\mathscr{B}$ be a basis of GF(q^2) over GF(q). If Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product, then so is $\mathscr{C}$.

Proof: From Theorem 7, it is enough to prove that for any basis $\{\alpha, \beta\}$, $\alpha^2 + \beta^2 \neq 0$. Let γ be a primitive element of GF(q). Since $4|q-1$, $\gamma^{\frac{q-1}{4}} = i$ is a square-root of -1 and belongs to GF(q). Since $\alpha^2 + \beta^2 = (\alpha + i\beta)(\alpha - i\beta)$ and $\{\alpha, \beta\}$ is a basis over GF(q) it follows that $\alpha^2 + \beta^2 \neq 0$ and we are done. ∎

It follows from Proposition 13 below that for the case of quadratic extensions, Im$_{\mathscr{B}}(\mathscr{C})$ being self-orthogonal forces $\mathscr{C}$ to be self-orthogonal if and only if q is even or $4|(q-1)$. Therefore, if $4|(q-3)$ one can have a non-self-orthogonal code $\mathscr{C}$ such that Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product. Here is one possibility.

Example: Consider self-orthogonality of images of codes from GF(9) over GF(3) w.r.t the canonical inner product. Let γ be a primitive element of GF(9) such that $\gamma^2 + \gamma + 2 = 0$, $\gamma^8 = 1$ and $\gamma^4 = -1$. The power sums of interest for a basis $\{\beta_1, \beta_2\}$ are $\beta_1^2 + \beta_2^2$ and $\beta_1^4 + \beta_2^4$. The basis $\mathscr{B} = \{1, \gamma^2\}$ is such that $1 + \gamma^4 = 0$ and $1 + \gamma^8 = -1$. Therefore, a scalable code $\mathscr{C}$ self-orthogonal w.r.t the Hermitian-type product $\sum xy^3$ but non-self-orthogonal w.r.t the canonical inner product $\sum xy$ will result in an image (w.r.t the basis $\mathscr{B}'$) that is self-orthogonal w.r.t the canonical inner product. Such a code can be easily constructed using the method given in Section VI.

Finally, we remark that self-dual codes can be obtained as images of codes as well. Self-dual codes are linear codes which have rate half and are self-orthogonal w.r.t the canonical inner product. Since rate is preserved by imaging, image of a code is self-dual if and only if it is self-orthogonal w.r.t the canonical inner product and the original code has rate half. Like in the above example, it is possible to have a non-self-orthogonal, rate-1/2 code to result in a self-dual image, if the basis is chosen carefully.

V. Quadratic Extensions

We have seen before that if the trace of a code is self-orthogonal, all images are self-orthogonal. Converse is also true except in the case of binary images of 4-ary codes. This leads us to the search for situations where trace of a code is not self-orthogonal but an image with respect to some basis is self-orthogonal w.r.t a given Hermitian-type product. We begin by looking at quadratic extensions - i.e., GF(q^2) over GF(q).

Let $q = p^r$, where p is a prime number. Let $\mathscr{C}$ be a scalable code of length n over GF(q^2) and $\mathscr{B}$ be a basis of GF(q^2) over GF(q) such that $\mathscr{B}' = \{\alpha, \beta\}$. Let f_{kl} be the Hermitian-type product as defined before. From Theorems 7 and 8, we know that self-orthogonality of Im$_{\mathscr{B}}(\mathscr{C})$ and Tr$(\mathscr{C})$ w.r.t $\tilde{h}_l$ and h_l, respectively, is determined by self-orthogonality of $\mathscr{C}$ w.r.t the forms $\sum_{i=1}^n x_i y_i^{p^l}$ and $\sum_{i=1}^n x_i y_i^{p^{l+r}}$ and the power sums $\alpha^{1+p^l} + \beta^{1+p^l}$ and $\alpha^{1+p^{l+r}} + \beta^{1+p^{l+r}}$. Here we would like to determine when these power sums can vanish and hence determine what self-orthogonality of Im$_{\mathscr{B}}(\mathscr{C})$ w.r.t $\tilde{h}_l$ implies about $\mathscr{C}$.

Consider the power sum $\alpha^{1+p^l} + \beta^{1+p^l}$, where $0 \leq l \leq 2r-1$ and $\{\alpha, \beta\}$ is a basis of GF(q^2) over GF(q). This sum vanishes if and only if there is a root of the equation $X^{1+p^l} + 1 = 0$ in GF(q^2) which is not in GF(q), the root being $\frac{\alpha}{\beta}$. Hence, we would like to determine when every root of the equation $X^{1+p^l}+1=0$ in GF(q^2) is in GF(q). We distinguish two cases, viz. $p=2$ and p odd.

Proposition 13: Let $q=p^r$. Every root of the equation $X^{1+p^l}+1=0$ in GF(q^2) is in GF(q) - i.e., the power sum $\alpha^{1+p^l}+\beta^{1+p^l}$ does not vanish for any basis $\{\alpha,\beta\}$ of GF(q^2) over GF(q), if and only if
(i) $p=2$ and gcd$(2^l+1,2^r+1)=1$ or
(ii) p is odd and " there is a power of two which divides p^r-1 but not p^l+1 and gcd$(p^l+1,p^r+1)=2$" or "every power of two dividing $p^{2r}-1$ divides p^l+1".

Proof: First consider the case $p=2$. There is a root of the equation $X^{1+2^l}+1=0$, say γ, in GF(q^2) if and only if order of γ, which divides $2^{2r}-1$, also divides $1+2^l$. Hence, there is a root of X^{1+2^l} in GF(q^2) if and only if gcd$(1+2^l,2^{2r}-1)>1$. γ is in GF(q) if and only if order of γ divides 2^r-1. Hence, the following two statements are equivalent:
(i) Every root of the equation $X^{1+2^l}+1=0$ in GF(q^2) is in GF(q)
(ii) Every number dividing gcd$(1+2^l,2^{2r}-1)$ divides 2^r-1.
(ii) is clearly equal to the statement that gcd$(1+2^l,2^{2r}-1)|(2^r-1)$. Now, gcd$(2^r+1,2^r-1)=1$ and $2^{2r}-1=(2^r-1)(2^r+1)$. Hence, gcd$(1+2^l,2^{2r}-1)|(2^r-1)$ if and only if gcd$(2^l+1,2^r+1)=1$. Hence, part (i) is true.

Suppose p is odd. The equation $X^{1+p^l}+1=0$ has a root in GF(q^2) if and only if there is an element whose order divides $2(1+p^l)$ and $p^{2r}-1$ but not $1+p^l$. This root is in GF(q) if and only if its order divides p^r-1. Hence, the following two statements are equivalent:
(i) Every root of the equation $X^{1+p^l}+1=0$ in GF(q^2) is in GF(q)
(ii) Every number dividing gcd$(2(1+p^l),p^{2r}-1)$ but not $1+p^l$ divides p^r-1.
(ii) is clearly equivalent to the following statement:
(iii) gcd$(2(1+p^l),p^{2r}-1)|(p^r-1)$ or gcd$(2(1+p^l),p^{2r}-1)|(p^l+1)$

Let $p^l+1=2^a\prod_{i=1}^{s}p_i^{a_i}$, where p_i are prime numbers and a_i are non-negative numbers. We note that gcd$(p^r+1,p^r-1)=2$. Let $p^r+1=2^b\prod_{i=1}^{t}p_i^{b_i}$ and $p^r-1=2^c\prod_{i=t+1}^{s}p_i^{b_i}$, where b_i are non-negative numbers. We have gcd$(2(1+p^l),p^{2r}-1)=2^{\min(1+a,b+c)}\prod_{i=1}^{s}p_i^{\min(a_i,b_i)}$.

Hence, gcd$(2(1+p^l),p^{2r}-1)|(p^r-1)$ if and only if min$(1+a,b+c)\leq c$ and min$(a_i,b_i)=0$ for $1\leq i\leq t$. min$(1+a,b+c)\leq c$ if and only if $a<c$. We know that $a\geq 1$. Since gcd$(p^r+1,p^r-1)=2$, $c\geq 2$ if and only if $b=1$. Hence, min$(1+a,b+c)\leq c$ and min$(a_i,b_i)=0$ for $1\leq i\leq t$ if and only if $a<c$ and gcd$(p^l+1,p^r+1)=2$. Hence, gcd$(2(1+p^l),p^{2r}-1)|(p^r-1)$ if and only if there is a power of two which divides p^r-1 but not p^l+1 and gcd$(p^l+1,p^r+1)=2$.

gcd$(2(1+p^l),p^{2r}-1)|(p^l+1)$ if and only min$(a+1,b+c)\leq a$ - i.e., if and only if $b+c\leq a$ - i.e., every power of two dividing $p^{2r}-1$ divides p^l+1. Hence, part (ii) is true. ■

Proposition 14: Let $q=p^r$ and $l\neq 0$. Every root of the equation $X^{1+p^l}+1=0$ in GF(q^2) is in GF(q)- i.e., the power sum $\alpha^{1+p^l}+\beta^{1+p^l}$ does not vanish for any basis $\{\alpha,\beta\}$ of GF(q^2) over GF(q), if there is a power of two which divides r but not l.

Proof: Suppose $p=2$. From the proof of Proposition 13, every root of the equation $X^{1+p^l}+1=0$ in GF(q^2)

is in GF(q) if $\gcd(1+2^l, 2^{2r}-1)|(2^r-1)$. Clearly, $\gcd(1+2^l, 2^{2r}-1)|\gcd(2^{2l}-1, 2^{2r}-1) = 2^{2\gcd(l,r)}-1$. Additionally, $2^{2\gcd(l,r)}-1|2^r-1$ if and only if there is a power of two which divides r but not l. Hence, the result is true.

Suppose p is odd. From the proof of Proposition 13, every root of the equation $X^{1+p^l}+1=0$ in GF(q^2) is in GF(q) if $\gcd(2(1+p^l), p^{2r}-1)|(p^r-1)$. Since $(p^l-1)/2$ is an integer, $\gcd(2(1+p^l), p^{2r}-1)|\gcd(p^{2l}-1, p^{2r}-1) = p^{2\gcd(l,r)}-1$. Additionally, $p^{2\gcd(l,r)}-1|p^r-1$ if and only if there is a power of two which divides r but not l. Hence, the result is true. ■

Let $\tilde{h}_l$ and h_l be the Hermitian-type products as defined in the previous section. Proposition 14 immediately leads to the following two results:

Corollary 15: Let $q=p^r$ and $l \neq 0$. Let $\mathscr{C}$ be a scalable code over GF(q^2) and $\mathscr{B}$ be a basis of GF(q^2) over GF(q). If there is a power of two which divides r but not l, then Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{h}_l$ if and only if Tr$(\mathscr{C})$ is self-orthogonal w.r.t h_l.

Proof: By Theorems 7 and 8 and the discussion in the starting of this section, self-orthogonality of Im$_{\mathscr{B}}(\mathscr{C})$ w.r.t $\tilde{h}_l$ and Tr$(\mathscr{C})$ w.r.t h_l are equivalent if and only if every root of the equations $X^{1+p^l}+1=0$ and $X^{1+p^{l+r}}+1=0$ in GF(q^2) is in GF(q). By Proposition 14, this is possible if there is a power of two which divides r but not l and $r+l$ which is possible if and only if there is a power of two which divides r but not l. Hence, the result follows. ■

Corollary 16: Let $q=p^r$. Let $\mathscr{C}$ be a scalable code over GF(q^2) and $\mathscr{B}$ be a basis of GF(q^2) over GF(q). If r is a power of two, then Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t $\tilde{h}_l$ if and only if Tr$(\mathscr{C})$ is self-orthogonal w.r.t h_l for $1 \leq l \leq r-1$ and $r+1 \leq l \leq 2r-1$.

Proof: If r is a power of two and $1 \leq l \leq r-1$ and $r+1 \leq l \leq 2r-1$, then there is a power of two which divides r but not l, the power being r itself. Hence, the result follows from Corollary 15. ■

From Proposition 13, we see that studying the behavior of $\gcd(p^r+1, p^l+1)$ is beneficial. Suppose that $r \geq l$. Then r can be written as $r = al+b$, where $0 \leq b < l$. Hence, $\gcd(p^r+1, p^l+1) = \gcd(p^r-p^l, p^l+1) = \gcd(p^{r-l}-1, p^l+1) = \gcd(p^{r-l}+p^l, p^l+1) = \gcd(p^{r-2l}+1, p^l+1) = \ldots = \gcd(p^b+(-1)^a, p^l+1)$. Similarly we see that the following results are true:

$$\begin{aligned}
\gcd(p^{al+b}+1, p^l+1) &= \gcd(p^b+(-1)^a, p^l+1)\\
\gcd(p^{al+b}-1, p^l+1) &= \gcd(p^b-(-1)^a, p^l+1)\\
\gcd(p^{al+b}+1, p^l-1) &= \gcd(p^b+1, p^l-1)\\
\gcd(p^{al+b}-1, p^l-1) &= \gcd(p^b-1, p^l-1).
\end{aligned}$$

From this it follows that $\gcd(p^r \pm 1, p^l \pm 1)$ takes one of these four values: $1, 2, p^{\gcd(r,l)}+1, p^{\gcd(r,l)}-1$. Hence, just by computing $\gcd(l,r)$ and checking for divisibility we can compute the values of $\gcd(p^r \pm 1, p^l \pm 1)$.

Finally, we note that the results relating to power sums which have been derived in this section can be used to determine what self-orthogonality of Im$_{\mathscr{B}}(\mathscr{C})$ w.r.t $\tilde{f}$ implies about $\mathscr{C}$.

VI. Quantum Codes and other Examples

In this section, we specialize our results to cyclic codes and consider some examples of codes whose images but not traces are self-orthogonal w.r.t the canonical inner product for some bases. We also construct new quantum codes from 4-ary images of 4^m-ary codes.

A. Cyclic codes

We use cyclic codes since self-orthogonality can then be easily handled (see the two results below). Suppose $\mathscr{C}$ is a cyclic code of length n over GF(q^m) with generator polynomial $g(x) = \prod_{i \in Z}(x - \alpha^i)$, where α is a primitive nth root. Then the set Z is called the *zeros of the code* and its complement S is called the *nonzeros of the code*. If $n|(q^m - 1)$, $\mathscr{C}$ is called a *Reed-Solomon (RS) code* and any subset of $\{0, 1, \ldots, n-1\}$ can be its zero set.

Proposition 17: Let $\mathscr{C}$ be a cyclic code of length n over GF(q^m) with zero set Z and non-zero set S. For $0 \leq s \leq n-1$, let C_s denote the cyclotomic coset modulo n under multiplication by q containing s. Then Tr$(\mathscr{C})$ has non-zero set $S^c = \cup_{s \in S} C_s$ and zero set $Z^c = \cup_{\{s | C_s \subseteq Z\}} C_s$.

Proof: If $\mathscr{C}$ has zero set Z and non-zero set S, then the subfield subcode $\mathscr{C}|$GF(q) has zero set $\cup_{s \in Z} C_s$. By Delsarte's theorem [1], Tr$(\mathscr{C}) = (\mathscr{C}^{\perp}|\text{GF}(q))^{\perp}$. Hence, Tr$(\mathscr{C})$ has non-zero set $- \cup_{s \in -S} C_s = \cup_{s \in S} C_s = S^c$ and so Tr$(\mathscr{C})$ has zero set $\cup_{\{s|C_s \subseteq Z\}} C_s = Z^c$. $\blacksquare$

Proposition 18: Let $\mathscr{C}$ be a cyclic code of length n over GF(q^m) with zero set Z and non-zero set S. Then the following are equivalent:

(1)$\mathscr{C}$ is self-orthogonal w.r.t the form $\sum x_i y_i^{p^l}$

(2)$(-p^l S)(\text{mod } n) \subseteq Z$

(3)$(-p^{-l} S)(\text{mod } n) \subseteq Z$

Proof: Let $\mathscr{C}' = \{(x_1^{p^l}, \ldots, x_n^{p^l}) : (x_1, \ldots, x_n) \in \mathscr{C}\}$. $\mathscr{C}'$ has zero set $(p^l Z)(\text{mod } n)$ and non-zero set $(p^l S)(\text{mod } n)$. $\mathscr{C}$ is self-orthogonal w.r.t the form $\sum x_i y_i^{p^l}$ if and only if $\mathscr{C}' \subseteq \mathscr{C}^{\perp}$, which is equivalent to the condition $(p^l Z)(\text{mod } n) \supseteq -S$. Taking complements, we have $(1) \Leftrightarrow (2)$. Dividing both sides by $p^l(\text{mod } n)$, we have $(1) \Leftrightarrow (3)$ $\blacksquare$

Consider cyclic codes of length n over GF(q^m). Let $\mathscr{B}$ be a basis of GF(q^m) over GF(q) and $\mathscr{B}' = \{\beta_1, \ldots, \beta_m\}$ be the dual basis of $\mathscr{B}$. From Propositions 17 and 18 and Theorems 7 and 8, Tr$(\mathscr{C})$ is self-orthogonal w.r.t the canonical inner product if and only if

$$-S^c(\text{ mod } n) \subseteq Z^c,$$

and Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t canonical inner product if and only if

$$-q^k S \text{ mod } n \subseteq Z$$

$$\text{for } k \in \{0, 1, \ldots, m-1\} \text{ such that } \sum_{i=1}^{m} \beta_i^{1+q^k} \neq 0.$$

Example: Consider GF(16) over GF(4). Let $n = 15$ and α be a primitive root of the polynomial $X^4 + X + 1$ in GF(16). The power sums of interest in a dual basis $\{\beta_1, \beta_2\}$ are $\beta_1^2 + \beta_2^2 \neq 0$ and $\beta_1^5 + \beta_2^5$. Now $\mathscr{B}_1 = \{1, \alpha^3\}$ is a basis such that the sum of 5th powers is zero, since every element of GF(16) satisfies $X^{15} = 1$ and $1+1 = 0$. Hence, if we find $S \subseteq \{0, 1, 2, \ldots, 14\}$ such that $-S \subseteq Z$ and $-S^c \nsubseteq Z^c$, we have an RS code whose image w.r.t $\mathscr{B}_1'$ is self-orthogonal w.r.t the canonical inner product but trace is not self-orthogonal. $S = \{3\}$ satisfies the requirement $(S^c = \{3, 12\}, -S = \{12\}$, and $-S^c = \{3, 12\})$. Additionally, if $S = \{1, 2, 4\}$ then $S^c = \{1, 2, 4, 8\}$, and $-S^c = \{14, 13, 11, 7\}$. Hence, it is the nonzero set of an RS code whose trace is self-orthogonal w.r.t the canonical inner product.

Example: Consider GF(64) over GF(4). Let $n = 63$ and α be a primitive root of the polynomial $X^6 + X + 1$ in GF(64). The power sums of interest in a dual basis $\{\beta_1, \beta_2, \beta_3\}$ are $\beta_1^2 + \beta_2^2 + \beta_3^2 \neq 0$, $\beta_1^5 + \beta_2^5 + \beta_3^5$, and $\beta_1^{17} + \beta_2^{17} + \beta_3^{17}$. Now $\mathscr{B}_2 = \{1, \alpha, \alpha^{25}\}$ is a basis such that the sum of 5th and 17th powers is zero. Hence, if we find $S \subseteq \{0, 1, 2, \ldots, 62\}$ such that $-S \subseteq Z$ and $-S^c \nsubseteq Z^c$, we have an RS code whose image w.r.t $\mathscr{B}_2'$ is self-orthogonal w.r.t the canonical inner product but trace is not self-orthogonal. $S = \{11, 13\}$ satisfies the requirement $(S^c = \{11, 44, 50, 13, 52, 19\}, -S = \{52, 50\}$, and $-S^c = \{52, 19, 13, 50, 11, 44\})$. Additionally, if $S = \{1, 2, 3, 4, 5, 6\}$ then

$$S^c = \{1, 2, 3, 4, 5, 6, 8, 12, 16, 17, 20, 24, 32, 33, 48\}, \text{ and}$$
$$-S^c = \{62, 61, 60, 59, 58, 57, 55, 51, 47, 46, 43, 39, 31, 30, 15\}.$$

Hence, it is the nonzero set of an RS code whose trace is self-orthogonal w.r.t the canonical inner product.

B. Quantum codes

We now consider some examples of codes which can be used to generate quantum codes. As shown in [4], quantum error correcting codes can be obtained from linear codes over GF(4) which are self-orthogonal w.r.t the Hermitian inner product $\sum x_i y_i^2$. We state the theorem found in [4] for completeness:

Theorem 19: Suppose $\mathscr{C}$ is a (n, k) linear code over GF(4) self-orthogonal w.r.t the Hermitian inner product and d is the minimum weight of $\mathscr{C}^\perp \backslash \mathscr{C}$. Then, an $[[n, n-2k, d]]$ quantum code can be obtained from $\mathscr{C}$.

Hence, an (n, k, d) code over GF(4^m) with 4-ary images self-orthogonal w.r.t the Hermitian inner product leads to an $[[mn, mn-2mk, d']]$ quantum code, where d' is the minimum distance of $\mathscr{C}^\perp \backslash \mathscr{C}$. Additionally, $d' \geq d^\perp$, where $d^\perp$ is the minimum distance of $\mathscr{C}^\perp$.

In [3], cyclic codes over GF(4^m) whose 4-ary traces are self-orthogonal w.r.t the Hermitian inner product have been considered and their images have been used to obtain a class of quantum codes. From Theorems 7 and 8, we know that, in general, requiring Tr$(\mathscr{C})$ to be self-orthogonal is stronger that requiring Im$_{\mathscr{B}}(\mathscr{C})$ to be self-orthogonal. Here we give examples of some codes whose 4-ary images are self-orthogonal w.r.t the Hermitian inner product but not the trace thus getting a class of codes larger than that given in [3]. This also leads to codes having larger minimum distance for the same codelength than those given in [3].

Consider cyclic codes of length n over GF(4^m) with zero set Z and non-zero set S. Let $\mathscr{B}$ be a basis of GF(q^m) over GF(q) and $\mathscr{B}' = \{\beta_1, \ldots, \beta_m\}$ be the dual basis of $\mathscr{B}$. From Propositions 17 and 18 and Theorems 7 and 8, Tr$(\mathscr{C})$ is self-orthogonal w.r.t the Hermitian inner product if and only if

$$-2S^c(\bmod n) \subseteq Z^c,$$

and Im$_{\mathscr{B}}(\mathscr{C})$ is self-orthogonal w.r.t the Hermitian inner product if and only if

$$-2^{2k+1}S \bmod n \subseteq Z$$

$$\text{for } k \in \{0,1,\ldots,m-1\} \text{ such that } \textstyle\sum_{i=1}^{m} \beta_i^{1+2^{2k+1}} \neq 0.$$

From the BCH bound, the minimum distance of $\mathscr{C}$ and $\mathscr{C}^\perp$ is at least 1 greater than the number of consecutive integers in Z and S, respectively.

Example: Consider GF(16) over GF(4). Here $q = 4 = 2^2$ and $l = 1$. From Corollary 16, we know that there can be no scalable code whose image is self-orthogonal w.r.t the Hermitian inner product but not trace. Hence, in this case, there can be no improvement over the quantum codes given in [3].

Example: Consider GF(64) over GF(4). Let $n = 63$ and α be a primitive root of the polynomial $X^6 + X + 1$ in GF(64). The power sums of interest in a dual basis $\{\beta_1, \beta_2, \beta_3\}$ are $\beta_1^3 + \beta_2^3 + \beta_3^3$, $\beta_1^9 + \beta_2^9 + \beta_3^9$, and $\beta_1^{33} + \beta_2^{33} + \beta_3^{33}$.

1) Now $\mathscr{B}_1 = \{1, \alpha^3, \alpha^{15}\}$ is a basis such that the sum of 3rd and 33rd powers is zero. Hence, $S \subseteq \{0,1,2,\ldots,62\}$ such that $-8S \subseteq Z$ and $-2S^c \nsubseteq Z^c$ leads to an RS code whose image w.r.t $\mathscr{B}_1'$ is self-orthogonal but not trace. An example is $S = \{17, 23\}$ ($S^c = \{5, 20, 17, 23, 29, 53\}, -8S = \{53, 5\}$, and $-2S^c = \{53, 23, 29, 17, 5, 20\}$).
2) Additionally, $\mathscr{B}_2 = \{1, \alpha, \alpha^5\}$ is a basis such that the sum of 9th powers is zero. Hence, $S \subseteq \{1, 2, \ldots, 62\}$ such that $(-2S \cup -32S) \subseteq Z$ and $-2S^c \nsubseteq Z^c$ leads to an RS code whose image w.r.t $\mathscr{B}_2'$ is self-orthogonal but not trace. An example is $S = \{1, 2, \ldots, 20\}$. This code leads to an [[189,69,21]] quantum code and has largest minimum distance among quantum codes of length 189 obtained by images of RS codes. The table of codes from [3] shows that trace is self-orthogonal for codes with nonzero sets $\{1\}$ to $\{1, 2, 3, 4, 5, 6\}$. Hence, the maximum minimum distance possible was limited to 7 for trace-self-orthogonal codes. Using self-orthogonality of images has resulted in the possibility of codes with minimum distance up to 21.
3) If $n = 7$, then $S = \{3, 4\}$ is such that $(-2S \cup -32S) = \{1, 2, 5, 6\}, S^c = \{1, 2, 3, 4, 5, 6\}$, and $-2S^c = S^c$. Hence, its image w.r.t $\mathscr{B}_2'$ is self-orthogonal but not trace. $S = \{1, 2, 3\}$ is such that $-8S = \{4, 5, 6\}, S^c = \{1, 2, 3, 4, 5, 6\}$, and $-2S^c = S^c$. Hence, its image w.r.t $\mathscr{B}_1'$ is self-orthogonal but not trace. This code leads to an [[21,3,4]] quantum code and has largest minimum distance among quantum codes of length 21 obtained by images of RS codes.

Table I is a partial list of quantum codes obtained by taking 4-ary images of cyclic codes over GF(16) and GF(64).

VII. Conclusion

We have derived necessary and sufficient conditions for self-orthogonality of images of codes with respect to a general biadditive form. The conditions separate into a power sum criterion on the dual basis elements and self-orthogonality of the original code with respect to conjugate biadditive forms. The condition can be easily applied

TABLE I

PARAMETERS $[[n,k,d]]$ OF QUANTUM CODES FOR $m = 2, 3$ AND $n_0 = 15, 7, 63$. S IS THE NONZERO SET OF THE CYCLIC CODE OVER GF(4^m). $n = mn_0, k = n - 2m|S|, d = |S| + 1$. NOTATION FOR BASIS IS FROM EXAMPLES.

m	n_0	n	k	d	S	Basis
2	15	30	26	2	{1}	All
		30	22	3	{1,2}	All
		30	18	4	{1,2,3}	All
		30	14	5	{1,2,3,4}	All
3	7	21	15	2	{1}	All
		21	9	3	{1,2}	All
		21	3	4	{1,2,3}	$\mathscr{B}'_1$
3	63	189	183	2	{1}	All
		189	177	3	{1,2}	All
		189	171	4	{1,2,3}	All
		189	165	5	{1,2,3,4}	All
		189	159	6	{1,2,3,4,5}	All
		189	153	7	{1,2,3,4,5,6}	All
		189	147	8	{1,2,3,4,5,6,7}	$\mathscr{B}'_2$
		189	141	9	{1,2,3,4,5,6,7,8}	$\mathscr{B}'_2$
		⋮	⋮	⋮	⋮	⋮
		189	75	20	{1,2,3,...,18,19}	$\mathscr{B}'_2$
		189	69	21	{1,2,3,...,18,19,20}	$\mathscr{B}'_2$

to practical codes such as cyclic codes to construct self-orthogonal codes. We have derived several interesting corollaries to the main result and showed a possible application in the construction of quantum codes.

Several avenues for future work are possible. The case of quadratic extensions and Hermitian-type products has been studied in detail. In particular, we have been able to find many cases for which self-orthogonality of an image is possible only through the self-orthogonality of the trace. An interesting problem is to extend this study to images of codes from GF(q^m) over GF(q) for $m \geq 3$. Can there be situations where self-orthogonality of an image implies self-orthogonality of the trace for $m \geq 3$? The answer could probably be obtained through the study of power sums of basis elements.

REFERENCES

[1] F. MacWilliams, N. Sloane, "The Theory of Error-Correcting Codes," North-Holland Mathematical Library, Volume 16, North-Holland, Amsterdam, 1977.

[2] C. T. Retter, "Orthogonality of Binary Codes Derived from Reed-Solomon Codes," *IEEE Transactions on Information Theory*, vol. 37, no. 4, pp. 983-994, Jul 1991.

[3] A. Thangaraj, S. W. McLaughlin, "Quantum codes from cyclic codes over GF(4^m)," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1176-1178, Mar 2001.

[4] A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369-1387, Jul 1998.

[5] G. E. Seguin, “The q-ary image of a q^m-ary cyclic code,” IEEE Transactions on Information Theory, vol. 41, no. 2, pp. 387 - 399, Mar 1995.

[6] Sakakibara, K., Kasahara, M., “On the minimum distance of a q-ary image of a q^m-ary cyclic code,” *Information Theory, IEEE Transactions on*, vol. 42, no. 5, pp. 1631-1635, Sep 1996.

[7] C. T. Retter, “An average weight-distance enumerator for binary expansions of Reed-Solomon codes,” *IEEE Transactions on Information Theory*, vol. 48, no. 5, pp. 1195 - 1200, May 2002.

[8] J. Lacan, E. Delpeyroux, “The q-ary image of some q^m-ary cyclic codes: permutation group and soft-decision decoding,” *IEEE Transactions on Information Theory*, vol. 48, no. 7, pp. 2069-2078, Jul 2002.

[9] A. Vardy, Y. Be’ery, “Bit-level soft-decision decoding of Reed-Solomon codes,” *IEEE Transactions on Communications*, vol. 39, pp. 440-444, Mar 1991.