Split Group Codes

Cunsheng Ding, *Member, IEEE*, David R. Kohel, *Associate Member, IEEE*, and San Ling

***Abstract*—We construct a class of codes of length n such that the minimum distance d outside of a certain subcode is, up to a constant factor, bounded below by the square root of n, a well-known property of quadratic residue codes. The construction, using the group algebra of an Abelian group and a special partition or *splitting* of the group, yields quadratic residue codes, duadic codes, and their generalizations as special cases. We show that most of the special properties of these codes have analogues for split group codes, and present examples of new classes of codes obtained by this construction.**

***Index Terms*—Duadic codes, quadratic residue codes, split group codes.**

I. Introduction

THE codes of study in this article unify elements common to quadratic residue codes, duadic codes, and their generalizations with a common construction. Binary duadic codes were introduced in Leon, Masley, and Pless [7] as a generalization of quadratic residue codes, and further studies in Pless, Masley, and Leon. [12]. The authors exploited features particular to $\mathbb{F}_2$ in order to write down an idempotent generator defining the codes. Smid [17] (for summary see [18]) removed the base field restriction and brought the definition in line with the constructive definition for quadratic residue codes. Under this definition, the Q-codes of Pless [11] are duadic codes over $\mathbb{F}_4$. Further aspects of these codes can be found in Rushanan [15] and Pless [13], [14].

Previously quadratic residue codes had been generalized in another direction in Camion [3] and in Ward [20]. In the approach of Camion, developed further in van Lint and MacWilliams [9], the generalized quadratic residue codes are defined as ideals in Abelian group algebras, a generalization of cyclic codes. Since most of the features of duadic codes also carry over to the Abelian group algebras, Rushanan [16] defines duadic codes in this setting, but reverts to a nonconstructive idempotent definition.

In the present work we unify the various Abelian group algebra constructions. By working with the dual group G of an Abelian group A, we can view the group algebra as a ring of functions on A. As a generalization of the duadic construction we broaden the definition of partitions, or splittings, and show that the main theorems for duadic codes hold in this larger setting. In particular, Theorem IV.5, Theorem IV.10, and Theorem IV.11 are analogues of the main theorems for duadic codes, which hold in this general context as well. By example we show that new subclasses introduced here hold good codes.

The paper is structured as follows. In Section II we introduce the Abelian group rings and the family of split group codes which form the objects of study in this work. The main body of this section is devoted to properties of the ideals and ideal codes in these rings. We follow in Section III with an investigation of the problem of determining the minimal subfield F over which a code can be defined and describe algorithmic aspects of computing with group algebra codes. Section IV treats duality, code extensions, and minimum-distance bounds, and Section V gives explicit examples and computational results for select subclasses of split group codes.

II. Split Group Codes

Let R be a finite commutative ring and let A be its underlying Abelian group. Then A is a finite Abelian group, written additively, whose exponent and order we denote by m and n, respectively. Let K be a field containing all the mth roots of unity and in which n is invertible. We write the group operation additively. Define $G = \mathrm{Hom}(A, K^*)$ to be the group of homomorphisms from A to K^*, or characters, and let $K[G]$ be the group ring over K. Since G and A are isomorphic, albeit noncanonically, the ring $K[G]$ is a commutative algebra of dimension n over K. For any character ψ in G we also denote by ψ its image in $K[G]$. By extending characters linearly, we interpret the elements of $K[G]$ as functions from A to K.

A. Abelian Group Rings and Decompositions

The following form of the discrete Fourier transform provides the basis for the later study of ideals and ideal codes in the ring $K[G]$.

Theorem II.1: Evaluation at x defines a homomorphism $K[G] \to K$ with kernel $m_x = \{f \in K[G] | f(x) = 0\}$, such that the map

$$\epsilon : K[G] \to K^A = \prod_{x \in A} K$$
$$f \mapsto (f(x))_{x \in A}$$

is an isomorphism of rings with inverse defined by

$$\lambda : K^A \to K[G].$$
$$(c_x)_{x \in A} \mapsto \frac{1}{n} \sum_{\psi \in G} \left(\sum_{x \in A} c_x \psi(x)^{-1} \right) \psi.$$

Manuscript received January 21, 1999; revised October 4, 1999. The work of D. Kohel was supported by an NSTB Grant as a Post-Doctoral Fellow at the National University of Singapore, and the work of C. Ding and S. Ling was supported in part by the NSTB-MOE under Grant RP 960668/M. Part of this work was done while S. Ling was visiting the Graduate School of Mathematical Sciences of the University of Tokyo under the Hitachi Fellowship from the Hitachi Scholarship Foundation.

C. Ding is with the Department of Computer Science, National University of Singapore, Singapore 117543 (e-mail: dingcs@comp.nus.edu.sg}.

D. R. Kohel is with the School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia (e-mail: kohel@maths.usyd.edu.au).

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

Communicated by I. F. Blake, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(00)01680-1.

The theorem is an immediate consequence of the orthogonality relations for characters (see Lang [6, ch. VIII, Pars. 4–5]). In the special case $A = \mathbb{Z}/n\mathbb{Z}$, we have an isomorphism $K[G] \cong K[X]/(X^n - 1)$ where X is the image of a generator for G. For a primitive nth root of unity ζ, we suppose, under the isomorphism with $K[G]$, that X acts on A by $X(r) = \zeta^r$. Then the evaluation map ϵ takes the usual form

$$f(x) \mapsto (f(1), f(\zeta), \cdots, f(\zeta^{n-1}))$$

of the discrete Fourier transform (see, for instance, Knuth [5, Par. 4.3.3C]).

An *idempotent* of a ring S is a nonzero element e such that $e^2 = e$, and is called *primitive* if for every other idempotent f, either $ef = e$ or $ef = 0$. The primitive idempotents in K^A are clearly the elements $\delta_x = (0, \cdots, 1, 0, \cdots, 0)$, having a 1 in the x-position. Under the isomorphism of rings, we obtain the following form for the primitive idempotents of $K[G]$.

Corollary II.2: The primitive idempotents of $K[G]$ are given by

$$e_x = \frac{1}{n} \sum_{\psi \in G} \psi(x)^{-1} \psi \tag{1}$$

one for each x in A, and the maximal ideal $\mathfrak{m}_x$ is generated by $1 - e_x$.

We return later to the role of idempotents in decompositions of rings and their ideal codes.

B. Splittings and Codes

For an element s of R we denote the corresponding endomorphism $x \mapsto sx$ of A by τ_s. We denote the induced *pullback* map on G and on $K[G]$ by μ_s, defined as $\mu_s(f) = f \circ \tau_s$, so that

$$\mu_s(f)(x) = f(sx)$$

for all $x \in A$ and all $f \in K[G]$. We define a *splitting* of A over Z to be a triple (Z, X_0, X_1) giving a partition $A = Z \cup X_0 \cup X_1$ for which there exists an element s in the unit group R^* of R with $\tau_s(X_0) = X_1$ and $\tau_s(X_1) = X_0$. We say that such an s *splits* (Z, X_0, X_1) and we say that an element s in R^* such that $\tau_s(X_0) = X_0$ and $\tau_s(X_1) = X_1$ *stabilizes* the splitting. This definition generalizes the splittings considered in Leon, Masley, and Pless [7].

For any subset X of A we define an ideal

$$I_X = \{f \in K[G] | f(x) = 0 \text{ for all } x \in X\}. \tag{2}$$

The *split group code* $C_0(K)$ over K associated to a splitting (Z, X_0, X_1) is defined to be the ideal $C_0(K) = I_{X_0}$ and the *conjugate* split group code to be $C_1(K) = I_{X_1}$. In a like manner, we define the subcodes $C_0^Z(K) = I_{Z \cup X_0}$, $C_1^Z(K) = I_{Z \cup X_1}$, and $C_Z(K) = I_{X_0 \cup X_1}$.

The code C_0 is said to be *split* by a unit s of R if $\mu_s(C_0) = C_1$ and $\mu_s(C_1) = C_0$ and *stabilized* by s if μ_s stabilizes C_0 and C_1. One verifies that μ_s acts on the set of maximal ideals by sending m_x to $m_{s^{-1}x}$, from which we obtain the following property of splittings.

Proposition II.3: A split group code C_0 is split or stabilized by s if and only if s splits or stabilizes (Z, X_0, X_1), respectively.

C. Idempotent Decompositions

In this section we indicate how Theorem II.1 gives the idempotent decomposition of $K[G]$. The following formulation gives this decomposition in terms of the primitive idempotents.

Proposition II.4: The ring $K[G]$ decomposes as a direct sum $\bigoplus_{x \in A} Ke_x$ such that $fe_x = f(x)e_x$, so that f has the form

$$f = \sum_{x \in A} f(x) e_x.$$

Every idempotent e in $K[G]$ can be uniquely written in the form

$$e = \sum_{x \in X} e_x$$

for a nonempty subset X of A.

Proof: By construction of e_x, under the ring isomorphism $K[G] \cong K^A$, the ideal Ke_x in $K[G]$ corresponds to the x-component in K^A with the image of e_x equal to the unity in that component. By definition of the isomorphism, the coefficient of e_x in an element f of $K[G]$ is $f(x)$. By definition an idempotent e satisfies $e^2 = e$, so is either zero or unity in each component, hence can be written as a sum of the primitive idempotents as indicated. □

Corollary II.5: All nonzero ideals of $K[G]$ are of the form

$$I_X = \bigoplus_{x \in X^c} Ke_x$$

generated by the idempotent $e = \sum_{x \in X^c} e_x$ for a unique proper subset X of A.

Proof: Let I be a nonzero ideal of $K[G]$ and set

$$X = \{x \in A | f(x) = 0 \text{ for all } f \text{ in } I\}.$$

From Proposition II.4 it is clear that if x is in X^c then I contains $Ie_x = Ke_x$ and that conversely $I \cap Ke_x = Ie_x = (0)$ for all x in X. Thus I is the ideal I_X, having the indicated form. Representing I as the product $\prod_{x \in X} \mathfrak{m}_x$ (see, for instance, Atiyah and MacDonald [1, Proposition 1.10]), Corollary II.2 implies that I is generated by the idempotent $e = \prod_{x \in X} (1 - e_x)$. Expanding e as a product, we find

$$e = \prod_{x \in X} (1 - e_x) = 1 - \sum_{x \in X} e_x = \sum_{x \in X^c} e_x$$

proving the form of the generator. □

Theorem II.6: Let (Z, X_0, X_1) be a splitting and let $C_0(K)$ be the associated split group code. Then the following results hold.

1) The codes $C_0(K)$ and $C_1(K)$ are generated by the idempotents

$$e = \sum_{x \in X_0^c} e_x \quad \text{and} \quad f = \sum_{x \in X_1^c} e_x.$$

Likewise, the codes $C_0^Z(K)$, $C_1^Z(K)$, and $C_Z(K)$ are generated by

$$\sum_{x \in X_1} e_x, \sum_{x \in X_0} e_x, \quad \text{and} \quad \sum_{z \in Z} e_z.$$

2) If the splitting is given by s, then μ_s induces an equivalence of $C_0(K)$ with its conjugate $C_1(K)$, and of the subcode $C_0^Z(K)$ with $C_1^Z(K)$.

3) $K[G]$ decomposes as a direct sum $C_Z(K) \oplus C_0^Z(K) \oplus C_1^Z(K)$.

Proof: The first statement follows from Corollary II.5 and the respective definitions of the codes. The second statement then follows by noting that $\mu_s(e_x) = e_{s^{-1}x}$, which implies that μ_s exchanges the idempotents e and f. Since μ_s also permutes the code basis G, this is an equivalence of codes. The decomposition of $K[G]$ follows by Proposition II.4 and the grouping

$$K[G] = \left(\bigoplus_{x\in Z} Ke_x\right) \oplus \left(\bigoplus_{x\in X_1} Ke_x\right) \oplus \left(\bigoplus_{x\in X_0} Ke_x\right)$$

according to the partition $A = Z \cup X_0 \cup X_1$. □

The next corollary is an elementary consequence of the theorem.

Corollary II.7: The codes $C_0(K)$ and $C_1(K)$ have dimension $(n + |Z|)/2$; the subcodes $C_0^Z(K)$ and $C_1^Z(K)$ have dimension $(n - |Z|)/2$; and the dimension of $C_Z(K)$ is $|Z|$.

III. Descending the Base Field

The field K was defined to contain the mth roots of unity. However, we generally want to define codes over fields on which we place no such requirement. Indeed, the principal field of interest is $\mathbb{F}_2$, which contains no nontrivial roots of unity at all!

In this section, we let F be a subfield of K of q elements, and extend the definition of split group codes to F. The main goal of the section is to give necessary and sufficient conditions for split group codes to be defined over F, and to describe constructive methods for producing such codes.

For any vector subspace $V = V(K)$ in K^n we define the descent problem as follows. Define $V(F) = V \cap F^n$, and note that

$$\dim_F(V(F)) \le \dim_K(V(K)).$$

If equality holds we say that V is *defined over the field* F. For fixed field F, over which the vector space $C_0(K)$ of $K^n = K[G]$ is defined, we write $C_0 = C_0(F)$, and refer to C_0 as the *split group code* over F. Similarly, we write C_1, C_0^Z, C_1^Z, and C_Z for the subcodes in $F^n = F[G]$ defined over F.

A. Defining Fields of Codes

The following split group code provides an example for the descent problem, namely, reducing to a minimal field F over which a code is defined. Implicit in this example and the following one, is the principle that the vector space of an ideal is defined over F if and only if it contains a generator in $F[G]$. The role of $\langle\tau_q\rangle$-orbit decompositions should also be apparent to the reader familiar with the cyclotomic coset decompositions and cyclic codes, but we leave the proofs of these result for the next section.

Example III.1: Let $F = \mathbb{F}_2$ and set $R = \mathbb{Z}/15\mathbb{Z}$. The 15th cyclotomic polynomial has a factor $p(X) = X^4 + X + 1$ over $\mathbb{F}_2$. Setting $K = \mathbb{F}_2[T]/(p(T))$, the image of T is a 15th root of unity, which we denote ζ.

Set $Z = 3\mathbb{Z}/15\mathbb{Z} \cup 5\mathbb{Z}/15\mathbb{Z}$. Its complement splits into $\langle\tau_2\rangle$-orbits $X_0 = \{1, 2, 4, 8\}$ and $X_1 = \{7, 13, 14, 11\}$, giving a splitting (Z, X_0, X_1) by -1. The polynomials

$$\begin{aligned} g_0(X) &= (X-\zeta)(X-\zeta^2)(X-\zeta^4)(X-\zeta^8) \\ &= X^4 + X + 1, \\ g_1(X) &= (X-\zeta^7)(X-\zeta^{13})(X-\zeta^{14})(X-\zeta^{11}) \\ &= X^4 + X^3 + 1. \end{aligned}$$

are then the generator polynomials of split group codes C_0 and C_1 defined over $\mathbb{F}_2$. Raising $g_i(X)$ in $\mathbb{F}_2[X]/(X^{15} - 1)$ to the power $2^4 - 1 = 15$ (see Proposition III.12), we obtain the idempotent generators

$$\begin{aligned} e_0 &= X^{12} + X^9 + X^8 + X^6 + X^4 + X^3 + X^2 + X + 1 \\ e_1 &= X^{14} + X^{13} + X^{12} + X^{11} + X^9 + X^7 + X^6 + X^3 + 1 \end{aligned}$$

over $\mathbb{F}_2$ for the split group code C_0 and its conjugate. □

The above shows how split group codes generalize the duadic codes of Leon, Masley, and Pless [7]—the latter being binary split group codes for splittings of $A = \mathbb{Z}/n\mathbb{Z}$ over the set $Z = \{0\}$ in the present terminology. Smid [17] extended the definition to arbitrary finite fields via generator polynomials, modeled on the standard one for quadratic residue codes. We summarize this correspondence in the present language as the following theorem. The proof is omitted, as it is a direct analog of [10, Theorem 6.9.3] of van Lint for quadratic residue codes, and both theorem and proof can be extracted from the proof and discussion following Theorem 2 of Pless [13].

Theorem III.2: Let $(\{0\}, S_0, S_1)$ be a splitting of $\mathbb{Z}/n\mathbb{Z}$, split by s in $\mathbb{Z}/n\mathbb{Z}^*$ and stabilized by τ_2. Then the element

$$e_0 = ((n+1)/2) + \sum_{a\in S_0} X^a \in \mathbb{F}_2[X]/(X^n - 1)$$

is an idempotent. Let G be the dual group of $\mathbb{Z}/n\mathbb{Z}$ and fix a primitive nth root of unity ζ. Then the isomorphism of rings

$$\mathbb{F}_2[X]/(X^n - 1) \to \mathbb{F}_2[G]$$

given by $X \mapsto \chi$, where $\chi(a) = \zeta^a$, maps the ideal generated by e_0 to a split group code C_0 defined with respect to a splitting $(\{0\}, X_0, X_1)$ of $\mathbb{Z}/n\mathbb{Z}$ by s.

Remark III.3: Note that the set X_0 can be effectively recovered as

$$X_0 = \{a \in \mathbb{Z}/n\mathbb{Z} | e_0(\zeta^a) = 0\}.$$

Except for the quadratic residue splitting, the map sending S_0 to X_0 is generally not the identity for any choice of root of unity. Thus the idempotent construction of Theorem III.2, used as the definition of duadic codes in Leon *et al.* [7], gives an entirely different construction for binary cyclic duadic codes. As seen in Example III.1, this special construction does not generalize to binary cyclic split group codes. Moreover, definitions via idempotent relations as employed in Pless [11] and [12] are nonconstructive so are deduced here only as consequences of split group code constructions. □

To emphasize that not all codes covered by this work are binary, we conclude this section with a pair of duadic codes over the field $\mathbb{F}_3$. It has been noted [17] that there exist splittings

of $\mathbb{Z}/n\mathbb{Z}$ over $\{0\}$ stabilized by τ_q if and only if q is a square modulo n. For binary codes, this implies that every prime divisor ℓ of n is congruent to $\pm 1 \bmod 8$ (of Leon *et al.* [7, Theorem 2]). For ternary codes, each ℓ must be congruent to $\pm 1 \bmod 12$. For $n = 11$ there are only two orbits of $\langle \tau_3 \rangle$ in $\mathbb{Z}/11\mathbb{Z}^*$, so the only ternary duadic code of this length is the $[11, 6, 5]$-quadratic residue code. The first new example occurs for block length 13.

Example III.4: Let $F = \mathbb{F}_3$ let $R = \mathbb{Z}/13\mathbb{Z}$. Since 3 generates the biquadratic residues in R^*, there exist two nonequivalent splittings over $Z = \{0\}$. These give the quadratic residue code and a distinct duadic code, respectively. First consider the quadratic residue code Q_0 of length 13, a $[13, 7, 5]$-code over $\mathbb{F}_3$. Its subcode Q_0^Z of functions vanishing on Z is a $[13, 6, 6]$-code with weight enumerator polynomial

$$1+104X^6+78X^7+156X^8+130X^9+156X^{10}+78X^{11}+26X^{12}.$$

Both codes are best possible for this length and their dimensions. For comparison, now consider the nonquadratic residue duadic code C_0. It is a $[13, 7, 4]$-code, but has subcode C_0^Z also of minimum distance 6. We find the weight enumerator polynomial to be

$$1 + 156X^6 + 494X^9 + 78X^{12},$$

so that the two subcodes Q_0^Z and C_0^Z are clearly nonequivalent codes with the same optimal minimum distance. □

B. Descent by Galois Action

Let $\mathcal{G} = \mathrm{Gal}(K/F)$ be the Galois group of the extension K/F, and let σ be the Frobenius automorphism $c \mapsto c^q$ which generates $\mathcal{G}$. Then $\mathcal{G}$ acts on $K[G]$ by the natural action on the coefficients, with $F[G]$ equal to the set of elements fixed under the action of $\mathcal{G}$. In this section we are interested in the action of this group on the collection of ideals in $K[G]$ in order to determine those ideals which are defined, as vector spaces, over F.

By assumption the integer q is relatively prime to m, so that as an element of the finite ring R, it is invertible, and τ_q is a well-defined automorphism of A. In this section we relate the action of τ_q to the Galois group $\mathcal{G}$. This lets us reduce the study of the Galois action on ideals in $K[G]$ to the action of the group $\langle \tau_q \rangle$ on subsets in A. The action of the Frobenius automorphism is described by the following elementary lemma.

Lemma III.5: The Frobenius automorphism σ acts on the primitive idempotents of $K[G]$ by $e_x^\sigma = e_{qx}$ and similarly on the maximal ideals by $\mathfrak{m}_x^\sigma = \mathfrak{m}_{qx}$.

Proposition III.6: The idempotents of $F[G]$ are those e in $K[G]$ of the form

$$e = \sum_{x \in Y} e_x$$

for which Y can be written as a union of orbits of $\langle \tau_q \rangle$ in A, and e is primitive if and only if $Y = \langle \tau_q \rangle x$ for some x in A. Let $\{e_1, \cdots, e_r\}$ be the set of primitive idempotents of $F[G]$ with corresponding orbits $\{Y_1, \cdots, Y_r\}$. Then in the local decomposition

$$F[G] = \bigoplus_{i=1}^{r} F[G]e_i$$

each $F_i = F[G]e_i$ is a field extension of degree $|Y_i|$ over $Fe_i \cong F$.

Proof: The form of the idempotents of $K[G]$ follows from Proposition II.4. The idempotents of $F[G]$ are then the idempotents of $K[G]$ which are invariant under the Galois group $\mathcal{G}$. By Lemma III.5 these must be the idempotents for which the index set Y is invariant under τ_q, that is, Y decomposes into a union of orbits of the group $\langle \tau_q \rangle$.

To show that $F[G]$ is isomorphic to a product of fields is to show that each local Artin factor F_i contains no nilpotents. But this is clear since $K[G]$ is a product of fields, hence contains no nilpotents.

To prove the statement about the degree of the extension F_i/Fe_i, it suffices to show that $\dim_F(F_i) = |Y_i|$. Equivalently, we show that $K[G]e_i = F_i \otimes_F K$ has dimension $|Y_i|$ over K. But $K[G]$ decomposes over K into one-dimensional factors, so we have

$$\dim_K(K[G]e_i) = \dim_K \left(\bigoplus_{x \in Y_i} Ke_x \right) = |Y_i|$$

and the statement follows. □

Corollary III.7: Every nonzero ideal I of $F[G]$ is of the form $\bigoplus_{i \in T} F[G]e_i$ and generated by the idempotent $e = \sum_{i \in T} e_i$, where $\{e_1, \cdots, e_r\}$ is the set of primitive idempotents and T is a nonempty subset of $\{1, \cdots, r\}$. Moreover, there exists a unique ideal J in $F[G]$ such that $I \oplus J = F[G]$.

Proof: Let I be an ideal of $F[G]$ and set

$$T = \{i \in \{1, \cdots, r\} | fe_i \neq 0 \text{ for some } f \text{ in } I\}.$$

Then for all i in $\{1, \cdots, r\}$ and all f in I such that fe_i is nonzero, $F_i = F_i f$ is contained in I and $Ie_j = \{0\}$ for j not in T. Thus $I = \bigoplus_{i \in T} F[G]e_i$, which is generated by the idempotent $e = \sum_{i \in T} e_i$. By Proposition III.6, it is clear that the ideal $J = \bigoplus_{i \in T^c} F[G]e_i$, where T^c is the complement of T in $\{1, \cdots, r\}$, is the unique ideal complementing I in $F[G]$. □

Theorem III.8: Let I be an ideal in $K[G]$. Then the following conditions are equivalent.

1) The ideal I is defined over F.
2) The set $X = \{x \in A | f(x) = 0 \text{ for all } f \text{ in } I\}$ is a union of $\langle \tau_q \rangle$-orbits.
3) The idempotent of I lies in $F[G]$.

Moreover, there exists a unique minimal subfield of K over which I is defined.

Proof: Suppose that I is defined over F. By Corollary II.5 we have $I = I_X$, where X is as defined in the theorem. Since I has a basis in $F[G]$, it must be stabilized by the Galois Group. By Lemma III.5 we then have

$$I_X = I_X^\sigma = \bigoplus_{x \in X^c} Ke_{qx} = \bigoplus_{x \in qX^c} Ke_x.$$

Therefore, $X^c = qX^c$ and so also $X = qX$. Suppose now that X is stabilized by τ_q, and let e be the idempotent of I. Then also by Lemma III.5

$$e^\sigma = \sum_{x \in X^c} e_{qx} = \sum_{x \in X^c} e_x = e$$

so e lies in $F[G]$. To complete the cycle, assume that $I = K[G]e$ for e in $F[G]$. Then since $F[G]e$ is contained in $I(F) = F[G] \cap I$, we have

$$\dim_F(I(F)) \geq \dim(F[G]e).$$

But $K[G]e = K \otimes_F F[G]e$, so the dimensions of vector spaces are preserved

$$\dim_F(F[G]e) = \dim_K(K[G]e) = \dim_K(I).$$

Thus by definition I is defined over F. □

Corollary III.9: If $C_0(K)$ is defined over F then so is $C_1(K)$, and $F[G]$ has the decomposition

$$F[G] = C_Z(F) \oplus C_0^Z(F) \oplus C_1^Z(F).$$

If s gives the splitting, then μ_s determines an equivalence of C_0 with C_1 and of C_0^Z with C_1^Z.

Proof: Since q lies in the center of R, the automorphisms τ_s and τ_q commute, hence τ_s permutes the $\langle \tau_q \rangle$-orbits. In particular, as the image of X_0, the set X_1 must also be the union of $\langle \tau_q \rangle$-orbits, hence $C_1(K)$ is defined over F. By Corollary III.7, the ideals $C_1^Z(F)$ and $C_0^Z(F)$, as the complementary ideals to $C_0(F)$ and $C_1(F)$, are defined over F. Moreover, either as the complement to $C_0^Z(F) \oplus C_1^Z(F)$, or as the intersection of $C_0(F)$ and $C_1(F)$, we find that $C_Z(F)$ is defined over F. The decomposition of $F[G]$ and the equivalence of codes follow from the corresponding results of Theorem II.6 over K. □

Theorem III.10: The block length, dimension, and minimum distance are well-defined invariants of C_0, independent of the field F over which C_0 is defined.

Proof: The block length and dimension are invariant by definition. Let F be the minimal field of definition for C_0. Consider an extension L/F, and let σ be the Frobenius automorphism. For any element $g = \sum_{\psi \in G} a_\psi \psi$ in $C_0(L)$ of minimum nonzero weight, we choose ϕ in $\mathrm{Supp}(g)$. Then $\mathrm{Supp}(g) = \mathrm{Supp}(g^\sigma)$ and $\mathrm{Supp}(a_\phi^\sigma g - a_\phi g^\sigma)$ is a proper subset, since it does not contain ϕ. Since g has minimal nonzero weight in $C_0(L)$, we must have $a_\phi^\sigma g - a_\phi g^\sigma = 0$. Setting $h = g/a_\phi = g^\sigma / a_\phi^\sigma$, it follows that h is defined over F, so the minimum distance of $C_0(F)$ equals that of $C_0(L)$. □

We note that the proof makes no use of special properties of the code C_0; in fact, the theorem holds for any linear code.

C. Explicit Constructions

Every finite Abelian group A of exponent m is isomorphic to a unique product of the form

$$\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

where m_i divides m_{i+1} and $m_r = m$. We set M equal to $\mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z})$. Then for such a decomposition of A, we choose generators $x_1, \cdots, x_r$ of the factors, and take $\pi_1, \cdots, \pi_r$ in M defined by

$$\pi_i(x_j) = \begin{cases} n_i, & \text{if } j = i \\ 0, & \text{otherwise} \end{cases}$$

where $n_i m_i = m$. One readily verifies that $\{\pi_1, \cdots, \pi_r\}$ is a basis for M.

Suppose χ is a fixed primitive character of $\mathbb{Z}/m\mathbb{Z}$. For any v in M we define $\chi^v = \chi \circ v$, and in particular set $\chi_i = \chi^{\pi_i}$ for $1 \leq i \leq r$. Then $\chi_1, \cdots, \chi_r$ generate G and we fix an isomophism

$$F[G] = F[\chi_1, \cdots, \chi_r] \cong \frac{F[X_1, \cdots, X_r]}{(X_1^{m_1} - 1, \cdots, X_r^{m_r} - 1)}$$

sending χ_i to X_i. Any v in M can be written as $c_1\pi_1 + \cdots + c_r\pi_r$, so $\chi^v = \chi_1^{c_1} \cdots \chi_r^{c_r}$ which is represented by the monomial $X_1^{c_1} \cdots X_r^{c_r}$ under the above isomorphism. We denote this element $\boldsymbol{X}^v$ when we want to think of it as a monomial in the quotient polynomial ring and as χ^v when we view it as a function.

For any subset Y of A stabilized by $\langle \tau_q \rangle$ we construct the ideal I_Y as follows. For $Y = Y_1 \cup Y_2$, we have $I_Y = I_{Y_1} I_{Y_2}$, so it suffices to determine the maximal ideals $\mathfrak{m}_Y = I_Y$. For $Y = \langle \tau_q \rangle z$, we define $M_Y = \{v \in M | v(z) = 0\}$, and let B_Y be a basis.

Let δ be the largest divisor of m such that $Y \subseteq \delta A$. We find $a_1, \cdots, a_r \in \mathbb{Z}/m\mathbb{Z}$ such that $\sum_{i=1}^r a_i \pi_i(z) = \delta$, and define $\pi = \sum_{i=1}^r a_i \pi_i$. With this notation we can write down a collection of generators for $\mathfrak{m}_Y$.

Proposition III.11: The maximal ideal $\mathfrak{m}_Y$ is generated by the set

$$\mathcal{S} = \left\{ g^\pi = \prod_{y \in Y} (\boldsymbol{X}^\pi - \chi^\pi(y)) \right\} \cup \{\boldsymbol{X}^v - 1 | v \in B_Y\}.$$

Proof: By definition, for any y in Y and v in B_Y we have

$$\boldsymbol{X}^v(y) = \chi(v(y)) = \chi(0) = 1.$$

Likewise, it is clear that $g^\pi(y) = 0$, so $\mathcal{S}$ is contained in $\mathfrak{m}_Y$. It suffices to show the converse: if y is a root of all functions in $\mathcal{S}$, then y lies in Y. Let $\phi : \mathbb{Z}/m\mathbb{Z} \to A$ be a splitting of π, i.e., $\phi : \mathbb{Z}/m\mathbb{Z} \to A$ so that $\pi\phi$ is the identity on $\mathbb{Z}/m\mathbb{Z}$. Suppose that y is in A such that $\chi^v(y) = 1$ for all v in B_Y. Then y lies in the subgroup $\mathbb{Z}/m\mathbb{Z}\, z$ of $\mathbb{Z}/m\mathbb{Z}\, \phi(1)$ generated by Y. Since Y is in bijection with $\pi(Y)$, in order to show that a root of g^π in $\mathbb{Z}/m\mathbb{Z}\, \phi(1)$ actually lies in Y, we show that $g = (g^\pi)^\phi$ in $F[\chi]$ has roots only in $\pi(Y)$. But by definition g equals

$$\prod_{y \in Y} (\boldsymbol{X}^{\pi\phi} - \chi^\pi(y)) = \prod_{y \in Y} (\chi - \chi^\pi(y)).$$

So the roots of g in $\mathbb{Z}/m\mathbb{Z}$ are precisely those in $\pi(Y)$. □

A set of generators for an ideal I may be reduced to the single idempotent generator by the following proposition.

Proposition III.12: Let g be a nonzero element in $F[G]$, let d be the order of the group $\langle \tau_q \rangle$, and set $\ell = q^d - 1$. Then $e = g^\ell$ is an idempotent. For any collection of generators $g_1, \cdots, g_t$ of an

ideal I with corresponding idempotents $e_1 = g_1^\ell, \cdots, e_t = g_t^\ell$, the element

$$e = \sum_{i=1}^{t} e_i \prod_{j<i} (1 - e_j)$$

is the idempotent generator for I.

Proof: By Proposition III.6, the group algebra $F[G]$ is isomorphic to a product of field extensions of F, each of degree dividing d over F. In particular, $e = g^\ell$ is congruent to one or zero in every quotient, hence is an idempotent. To prove the main statement, we note that a collection of elements $f_1, \cdots, f_t$ generates the ideal $I = I_Y$ if and only if the intersection of the zero sets Y_i of f_i equals Y. It is clear that each e_i has the same zeros as the corresponding g_i. Suppose that e_1 and e_2 are idempotents whose zero sets are subsets Y_1 and Y_2 of A. Then it is immediately verified that $e = e_1 + e_2 - e_1 e_2$ is an idempotent, and by evaluating at each x in A, we check that e has zero set $Y_1 \cap Y_2$. By induction on t, it follows that the idempotent of I has the indicated form. □

In the above construction we have omitted the issue of constructing the character χ. The definition of χ requires only that we construct an extension field of F with a prescribed nth root of unity. This reduces to a standard polynomial factorization problem over finite fields, as already seen in Example III.1. The following provides a complete worked example of the idempotent construction.

Example III.13: Let $F = \mathbb{F}_2$ and set $R = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Define $K = F_2[\zeta]$ and $\chi(1) = \zeta$ where ζ satisfies the irreducible factor $X^3 + X + 1$ of the seventh cyclotomic polynomial. If Y is the orbit generated by $(1, 2)$, then the group M_Y has basis $\{v\}$ where $v((x_1, x_2)) = x_1 + 3x_2$. We can take π to be the homomorphism defined by $\pi((x_1, x_2)) = x_1$. By Proposition III.11, this gives generators $X_1 X_2^3 + 1$ and $X_1^3 + X_1 + 1$, so we find a generating set of idempotents

$$\begin{aligned} e_0 &= (X_1^3 + X_1 + 1)^7 = X_1^4 + X_1^2 + X_1 \\ e_1 &= (X_1 X_2^3 + 1)^7 = X_1^2 X_2^6 + X_1^4 X_2^5 + X_1^6 X_2^4 \\ &\quad + X_1 X_2^3 + X_1^3 X_2^2 + X_1^5 X_2. \end{aligned}$$

The idempotent generator $e = e_0 + e_1 - e_0 e_1$ of $\mathfrak{m}_Y$ is then

$$\begin{aligned} &(X_1^6 + X_1^4 + X_1^3 + X_1^2) X_2^6 + (X_1^6 + X_1^5 + X_1^4 + X_1) X_2^5 \\ &\quad + (X_1^6 + X_1^3 + X_1 + 1) X_2^4 + (X_1^5 + X_1^3 + X_1^2 + X_1) X_2^3 \\ &\quad + (X_1^5 + X_1^4 + X_1^3 + 1) X_2^2 + (X_1^6 + X_1^5 + X_1^2 + 1) X_2 \\ &\quad + X_1^4 + X_1^2 + X_1. \end{aligned}$$

In terms of the basis

$$\{1, X_1, \cdots, X_1^6, X_2, \cdots, X_1^6 X_2^6\}$$

the idempotent is the weight 27 vector

$$(01101001010011100111001110101101001010011100111101)$$

and a subset of

$$\{X_1^i X_2^j e | 0 \le i < 7, 0 \le j < 7\}$$

gives a vector space basis for the ideal generated by e.

IV. Duality, Extensions, and Minimum Distance

In this section we analyze the decomposition of split group codes into orthogonal ideals under certain conditions on the splittings. In Section IV-B we introduce extensions of split group codes, define an inner product, and find conditions for the extended codes to be self-dual. In general, the extension need not exist; we require that the base field F contain sufficiently many roots of unity. In a typical situation Z is a subgroup of A and the condition is that the image of Z under all characters in G is contained in F. For the duadic codes $Z = \{0\}$ and this condition is void. In the general case this extends the theory of duality for duadic codes to general split group codes.

A. Orthogonal Decompositions

For $f = \sum_{\psi \in G} a_\psi \psi$ in $K[G]$ we define the *support* of f to be the set

$$\mathrm{Supp}\,(f) = \{\psi \in G | a_\psi \neq 0\}$$

such that the *weight* of f is $||f|| = |\mathrm{Supp}\,(f)|$.

Proposition IV.1: The standard Euclidean inner product of f and g in $F[G]$ is

$$\langle f, g \rangle = \frac{1}{n} \sum_{x \in A} f(x) g(-x).$$

Proof: Let $f = \sum_\psi a_\psi \psi$ and $g = \sum_\psi b_\psi \psi$, and set

$$f * g = f \mu_{-1}(g).$$

Then the coefficient of the trivial character in $f * g$ is

$$\langle f, g \rangle = \sum_\psi a_\psi b_\psi.$$

Expanding $f * g$ in terms of its idempotent decomposition, we find

$$f * g = \frac{1}{n} \sum_{\psi \in G} \sum_{x \in A} f(x) g(-x) \psi^{-1}(x) \psi.$$

But by Theorem II.1 the coefficient of the trivial character is also $n^{-1} \sum_x f(x) g(-x)$. □

Remark IV.2: Since f and g lie in $F[G]$, the inner product lies in F even though the summation occurs in the extension K.

Corollary IV.3: Suppose that Z is stabilized by -1. Then the dual of C_Z is $C_0^Z \oplus C_1^Z$. If -1 splits C_0 then $C_0^\perp = C_0^Z$, and if -1 stabilizes C_0 then $C_0^\perp = C_1^Z$. In the latter case, the ideal decomposition

$$F[G] = C_Z \oplus C_0^Z \oplus C_1^Z$$

is an orthogonal decomposition of $F[G]$.

Proof: Suppose that -1 stabilizes Z, and let f lie in C_Z and g lie in $C_0^Z \oplus C_1^Z$. Then

$$\langle f, g \rangle = \frac{1}{n} \sum_{x \in A} f(x) g(-x) = 0$$

since $f(x) = 0$ for all x in $X_0 \cup X_1$ and $g(-x) = 0$ for all x in Z. The remaining orthogonality results are similar. □

We can now state the following theorem, which generalizes a well-known property of binary quadratic residue codes.

Theorem IV.4: Suppose that $F = \mathbb{F}_2$ and C_0^Z is contained in its dual. Then the weight of every codeword in C_0^Z is congruent to $0 \bmod 4$.

Proof: Since 0 lies in Z, every element f of C_0^Z satisfies $f(0) = 0$, hence has even weight. Since C_0^Z is contained in its dual

$$0 = \langle f, g \rangle = |\mathrm{Supp}\,(f) \cap \mathrm{Supp}\,(g)| \bmod 2$$

for all f and g in C_0^Z. From the equality

$$\|f + g\| = \|f\| + \|g\| - 2|\mathrm{Supp}\,(f) \cap \mathrm{Supp}\,(g)|$$

we conclude that $\|\cdot\| : C_0^Z \to \mathbb{Z}/4\mathbb{Z}$ is a well-defined group homomorphism with image in $2\mathbb{Z}/4\mathbb{Z}$. Let D_0^Z be the kernel of this map. Then it is clear that it is an ideal for $F[G]$, and is of codimension zero or one in C_0^Z. By Corollary III.7, there exists a complementary ideal J such that $C_0^Z = D_0^Z \oplus J$. By Proposition III.6, the only ideal of dimension one is that which corresponds to the orbit $\{0\}$. The idempotent generator of this ideal, the odd weight element $\sum_{\psi \in G} \psi$, does not lie in C_0^Z, so $J = 0$ and $C_0^Z = D_0^Z$. □

B. Code Extensions

Let (Z, X_0, X_1) be a splitting of A giving a code C_0 over F. Suppose that -1 either splits or stabilizes the code and that F contains the image of Z under all characters in G.

Let $F^Z = \prod_{z \in Z} F$ and define a map $F[G]$ to F^Z by evaluation at elements of Z. For each $f \in F[G]$ we define $f_Z = (f(z))_{z \in Z}$. The extended code $\bar{C}_0$ is defined to be the subspace

$$\bar{C}_0 = \{\tilde{f} = (f, f_Z) | f \in C_0\} \subseteq F[G] \times F^Z.$$

$\bar{C}_1$ is defined similarly. We define an inner product on F^Z by

$$\langle u, v \rangle = -\frac{1}{n} \sum_{z \in Z} u_z v_{-z}$$

for all $u = (u_z)_{z \in Z}$ and $v = (v_z)_{z \in Z}$ in F^Z. Using this inner product on F^Z, we extend the usual Euclidean inner product on $F[G]$ to the extended word space $F[G] \times F^Z$ by defining $F[G]$ and F^Z to be orthogonal subspaces.

Theorem IV.5: The extended codes $\bar{C}_0$ and $\bar{C}_1$ are equivalent. If -1 splits C_0, then $\bar{C}_0$ and $\bar{C}_1$ are self dual, and if -1 stabilizes C_0, then $\bar{C}_0$ is dual to $\bar{C}_1$.

Proof: The equivalence of $\bar{C}_0$ and $\bar{C}_1$ follows immediately from the equivalence of C_0 and C_1 in Corollary III.9. Suppose that $\mu_{-1}(C_0) = C_1$, and let f and g be in C_0. Then $f * g = f\mu_{-1}(g)$ lies in $C_0 \cdot C_1 = C_0 \cap C_1$. Thus $f * g$ has the form

$$\sum_{z \in Z} f(z) g(-z) e_z = \frac{1}{n} \sum_{\psi \in G} \sum_{z \in Z} f(z) g(-z) \psi^{-1}(z) \psi.$$

On the other hand, if we write $f = \sum_\psi a_\psi \psi$ and $g = \sum_\phi b_\phi \phi$, then expanding the product, we find $f * g$ equals

$$\left(\sum_{\psi \in G} a_\psi \, \psi \right) \left(\sum_{\phi \in G} b_\phi \, \phi^{-1} \right) = \sum_{\psi \in G} \sum_{\phi \in G} a_\psi b_\phi \psi \phi^{-1}.$$

Equating coefficients of the trivial character, we find that

$$\langle f, g \rangle = \sum_{\psi \in G} a_\psi b_\psi = \frac{1}{n} \sum_{z \in Z} f(z) g(-z) = -\langle f_Z, g_Z \rangle$$

which implies the triviality of the inner product $\langle \tilde{f}, \tilde{g} \rangle$. The duality of $\bar{C}_0$ and $\bar{C}_1$ when $\mu_{-1}(C_0) = C_0$ follows similarly. □

C. Minimum Distance Bounds

Let C_0 be the split group code over F relative to a splitting (Z, X_0, X_1). We assume a fixed element s which splits C_0 and for $f \in F[G]$ define $f^* = f\mu_s(f)$.

Let N be the additive subgroup of A generated by Z. Define H to be the subgroup of G vanishing on Z (equivalently on N), and let $\mathcal{C}$ be a set of coset representatives for G/H. Then G/H is identified with the dual of N and H with the dual of A/N, whose order we denote by h. We define an element e_H by

$$e_H = \frac{1}{h} \sum_{\psi \in H} \psi.$$

Lemma IV.6: Let C_0 be a split group code over a field of q elements. If τ_s agrees with a power of τ_q on Z, then for each z in Z, $f(z) = 0$ if and only if $f^*(z) = 0$.

Proof: If $\tau_s = \tau_q^r$ on Z, then $f(sz) = f(q^r z) = f(z)^{q^r}$, for all z in Z. □

Lemma IV.7: If C_0 is split by s then the subgroup H is stabilized by μ_s.

Proof: Elements ϕ in H are characterized by the condition that $\phi(z) = 0$ for all z in Z. Since τ_s stabilizes Z, for any ϕ in H and z in Z, $\mu_s(\phi)(z) = \phi(sz) = 0$, so $\mu_s(\phi)$ lies in H. □

Lemma IV.8: The element e_H is the idempotent generator of I_{N^c}, and every g in C_Z is of the form

$$g = \sum_{\phi \in \mathcal{C}} c_\phi e_H \phi.$$

In particular, the support of g is a union of cosets of H.

Proof: Viewing H as the group of characters on A/N, the value of e_H equals 1 on N and zero elsewhere by the orthogonality relations for characters. Therefore, e_H is the idempotent generator for I_{N^c}. Since Z^c contains N^c, the ideal I_{N^c} contains $C_Z = I_{Z^c}$, so every element g of C_Z can be written

$$g = f e_H = \sum_{\phi \in \mathcal{C}} c_\phi e_H \phi,$$

as indicated. □

Proposition IV.9: Let C_0 be split by s and let f be in C_0. Then f^* is of the form $\sum_{\phi \in \mathcal{C}} c_\phi e_H \phi$. Moreover, if the support of f is contained in a coset of H, then f^* is of the form

$$f^* = c_\xi e_H \xi$$

for some ξ in G. If $s = -1$ then the coefficient c_ε of the trivial character ε is $\langle f, f \rangle h$.

Proof: Since f^* lies in $C_0 C_1 = C_Z$, by Lemma IV.8 we have

$$f^* = \sum_{\phi \in \mathcal{C}} c_\phi e_H \phi.$$

Since $Q = \mathrm{Supp}\,(f)$ is contained in a coset $H\rho$ of H, by Lemma IV.7 the set $\mathrm{Supp}\,(\mu_s(f)) = \mu_s(Q)$ is contained in $H\mu_s(\rho)$. Then

$$\mathrm{Supp}\,(f^*) \subseteq Q\mu_s(Q) \subseteq H\xi$$

where $\xi = \rho^*$. Thus f^* has support on $H\xi$ and is of the form $f^* = c_\xi e_H \xi$.

Now suppose that $s = -1$, then $\xi = \rho\rho^{-1}$ is the trivial character. Write $f = \sum_{\psi\in G} a_\psi\psi$. Then the coefficient of the trivial character in the expansion

$$f^* = \sum_{\phi\in G}\sum_{\psi\in G} a_\psi a_\phi \psi\phi^{-1}$$

is $\sum_{\psi\in G} a_\psi^2 = \langle f, f\rangle$. It follows that $c_\varepsilon = \langle f, f\rangle h$. □

Theorem IV.10: Suppose that C_0 is the split group code over a field of q elements, and suppose that τ_s agrees with a power of τ_q on Z. Then the minimum weight d of a codeword in $C_0\backslash C_0^Z$ satisfies the bound

$$h \le \begin{cases} d^2 - d + 1, & \text{if } s = -1 \\ d^2, & \text{otherwise.} \end{cases}$$

Proof: If f lies in $C_0\backslash C_0^Z$, then f^* is nonzero by Lemma IV.6. Since $f^*(x) = 0$ for all x in $X_0 \cup X_1$, we have

$$f^* = \sum_{z\in Z} f^*(z)e_z = \frac{1}{n}\sum_{\psi\in G}\sum_{z\in Z} f^*(z)\psi(z)^{-1}\psi.$$

Since $\phi(z) = \psi(z)$ for all ϕ and ψ in the same coset of H and all z in Z, the sum for f^* can be expressed as

$$f^* = \frac{h}{n}\sum_{\phi\in\mathcal{C}}\left(\sum_{z\in Z} f^*(z)\phi(z)^{-1}\right)e_H\phi.$$

Thus f^* has a positive multiple of h nonzero coefficients. On the other hand, f^* has at most d^2 nonzero coefficients, which implies $d^2 \ge h$. If C_0 is split by $s = -1$, then d coefficients of expansion for f^* contribute to the coefficient of the trivial character, so $d^2 - d + 1 \ge h$. □

We define an *incidence relation* $i : K[G] \times G \to \{0, 1\}$ by setting $i(f, \psi) = 1$ if ψ is in the support of f and $i(f, \psi) = 0$ otherwise. In reference to the incidence structure, we refer to functions in $K[G]$ as *lines* and characters in G as *points*. Moreover, if $i(f, \psi) = 1$, then we say that f *meets* ψ.

Theorem IV.11: Let C_0 be a split group code over F which is split by -1, and suppose that $\tau_{-1} = \tau_q^r$ on Z for some integer r. If $C_0\backslash C_0^Z$ has a codeword f of minimum weight d, satisfying $h = d^2 - d + 1$, then if f meets the trivial character, the following statements hold.

1) The set $Q = \mathrm{Supp}\,(f)$ is a difference set for H with parameter $\lambda = 1$.
2) Each coset $\mathbb{P}_\phi = H\phi$ comprises the set of points of a combinatorial projective plane of order $d-1$ with respect to the set of lines $\mathcal{L}_\phi = fH\phi$.
3) The minimum distance of C_0 is d.

Proof: Since f^* lies in C_Z, by Proposition IV.9, its support is a union of cosets of H. On the other hand, $\mathrm{Supp}\,(f^*)$ lies in $\{\psi\phi^{-1} | \psi, \phi \in Q\}$, so has at most $h = d^2 - d + 1$ elements. Since f^* is nonzero, it follows that $\mathrm{Supp}\,(f^*) = H$, and every nontrivial element of H can be uniquely represented in the form $\psi\phi^{-1}$ for ψ and ϕ in Q. Since f meets the trivial character, Q is contained in H, and the first statement holds.

The support of a line in $\mathcal{L}_\phi = fH\phi$ is clearly contained in the set $\mathbb{P}_\phi = H\phi$. It suffices to show that two distinct lines in $\mathcal{L}_\phi$ meet at a unique point. Let $g_1 = f\nu$ and $g_2 = f\xi$ be two such lines with support $Q_1 = Q\nu$ and $Q_2 = Q\xi$, respectively. Consider the product map

$$Q_1 \times Q_2^{-1} \to H\nu\xi^{-1} = H$$

given by the restriction of the group law on G. The inverse image of $\nu\xi^{-1}$ has d elements and elsewhere the map is bijective. In particular, since $\nu \ne \xi$, there is a unique pair (ψ, ψ^{-1}) mapping to the trivial character, implying g_1 and g_2 meet uniquely at the point ψ.

Now let g be in C_0^Z. We may assume that g meets the trivial character. C_0 and C_0^Z are dual by Corollary IV.3, so $\langle f\psi^{-1}, g\rangle = 0$. Thus if $f\psi^{-1}$ and g meet, they must do so at more than one point. By construction g and $f\psi^{-1}$ meet at the trivial character for all ψ in Q. Since the lines $\{f\psi^{-1} | \psi \in Q\}$ are pairwise-disjoint away from the trivial character, it follows that g has weight at least $d + 1$. □

V. Examples of Split Group Codes

In this section we demonstrate two constructions by which we remove the restriction that q be a square modulo all prime divisors of the block length. We focus on the cyclic case; examples of the general construction for noncyclic Abelian groups will be reserved for treatment in a later article.

A. Dual Nonresidue Split Group Codes

Let ℓ and m be distinct primes such that q is not a square $\bmod \ell$ or $\bmod m$. Set $R = \mathbb{Z}/n\mathbb{Z}$ where $n = \ell m$, and let A its Abelian group. Let

$$\left(\frac{\cdot}{n}\right) : \mathbb{Z}/n\mathbb{Z} \to \{0, 1, -1\}$$

be the Kronecker symbol (see Cohen [4, Par. 1.4]). We set $Z = m\mathbb{Z}/n\mathbb{Z} \cup \ell\mathbb{Z}/n\mathbb{Z}$ and take X_0 to be the set

$$X_0 = \left\{a \in R \,\middle|\, \left(\frac{a}{n}\right) = 1\right\}$$

which is stable under $\langle\tau_q\rangle$, and X_1 its complement outside of Z. The following theorem shows that the codes C_0 relative to this splitting are bad.

Theorem V.1: Suppose (Z, X_0, X_1) is a splitting of an Abelian group A such that Z contains a subgroup N of order m. Let G be the dual group of A, and let H be the subgroup which is trivial on N. Then $f = \sum_{\phi\in H}\phi$ is a codeword in C_0 of weight n/m. In particular, the minimum distance is bounded above by n/m.

Proof: We may view H as the group of characters on A/N. Then

$$f(x) = \sum_{\phi\in H}\phi(1) = |H|$$

for x in N, and by the orthogonality relations for characters, is 0 on all other elements of A. Since X_0 does not meet $N \subseteq Z$, it is clear that f is in C_0. □

Applying the theorem to the construction, we find that the code C_0 has minimum distance bounded above by ℓ, the smaller of the two prime divisors of n. In contrast, the subcode C_0^Z contains no obvious codeword of small weight, and, experimentally, appears to generally have large minimum weight. The simplest

example is that in Example III.1. In Table I we present data for the block length, dimension, and minimum weight of these codes over $\mathbb{F}_2$ up to block length 209.

B. Twisted Lifts of Split Group Codes

Although the codes C_0^Z described above perform well, in order to have reasonable minimum distance for C_0, it is clear from Theorem V.1 that we should avoid splittings for which Z contains a large subgroup of A. Also in light of Theorem IV.11, we may want to consider splittings for which Z is a small subgroup of A. We thus present another example in which the block length is divisible by a single small prime in which q is a quadratic nonresidue.

Example V.2: Let $F = F_2$, set $R = \mathbb{Z}/21\mathbb{Z}$ and let A be its additive group. Since the subset $7R^*$ of A consists of a single $\langle\tau_2\rangle$-orbit of two elements, we set $Z = 7\mathbb{Z}/21\mathbb{Z}$, and take X_0 to be

$$X_0 = \left\{a \in R \,\middle|\, \left(\frac{a}{7}\right) = 1\right\}$$

where $(a/7)$ is the Legendre symbol. Since 2 is a quadratic residue in $\mathbb{Z}/7\mathbb{Z}$, it is clear that τ_2 stabilizes the splitting. Moreover, -1 is a quadratic nonresidue $\bmod 7$, so gives the splitting. The associated split group code, denoted Q_0, is a $[21, 12, 3]$-code, while the subcode Q_0^Z of functions vanishing on Z is a $[21, 9, 4]$-code, both poor codes. If instead we choose X_0 equal to

$$\left\{a \in R^* \,\middle|\, \left(\frac{a}{7}\right) = 1\right\} \cup \left\{a \in 3R^* \,\middle|\, \left(\frac{a}{7}\right) = -1\right\}$$

then we obtain a split group code C_0 with parameters $[21, 12, 5]$ and subcode C_0^Z with parameters $[21, 9, 8]$, both of which are best possible for length 21 and their respective dimensions.

In the next construction we develop this idea further, showing that the special case above is typical. We describe first a formal construction for provably bad codes, and discuss how to "twist" them to obtain codes which experimentally perform well.

Let (W, Y_0, Y_1) be a splitting of the additive group of a finite ring S with associated split group code Q_0 and subcode Q_0^W. Suppose that there exists a surjective homomorphism $\pi : R \to S$ with kernel of order ℓ. We form the lifted splitting (Z, X_0, X_1) of A by setting

$$Z = \pi^{-1}(W), \quad X_0 = \pi^{-1}(Y_0), \quad \text{and} \quad X_1 = \pi^{-1}(Y_1)$$

and let C_0 and C_0^Z be the associated split group codes. For such codes we have the following theorem, which shows that these codes are bad.

Theorem V.3: The weight enumerator polynomial of C_0 is $w(T)^\ell$, where $w(T)$ is the weight enumerator polynomial of Q_0. The same relation holds between the respective weight enumerator polynomials of C_0^Z and of Q_0^W. In particular, the minimum distances of C_0 and C_0^Z are the same as the minimum distances of Q_0 and Q_0^W, respectively.

Proof: Denote the additive groups of R and S by A and B, respectively, and set $M = \mathrm{Hom}(B, K^*)$ and $G = \mathrm{Hom}(A, K^*)$. Then the pullback $\pi^* : M \to G$ is an injective homomorphism with cokernel of order ℓ. Denote also by π^* the induced ring homomorphism $F[M] \to F[G]$. Under this homomorphism, $F[G]$ decomposes as an $F[M]$-module into a direct sum $F[G] = \bigoplus \pi^*(F[M])\psi$, where ψ ranges over coset representatives of G/M. Consider the idempotent e_0 for Q_0. Then by definition, for all x in A, $\pi^*(e_0)$ satisfies

$$\pi^*(e_0)(x) = e_0(\pi(x)) = \begin{cases} 0, & \text{if } \pi(x) \in Y_0 \\ 1, & \text{otherwise} \end{cases}$$

so is the idempotent for C_0. In particular, C_0 is generated by the image of Q_0, so we have an $F[M]$-module decomposition

$$C_0 = F[G]\,\pi^*(Q_0) = \bigoplus \pi^*(Q_0)\psi.$$

The form of the weight enumerator polynomial follows from the fact that each $\pi^*(F[M])\,\psi$, hence $\pi^*(Q_0)\,\psi$, has disjoint support in G, and from the independence of the equivalent subcodes $\pi^*(Q_0)\psi$. The decomposition of C_0^Z into copies of Q_0^W follows by the same argument, and equality of the minimum distances is then clear. □

We apply the above theorem to the following setting. Let $S = \mathbb{Z}/m\mathbb{Z}$, for a prime m, let $R = \mathbb{Z}/\ell m\mathbb{Z}$, and let π be the surjective homomorphism $R \to S$. Let Q_0 and Q_0^W be

TABLE I
DUAL NONRESIDUE CYCLIC SPLIT CODES OVER $\mathbb{F}_2$

		C_0			C_0^Z		
ℓ	m	n	k	d^a	n	k	d^a
3	5	15	11	3	15	4	8
3	11	33	23	3	33	10	12
3	13	39	27	3	39	12	12
5	11	55	35	5	55	20	16
3	19	57	39	3	57	18	16
5	13	65	41	5	65	24	16
5	13[c]	65	41	5	65	24	16
3	29	87	59	3	87	28	24
5	19	95	59	5	95	36	16
3	37	111	75	3	111	36	24
3	43	129	87	3	129	42	28[b]
11	13	143	83	11	143	60	24[b]
5	29	145	89	5	145	56	24[b]
5	29[c]	145	89	5	145	56	26[b]
3	53	159	107	3	159	52	32[b]
3	59	177	119	3	177	58	30[b]
3	61	183	123	3	183	60	36[b]
5	37	185	113	5	185	72	24[b]
5	37[c]	185	113	5	185	72	32[b]
3	67	201	135	3	201	66	36[b]
11	19	209	119	11	209	90	30[b]

[a] Minnimum distance computed with Magma [8].

[b] Upper bound found by probabilistic search for minimum-weight vectors with Magma; in each case the minimum distance is provably bounded below by 18.

[c] For $\gcd(\ell - 1, m - 1)$ greater than 2 there exist additional splittings over Z; for the pairs $(5, 13)$, $(5, 29)$, and $(5, 37)$ we find an additional inequivalent splitting, reported here.

TABLE II
QUADRATIC RESIDUE CODES OVER $\mathbb{F}_2$

C_0			C_0^Z			
m	k	d^a	m	k	d^a	d_0
7	4	3	7	3	4	3
17	8	5	17	7	6	5
23	12	7	23	11	8	6
31	16	7	31	15	8	6
41	21	9	41	20	10	7
47	24	11	47	23	12	8
71	36	11	71	35	12	9
73	37	13	73	36	14	9
79	40	15	79	38	16	9
89	45	17	89	44	18	10
97	49	15	97	48	16	10
103	52	19	103	51	20	11
113	57	15	113	56	16	11
127	64	19	127	63	20	12

[a] Minimum distance computed with Magma [8].

TABLE III
TWISTED LIFTS OF QR CODES OVER $\mathbb{F}_2$ FOR $\ell = 3$

	C_0			C_0^Z			
m	n	k	d^a	n	k	d^a	d_0
7	21	12	5	21	9	8	3
17	51	27	9	51	24	10	5
23	69	36	11	69	33	12	6
31	93	48	14	93	45	16	6
41	123	63	18	123	60	20	7
47	141	72	21	141	69	24	8
71	213	108	22^b	213	105	24^b	9
73	219	111	26^b	219	108	28^b	9
79	237	120	30^b	237	117	32^b	9
89	267	135	35^b	267	132	36^b	10
97	291	147	29^b	291	144	30^b	10
103	309	156	39^b	309	153	40^b	11
113	339	171	46^b	339	168	48^b	11
127	391	197	57^b	381	194	60^b	12

[a] Minimum distance computed with Magma [8].

[b] Upper bound found by probabilistic search for minimum-weight vectors with Magma; in each case the minimum distance is provably bounded below by 16.

the quadratic residue codes of length m defined by the splitting $(\{0\}, Y_0, Y_1)$, where

$$Y_0 = \left\{ a \in S \,\middle|\, \left(\frac{a}{m}\right) = 1 \right\}$$

and Y_1 is the complement in $S\backslash\{0\}$.

TABLE IV
NEW MINIMUM–DISTANCE BOUNDS OVER $\mathbb{F}_2$.

n	k	d	d_0^a
141	69	24	23
140	69	23	22
140	68	24	23
139	68	23	22
139	67	24	23
138	67	23	22
138	66	24	23
137	66	23	22
137	65	24	23
136	65	23	22

[a] Minimum distance of previously best known code in Brouwer [2].

First we consider the splitting over $Z = m\mathbb{Z}/\ell m\mathbb{Z}$ with $X_0 = \pi^{-1}(Y_0)$ and $X_1 = \pi^{-1}(Y_1)$; specifically, we note that

$$X_0 = \left\{ a \in R \,\middle|\, \left(\frac{a}{m}\right) = 1 \right\}.$$

The associated codes C_0 and C_0^Z are liftings of Q_0 and Q_0^W, so by Theorem V.3, the minimum distances of C_0 and C_0^Z are exactly the same as for the quadratic residue codes themselves.

Instead, we note that the set $R\backslash Z$ splits into the orbits of R^* and those of ℓR^*. We thus choose X_0 to be the subset of $A\backslash Z$ twisted by a quadratic nonresidue $\bmod m$ on one of these sets

$$\left\{ a \in R^* \,\middle|\, \left(\frac{a}{m}\right) = 1 \right\} \cup \left\{ a \in \ell R^* \,\middle|\, \left(\frac{a}{m}\right) = -1 \right\}.$$

Then any s in R^* which is not a square $\bmod m$ splits (Z, X_0, X_1), but this twisted lift avoids the conditions of Theorem V.3 which produced poor codes. Indeed, in the tables that follow we find that the minimum distances of the resulting twisted lifts well exceed those of the corresponding quadratic residue codes, and give some new minimum-distance records.

From Theorem V.3 it is clear that for each $[m, k, d]$-code above there exists a lifted $[\ell m, \ell k, d]$-code. Thus we provide Table II as reference for the parameters of quadratic residue codes of block length m, and in Table III give only the parameters of the twisted lifts, taking $\ell = 3$. In view of Theorem IV.10, we also indicate the smallest value d_0 for which $d_0^2 \geq m$ when $m \equiv 1 \bmod 8$, or for which $d_0^2 - d_0 + 1 \geq m$ when $m \equiv 7 \bmod 8$.

We note that the minimum distances of the examples in Table III are consistently close to the best known of their length and dimension. In particular, the $[21, 12, 5]$ and $[93, 48, 14]$ codes C_0 and the $[21, 9, 8]$ code C_0^Z match the best known in Brouwer [2]. The minimum distance of the $[141, 69, 24]$ code C_0^Z gives a new minimum distance record for codes of length 141 and dimension 69. By the Spoiling Lemma [19, Lemma 1.1.34], this improves the lower bound on the best possible minimum distance of a code for the ten values of $[n, k]$ listed in Table IV.

VI. CONCLUSION

We have shown that the main results and methods for various Abelian group codes can be studied as a uniform family of

codes, and that these generalize duadic codes. Moreover, within this family there exist subclasses not included in the previously described family of duadic codes. As demonstrated by examples constructed within special subclasses, these include codes which have good parameters. It is also of interest that results are obtained regarding classes of codes which have poor parameters. The examples in this work emphasize the cyclic split group codes; in future work we expect to extend the computational efforts to split group codes in for noncyclic Abelian groups, which include the generalized quadratic residue codes and generalized duadic codes.

ACKNOWLEDGMENT

S. Ling would like to thank the Graduate School of Mathematical Sciences of the University of Tokyo and Prof. S. Nakajima for their hospitality and support. The authors wish to thank the referees for their valuable comments that improved this paper considerably.

REFERENCES

[1] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*. Reading, MA: Addison-Wesley, 1969.

[2] *Bounds on the Size of Linear Codes*, vol. I, Handbook of Coding Theory, V. Pless and W. Huffman, Eds., North-Holland, Amsterdam, The Netherlands, 1998, pp. 295–462.

[3] P. Camion, "Global quadratic Abelian codes," in *Information Theory*, G. Longo, Ed. Vienna: Springer-Verlag, 1975, vol. 219, pp. 293–310. CISM Courses and Lectures.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics*, Berlin: Springer-Verlag, 1993, vol. 138.

[5] D. Knuth, *The Art of Computer Programming. Volume 2: Seminumerical Algorithms*, 2nd ed. Reading, MA: Addison-Wesley, 1981.

[6] S. Lang, *Algebra*, 3rd ed. Reading, MA: Addison-Wesley, 1993.

[7] J. S. Leon, J. M. Masley, and V. Pless, "Duadic codes," *IEEE Trans. Inform. Theory*, vol. 30, pp. 709–714, 1984.

[8] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system I: The user language," *J. Symb. Comp.*, vol. 24, no. 3–4, pp. 235–265, 1997.

[9] J. H. van Lint and F. J. MacWilliams, "Generalized quadratic residue codes," *IEEE Trans. Inform. Theory*, vol. 24, no. 6, pp. 730–737, 1978.

[10] J. H. van Lint, *Introduction to Coding Theory. Graduate Texts in Mathematics*, Berlin: Springer-Verlag, 1992, vol. 86.

[11] V. Pless, "Q-codes," *J. Combin. Theory Ser. A*, vol. 43, pp. 258–276, 1986.

[12] V. Pless, J. M. Masley, and J. S. Leon, "On weights in duadic codes," *J. Combin. Theory Ser. A*, vol. 44, pp. 6–21, 1987.

[13] V. Pless, "Duadic codes revisited," *Congressus Numerantium*, vol. 59, pp. 225–233, 1987.

[14] V. Pless, "Duadic codes and their generalizations," in *Eurocode'92 (Udine, Italy)*, *CISM Courses and Lectures*, Vienna: Springer-Verlag, 1993, vol. 339, pp. 3–15.

[15] J. J. Rushanan, "Topics in Integral Matrices and Abelian Group Codes," Ph.D. Dissertation, Caltech, Pasadena, CA, 1986.

[16] J. J. Rushanan, "Duadic codes and difference sets," *J. Combin. Theory Ser. A*, vol. 57, pp. 254–261, 1991.

[17] M. Smid, "On Duadic Codes," Dept. Math., Tech. Univ., Eindhoven, The Netherlands, Tech. Rep. 86-WSK-04, May 1986.

[18] M. Smid, "Duadic codes," *IEEE Trans. Inform. Theory*, vol. 33, no. 3, pp. 432–433, 1987.

[19] M. A. Tsfasman and S. G. Vladut, *Algebraic-Geometric Codes. Mathematics and Its Applications (Soviet Series)*, Dordrecht: Kluwer, 1991, vol. 58.

[20] H. N. Ward, "Quadratic residue codes and symplectic groups," *J. Algebra*, vol. 29, pp. 150–171, 1974.