Note

Existence of Abelian Group Code Partitions

HAROLD N. WARD*

Department of Mathematics, University of Virginia, Charlottesville, Virginia 22903

AND

L. ZHU

Department of Mathematics, Suzhou University, Suzhou, 215006, People's Republic of China

Communicated by the Managing Editors

Received February 24, 1993

This note presents necessary and sufficient conditions for the existence of generalizations of m-adic residue codes in Abelian group algebras. © 1994 Academic Press, Inc.

INTRODUCTION

Duadic codes were introduced by Leon et al. [5] as cyclic codes generalizing quadratic residue codes. Brualdi and Pless generalized them to polyadic cyclic codes [2] and Rushanan did so to duadic Abelian group codes [9]. Theorems concerning the existence of these codes in terms of field and group restrictions have been proved during this development, beginning with the one of Smid for cyclic duadic codes [10].

In this note we shall deal with a generalization of duadic codes for Abelian groups analogous to the cyclic m-adic residue codes in [2]. The goal is the necessary and sufficient conditions for existence presented in the Proposition and Theorem. The next section summarizes background for the lines we shall follow. Such background can be found in [8] and the book by Blake and Mullin [1], and it is surveyed in [12].

The U. S. Government's right to retain a nonexclusive royalty-free license in and to the copyright covering this paper, for governmental purposes, is acknowledged.

* Supported in part by NSA Contract MDA 904-92-H-3008.
ABELIAN GROUP CODES

Let $G$ be a finite Abelian group written additively, and let $K$ be the finite field $GF(q)$ of $q$ elements. The ambient space for Abelian group codes based on $G$, or $G$-codes for short, is the group algebra $KG$ of $G$ over $K$. This is the space of $K$-valued functions on $G$ under the convolution product. As usual, we view it as the space of linear combinations $\sum x^g$, where $x^g \in K$, the sum is over $G$ (as all unrestricted sums will be), and $x^g$ denotes the characteristic function of $\{g\}$, $g \in G$. These $x^g$ form the coding basis and multiply by the rule $x^g x^h = x^{g+h}$. They make up a multiplicative group isomorphic to $G$.

Any homomorphism of $G$ into the multiplicative semigroup of a $K$-algebra extends by linearity to an algebra homomorphism of $KG$. In particular, an automorphism $\sigma$ of $G$ becomes one of $KG$ by the formula $\sigma(\sum x^g) = \sum \sigma(x)^g$, and a character $\chi$ of $G$ yields the character $\chi$ of $KG$ given by $\chi(\sum x^g) = \sum \chi(x^g)$.

A $G$-code is an ideal in $KG$. $G$ automatically becomes a subgroup of the group of the code through multiplication by the $x^g$; that is the motivation behind this generalization of cyclic codes. We shall assume that $q$ and $|G|$ are relatively prime. In this semisimple case, each $G$-code is a principal ideal generated by an idempotent. For example, the idempotent generating the repetition code is

$$e_0 = |G|^{-1} \sum x^g.$$  

The dual code, $E$, is $KG(1 - e_0)$, where $1 = x^0$. It consists of the “even-like” words whose digit sum is 0, the analogues of binary words of even weight.

The idempotents in turn correspond to sets of characters of $G$ in the following way. Let $\hat{G}$ be the whole set of characters of $G$, the homomorphisms of $G$ into the multiplicative group of an algebraic closure of $K$. If $\chi_1, \chi_2 \in \hat{G}$, their sum, defined by

$$(\chi_1 + \chi_2)(g) = \chi_1(g) \chi_2(g),$$  

is also in $\hat{G}$. $\hat{G}$ becomes an additive group isomorphic to $G$. The automorphisms $\sigma$ of $G$ induce those of $\hat{G}$ by the rule

$$(\sigma\chi)(g) = \chi(\sigma^{-1}g).$$  

If $e$ is an idempotent, $e^2 = e$ implies $\chi(e) = 0$ or 1 for $\chi \in \hat{G}$. Those characters with $\chi(e) = 1$ make up the set $X(e)$ corresponding to $e$. The idempotent $e$ is then

$$e = |G|^{-1} \sum \left( \sum_{\chi(e)} \chi(g)^{-1} \right) x^g.$$
Since \((q\chi)(a) = \chi(a)^q\), \(X(e)\) is a union of \(q\)-orbits, the orbits in \(\hat{G}\) of the permutation \(\chi \to q\chi\). This is the condition needed to make the inner sum in the formula for \(e\) a member of \(K\).

**ANALOGUES OF \(m\)-ADIC RESIDUE CODES**

In their paper [2], Brualdi and Pless defined \(m\)-adic residue codes in an intermediate step for their definition of polyadic codes. Here we present generalizations of them that incorporate some of their homogeneity properties.

The family of even-like \(m\)-adic residue codes of class I gives a direct sum decomposition of the even-like subspace for a cyclic group. Consider then a decomposition of \(E\) for a general Abelian group as a direct sum of \(m\) \(G\)-codes. The decomposition corresponds to a set \(e_1, \ldots, e_m\) of mutually orthogonal idempotents adding to \(1-e_0\):

\[
1-e_0 = \sum_{i=1}^{m} e_i \quad \text{and} \quad e_ie_j = 0 \quad \text{for} \quad i \neq j.
\]

Any pair of even-like duadic codes also produces such an orthogonal decomposition for \(m=2\). For, their idempotents \(e_1\) and \(e_2\) satisfy \(1-e_0 = e_1 + e_2\) and \(e_0e_1 = e_0e_2 = 0\) [8]. Then \(e_1 - e_0e_1 = e_1^2 + e_1e_2\), whence \(e_1e_2 = 0\).

If \(\chi \in \hat{G}\), \(\chi(e_i)\chi(e_j) = 0\) \((i \neq j)\) implies \(\chi\) is in at most one \(X(e_i)\). If \(\chi_0\) is the trivial character (the zero of \(\hat{G}\), for which \(\chi_0(g) = 1\) for all \(g\) in \(G\)), then

\[
\sum_{i=1}^{m} \chi_0(e_i) = \chi_0(1-e_0) = 0,
\]

and \(\chi_0\) is in no \(X(e_i)\). But if \(\chi \neq \chi_0\), \(\chi(1-e_0) = 1\) and \(\chi\) is in exactly one \(X(e_i)\). Thus the \(X(e_i)\) partition \(\hat{G} - \{\chi_0\}\). Conversely, such a partition gives an orthogonal decomposition of \(1-e_0\) if in addition each \(X(e_i)\) is a union of \(q\)-orbits.

The \(m\)-adic residue codes are also permuted by an automorphism of the cyclic group involved. Thus the decomposition of \(E\) they produce is balanced in the sense of the following definition; again, this will also be true for even-like duadic codes.

**DEFINITION 1.** The decomposition is called balanced if the number of characters of any given order in each \(X(e_i)\) is the same.

We shall say that the codes of a balanced decomposition form an \(m\)-balanced family of even-like codes.
NOTE

This will be the case, for example, if there is an idempotent $e$ and $m$ automorphisms $\sigma_i$ of $G$ for which $\sigma_i(e) = e_i$. In a balanced decomposition one must have $m \mid |G| - 1$, the number of nontrivial characters.

The existence of a balanced decomposition is connected to the structural property of $G$ described next. Given $m$ relatively prime to $|G|$ and a prime $p$ dividing $|G|$, let $o(q)$ be the order of $q$ modulo $p$. Then let $o(p)$ be the order of $p$ modulo $mo(q)$.

**Definition 2.** $G$ is called $p$-homogeneous if the number of elementary divisors of $G$ equal to each power of $p$ is a multiple of $o(p)$.

For instance, suppose $G$ is cyclic. Then $p$-homogeneity requires $o(p) = 1$, that is, $mo(q) \mid p - 1$. This means $m \mid p - 1$ and $o(q) \mid (p - 1)/m$; the second divisibility says $q$ is an $m$th power modulo $p$. $G$ will be $p$-homogeneous for all primes $p$ dividing $|G|$ if and only if $m \mid p - 1$ for each $p$ and $q$ is an $m$th power residue modulo $|G|$ [3, Chapter 8]. When $m = 2$, this is the condition of Smid for duadic codes [10].

If $G$ is elementary Abelian of order $p^n$, $p$-homogeneity requires $o(p) \mid n$. Again, this means $m \mid p^n - 1$ and $o(q) \mid (p^n - 1)/m$. The second divisibility says $q$ is an $m$th power in $GF(p^n)$.

**Existence of a Balanced Decomposition**

**Proposition.** Let $E$ have a balanced decomposition into $m$ terms. Then $G$ must be $p$-homogeneous for each prime $p$ dividing $|G|$.

**Proof.** Because of the partition of $\hat{G} - \{\chi_0\}$ associated with the decomposition, the number of $q$-orbits of elements of $\hat{G}$ (and of $G$) of any order bigger than 1 is a multiple of $m$. The size of a $q$-orbit of elements of order $t$ is the order of $q$ modulo $t$. If $t$ is a power of $p$, this order is $o(q)$ times another power of $p$.

Fix $p$ dividing $|G|$ and let $d(h)$ be the number of elementary divisors of $G$ equal to $p^h$, $h \geq 1$. Let $d'(h) = \sum_{k \geq h} d(k)$ and $d''(h) = \sum_{k < h} d'(k)$. Then the number of elements of $G$ of order $p^h$ is $(p^{d'(h)} - 1) p^{d''(h)}$ [7, Section 37]. Thus we must have $mo(q) \mid p^{d'(h)} - 1$, that is, $o(p) \mid d'(h)$. Since $d(h) = d'(h) - d'(h + 1)$, this implies $o(p) \mid d(h)$ for each $h \geq 1$, and $G$ is $p$-homogeneous.

**Theorem.** Suppose $m$ is relatively prime to $|G|$ and $G$ is $p$-homogeneous for each prime $p$ dividing $|G|$. Then there is an $m$-balanced family of even-like codes whose members are permuted in a cycle of length $m$ by some automorphism of $G$. 
Proof. What is needed is an automorphism of $G$ that permutes the $q$-orbits of nonzero members of $G$ in cycles whose lengths are divisible by $m$. We shall set up the induced automorphism of $\hat{G}$ (which is also $p$-homogeneous). By the $p$-homogeneity, the $p$-Sylow subgroup of $\hat{G}$ is a direct sum of subgroups, each of which is in turn a direct sum of $\sigma(p)$ isomorphic cyclic subgroups.

Let $H$ be such a summand, the cyclic groups having order $p^r$. Then by the description in [11, Section 43], $H$ has an automorphism $\tau$ of order $mo(q)$ inducing a regular permutation of that order on the set of nonzero elements in each section $p^rH/p^{r+1}H$, $r < s$. It corresponds to multiplication by an element of order $mo(q)$ in the field $GF(p^{\sigma(p)})$. If $\tau h = q^i h$ for $h \neq 0$, suppose $h \in p^rH - p^{r+1}H$. Then $\tau^{mo(q)}(h + p^{r+1}H) = h + p^{r+1}H$, so that $m \mid i$. That means the cycles of $\tau$ on the set of $q$-orbits of $H - \{0\}$ all have lengths divisible by $m$.

Now write $\hat{G}$ as a direct sum of such subgroups $H$, and let $\sigma$ be the direct sum of the corresponding $\tau$'s. Then $\sigma$ also permutes the $q$-orbits of nonzero elements in cycles of lengths divisible by $m$, as required.

**Corollary 1.** Suppose $G$ is a finite Abelian group of odd order. Then $GF(q)G$ contains duadic codes as ideals if and only if $G$ is $p$-homogeneous for each prime $p$ dividing $|G|$.

Proof. The necessity comes from the Proposition and the sufficiency from the Theorem.

The comments after Definition 2 imply the following special case.

**Corollary 2.** If $G$ is elementary Abelian of order $p^n$, $p$ an odd prime, then duadic $G$-codes exist exactly when $q$ is a square in $GF(p^n)$.

The condition in Corollary 2 is equivalent to the circumstance that the quadratic residue codes based on $GF(p^n)$ can be written in $GF(q)$. There are two ways to see that from the exposition by van Lint and MacWilliams [6]: one is to use their expressions for the idempotents of the quadratic residue codes and apply quadratic reciprocity to discover when the coefficients are in $GF(q)$. The other, more direct, is to invoke the condition that the characters defining the quadratic residue codes must form a union of $q$-orbits. In fact, connecting these two approaches provides a proof of quadratic reciprocity amounting to the proof by Gaussian sums in finite fields [4].

**References**