Topics in Integral Matrices and Abelian Group Codes

Thesis by

Joseph John Rushanan

In Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California

1986

(Submitted May 22, 1986)

Time for you and time for me,
And time yet for a hundred indecisions,
And for a hundred visions and revisions,
Before the taking of a toast and tea.
The Love Song of J.Alfred Prufrock
T.S. Eliot

When research isn't going well,
Or rather, when it's shot to hell—
My advisor's asked for show & tell
    And all I have are dried-up newts,
When outside life completely fades,
When some TA screws up the grades,
Or when they're bidding slam in spades,
    And I have only minor suits ...

Then I'll sit and stay awhile
With friends who laugh and jest and smile,
Where cuteness is the latest style,
    And rarely will the jokes wear thin.
They'll hear my thoughts and hear my rhyme,
They'll join me in a wild time,
They'll even go and slice the lime,
    (Where's the tonic?),
                                        and pour the gin.

This thesis is dedicated to my friends at Caltech,
and especially to

Nancy,	for music & lunch
Bobbie,	for basketball & cribbage
Carol,	for ping-pong & poetry
Bart,	for financial stability, piano & Bruce
Warren,	for the Bench, the Minstrel, & the Bard
Jeffrey,	for his voice, Butterball, & Capt. Napalm
Tina,	for being my favorite bridge partner
Jennifer,	for English, dancing, & bread
Sue,	for bubble-water, frogs, & tea.

Acknowledgements

> I'm very well acquainted, too, with matters mathematical,
> I understand equations, both the simple and quadratical;
> About binomial theorem I'm teeming with a lot o'news,
> With interesting facts about the square of the hypotenuse.
>
> *The Modern Major-General*
> W. S. Gilbert

The Department of Mathematics at Caltech has provided the best conceivable environment for my mathematical maturation. In particular, I especially thank: Rick Wilson, for being an enlightening and inspiring advisor, and for suggesting the impetus of Chapter I; Vera Pless, for her enthusiasm and encouragement, and for providing the foundation of Chapter II; Richard Brualdi, for reading Chapter I; Bob Roth, for leading me to insights in Chapter II; the above four, for being on my committee, and for Tuesday and Friday mornings; David Wales and W.A.J. Luxemburg, for completing my committee; Lynne Butler, for the truth of Theorem I.6.5; the late Herb Ryser, for his kindness, and for acquiring, with Rick, NSF grant DMS82-17596, which partially supported this work.

Since competence in mathematics is easier from a general competence in *thinking*, I deeply acknowledge those who have helped me improve my rationality, through numerous discussions, debates, arguments, dialogues, and chats:

Greg, Larry, Bart, Jonathan, Jack, and Dale, and,
most importantly, Dan (*Allez avec Le Flamant*).

Just as sincerely, I thank the following which have made the work for this thesis almost trivial: TeX, APL, the Chipmunks, KLOS, Coca-Cola's numerous sugar-free and caffeinated soft drinks, the staff and beverages of the Red Door Cafe, and my patient, faithful, and much beloved COMPAQ PLUS™.

Finally, thanks so much J.Alfie, let's do lunch.

Abstract

This thesis consists of two independent chapters.

The first chapter concerns the Smith Normal Form (SNF) over the integers $\mathbb{Z}$ of integral matrices. We consider the SNF of a matrix A to be the ratio of two $\mathbb{Z}$-modules—a finitely generated abelian group; this is called the *Smith group* of A. The Smith group provides a unified setting to present both new and old results. The new results concern the relationship between the eigenvalues of an integral matrix and its SNF. In particular, the multiplicities of integer eigenvalues are shown to relate to the multiplicities in the type of the Smith group. Bounds are also given for the exponent of the Smith group. In some cases, these are best possible. The old results discussed are the interlacing of the SNF in the case of augmented matrices and the symmetries of the SNF for certain combinatorial matrices. The latter results are extended to rectangular matrices. Numerous examples are given throughout, along with many conjectures based on computation.

The second chapter generalizes the work of Pless, et al. on duadic codes and Q-codes. We take abelian group codes to be ideals in the group ring $\mathbf{F}[G]$, where G is a finite abelian group of odd order n and $\mathbf{F}$ is a finite field with characteristic relatively prime to n. We define *generalized Q-codes* from a pair of idempotents of $\mathbf{F}[G]$ and an automorphism of G which together obey two simple equations. These codes are $(n, \frac{n+1}{2})$ and $(n, \frac{n-1}{2})$ linear codes. We show that all of the properties of duadic and Q-codes generalize. In particular, we extend the results on the relationship of these codes to projective planes with regular automorphism group G. When $\mathbf{F}$ has characteristic 2, we give simple numerical conditions on G and $\mathbf{F}$ which determine when generalized Q-codes exist. We also give some techniques for constructing these codes.

Table of Contents

Chapter I

The Smith Normal Form as a Finitely Generated Abelian Group

1. Introduction

One of the standard results in matrix theory is the construction of the Smith Normal Form for matrices over a principal ideal domain (p.i.d.); see, for example, [Nel]. By changing the p.i.d., one can derive quickly the classification of finitely generated abelian groups or even the Jordan Canonical Form. Besides these applications, an occasional paper appears, such as [De], [MdS], and [Th], which indicates that there are some basic results still to be obtained about the Smith Normal Form. Our goal is to put some of these recent results and some new ones about the Smith Normal Form into a unified setting. In the process we hope that the techniques given may lead to even more new results.

The major drawback to the results in this chapter, however, is that we are restricted to the case when the principal ideal domain is the integers, $\mathbb{Z}$. Most of the results in the literature do not require this limitation. The advantage gained is that we can consider the Smith Normal Form of an integral matrix to be a finitely generated abelian group. This interplay between matrix theory and the theory of $\mathbb{Z}$-modules will more than justify the generalization lost.

Besides the natural beauty inherent in the Smith Normal Form itself, there is another important reason for pursuing the results herein. We contend that the

Smith Normal Form over the integers for an integral matrix has a combinatorial significance analagous to but separate from such more common concepts as the spectrum of the matrix, the matrix formed by row intersections, and so forth. It is to be hoped that the numerous examples which we give will support this remark.

After giving our definitions and preliminary results, we proceed to the relationship of the spectrum of a matrix to its Smith Normal Form. We follow this with examples and conjectures from the theory of strongly regular graphs. These results are all new. In the last sections we put known results into our context. Much of the time the proofs will be seen to be simpler.

2. Definitions and Preliminaries

In the usual discussion of the Smith Normal Form (SNF) of a matrix whose entries are in some principal ideal domain $\Re$, one begins with an equivalence relation on matrices and then proceeds to derive a canonical representation which uniquely determines an equivalence class. A square matrix is called *unimodular* if its determinant is a unit in $\Re$ (and so is invertible). The equivalence relation is then defined as follows: two matrices A and B are *equivalent*, written here as $A \simeq B$, if there exist unimodular matrices E and F such that $EAF = B$. One then goes on to show that every matrix A is equivalent to a diagonal matrix

$$D = \begin{pmatrix} d_1 & & & & \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}, \tag{2a}$$

where r is the rank over $\Re$ of A and the $d_i \in \Re$ with $d_{i-1} \mid d_i$, for $i = 2, \ldots, r$. This can be done in several ways, ranging from the classical method of elementary row operations, to computing gcd's of $k \times k$ minors, to the nowadays standard approach of decomposing modules over $\Re$. The resulting diagonal matrix D in $(2a)$ is unique up to the constraints given for the d_i and multiplication of the d_i by units in $\Re$. We will call the main diagonal of D the SNF of A. We assume that the reader has seen these topics in some manner before. As references, we offer [H&H], [Ne1], and [Bo]. We restrict to the case $\Re = \mathbb{Z}$; all modules, submodules and factor modules are then finitely generated abelian groups.

Let A be an integral $m \times n$ matrix. We set the row space of A over $\mathbb{Z}$ to be $R(A)$ and the row space over the rationals to be $V(A)$. Furthermore, let $L(A) = V(A) \cap \mathbb{Z}^n$. Then $R(A)$ and $L(A)$ are clearly finitely generated $\mathbb{Z}$-modules contained in the $\mathbb{Z}$-module of all integral vectors of length n, written $\mathbb{Z}^n$. From this observation we make the following definition which provides the unifying concept for this chapter. This definition is not new; see, for example, the techniques in [Wi] and [La].

Definition: The factor module

$$\Gamma(A) = \mathbb{Z}^n \big/ R(A)$$

is the *Smith group* of A. The submodule

$$\overline{\Gamma}(A) = L(A) \big/ R(A)$$

is the *finite part* of $\Gamma(A)$.

The justification for the last statement of the definition is in the next two lemmas. First observe that for $\underline{v} \in \mathbb{Z}^n$, the order of $\underline{v} + R(A) \in \Gamma(A)$ is the smallest positive integer l such that $l\underline{v} \in R(A)$; if there is no such l, then the order is infinite.

Lemma 2.1. *$\overline{\Gamma}(A)$ is a finite abelian group.*

Proof: Let $\underline{v} \in L(A)$. Then $\underline{w}A = \underline{v}$ for some rational vector $\underline{w}$. Let $m \in \mathbb{Z}$ be such that $m\underline{w}$ is integral. Then $m\underline{v} \in R(A)$, so that $\underline{v}$ has finite order. The result then follows as $\overline{\Gamma}(A)$ is generated by a finite number of elements each of finite order.

♣◇

Lemma 2.2. $\Gamma(A) \big/ \overline{\Gamma}(A)$ *has no nonidentity element of finite order.*

Proof: From module theory, we have the isomorphism

$$\Gamma(A) \big/ \overline{\Gamma}(A) = \mathbb{Z}^n \big/ R(A) \Big/ L(A) \big/ R(A) \cong \mathbb{Z}^n \big/ L(A).$$

Pick $\underline{v} \in \mathbb{Z}^n, \underline{v} \notin L(A)$. Then no integer multiple of $\underline{v}$ can be in $V(A)$, so that the order of $\underline{v}$ in $\mathbb{Z}^n \big/ L(A)$ is infinite.

♣◇

For emphasis, we record the following.

Lemma 2.3. *These are equivalent:*

i. $\Gamma(A) = \overline{\Gamma}(A)$

ii. $L(A) = \mathbb{Z}^n$

iii. *The rank of A is n.*

Proof: This is clear after the observation that the rank of A is n iff $\mathbb{Z}^n \leq V(A)$.

♣◇

From the classification of finitely generated abelian groups (say in [Ca] or [H&H]), we know that $\Gamma(A) \cong \overline{\Gamma}(A) \oplus \Gamma(A) \big/ \overline{\Gamma}(A)$, where the second direct summand is a free $\mathbb{Z}$-module of rank $n - r$, r the rank of A. This observation and the following serves to justify the term "Smith group."

Theorem 2.4. *Let A and B be two integral $m \times n$ matrices. Then*

$$A \simeq B \qquad \text{implies} \qquad \Gamma(A) \cong \Gamma(B).$$

Proof: Let $A \simeq B$. So there exist unimodular matrices E and F such that $EAF = B$. Define the map

$$\varphi : \ L(A) \longrightarrow \overline{\Gamma}(B)$$

$$\text{by} \qquad \varphi(\underline{v}) = \underline{v}F + R(B) \qquad \text{for} \quad \underline{v} \in L(A).$$

This map is well-defined, since if $\underline{v} = \underline{w}A \in L(A)$, then

$$\underline{v}F = \underline{w}E^{-1}\,EAF = (\underline{w}E^{-1})B \,\in L(B).$$

A similar calculation shows that φ is onto. It is also clearly a homomorphism of $\mathbb{Z}$-modules. Finally, if $\varphi(\underline{v}) = \mathbf{0}$, the identity in $\overline{\Gamma}(B)$, then $\underline{v}F \in R(B)$. But $\underline{v}F \in R(B)$ iff $\underline{v} = \underline{x}BF^{-1} = \underline{x}EA$ for some $\underline{x} \in \mathbb{Z}^n$. In other words, the kernel of φ is $R(A)$. This proves that φ is an isomorphism from $\overline{\Gamma}(A)$ to $\overline{\Gamma}(B)$. To finish the proof, A and B have the same same rank, and as the finite parts are isomorphic, it must then follow that $\Gamma(A) \cong \Gamma(B)$.

♡♠

Theorem 2.4 allows us to state in terms of the SNF the structure of $\Gamma(A)$. To whit, if the SNF is given as in $(2a)$, then

$$\Gamma(A) \;\cong\; \mathbb{Z}^{n-r} \,\oplus\, \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}. \tag{2b}$$

Here $\mathbb{Z}_m$ denotes the integers modulo m, where m can be either positive or negative and the resulting group is trivial iff $m = \pm 1$. The converse of Theorem 2.4 is also true.

Theorem 2.5. *A and B as in Theorem 2.4. Then*

$$\Gamma(A) \cong \Gamma(B) \qquad \text{implies} \qquad A \simeq B.$$

Proof: Both $\Gamma(A)$ and $\Gamma(B)$ can be assumed to be in the form of $(2b)$ using the respective SNFs. From the classification of finitely generated abelian groups and the constraints on the SNFs, the resulting forms are identical. That is, A and B have the same SNF, or $A \simeq B$.

♡♠

Theorems 2.4 and 2.5 together show that the SNF and the Smith group for a matrix give the same information about the matrix. It is the interplay between these two concepts, and between linear algebra and $\mathbb{Z}$-module theory, that we will exploit.

In order to make our techniques go more smoothly, we will assume the acquaintance of most standard results in module and group theory. In the former, we will use the concept of a $\mathbb{Z}$-basis: if M is a finitely generated $\mathbb{Z}$-module, then a *$\mathbb{Z}$-basis* for M is a set of elements which span M over $\mathbb{Z}$ and are independent over $\mathbb{Z}$. Any $\mathbb{Z}$-basis can be computed from another by multiplication by some unimodular matrix. This is the so-called *Hermite Normal Form* (see [Ne1], chap. 2). In group theory, we need most of the basic facts about finite abelian groups. Any unusual result will be offered as a lemma.

We also use standard notation as much as possible. Along with those items already mentioned, we need the matrices I_m, the $m \times m$ identity matrix; J_m, the $m \times m$ matrix of all ones; and $\underline{j}$, a row of all ones (the length should be clear from context).

As for the actual computing of the SNF, we take this as a given. That is, we usually just state what the SNF is of the specific matrix being discussed. The SNF can be computed in a number of ways, but for the smaller examples which we use, calculating gcd's of minor determinants is as good a method as any other.

We end this section with results which illustrate the information inherent in the Smith group. If U is a subspace of the space of all rational vectors of length n, we set $L(U) = U \cap \mathbb{Z}^n$. Then it is natural to use the notation $\Gamma(U)$ for the subgroup of $\Gamma(A)$ defined by

$$\langle \underline{u} + R(A) \ : \ \underline{u} \in L(U) \rangle .$$

Notice that $L(A) = L\big(V(A)\big)$ and $\Gamma(A) = \Gamma\big(V(A)\big)$. Recall that U is *invariant* under A if $UA \leq U$.

Lemma 2.6. *Let A be an $n \times n$ integral invertible matrix and U a subspace invariant under A. Then*

$$\Gamma(U) \cong {L(U)}\big/{L(U)A}.$$

Proof: Define the map

$$\varphi : \ L(U) \longrightarrow \Gamma(U)$$

$$\text{by} \qquad \varphi(\underline{u}) = \underline{u} + R(A) \qquad \text{for} \quad \underline{u} \in L(U).$$

Observe that φ is clearly well-defined, onto and a homomorphism. We claim that the kernel of φ is $L(U)\,A$. Clearly $L(U)\,A \leq R(A)$. Suppose that $\underline{u} + R(A) = R(A)$ for some $\underline{u} \in L(U)$. Then there is an integral vector $\underline{w}$ with $\underline{u} = \underline{w}A$. By the invariance of U and the invertibility of A, $\underline{w} \in L(U)$. That is, $\underline{u} \in L(U)\,A$.

♣◇

Lemma 2.7. *Let A as in Lemma 2.6, U and W two subspaces invariant under A. If*

$$L(U \oplus W) = L(U) \oplus L(W),$$

then

$$\Gamma(U \oplus W) = \Gamma(U) \oplus \Gamma(W).$$

Proof: Let $L(U \oplus W) = L(U) \oplus L(W)$. Then by the invertibility of A and the invariance of U and W, $L(U \oplus W)A = L(U)A \oplus L(W)A$. By the standard module isomorphism theorems,

$$\begin{aligned} {}^{L(U \oplus W)}\big/_{L(U \oplus W)A} &= {}^{L(U) \oplus L(W)}\big/_{L(U)A \oplus L(W)A} \\ &\cong \left({}^{L(U)}\big/_{L(U)A}\right) \oplus \left({}^{L(W)}\big/_{L(W)A}\right). \end{aligned} \tag{2c}$$

The result then follows from Lemma 2.6.

♣◇

Example: Suppose that A is the direct sum of two matrices, that is

$$A = \begin{pmatrix} A_1 & \\ & A_2 \end{pmatrix},$$

where blanks denote zeros. Here take A_1 and A_2 integral invertible matrices. Notice that the row spaces of A_1 and A_2 have only the zero vector in common. Hence Lemma 2.7 applies and we can conclude that

$$\Gamma(A) \cong \Gamma(A_1) \oplus \Gamma(A_2).$$

This conclusion holds even if A_1 and A_2 are arbitrary (possibly nonsquare) integral matrices. Indeed, just put A_1 and A_2 into SNF. Lemma 2.6 (and so 2.7) will provide a good heuristic for the results in the next section.

♣◇

Ex. 2-1: We conclude with a numerical example. Let

$$A = \begin{pmatrix} 4 & 1 \\ 1 & 4 \end{pmatrix}.$$

One quickly sees that $\Gamma(A) \cong \mathbb{Z}_{15}$. A has two invariant subspaces, namely the eigenspaces associated to the eigenvalues 3 and 5. These are respectively the spans of the vectors $[1,-1]$ and $[1,1]$. Call the former U and the latter W. We then see that $\Gamma(U) \cong \mathbb{Z}_3$ and $\Gamma(W) \cong \mathbb{Z}_5$. Therefore, $\Gamma(A) \cong \Gamma(U) \oplus \Gamma(W)$. Observe that $L(U \oplus W) = L(A) = \mathbb{Z}^2$. Then, in particular, $[1,0] \in L(U \oplus W)$, but it is not an integral linear combination of vectors in $L(U)$ and $L(W)$. This example then serves as a counterexample to the converse of Lemma 2.7. It also foreshadows the results of the next section.

3. Eigenvalues and the SNF

We begin in this section to show the usefulness of the Smith group of an integral matrix by giving some results relating the spectrum of the matrix to its SNF. There does not appear to be much in the literature relating these two concepts. The closest discussion concerns the results on similarity by integral matrices (see [Ne1], chap.

3). Those results are very strong since two integral matrices integrally similar possess the same SNF and the same spectrum. We are concerned with the weaker hypothesis of assuming that a spectrum for a matrix is known and determining limits on its SNF via its Smith group.

In order to show that we cannot expect to learn too much from the spectrum, consider the following example. Let λ_1 and λ_2 be two nonzero and nonequal integers. Set

$$A_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

and

$$A_2 = \begin{pmatrix} \lambda_1 & 1 \\ 0 & \lambda_2 \end{pmatrix}.$$

Then both A_1 and A_2 have the same spectrum, namely the eigenvalues λ_1 and λ_2 each with multiplicity one. We see, however, that

$$\Gamma(A_1) \cong \mathbb{Z}_{\lambda_1} \oplus \mathbb{Z}_{\lambda_2}$$

while

$$\Gamma(A_2) \cong \mathbb{Z}_{\lambda_1 \lambda_2}.$$

These two groups are isomorphic precisely when the two eigenvalues are relatively prime. This example is indicative in some sense to the restrictions that the spectrum puts on the SNF.

In the sequel, fix an $n \times n$ integral nonsingular matrix A with SNF $d_1, \ldots, d_n$. Furthermore, let the eigenvalues of A be $\lambda_1, \ldots, \lambda_s$ with respective multiplicities $m_1, \ldots, m_s$. Our first result is the most general and also the simplest to prove:

Theorem 3.1. *Let $\lambda_i \in \mathbb{Z}$. Then $\lambda_i \mid d_n$.*

First Proof: There exist unimodular matrices E and F with $EAF = D$, where $D = \text{diag}(d_1, \ldots, d_n)$. Then $A^{-1} = FD^{-1}E$ and so $d_n A^{-1}$ is integral. This latter matrix has $\frac{d_n}{\lambda_i}$ as an eigenvalue, and since the only rational eigenvalues of an integral matrix are integers, we see that $\lambda_i \mid d_n$. In spite of the simple proof just given, we give a second proof, the techniques of which will apply more generally.

Second Proof: Let $\underline{e} = (e_1, \ldots, e_n)$ be an integral eigenvector for λ_i such that the gcd of its components is 1. From $\underline{e}A = \lambda_i \underline{e}$ we have that $\frac{1}{\lambda_i}\underline{e}A = \underline{e}$. Hence, $\underline{e} \in V(A) \cap \mathbb{Z}^n$. As A is nonsingular, the order of the element $\underline{e} + R(A)$ in $\Gamma(A)$ is the smallest *positive integer l such that $\frac{l}{\lambda_i}\underline{e}$ is an integral vector. By our choice of* $\underline{e}$, this is $|\lambda_i|$. Since d_n is the exponent of $\Gamma(A)$ it is divisible by the order of any element in the group, in particular, $\lambda_i \mid d_n$.

♡♠

Ex. 3-1: As an illustration of the above result, we consider the case when A is a circulant matrix formed from a first row of k consecutive 1's followed by $n - k$ consecutive 0's, where $\gcd(k, n) = 1$:

$$A = \begin{pmatrix} 1 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 1 & 0 & \cdots \\ \vdots & & & \ddots & & \\ \cdots & 1 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Newman shows in [Ne2] that in this case $\det(A) = k$ (the proof is a straightforward calculation involving the eigenvalues of A). Therefore $|\Gamma(A)| = k$. There is one immediate eigenvalue, namely k, since $\underline{j}A = k\underline{j}$, and so Theorem 3.1 says that k divides the exponent of $\Gamma(A)$. That is, $\Gamma(A) \cong \mathbb{Z}_k$

♣◇

If all of the λ_i are integers, then by Theorem 3.1 each must divide d_n. This gives a lower bound on d_n, which we record as the following.

Corollary 3.2. *Let each $\lambda_i \in \mathbb{Z}$. Then $lcm(\lambda_1, \ldots, \lambda_s) \mid d_n$.*

♡♠

Can we eliminate the assumption of the invertibility of A? If A is singular, then the last term of its SNF is 0, and easily each λ_i divides it. One would hope that if we let d be the exponent of the finite part of $\Gamma(A)$, then $\lambda_i \mid d$. Unfortunately, this is not generally true. Let

$$A = \begin{pmatrix} 3I_3 & J_3 \\ J_3 & 3I_3 \end{pmatrix}.$$

Calculation gives

$$\Gamma(A) \cong \mathbb{Z} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9.$$

A has the eigenvalue 6 (with $\underline{j}$ as an eigenvector), but $6 \nmid 9$. In later sections techniques will be given which will help circumvent the singularity of A.

How can we then extend Theorem 3.1? For each i we know only that $\lambda_i^{m_i} \mid \det(A)$ and hence the product of the d_j. We could therefore have that $\lambda_i \nmid d_j$ for $j < n$. The following theorem gives sufficient conditions for this not to happen. Here we say that a matrix *diagonalizes* with respect to an eigenvalue λ if the geometric multiplicity of λ equals its algebraic multiplicity. Equivalently, the linear term $x - \lambda$ is a simple factor of the minimum polynomial of the matrix.

Theorem 3.3. *Suppose that A diagonalizes with respect to $\lambda_i \in \mathbb{Z}$. Then the group $(\mathbb{Z}_{\lambda_i})^{m_i}$ is isomorphic to a subgroup of $\Gamma(A)$.*

Remark: The conclusion of the theorem can be put directly in terms of the SNF. If $(\mathbb{Z}_{\lambda_i})^{m_i}$ is imbeddable in $\Gamma(A)$, then at least m_i of the d_j must be divisible by λ_i. In particular, the last m_i terms of the SNF are divisible by λ_i. A justification of this remark will appear in section 5.

Proof of theorem: Let V_i be the eigenspace (over the rationals) associated with λ_i, and appealing to section 2, set $L_i = L(V_i)$ and $\Gamma_i = \Gamma_i(V_i)$. Our claim is that $\Gamma_i \cong (\mathbb{Z}_{\lambda_i})^{m_i}$, which completes the result. This is easily visualized from lemma 2.6 since A acts as λ_i times the identity on L_i.

L_i is a finitely generated $\mathbb{Z}$-module, so we can choose a $\mathbb{Z}$-basis for L_i, say $\{\underline{e}_1, \ldots, \underline{e}_{m_i}\}$. That the number of vectors in this $\mathbb{Z}$-basis is m_i follows from $\dim(V_i) = m_i$, which in turn comes from the hypothesis of the diagonalizablity of A with respect to λ_i. Furthermore, for each j the components of $\underline{e}_j$ must be relatively prime. This follows from the uniqueness of representation of the $\mathbb{Z}$-basis, i.e., divide $\underline{e}_j$ by the gcd of the components to get a vector which must be an integral multiple of $\underline{e}_j$. From the second proof of Theorem 3.1 it then follows that the order of $\underline{e}_j + R(A)$ in Γ_i is $|\lambda_i|$.

To finish the claim it suffices to show that the $\underline{e}_j + R(A)$ are independent in the sense that if

$$\sum_{j=1}^{m_i} \left(a_j \underline{e}_j + R(A)\right) = R(A), \qquad a_j \in \mathbb{Z}, \tag{3a}$$

then $\lambda_i \mid a_j$ for each j. Suppose then that $(3a)$ holds and let

$$\underline{v} = \sum_{j=1}^{m_i} a_j \underline{e}_j \,.$$

By $(3a)$, $\underline{v} \in R(A)$, and so as A is nonsingular, the unique preimage of $\underline{v}$, $\frac{1}{\lambda_i}\underline{v}$, must be integral. Therefore $\frac{1}{\lambda_i}\underline{v} \in L_i$ and is expressed uniquely as an integral linear combination of the $\underline{e}_j$. But the coefficients of this linear combination are the $\frac{a_j}{\lambda_i}$. Therefore $\lambda_i \mid a_j$ for each j.

♡♠

Corollary 3.4. *Let A be diagonalizable with all integral eigenvalues and suppose that $\gcd(\lambda_i, \lambda_j) = 1$ for $i \neq j$. Then*

$$\Gamma(A) \cong \bigoplus_{i=1}^{s} (\mathbb{Z}_{\lambda_i})^{m_i}.$$

Proof: For $i = 1, \ldots, s$, let $\Gamma_i = \left(\mathbb{Z}_{\lambda_i}\right)^{m_i}$. From Theorem 3.3 each Γ_i is imbeddable in $\Gamma(A)$. Since the order of the Γ_i's are pairwise relatively prime, their direct sum can be imbedded in $\Gamma(A)$. Since this direct sum and $\Gamma(A)$ have the same order, we can conclude that they are isomorphic.

♡♠

Ex. 3-2: We illustrate the above results with an easy but nontrivial example. Pick nonzero integers a and b such that $\gcd(a,b) = 1$. Define the $n \times n$ matrix, $n \geq 2$,

$$A = aI_n + bJ_n = \begin{pmatrix} a+b & b & \cdots & b \\ b & a+b & & \vdots \\ \vdots & & \ddots & \\ b & \cdots & & a+b \end{pmatrix}.$$

A has two eigenvalues, namely $a + bn$ and a. The eigenspace of the first is the span of $\underline{j}$; its multiplicity is one. The eigenspace of the second is the span of all of the $\underline{v}_i - \underline{v}_j$, where $i \neq j$ and $\underline{v}_i$ is the vector of all zeros except for a one in the ith spot. Notice that the dimension of this eigenspace is $n - 1$.

We assert that

$$\Gamma(A) \cong \left(\mathbb{Z}_a\right)^{n-2} \oplus \mathbb{Z}_{a(a+bn)}.$$

If the two eigenvalues are relatively prime, then this follows from Corollary 3.4. This occurs,however, iff we also have $\gcd(a,n) = 1$. For a general argument, notice that in conjunction with Theorem 3.3, it would suffice to show that there is an element of $\Gamma(A)$ with order $a(a+bn)$. This is because we could then conclude that $\Gamma(A)$ has one factor divisible by $a(a+bn)$ and, by Theorem 3.3, at least another $n-2$ factors divisible by a. But since the size of $\Gamma(A)$ is known, the result follows.

We construct an element of the desired order. Let

$$\underline{v} = \sum_{i=2}^{n} \left(\underline{v}_1 - \underline{v}_i\right) = [n-1, -1, \ldots, -1].$$

Then $n\,\underline{v}_1 = \underline{v} + \underline{j}$. Now we let

$$\underline{w} = \frac{1}{a\,n}\underline{v} + \frac{1}{n(a+bn)}\underline{j}.$$

Then $\underline{w}A = \underline{v}_1$. The order of $\underline{v}_1 + R(A)$ in $\Gamma(A)$ is then the smallest positive integer l such that $l\underline{w}$ is an integral vector. The second coordinate of $l\underline{w}$ is $\frac{-lb}{a(a+bn)}$. Since $\gcd(a,b) = 1$, we must have $a(a+bn) \; \big| \; l$, which was the desired result.

Notice that the restriction $\gcd(a,b) = 1$ isn't that limiting, since in general, if A has SNF $(d_1, \ldots, d_n)$, then the SNF of dA is $(dd_1, \ldots, dd_n)$.

♣◇

Corollary 3.4 gives us sufficient conditions for the spectrum of a matrix to uniquely determine its SNF. In evidence of the example at the beginning of this section, a generalization of this result is not readily apparent. If a more extreme example is wanted, let

$$A_1 = \begin{pmatrix} 2 & 1 & & & \\ & 4 & 1 & & \\ & & \ddots & \ddots & \\ & & & 2^{n-1} & 1 \\ & & & & 2^n \end{pmatrix}$$

and

$$A_2 = \begin{pmatrix} 2 & & & & \\ & 4 & & & \\ & & \ddots & & \\ & & & 2^{n-1} & \\ & & & & 2^n \end{pmatrix},$$

where blanks denote zeros. Then the respective Smith groups are

$$\Gamma(A_1) \cong \mathbb{Z}_N, \qquad N = 2^{\frac{n(n+1)}{2}}$$

and

$$\Gamma(A_2) \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{2^i}.$$

This example and Ex. 3-2 show that knowledge of the eigenspaces is also necessary to determine the SNF. The knowledge needed turns out to concern the interaction of these spaces as $\mathbb{Z}$-modules, and in general is hard. We can state a simple result using the results in section 2.

Corallary 3.5. *Suppose that λ_i,$\lambda_j \in \mathbb{Z}$ with respective eigenspaces V_i, V_j, and Γ_i, Γ_j are as in the proof of Corollary 3.4. If $L(V_i \oplus V_j) = L(V_i) \oplus L(V_j)$, then $\Gamma_i \oplus \Gamma_j$ is imbeddable in $\Gamma(A)$.*

Remark: The example at the end of section 2 shows that the converse is not generally true.

Proof of corollary: By Lemma 2.7 and the fact that V_i and V_j are invariant spaces,

$$\Gamma(V_i \oplus V_j) = \Gamma(V_i) \oplus \Gamma(V_j) \leq \Gamma(A).$$

But by Theorem 3.3, $\Gamma(V_i) \cong \Gamma_i$ and $\Gamma(V_j) \cong \Gamma_j$, which gives the result.

♡♠

The last step in trying to put limits on the SNF via the spectrum is to give an upper bound for the exponent, d_n, of $\Gamma(A)$. This is done in the following.

Theorem 3.6. *Let A be diagonalizable with all eigenvalues integers. Then $d_n \mid \lambda_1\lambda_2\cdots\lambda_s$.*

Remark: That this result is best possible is demonstrated by the examples in this section.

Proof of theorem: Our procedure will be to show that the order of every element in $\Gamma(A)$ divides the product $\lambda_1\lambda_2\cdots\lambda_s$. This then would imply the result.

Let $\underline{v} \in L(A)$. Then we can write

$$\underline{v} = \sum_{i=1}^{s} \underline{e}_i\,, \tag{3b}$$

where each $\underline{e}_i$ is a (perhaps nonintegral) rational eigenvector for λ_i. Let

$$\underline{w} = \sum_{i=1}^{s} \frac{1}{\lambda_i}\underline{e}_i\,.$$

Then $\underline{w}$ is the unique preimage of $\underline{v}$, i.e. $\underline{w}A = \underline{v}$. The order of $\underline{v} + R(A)$ is then the smallest positive integer l such that $l\underline{w}$ is integral. Hence we show that $l \mid \lambda_1\lambda_2\cdots\lambda_s$.

We proceed by induction on the number of nonzero vectors $\underline{e}_i$ in the sum $(3b)$. If there is only one, then $\underline{v} = \underline{e}_i$ for some i, and since it is integral, the second proof of Theorem 3.1 shows that $l \mid \lambda_i \mid \lambda_1\lambda_2\cdots\lambda_s$. Now suppose that we know that all vectors composed of at most $k-1$ nonzero eigenvectors have order dividing $\lambda_1\lambda_2\cdots\lambda_s$. WLOG, set

$$\underline{v} = \sum_{i=1}^{k} \underline{e}_i,$$

$$\underline{w} = \sum_{i=1}^{k} \frac{1}{\lambda_i}\underline{e}_i = \underline{v}A^{-1},$$

and

$$\underline{x} = \sum_{i=1}^{k} \lambda_i \underline{e}_i = \underline{v}A.$$

Then

$$\underline{y} = \underline{x} - \lambda_k \underline{v} = \sum_{i=1}^{k-1} (\lambda_i - \lambda_k)\underline{e}_i$$

is integral. By the induction hypothesis applied to $\underline{y}$,

$$\underline{z} = \lambda_1 \lambda_2 \cdots \lambda_{k-1} \left(\sum_{i=1}^{k-1} (\frac{\lambda_i - \lambda_k}{\lambda_i})\underline{e}_i \right)$$

is integral. Finally then

$$\lambda_1 \lambda_2 \cdots \lambda_{k-1}\underline{v} - \underline{z} = \lambda_1 \lambda_2 \cdots \lambda_k \underline{w}$$

is integral. Hence we have $l \mid \lambda_1 \lambda_2 \cdots \lambda_k \mid \lambda_1 \lambda_2 \cdots \lambda_s$.

♡♠

There are two annoying assumptions in the above results: the diagonalizabilty of A and integrality of the eigenvalues of A. There were many attempts to eliminate the former assumption, but the following example shows how difficult it will be to eliminate it completely. Let

$$A_1 = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 2 & 2 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix},$$

and

$$A_3 = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Then calculation gives

$$\Gamma(A_1) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,$$

$$\Gamma(A_2) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4,$$

and

$$\Gamma(A_3) \cong \mathbb{Z}_8.$$

Not surprisingly, one has to use knowledge of the location and values of the off diagonal terms; this is generally hard. As an aside, [Ne1], in chapter 3, gives results which imply that in the all integer eigenvalue case, A is integrally similar to an upper triangular matrix with the eigenvalues along the diagonal. Hence we could assume at least that the spectrum is known and that A is upper triangular.

We shouldn't be too disheartened by these examples, since for most of the matrices of general interest in discrete mathematics, and indeed those which were the impetus of this work, the diagonalizability is apparent. The second assumption of all integer eigenvalues cannot be so easily waved away; take as an example the prevalence of integral circulant matrices. We conjecture that some generalization of the above holds, and as evidence offer the following.

Ex. 3-3: Let p be a prime, $p \equiv 3 \pmod 4$, and $\Im$ the set of *nonzero* quadratic residues mod p. As is customary, set $n = \frac{p+1}{4}$ and $k = \frac{p-1}{2}$. Form the row $\underline{a} = [a_0, a_1, \ldots, a_{p-1}]$ where

$$a_i = \begin{cases} 1 & \text{for } i \in \Im; \\ 0 & \text{otherwise.} \end{cases}$$

Let A be the circulant matrix with $\underline{a}$ as its first row. It is well-known that the eigenvalues of A are given by $\delta(\xi)$ where ξ runs through the pth roots of unity and $\delta(\xi)$ is given by

$$\delta(x) = \sum_{i \in \Im} x^i \, .$$

Fix $\xi \neq 1$, a pth root of unity. For $i \in \Im$, $\delta(\xi) = \delta(\xi^i)$. There then are only three eigenvalues:

k	multiplicity 1
$\delta(\xi)$	multiplicity k
$\delta(\overline{\xi})$	multiplicity k.

Here we use the fact that -1 is a nonsquare mod p. We wish to explicitly calculate these eigenvalues. From [I&R],

$$\delta(\xi) - \delta(\overline{\xi}) = \sqrt{-p}. \tag{3d}$$

From the theory of difference sets [La],

$$\delta(\xi) \cdot \delta(\overline{\xi}) = n. \tag{3e}$$

Combining equations $(3d)$ and $(3e)$, we can conclude that

$$\delta(\xi) = \frac{1+\sqrt{-p}}{2} \qquad \text{and} \qquad \delta(\overline{\xi}) = \frac{1-\sqrt{-p}}{2}.$$

In particular, these are not integers. The SNF of these matrices is also known (see [La] and the results later on in this chapter) and can be given as

$$\Gamma(A) \cong \left(\mathbb{Z}_n\right)^k \oplus \mathbb{Z}_k.$$

The k factors of $\mathbb{Z}_n$ seem to coincide with k repetitions of equation $(3e)$, perhaps suggesting an analog for Theorem 3.3.

♣◇

In closing, it seems that heuristically the more structure, symmetry, and regularity that an integral matrix has, the more that its Smith group has high rank and low exponent. There is evidence that if a matrix possesses these types of properties, then the multiplicities of most of its eigenvalues are large (see, for example, [Te]). The discussion in this section serves to relate these two phenomena. We further illustrate these ideas and the techniques of this section next in our discussion of the adjacency matrices of strongly regular graphs.

4. An Example: Strongly Regular Graphs

In order to illustrate the results of the last section, we need some nonsingular integral matrices with all integer eigenvalues. Fortunately, the theory of strongly regular graphs provides a plethora of such matrices.

A *strongly regular graph (srg)* G is a regular graph on v vertices of valency k such that any two adjacent vertices are mutually adjacent to λ vertices, and any two nonadjacent vertices are mutually adjacent to μ vertices. There are many existence theorems and constructions known for these; see for example, [B&vL]. We need only the following results. We always let A be the adjacency matrix of the srg in question.

Fact: As A is real symmetric, A is diagonalizable with real eigenvalues. In fact, A has exactly three eigenvalues, k,r,and s, where r and s are roots of

$$x^2 - (\lambda - \mu)x - (k - \mu) = 0. \tag{4a}$$

We will always take r to be the greater of the roots of $(4a)$. Let m_r and m_s be the respective multiplicities of r and s. Their values can be calculated from the two equations

$$\begin{aligned} k + rm_r + sm_s &= 0 \\ 1 + m_r + m_s &= v. \end{aligned} \tag{4b}$$

Let G' denote the complement of G; the corresponding adjacency matrix is $A' = J_v - I_v - A$. The parameters are determined by

$$\begin{aligned} v' &= v, \\ k' &= v - k - 1, \\ \lambda' &= v - 2k + \mu - 2, \end{aligned} \tag{4c}$$

and

$$\mu' = v - 2k + \lambda.$$

The eigenvalues are a little more behaved: $r' = -(s+1)$ and $s' = -(r+1)$. The respective multiplicities are $m'_r = m_s$ and $m'_s = m_r$.

We observe that if $m_r \neq m_s$, then r and s must be integers (and also, of course, r' and s'). In this case, at least Theorem 3.3 and possibly Corollary 3.4 will apply. Furthermore, if $d = d_v$ denotes the exponent of $\Gamma(A)$, then using Corollary 3.2 and Theorem 3.6 we have

$$\operatorname{lcm}(k, r, s) \;\Big|\; d \;\Big|\; k \cdot r \cdot s\,. \tag{4d}$$

A similar equation holds for d', the exponent of $\Gamma(A')$.

Ex. 4-1: *The Petersen Graph*

We have $v = 10$, $k = 3$, $\lambda = 0$, and $\mu = 1$. An easy computation gives $r = 1$ and $s = -2$, and so $m_r = 5$ and $m_s = 4$. Corollary 3.4 applies and so (ignoring the trivial terms),

$$\begin{aligned} \Gamma(A) &\cong \left(\mathbb{Z}_2\right)^4 \oplus \mathbb{Z}_3 \\ &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6. \end{aligned}$$

Notice that the Smith group is then uniquely determined by the spectrum. The actual SNF is

$$(1, 1, 1, 1, 1, 1, 2, 2, 2, 6).$$

Since the SNF can always be computed easily from the Smith group by filling in the right number of 1's, we will omit it in the future examples.

♣◇

Ex. 4-2: *The Hoffman-Singleton Graph*

We have $v = 50$, $k = 7$, $\lambda = 0$, and $\mu = 1$. We then compute $r = 2$ and $s = -3$ and also $m_r = 28$ and $m_s = 21$. Again Corollary 3.4 applies to give

$$\begin{aligned}\Gamma(A) &\cong \left(\mathbb{Z}_2\right)^{28} \oplus \left(\mathbb{Z}_3\right)^{21} \oplus \mathbb{Z}_7 \\ &\cong \left(\mathbb{Z}_2\right)^{7} \oplus \left(\mathbb{Z}_6\right)^{20} \oplus \mathbb{Z}_{42}.\end{aligned}$$

♣◇

Ex. 4-3: *The Line Graph of the Complete Graph K_n.*

The vertices of G are the edges of K_n, so $v = \binom{n}{2}$. To avoid degeneracy, we take $n \geq 5$. Two edges are adjacent iff they share a common vertex of K_n. Evidently $k = 2(n-2)$, $\lambda = n-2$, and $\mu = 4$. We then compute $r = n-4$ and $s = -2$ with $m_r = n-1$ and $m_s = \frac{n(n-3)}{2}$. The eigenvalues are not pairwise relatively prime, so Corollary 3.4 doesn't apply. We consider two cases.

n is odd: From equation $(4d)$ and the fact that n is odd, we see

$$2(n-2)(n-4) \mid d \mid 4(n-2)(n-4).$$

This severely limits $\Gamma(A)$. From Theorem 3.3, either

$$\Gamma(A) \cong \left(\mathbb{Z}_2\right)^{m_s} \oplus \left(\mathbb{Z}_{n-4}\right)^{m_r} \oplus \mathbb{Z}_{2(n-2)},$$

or

$$\Gamma(A) \cong \left(\mathbb{Z}_2\right)^{m_s - 1} \oplus \left(\mathbb{Z}_{n-4}\right)^{m_r} \oplus \mathbb{Z}_{4(n-2)}.$$

Numerical evidence suggests, and so we conjecture, that the former equation holds in general.

n is even: Equation $(4d)$ now yields

$$(n-2)(n-4) \mid d \mid 4(n-2)(n-4).$$

There are many more possibilities for $\Gamma(A)$ than in the previous case. This is because there is now a distinction between $\mathbb{Z}_{2(n-4)}$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_{n-4}$. We conjecture, again based on numerical evidence, that

$$\Gamma(A) \cong \left(\mathbb{Z}_2\right)^{m_s - m_r + 2} \oplus \left(\mathbb{Z}_{2(n-4)}\right)^{m_r - 1} \oplus \mathbb{Z}_{(n-2)(n-4)}.$$

♣◇

Ex. 4-4: *The Complement of Ex. 4-3*

Again we have $v' = \binom{n}{2}$. Appealing to $(4c)$ we have $k' = \binom{n-2}{2}$, $\lambda' = \binom{n-4}{2}$, and $\mu' = \binom{n-3}{2}$. The remaining eigenvalues are given by $r' = 1$ with $m'_r = \binom{n}{2} - n$ and $s' = -(n-3)$ with $m'_s = n - 1$. Rather than go through the analogous discussion as in the previous case, we just state the general answer:

$$\Gamma(A) \cong \left(\mathbb{Z}_{(n-3)}\right)^{n-1} \oplus \mathbb{Z}_{\binom{n-2}{2}}.$$

This does not follow from our results, although we can provide some limitations to the Smith group. It follows, rather, from the results of Wilson [Wi] on the SNF of the incidence matrix of t-subsets versus k-subsets of a fixed n-set. In our case, A is the incidence matrix of 2-subsets, i.e., edges of K_n, and $(n-2)$-subsets, since two edges are disjoint iff one is contained in the set complement of the other. As already noted, Wilson's techniques also involve looking at the Smith group; they relate somewhat to the results in section 6. Notice that if $n = 5$ we get the Petersen Graph, and the above formula agrees with the result in Ex. 4-1. Also observe that the general answer agrees with Corollary 3.4.

♣◇

Ex. 4-5: *The Line Graph of The Complete Bipartite Graph* $K_{n,n}$

The vertices of G are the edges of $K_{n,n}$, so $v = n^2$. Again, to avoid degeneracy we take $n \geq 3$. Here two edges are adjacent iff they share a common vertex of $K_{n,n}$. We easily compute $k = 2(n-1)$, $\lambda = n-2$, and $\mu = 2$. These then yield $r = n-2$ and $s = -2$ with $m_r = 2(n-1)$ and $m_s = (n-1)^2$. The eigenvalues are again not pairwise relatively prime, so we cannot derive $\Gamma(A)$ uniquely. We do note that the exponent satisfies

$$(n-1)(n-2) \mid d \mid 4(n-1)(n-2), \qquad \text{if} \quad n \text{ is even},$$

and

$$2(n-1)(n-2) \mid d \mid 4(n-1)(n-2), \qquad \text{if} \quad n \text{ is odd}.$$

As before, there are only a few possibilities left for $\Gamma(A)$. Rather than list these, we give what we conjecture to be the answer:

$$\Gamma(A) \cong \left(\mathbb{Z}_2\right)^{m_s - m_r} \oplus \left(\mathbb{Z}_{2(n-2)}\right)^{m_r - 1} \oplus \mathbb{Z}_{2(n-1)(n-2)}.$$

Note the similarity to Ex. 4-3.

♣◇

Ex. 4-6: *The Complement of Ex. 4-5*

For completeness, we discuss the analog of Ex. 4. Again $v' = n^2$ with $n \geq 3$. Here two edges are adjacent iff they share a disjoint in $K_{n,n}$. We compute $k' = (n-1)^2$, $\lambda' = (n-2)^2$, and $\mu' = (n-1)(n-2)$. These yield $r' = 1$ and $s' = -(n-1)$ with $m'_r = (n-1)^2$ and $m'_s = 2(n-1)$. The limits on d' are not that useful in general, namely

$$(n-1)^2 \;\Big|\; d' \;\Big|\; (n-1)^3.$$

The Smith group, however, seems to be given as

$$\Gamma(A) \cong \left(\mathbb{Z}_{(n-1)}\right)^{2(n-1)} \oplus \mathbb{Z}_{(n-1)^2}.$$

Note the similarity to Ex. 4-4, and that this is the same answer as in Corollary 3.4.

♣◇

Ex. 4-7: *Latin Square Graphs*

Up to now, we have given no indication as to whether or not the parameters of an srg uniquely determine the SNF. Notice that since two isomorphic graphs give equivalent adjacency matrices, two srg's with nonisomorphic Smith groups must themselves be nonisomorphic. In this example, we give two srg's with the same parameters and nonisomorphic Smith groups.

Let X be a set of n^2 points, where n is fixed. A *parallel class* of X is a collection of n disjoint n-subsets of X. We define an (n, ρ)-*net* to be a set of ρ parallel classes of X. We note that the existence of an (n, ρ)-net is equivalent to the existence of $(\rho - 2)$ pairwise orthogonal Latin squares of order n.

To construct an srg G from an (n, ρ)-net, we let the vertices of G be the points of X, so $v = n^2$. Two vertices are adjacent iff the corresponding points lie on the same line in some parallel class. One can then show that

$$k = \rho(n-1),$$

$$\lambda = (\rho-1)(\rho-2) + (n-2),$$

and

$$\mu = \rho(\rho-1).$$

A straightforward calculation then gives

$$r = n - \rho \qquad \text{with multiplicity} \quad m_r = \rho(n-1)$$

$$s = -\rho \qquad \text{with multiplicity} \quad m_s = n^2 - \rho n - \rho - 1\,.$$

Rather than repeat the by now standard techiques of determining restrictions on the Smith group of A, we prefer just to mention two special cases.

If $n = 2\rho$, then $\lambda = \mu = \rho(\rho - 1)$. A then becomes the incidence matrix of a $(v, k, \lambda)-$symmetric design (v, k, and λ as above). The information from the techniques used in this section is the same as that garnered from the results of section 5.

Now let n be arbitrary and $\rho = 3$. Then G always exists, since we always have a Latin square of order n. The three eigenvalues of A are now $3(n-1)$, $n-3$, and -3 with respective multiplicities 1, $3(n-1)$, and n^2-3n+2. We further let $n=6$, then we get 15, 3, and -3 with multiplicities 1, 15, and 20. Because 3 divides all of the eigenvalues, the results of the last section are not that useful. These parameters provide the example of nonisomorphic graphs:

1). The Latin square

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \\ 5 & 6 & 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 1 & 2 & 3 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{bmatrix}$$

has as the Smith group of its srg

$$\Gamma(A) \cong \left(\mathbb{Z}_3\right)^{12} \oplus \left(\mathbb{Z}_9\right)^{11} \oplus \mathbb{Z}_{45}\,.$$

2). The srg from the Latin square

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \\ 3 & 6 & 1 & 5 & 4 & 2 \\ 4 & 5 & 6 & 1 & 2 & 3 \\ 5 & 4 & 2 & 3 & 6 & 1 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{bmatrix}$$

has for its Smith group

$$\Gamma(A) \cong \left(\mathbb{Z}_3\right)^{8} \oplus \left(\mathbb{Z}_9\right)^{13} \oplus \mathbb{Z}_{45}\,.$$

The first of these is essentially the group multiplication table for $\mathbb{Z}_6$; the second is the group multiplication table for the symmetric group S_3.

♣◇

Ex. 4-8: *Paley Graph*

Our last example relates to the Ex. 3-3; it is an instance when the eigenvalues of A are not all integers. Let v be a prime, $v \equiv 1 \pmod 4$. The vertices of G will be the elements of the field $\mathbb{Z}_v$. Two vertices x and y are adjacent iff their difference $x - y$ is a nonzero square in G. In particular, this relationship is symmetric since -1 is a square mod v. Let n be defined from $v = 4n + 1$. Then one can show, in a manner similar to that in Ex. 3-3, that G is an srg with the additional parameters $k = 2n$, $\lambda = n - 1$, and $\mu = n$. We then compute $r = \frac{-1+\sqrt{v}}{2}$ and $s = \frac{-1-\sqrt{v}}{2}$. Their multiplicities must be equal since they are not integers, i.e., $m_r = m_s = 2n$. We then conjecture, based on numerous examples, and the results of section 6, that

$$\Gamma(A) \cong \left(\mathbb{Z}_n\right)^{2n} \oplus \mathbb{Z}_{2n}.$$

Observe that $rs = -n$; perhaps this explains why there are $2n$ factors of $\mathbb{Z}_n$.

♣◇

We note that the above merely scratches the surface of the more general problem of the Smith groups of the adjacency matrices of association schemes; in this case the spectrum of the matrices is usually determined.

5. The SNF and Augmented Matrices

In this section we give additional computational techniques using the Smith group. These techniques will apply to matrices augmented by additional rows.

We require some additional results from the theory of finite abelian groups. Recall that the *type* of a finite abelian group G is the vector of positive integers $(g_1, \ldots, g_n)$ such that $g_{i-1} \mid g_i$ for $i = 2, \ldots, n$, and

$$G \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{g_i} .$$

We further suppose that $g_1 = 1$ implies that $n = 1$ and so G is trivial. Of course if G is the Smith group of a matrix A, as given in equation (2*b*), then the type of $\overline{\Gamma}(A)$ is just the vector of nonunitary d_i (or (1), if $\overline{\Gamma}(A)$ is trivial).

Lemma 5.1. *Let G be a finite abelian group of type $(g_1, \ldots, g_n)$, and let H be a subgroup of G of type $(h_1, \ldots, h_m)$. Then for $i = 1, \ldots, m$, $h_i \mid g_{n-m+i}$. Furthermore, if G/H has type $(k_1, \ldots, k_s)$, then for $i = 1, \ldots, s$, $k_i \mid g_{n-s+i}$.*

Remark: This is problem 8 in section 4 of Bourbaki[Bo]. It is also listed as a problem in [H&H]. This lemma justifies the remark to Theorem 3.3 by taking $G = \Gamma(A)$ and $H \leq G$ with type $(\lambda_i, \ldots, \lambda_i)$ of length m_i.

Proof of lemma: We prove the conclusion for the type of H; the second result is similar. It is not hard to see that $m \leq n$. By considering the generators of H, we must have for each i, $h_i \mid g_{j_i}$ for some $j_i = 1, \ldots, n$. By induction and the properties of the type of H, h_1 divides the smallest of the g_{j_i}, h_2 divides the next smallest, and so forth. Now using the properties of the type of G, it follows that we can take this now ordered set of the g_{j_i} to be the last m terms of the type of G; this is the result.

♣◇

The focal point of the results in this section is the following, essentially trivial, lemma.

Lemma 5.2. *Let A be an $m \times n$ integral matrix and $\underline{v}$ an integral row vector of length n. Let B be the matrix formed by augmenting A by $\underline{v}$,*

$$B = \begin{pmatrix} A \\ \underline{v} \end{pmatrix}.$$

Then $\Gamma(B)$ is a homomorphic image of $\Gamma(A)$, with the kernel of the homomorphism being ${R(B)}\big/{R(A)}$.

Proof: Observe that $R(A) \leq R(B) \leq \mathbb{Z}^n$. Then we have the $\mathbb{Z}$-module isomorphism

$$\begin{aligned} \Gamma(B) &= {\mathbb{Z}^n}\big/{R(B)} \\ &\cong {\mathbb{Z}^n}\big/{R(A)}\Big/{R(B)}\big/{R(A)} \qquad (5a) \\ &= \Gamma(A)\Big/{R(B)}\big/{R(A)}. \end{aligned}$$

♣◇

Lemma 5.3. *Assume the same notation as Lemma 5.2.*

i). If $\underline{v} \in L(A)$, then the conclusion of Lemma 5.2 is true if we replace the Smith groups by their finite parts.

ii). If $\underline{v} \notin L(A)$, then $\overline{\Gamma}(A)$ is imbeddable in $\overline{\Gamma}(B)$.

Proof: Observe that ${R(B)}\big/{R(A)}$ is a $\mathbb{Z}$-module with one generator, namely $\underline{v} + R(A)$. If $\underline{v} \in L(A)$, then this element has finite order, i.e., ${R(B)}\big/{R(A)}$ is finite. The conclusion then follows from $(5a)$. Let $\underline{v} \notin L(A)$. By definition, $\overline{\Gamma}(B) = {L(B)}\big/{R(B)}$ and $\overline{\Gamma}(A) = {L(A)}\big/{R(A)}$. Define the natural map from $\overline{\Gamma}(A)$ to $\overline{\Gamma}(B)$ by

$$\underline{w} + R(A) \longmapsto \underline{w} + R(B)\,.$$

This is seen to be a well-defined injective homomorphism, which is the result.

♣◇

Ex. 5-1: We illustrate all of the possibilities of augmentation. Let A be the 1×2 matrix $(4,4)$, so that $\Gamma(A) \cong \mathbb{Z} \oplus \mathbb{Z}_4$. In the following table, B is the matrix formed by augmenting A by the row vector $\underline{v}$.

$\underline{v}$	$\Gamma(B)$
$[2,2]$	$\mathbb{Z} \oplus \mathbb{Z}_2$
$[3,3]$	$\mathbb{Z}$
$[0,1]$	$\mathbb{Z}_4$
$[0,2]$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4$
$[1,3]$	$\mathbb{Z}_8$

♣◇

We can explain these examples somewhat by appealing to the results on interlacing. These are known results, see [Th] and [MdS]. For an application of these results, see [De]. We state these results in the context of abelian groups. Unfortunately, we have not as yet found simpler proofs for this special case.

Theorem 5.4. *(Interlacing) Let G be a finite abelian group of type $(g_1, \ldots, g_n)$ and let $H = \langle\gamma\rangle$ be a cyclic subgroup of G. Suppose that ${}^{G}\!/_{H}$ has type $(h_1, \ldots, h_m)$. Then for $i = 1, \ldots, m$,*

$$g_{n-i} \mid h_{m-i+1} \, .$$

Proof:

Let A be the $n \times n$ diagonal matrix with $(g_1, \ldots, g_n)$ as its main diagonal. In particular, A has rank n over the rationals. We consider the elements of G to be n-tuples of integers, where the jth coordinate is taken modulo the jth component of

$(g_1, \ldots, g_n)$. Under this identification, it follows that $G \cong \Gamma(A)$. We claim that the Smith group of A augmented by a row is the same as a factoring G by some cyclic subgroup. One half of this correspondence is just Lemma 5.2. Conversely, factoring by a cyclic subgroup of G is the same as putting one more linear relationship on the coordinates, which in turn is the same as augmenting A by a row.

The interlacing result then follows by Theorem 2 of [Th].

♡♠

We draw the following heuristic for the results of Theorem 5.4. Here the arrows indicate divisibility, i.e., "$a \to b$" means "$a \mid b$." Notice that $h_1 = 1$ if $m = n - 1$.

$$\begin{tikzcd}
g_1 \arrow[r] \arrow[dr] & g_2 \arrow[r] \arrow[dr] & \cdots \arrow[r] \arrow[dr] & g_{n-1} \arrow[r] \arrow[dr] & g_n \\
h_1 \arrow[u] \arrow[r] & h_2 \arrow[u] \arrow[r] & \cdots \arrow[r] & h_{n-1} \arrow[u] \arrow[r] & h_n \arrow[u]
\end{tikzcd} \tag{5d}$$

Using this picture we state the converse to Theorem 5.4.

Theorem 5.5. *Suppose that G is as in Theorem 5.4 and $(h_1, \ldots, h_n)$ is a vector of positive integers obeying the divisibility requirements of* (5*d*). *Then there is a cyclic subgroup H of G such that the type of G/H is $(h_1, \ldots, h_n)$.*

Proof: Recall the notation of the proof of Theorem 5.4 and the correspondence used there between factoring G by a cyclic subgroup and augmenting a certain matrix A by a row. The other half of Theorem 2 in [Th] and the divisibility hypotheses imply that we can augment A by a row such that the SNF of the augmented matrix is given by the vector $(h_1, \ldots, h_n)$. Our correspondence then says that we can find a cyclic subgroup in G such that the factor group has as its type $(h_1, \dots, h_n)$ (except for possible leading 1's).

♡♠

We apply these results to the above example. If $\underline{v}$ is a rational multiple of $[2,2]$, then we can apply Theorem 5.4 with $G = \overline{\Gamma}(A)$ and $H = \langle \underline{v} + R(A) \rangle$ to conclude that $\overline{\Gamma}(B)$ is trivial or isomorphic to $\mathbb{Z}_2$ or $\mathbb{Z}_4$. Hence $\Gamma(B)$ is isomorphic to the direct sum of $\mathbb{Z}$ with one of these three possibilities. If, on the other hand, $\underline{v}$ is not in $R(A)$, then the situation reverses and we apply Theorem 5.4 with $G = \overline{\Gamma}(B) = \Gamma(B)$. We then see that $\Gamma(B) \cong \mathbb{Z}_a \oplus \mathbb{Z}_b$ with $a \mid 4 \mid b$. By Theorem 5.5, all of these possibilities are realizable at least as groups, and by the results in [Th], we can find a $\underline{v}$ such that augmenting by $\underline{v}$ produces each of the possibilities. We will give more applications of interlacing after the following lemma.

Lemma 5.6. *Let A and B be integral $m \times n$ matrices.*

i). If $R(A) = R(B)$, then $\Gamma(A) = \Gamma(B)$.

ii). If $R(A + B) \leq R(A) \cap R(B)$, then $\Gamma(A) = \Gamma(B)$.

Proof: Part i) is trivial. The second follows from the first since $B = (A + B) - A$, and so $R(B) \leq R(A)$, and conversely.

♣◇

Application: There is one common occurance of the hypotheses of the last lemma. Let A and B be integral $n \times n$ matrices with

$$A + B = J_n = J.$$

Suppose that A, and hence B, have constant column sums, say k and $n-k$. Create the matrices A' and B' by augmenting A and B by $\underline{j}$. We can now apply Lemma 5.4 to conclude that

$$\Gamma(A') = \Gamma(B').$$

Notice that we have not had to assume the invertibility of A or B.

If A is nonsingular, then the relationship of $\Gamma(A)$ to $\Gamma(A')$ is given by

$$\Gamma(A') \cong \Gamma(A)\big/_{H}, \qquad \text{where} \quad H \cong \mathbb{Z}_k$$

The interlacing results then give all of the possibilities for $\Gamma(A)$. As one instance of this situation, suppose A is the incidence matrix of a symmetric (v,k,λ)-design and B is the incidence matrix of the complementary design. Then all of the above reasoning applies. In particular, $\Gamma(A)$ and $\Gamma(B)$ are identical after factoring by the appropriate cyclic subgroup (respectively isomorphic to $\mathbb{Z}_k$ and $\mathbb{Z}_{v-k}$).

We give two further examples.

1): Let $A = J_n - nI_n$, for $n \geq 3$. A is singular with eigenvalues n (multiplicity $n-1$) and 0 (multiplicity 1, eigenvector $\underline{j}$). Let $B = nI_n$. Then the situation of the above paragraphs holds, and in particular, an easy calculation gives

$$\Gamma(A') = \Gamma(B') \cong (\mathbb{Z}_n)^{n-1}. \tag{5e}$$

We can now apply interlacing to the type of $\overline{\Gamma}(A)$ with respect to $\Gamma(B')$. In particular, for some $a_1 \mid n \mid a_2$,

$$\overline{\Gamma}(A) \cong \mathbb{Z}_{a_1} \oplus (\mathbb{Z}_n)^{n-3} \oplus \mathbb{Z}_{a_2}.$$

The SNF of A has $n-1$ nonzero terms. The first must be 1 since it is the gcd of the entries of A, and so $a_1 = 1$. It easy to see that the exponent of $\overline{\Gamma}(A)$ is n, so that $a_2 = n$. These remarks show that

$$\overline{\Gamma}(A) \;\cong\; (\mathbb{Z}_n)^{n-2}.$$

Finally, from the rank of A we can conclude that

$$\Gamma(A) \;\cong\; \mathbb{Z} \oplus (\mathbb{Z}_n)^{n-2}. \tag{5f}$$

♣◇

2): Let A_{mn} be the following $mn \times mn$ blocked matrix,

$$\begin{pmatrix} nI_n & J_n & \cdots & J_n \\ J_n & nI_n & & \vdots \\ \vdots & & \ddots & \\ J_n & \cdots & & nI_n \end{pmatrix}.$$

If $B_{mn} = J_{mn} - A_{mn}$, then B_{mn} is the direct sum of m copies the matrix A from example 1) above. Therefore we have from $(5f)$

$$\Gamma(B_{mn}) \;\cong\; \mathbb{Z}^m \oplus (\mathbb{Z}_n)^{m(n-2)}.$$

Notice that $\underline{j}$ (of length mn) is not in $R(B_{mn})$. This implies that $\overline{\Gamma}(B_{mn})$ is imbeddable in $\overline{\Gamma}(B'_{mn})$. Applying interlacing, for some $a_1 \mid n \mid a_2$ we have

$$\overline{\Gamma}(A'_{mn}) \;=\; \overline{\Gamma}(B'_{mn}) \;\cong\; \mathbb{Z}_{a_1} \oplus (\mathbb{Z}_n)^{m(n-2)-1} \oplus \mathbb{Z}_{a_2}.$$

For the same reason as in example 1), the exponent of $\overline{\Gamma}(B'_{mn})$ is n, so that $a_2 = n$.

Next notice that $\underline{j} \in R(A_{mn})$, so that $\overline{\Gamma}(A'_{mn})$ is an image of $\overline{\Gamma}(A_{mn})$. Interlacing then says that for $b_1 \mid a_1 \mid b_2 \mid n$, and $n \mid b_3$

$$\overline{\Gamma}(A_{mn}) \;\cong\; \mathbb{Z}_{b_1} \oplus \mathbb{Z}_{b_2} \oplus \left(\mathbb{Z}_n\right)^{m(n-2)-1} \oplus \mathbb{Z}_{b_3}\,.$$

Numerical evidence indicates that for $d = \gcd(m-1, n)$, $b_1 = d$, $b_2 = n$, and $b_3 = \frac{n^2}{d}$. That is, we conjecture

$$\Gamma(A_{mn}) \;\cong\; \mathbb{Z}^{m-1} \oplus \mathbb{Z}_d \oplus \left(\mathbb{Z}_n\right)^{m(n-2)} \oplus \mathbb{Z}_{\frac{n^2}{d}}\,. \qquad (5g)$$

♣◇

We remark in closing that augmenting by more than one row yields results similar to Lemmas 5.2 and 5.3, except for an increased number of possibilities for the image of the Smith group. We have omitted these generalizations; by far the most common instance in practice is augmenting by a single row.

6. The SNF and Products of Matrices

We finish in this last section with results on the SNF for a product of matrices. As in the previous sections, the techniques which will be developed will be used to prove known results in our general setting, and some new ones besides. All of our results follow essentially from the following simple theorem.

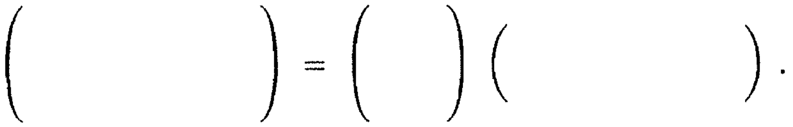
Theorem 6.1. *Let A be an integral $t \times n$ matrix and B an integral $m \times t$ matrix of rank t. Let $C = BA$. Then $\overline{\Gamma}(A)$ is a homomorphic image of $\overline{\Gamma}(C)$ where the kernel of the homomorphism is $R(A)\big/R(C)$. If, in addition, the rank of A is t, then $\overline{\Gamma}(B) \cong R(A)\big/R(C)$. In particular,*

$$\Gamma(A) \simeq \Gamma(C)\big/\Gamma(B) \tag{6a}$$

and

$$\overline{\Gamma}(A) \cong \overline{\Gamma}(C)\big/\overline{\Gamma}(B)\,. \tag{6b}$$

Remark: The general picture looks like



Proof of theorem: From $C = BA$ we can in general conclude that $R(C) \leq R(A)$, and also $V(C) \leq V(A)$. Since the rank of B is t, A and C have the same rank, so that $V(C) = V(A)$. By the usual isomorphism theorem,

$$\begin{aligned}
\overline{\Gamma}(A) &= L(A)\big/R(A) = L(C)\big/R(A) \\
&\cong L(C)\big/R(C) \Big/ R(A)\big/R(C) \\
&= \overline{\Gamma}(C) \Big/ R(A)\big/R(C)\,.
\end{aligned}$$

Suppose further that A has rank t. We construct an isomorphism from $\Gamma(B)$ to $R(A)\big/R(C)$. Define the map φ from $L(B)$ to $R(A)\big/R(C)$ by

$$\varphi: \quad \underline{v} \longmapsto \underline{v}A + R(C)\,.$$

It is clear that φ is well-defined and a homomorphism. It is onto since $L(B) = \mathbb{Z}^t$. We assert that the kernel of φ is $R(B)$, which would then finish the result. Clearly $R(B)$ is in the kernel of φ. Conversely, if $\underline{v}A + R(C) = R(C)$ for integral t-vector $\underline{v}$, then there exists an integral m-vector $\underline{w}$ such that

$$\underline{v}A = \underline{w}C = \underline{w}BA\,.$$

Since A has rank t, we can conclude that $\underline{v} = \underline{w}B$. So $\underline{v} \in R(B)$. Finally, equations (6*a*) and (6*b*) hold subject to this identification of $\Gamma(B) = \overline{\Gamma}(B)$.

$\heartsuit\spadesuit$

Recall that a square integral matrix A is equivalent to its transpose A^T. From this it follows that $\Gamma(A) \cong \Gamma(A^T)$. If A is not square, it still is true that the nonzero terms of the SNF's of A and A^T are the same. That is, we always have $\overline{\Gamma}(A) \cong \overline{\Gamma}(A^T)$. This observation leads to the following.

Corollary 6.2. *Let A, B, and C be as in Theorem 6.1, all of rank t. Then*

$$\overline{\Gamma}(B) \cong \overline{\Gamma}(C)\big/\overline{\Gamma}(A)\,.$$

Proof: Apply Theorem 6.1 to $C^T = A^T B^T$.

$\heartsuit\spadesuit$

We are now in the position to prove two results which are, in part, in [Nel]. For an integral matrix A, we let $d_i(A)$ denote the ith term of its SNF. We caution that this is what Newman calls $s_i(A)$; he uses $d_i(A)$ for the gcd of $i \times i$ minors.

Theorem 6.3. *Let A, B, and C be as in Corollary 6.2. Then for $i = 1, \ldots, t$,*

$$d_i(A) \mid d_i(C) \qquad \text{and} \qquad d_i(B) \mid d_i(C)\,. \tag{6c}$$

Remark: When A and B are square, this is Theorem II.14 in [Nel].

Proof of theorem: From Theorem 6.1 and Lemma 5.1, the types of $\overline{\Gamma}(A)$ and $\overline{\Gamma}(B)$ each divide term by term the appropriate last terms of the type of $\overline{\Gamma}(C)$. Since the rank of each matrix is t, the vector of nonzero elements of the SNF of each matrix is just the type of the Smith group's finite part proceeded by an appropriate number 1's (to make a vector of length t). The equations in (6c) quickly follow.

♡♠

Theorem 6.4. *Let A, B, and C be as in Corollary 6.2 such that the orders of $\overline{\Gamma}(A)$ and $\overline{\Gamma}(B)$ are relatively prime. Then for $i = 1, \ldots, t$,*

$$d_i(A) d_i(B) \;=\; d_i(C)\,. \tag{6d}$$

Remark: When A and B are square, this is Theorem II.15 in [Nel].

Proof of theorem: As in Theorem 6.3, let $\underline{d}_A$ and $\underline{d}_B$ be the vectors of length t formed by adding leading 1's to the type of A and B, respectively. Let $\underline{d}_A * \underline{d}_B$ denote the term by term product of $\underline{d}_A$ and $\underline{d}_B$. Since the orders of $\overline{\Gamma}(A)$ and $\overline{\Gamma}(B)$

are relatively prime, $\overline{\Gamma}(C) \simeq \overline{\Gamma}(A) \oplus \overline{\Gamma}(B)$. Hence, the terms of $\underline{d}_A * \underline{d}_B$ correspond to direct summands of $\overline{\Gamma}(C)$, and therefore the nonunitary terms of $\underline{d}_A * \underline{d}_B$ must be the type of $\overline{\Gamma}(C)$. Equation (6d) easily follows.

♡♠

Example: This example comes from [Ne1]. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & \lambda \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 1 & 0 \\ -1 & \lambda \end{pmatrix} .$$

Then $\Gamma(A) \cong \mathbb{Z}_\lambda$ and $\Gamma(B) \cong \mathbb{Z}_\lambda$. Since

$$AB = \begin{pmatrix} 0 & -\lambda \\ \lambda & \lambda^2 \end{pmatrix} \qquad \text{and} \qquad BA = \begin{pmatrix} 1 & 1 \\ -1 & \lambda^2 - 1 \end{pmatrix} ,$$

we have $\Gamma(AB) \cong \mathbb{Z}_\lambda \oplus \mathbb{Z}_\lambda$ and $\Gamma(BA) \cong \mathbb{Z}_{\lambda^2}$. This shows that the conclusion of Theorem 6.4 is not true in general if the orders of $\overline{\Gamma}(A)$ and $\overline{\Gamma}(B)$ are not relatively prime. Furthermore, it shows that $\Gamma(AB)$ need not be isomorphic to $\Gamma(BA)$.

♣♢

In order to further exploit Theorem 6.1, we need to digress to more results in the theory of abelian groups. Let G be a finite abelian group, and fix a prime p. Following Lander [La], for $i \geq 0$ let π_i denote the number of factors of the type of G which are exactly divisible by p^i. If $H \leq G$ and the type of G has length m, then we set

$$\pi_0(H) = m - \{\pi_1(H) + \pi_2(H) + \cdots\} .$$

We define $\pi_0(H)$ similarly if H is a factor group of G.

Theorem 6.5. *Let $G = \left(\mathbb{Z}_{p^s}\right)^m$, where p is prime and $s \geq 1$. Let $H < G$ and $K = {}^{G}\big/_{H}$. Then for $i = 0, 1, \ldots, s$,*

$$\pi_i(H) \;=\; \pi_{s-i}(K)\,.$$

Proof: Let H be generated by the independent elements α_{ij}, where the order of α_{ij} is p^i for $j = 1, \ldots, \pi_i(H)$, and $i = 1, \ldots, s$. For each α_{ij} there exists a $\beta_{ij} \in G$ such that β_{ij} has order p^s and $p^{s-i}\,\beta_{ij} = \alpha_{ij}$. This is easily seen by taking elements of G to be m-tuples of integers mod p^s. Define

$$H' = \langle \beta_{ij} \;:\; j = 1, \ldots, \pi_i(H)\;,\; i = 1, \ldots, s\rangle\,.$$

We assert that

$$H' \;\cong\; \left(\mathbb{Z}_{p^s}\right)^{m-\pi_0(H)}\,.$$

It suffices to show that the g_{ij}'s are independent. But since $H \leq H'$, H' has at least $m - \pi_0(H)$ independent terms, and two different β_{ij}'s cannot lie in the same one.

Since $H' \leq G$, we can find $\pi_0(H)$ elements of order p^s, say $\gamma_1, \ldots, \gamma_{\pi_0(H)}$, such that

$$G \;\cong\; H' \oplus \langle\gamma_1\rangle \oplus \cdots \oplus \langle\gamma_{\pi_0(H)}\rangle\,. \tag{6d}$$

Notice that the order of $\beta_{ij} + H$ in K is p^{s-i} and that the order of $\gamma_j + H$ is p^s. This and equation (6d) are enough to show the result.

♡♠

Application: Theorem 6.5 leads to the symmetry results of the SNF found in [La] and [De].

1): We first do the case $AA^T = nI_m$, where A is an integral $m \times m$ matrix and $n \neq 0$. From Theorem 6.1 we have

$$\Gamma(A) \cong {(\mathbb{Z}_n)^m}\big/{\Gamma(A^T)}\,.$$

From the remarks before Corollary 6.2, $\Gamma(A) \cong \Gamma(A^T)$. Theorem 6.5 then says that if p^s exactly divides m, p prime, then

$$\pi_i\big(\Gamma(A)\big) \;=\; \pi_{s-i}\big(\Gamma(A)\big) \qquad \text{for } i = 0, 1, \ldots, s\,. \tag{6e}$$

Equation $(6e)$ is what is meant by the symmetry of the SNF, since the number of terms of the SNF of A exactly divisible by p^i is the same as the number exactly divisible by p^{s-i}. Notice that $(6e)$ holds if we generalize to the case $AEA^T = nF$ where E and F are $m \times m$ unimodular matrices. Lander in [La] shows this result in almost our generality; he further requires that E be symmetric. Of course, the same argument works if $A^2 = nI_m$ or $AEA = nF$.

As a special case, suppose that A is a Hadamard matrix of order $4n$. Then $(6e)$ holds. Since the first term of the SNF is 1, the last term of the SNF is $4n$. Since the only possible 2×2 determinants are 0 or 2, we see that the second term of the SNF is 2. That is, the second to last term of the SNF is $2n$. An interesting question is what combinatorial significance, if any, the multiplicities of the diagonal terms of the SNF have.

♣◇

2): The first matrices studied with regard to this type of symmetry were the incidence matrices of (v, k, λ)-symmetric designs. Let A be such an incidence matrix, so that if $n = k - \lambda$,

$$AA^T = nI_v + \lambda J_v \,. \tag{6f}$$

Define

$$B = \begin{pmatrix} & & & 1 \\ & A & & \vdots \\ & & & 1 \\ \lambda & \cdots & \lambda & k \end{pmatrix} .$$

Let Λ be the $(v+1) \times (v+1)$ matrix $\mathrm{diag}(1, \ldots, 1, -\lambda)$. Computation shows that $B \Lambda B^T = n\Lambda$. Hence we get the equations in $(6e)$ for prime p dividing n if p also does not divide λ, since the Smith group of Λ can then be ignored.

We can also proceed a little more directly from $(6f)$. From the example in section 3, we know the Smith group of the right side of $(6f)$. That is,

$$\Gamma(A) \cong {(\mathbb{Z}_n)}^{v-2} \oplus \mathbb{Z}_{nk^2} \Big/ \Gamma(A^T) ,$$

where we use the fact that $k^2 = n + v\lambda$. If prime p divides n and does not divide λ, then p does not divide k. We can then derive equations similar to $(6e)$; the symmetry would apply only to the last $v-1$ terms. The advantage to this method is that the result applies to A and not the padded matrix B. This is essentially what [De] does except that the actual techniques there involve interlacing.

♣◇

3): Our last example concerns affine resolvable designs. We take an *affine resolvable design* to be a (v, b, r, k, λ)-design such that the blocks can be partitioned into parallel classes of size s with blocks in the same class disjoint and blocks in different classes meeting in μ points (see, for example, [Wa] or [La]). Let A be the $v \times b$ incidence matrix of points versus blocks of such a nondegenerate design. Then

$$AA^T = (r - \lambda) I_v + \lambda J_v ,$$

and by nondegeneracy, AA^T is nonsingular. Therefore, the rank of A is v. (This is just the proof of Fisher's inequality: $b \geq v$.) Notice that we cannot apply Theorem 6.1, since in general $b > v$. Instead, order the columns of A by parallel classes. Then we have the $b \times b$ matrix of $s \times s$ blocks (r blocks in each row)

$$A^T A = \begin{pmatrix} kI_s & \mu J_s & \cdots & \mu J_s \\ \mu J_s & kI_s & & \vdots \\ \vdots & & \ddots & \\ \mu J_s & \cdots & & kI_s \end{pmatrix} . \tag{6g}$$

Since all of the parameters are nonnegative, a straightforward calculation shows that $A^T A$ is nonsingular unless $k = \mu s$. When $k \neq \mu s$, the Smith group of $A^T A$ doesn't seem to be that well-behaved, although the techniques of sections 3 and 5 may help in specific cases. Suppose that $k = \mu s$. Then factoring the right side of $(6g)$ by μ leaves the matrix A_{rs} from example 2) at the end of section 5. Therefore our conjecture, $(5g)$, says that in this case,

$$\overline{\Gamma}(A^T A) \cong \mathbb{Z}_{d\mu} \oplus \left(\mathbb{Z}_{s\mu}\right)^{r(s-2)} \oplus \mathbb{Z}_{\frac{s^2\mu}{d}} , \tag{6h}$$

where $d = \gcd(r-1, s)$. As one example of this, consider the affine plane of order n. Then $v = n^2$, $b = n(n+1)$, $r = n+1$, $k = n$, $\lambda = 1$, $s = n$, and $\mu = 1$. Then $d = n$ and (6h) becomes

$$\overline{\Gamma}(A^T A) \;\cong\; (\mathbb{Z}_n)^{n(n-1)} .$$

Hence given our conjecture, there is the same sort of symmetry from Theorem 6.5 as in the symmetric design case. This symmetry applies to the middle $n(n-1)$ terms of the SNF, since the first n terms are 1's and the last n terms are 0's. In particular, if prime p exactly divides n, then the rank of A mod p is less than or equal to

$$n + \frac{n(n-1)}{2} \;=\; \frac{b}{2} .$$

♣◇

There is one more application of Theorem 6.1 worth mentioning. Following Wilson [Wi], we call an integral matrix A *primitive* if $\overline{\Gamma}(A)$ is trivial. Let A, B, and C be as in Corollary 6.2. If A is primitive, then $\overline{\Gamma}(C) \cong \overline{\Gamma}(B)$, and similarly if B is primitive. Notice that if the matrices are square, than a primitive matrix of the given rank must be unimodular, and so this observation is trivial. In some problems, however, such as in [Wi], it seems easier to find nonsquare primitive matrices which give simple computations using Theorem 6.1

References

[Bo] N. Bourbaki, *Eléments de Mathematique*,Vol. 1,Book II *Algèbra*,chap. 6–7,2nd ed.,Hermann,Paris,1964

[B&vL] A.E. Brouwer & J.H. van Lint, Strongly Regular Graphs and Partial Geometries,in *Enumeration and Design*, ed. D.M. Jackson & S.A. Vanstone,Academic Press,New York,1984

[Ca] R.D. Carmichael, *Groups of Finite Order*,Dover,1937

[De] Z. Deretsky, On the Smith Normal Form for (v, k, λ) Designs, *Linear and Multilinear Algebra*,**14**(1983),187–193

[H&H] B. Hartley & T.O.Hawkes, *Rings, Modules, and Linear Algebra*, Chapman and Hall,London,1970

[I&R] K. Ireland & M.I. Rosen, *Elements of Number Theory*, Bogden & Quigley, Tarrytown-on-Hudson,1972

[La] E.S. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press,Cambridge,1983

[MdS] E. Marques de Sa, Imbedding Conditions for λ-Matrices, *Linear Algebra and its Applications*,**24**(1979),33–50

[Ne1] M. Newman, *Integral Matrices*,Academic Press,New York,1972

[Ne2] M. Newman, On a Problem Suggested by Olga Taussky-Todd, *Illinois J. Math.*,**24**(1980),156–158

[Te] P. Terwilliger, Eigenvalue Multiplicities of Highly Symmetric Graphs, *Discrete Math.*,**41**(1982),295–302

[Th] R.C. Thompson, Interlacing Inequalities for Invariant Factors, *Linear Algebra and its Applications*,**24**(19~~82~~71),1–31

[Wa] W.D. Wallis, Construction of Strongly Regular Graphs using Affine Designs,*Bull. Australian Math. Soc.*,**4**(1971),41–49

[Wi] R.M. Wilson, Something on t-subsets vs. k-subsets matrices, *in preparation*

Chapter II

Generalized Q-codes

1. Introduction

In this chapter we generalize the work of V. Pless, et al. (specifically [L,M,&Pl],[Pl,M,&L],[Pl1], and [Pl2]) by describing new families of abelian group codes. That is, for an abelian group G of odd order n and a finite field $\mathbf{F}$ of characteristic relatively prime to n, we construct, by means of their idempotents, $(n, \frac{n+1}{2})$ and $(n, \frac{n-1}{2})$ linear codes with G in their automorphism groups. These will be called generalized Q-codes. We show how all of the properties of the duadic codes([L,M,&Pl],[Pl,M,&L],and [Pl1]) and Q-codes ([Pl2]) extend and we derive these codes as special instances of ours. In particular, we state when the minimum weight vectors of the codes support a projective plane with regular automorphism group G.

When the characteristic of $\mathbf{F}$ is 2, we give easy conditions on G and $\mathbf{F}$ for the existence of these generalized Q-codes. We will furnish constructions in all cases when we know that Q-codes exist; in every such case we describe an idempotent with binary coefficients or coefficients in GF(4). Our methods of construction also yield interesting codes over larger fields of characteristic 2, some of which are MDS. We give numerous examples throughout.

The results in this chapter are proven using algebraic techniques. In particular, we take abelian group codes to be ideals in the group ring $\mathbf{F}[G]$. As such, we assume familarity with the theory of abelian groups and semi-simple algebras. Major results needed in these areas are stated without proof. For references, we suggest [B&M] and [La].

2. Preliminaries

In this chapter, G always denotes a finite abelian group of order n and $\mathbf{F}$ will be the finite field GF(q) of characteristic p where $p \nmid n$. From these we form the group ring $\mathbf{F}[G]$ whose elements are the formal sums

$$a(x) = \sum_{g \in G} \alpha_g \, x^g \,, \tag{2a}$$

where the coefficients α_g are in $\mathbf{F}$. The symbols "x^g" are indeterminants. We define the arithmetic on $\mathbf{F}[G]$ as follows. For $\alpha \in \mathbf{F}$,

$$\alpha \left(\sum_{g \in G} \alpha_g \, x^g \right) = \sum_{g \in G} \alpha \alpha_g \, x^g \,.$$

Addition of elements in $\mathbf{F}[G]$ is defined by

$$\left(\sum_{g \in G} \alpha_g \, x^g \right) + \left(\sum_{g \in G} \beta_g \, x^g \right) = \sum_{g \in G} (\alpha_g + \beta_g) \, x^g \,,$$

and multiplication by

$$\left(\sum_{g \in G} \alpha_g \, x^g \right) \cdot \left(\sum_{g \in G} \beta_g \, x^g \right) = \sum_{g \in G} \Big(\sum_{k \in G} \alpha_k \beta_{g-k} \Big) \, x^g \,,$$

where the operation "$g - k$" in the last summation is in G. In general, we use the same symbols to denote operations in G, $\mathbf{F}$, and $\mathbf{F}[G]$. We use the symbol "$\subseteq$" to denote set containment and the symbol "$\leq$" to denote a set containment preserving underlying structure, i.e., subgroup, subfield, ideal and so forth.

It is straightforward to see that these definitions make $\mathbf{F}[G]$ into a commutative algebra over $\mathbf{F}$. In particular, we denote the zero of $\mathbf{F}[G]$ by $\underline{0}$ and the identity of $\mathbf{F}[G]$ by $\underline{1}$. Notice that $\underline{1} = x^0$, where 0 is the identity element in G. In general, we call a monomial term x^g for $g \in G$ a *shift*; multiplying an element by a shift just permutes its coefficients. For a subset $S \subset G$ we write $S(x)$ for the sum of shifts x^g for $g \in S$. The *support* of an element $a(x) \in \mathbf{F}[G]$ is the set of $g \in G$ such that the coefficient of x^g in $a(x)$ is nonzero. For $S \subseteq G$, we also speak of a shift of S, i.e., the support of a shift of $S(x)$. For historical reasons, we write $\underline{h}$ for $G(x)$.

We call the ideals of $\mathbf{F}[G]$ *codes* or, more specifically, *G-codes.* When G is a cyclic group, these are the usual cyclic codes of length n. Other G-codes have also been studied, in particular in [MW] and [B&M]. In order to emphasize the more usual coding theoretic interpretation of these ideals, we also write $\underline{a}$ for an element $a(x)$ given as in (2a), where $\underline{a}$ is the n-vector $(\alpha_{g_1}, \alpha_{g_2}, \ldots)$ for some fixed order of the elements of G. A G-code is then a collection of vectors of length n, coefficients in $\mathbf{F}$, which is invariant under the coordinate permutations induced by the shifts.

We use the common terminology from coding theory: weight, minimum distance, dimension, and so forth. Two codes are *permutation equivalent* if there is a coordinate permutation sending one code into the other. We denote this equivalence by "$\sim$." The *extension* of a code is the collection of vectors of length $n+1$ constructed by adding a leading "parity check" coordinate so that the sum of all of the coordinates is now zero. For a code C, we write C^* for its extension. The quantity δ_C will denote the minimum weight of the code C; we suppress "C" if it is clear from context. If the dimension of a given code C is k, we have the *Singleton bound*:

$$\delta + k \leq n + 1 \,.$$

If equality holds, C is called *maximum distance separable (MDS)*. See [MW&Sl] for the importance of such codes. Finally, the *weight distribution* of a code C is the vector $(w_0, w_1, \ldots, w_n)$, where w_i is the number of codewords of weight i in C.

Besides $\mathbf{F}[G]$ and the zero ideal, $\mathbf{0}$, there are two codes easily described for general $\mathbf{F}[G]$. The first is just the span of $\underline{h}$—we call this code H. For the second, as suggested by the notation in (2a), let $a(1)$ denote the sum of all the coefficients of $a(x)$,i.e., $\underline{a}\,\underline{h} = a(1)\underline{h}$. As in [P12], we say that an element $a(x)$ is *even-like* if $a(1) = 0$ and *odd-like* otherwise, and we call a code even-like if all of its codewords are even-like. The collection of all even-like words is an ideal in $\mathbf{F}[G]$ which we denote by E. We note that E and H are duals with respect to the usual inner product, and so their respective dimensions are $n-1$ and 1. We will talk in more depth about inner products and duality of G-codes in section 4.

Because $p \not| \ n$, $\mathbf{F}[G]$ is semi-simple. As a reference for the structure of $\mathbf{F}[G]$, see [B&M]. Recall that an *idempotent* of $\mathbf{F}[G]$ is an element $\underline{e}$ such that $\underline{e}\,\underline{e} = \underline{e}$. Then $\mathbf{F}[G]$ is the direct sum of ideals generated by idempotents $\underline{f}_1, \underline{f}_2, \ldots, \underline{f}_r$ such that

$$\underline{1} = \underline{f}_1 + \underline{f}_2 + \cdots + \underline{f}_r$$

where

$$\underline{f}_i\,\underline{f}_j = \underline{0} \qquad \text{if} \quad i \neq j\,.$$

The $\underline{f}_i$'s are the *primitive* idempotents of $\mathbf{F}[G]$. Every ideal in $\mathbf{F}[G]$ is generated by an idempotent which is uniquely expressible as the sum of primitive idempotents. In particular, $\mathbf{F}[G]$ has exactly 2^r ideals.

Let C_1 and C_2 be two codes with respective generating idempotents $\underline{e}_1$ and $\underline{e}_2$. It is well-known ([vL]) that the idempotent for the code $C_1 \cap C_2$ is $\underline{e}_1\underline{e}_2$ and that the idempotent for the code $C_1 + C_2$ is $\underline{e}_1 + \underline{e}_2 - \underline{e}_1\underline{e}_2$. If $\underline{e}$ is an idempotent then so is $\underline{1} - \underline{e}$. From $\underline{e}\,\underline{e} = \underline{e}$ we see that $e(1) = 0$ or 1. Therefore, one of the codes $\langle \underline{e} \rangle$ or $\langle \underline{1} - \underline{e} \rangle$ is even-like. The next simple lemma describes the relationship between these two codes.

Lemma 2.1. *Let $\underline{e}$ be an idempotent of $\mathbf{F}[G]$. Then*

$$\mathbf{F}[G] = \langle \underline{e} \rangle \oplus \langle \underline{1} - \underline{e} \rangle\,.$$

In particular, if $\dim(\langle \underline{e} \rangle) = k$, then $\dim(\langle \underline{1} - \underline{e} \rangle) = n - k$.

Remark: As an example of this lemma, notice that the idempotent for H is $\frac{1}{n}\underline{h}$ and that the idempotent for E is $\underline{1} - \frac{1}{n}\underline{h}$.

Proof of lemma: The idempotent of $\langle \underline{e} \rangle \cap \langle \underline{1} - \underline{e} \rangle$ is $\underline{e}(\underline{1} - \underline{e})$, which is $\underline{0}$. The idempotent for $\langle \underline{e} \rangle + \langle \underline{1} - \underline{e} \rangle$ is $\underline{e} + (\underline{1} - \underline{e})$, which is $\underline{1}$. The result easily follows.

♣◇

We generalize the constructions in [L,M,&Pl],[Pl,M,&L], and [Pl2] for obtaining G-codes from idempotents using the automorphism group of G. We denote this automorphism group by $\mathrm{Aut}(G)$ and write automorphisms acting from the right. Let $\mu \in \mathrm{Aut}(G)$. Then μ induces an automorphism of $\mathbf{F}[G]$ given by

$$\mu : \qquad \sum_{g \in G} \alpha_g \, x^g \quad \longmapsto \quad \sum_{g \in G} \alpha_g \, x^{g\mu} \, .$$

We use the same symbol for both automorphisms. If μ leaves a code C of $\mathbf{F}[G]$ set-wise fixed, then we say that μ is a *multiplier* of C. Notice that $C \sim C\mu$.

Let $\ell \in \mathbb{Z}$ with $\gcd(\ell, n) = 1$. Define a function μ_ℓ on G by

$$\mu_\ell : \qquad g \quad \longmapsto \quad \ell g \, ,$$

where, by additive notation on G, "ℓg" means g added to itself ℓ times. Since ℓ is relatively prime to the order of G, $\mu_\ell \in \mathrm{Aut}(G)$. Such an automorphism is called *numerical.* One then speaks of numerical multipliers for G-codes.

Lemma 2.2. *Let $a(x) \in \mathbf{F}[G]$ and $q = |\mathbf{F}\ |$. Then $a(x)^q = a(x)\mu_q$. In particular, μ_q is a numerical multiplier for every ideal.*

Proof: This is known, for example in [La]. Let $a(x)$ be given as in $(2a)$. Since the characteristic of $\mathbf{F}$ is p and q is a power of p, we have

$$\left(\sum_{g\in G} \alpha_g\, x^g\right)^q = \sum_{g\in G} (\alpha_g\, x^g)^q = \sum_{g\in G} \alpha_g^q\, x^{g\mu_q}\,.$$

The first statement of the lemma then follows from the fact that $\alpha^q = \alpha$ for all $\alpha \in \mathbf{F}$. The second statement is a direct result of this result, since $a(x)$ in an ideal implies that $a(x)^q$ is also in the ideal.

♣◇

The automorphism μ_q partitions G into orbits. We denote the orbit containing nonzero $g \in G$ by $\mathrm{C}_g^{(q)}$. If q is clear from context, we may suppress it and just write C_g. These orbits are called ***cyclotomic cosets*** (see [L,M,&Pl1] and [Pl2]). The importance of these cyclotomic cosets is given by the next well-known lemma (given in the binary case in [MW&Sl]).

Lemma 2.3. *Let $\underline{e}$ be an idempotent of $\mathbf{F}[G]$ and $\Im$ a complete set of representatives from the nonzero cyclotomic cosets. Then $\underline{e}$ is constant on C_g for each $g \in \Im$. That is, for some $\beta_0, \beta_g \in \mathbf{F}$,*

$$\underline{e} = \beta_0\underline{1} + \sum_{g\in\Im} \beta_g\, \mathrm{C}_g(x)\,. \tag{2b}$$

Proof: Since $\underline{e}$ is an idempotent, $\underline{e}^2 = \underline{e}\,\underline{e} = \underline{e}$, so that $\underline{e}^q = \underline{e}$. Then from Lemma 2.2, $\underline{e} = \underline{e}\mu_q$. The result is immediate.

♣◇

Let $\mathbf{E}$ be an extension field of $\mathbf{F}$ which contains an nth root of unity. A *character* χ of G into $\mathbf{E}$ is a homomorphism from G to the multiplicative group of $\mathbf{E}$. Characters are useful in the study of G-codes (see [MW] and [La]). They are the natural generalization of the concept of roots of a cyclic code (see [MW&Sl]). The characters form a group under multiplication which is isomorphic to G. We index the characters of G by elements in G and write χ_g. A cyclotomic coset of characters for $g \in G$ is the set

$$\mathrm{X}_g^{(q)} = \left\{\chi_g \ : \ g \in \mathrm{C}_g^{(q)}\right\}.$$

Here q is the size of $\mathbf{F}$; we suppress it if it is clear from context. It can be shown (see the above references) that there is a one-to-one correspondence between the cyclotomic cosets X_g and the primitive idempotents of $\mathbf{F}[G]$. The characters in the cyclotomic coset corresponding to a primitive idempotent are called the *non-roots* of the idempotent. In particular, χ_0 is the only non-root of $\frac{1}{n}\underline{h}$. In general, the set of non-roots of an ideal is the union of the non-roots of the minimal ideals contained in the ideal. The following lemma will be used in section 4 and illustrates the usefulness of the above concepts.

Lemma 2.4. *Let $\underline{f}$ be a primitive idempotent for $\mathbf{F}[G]$ such that $\underline{f} \neq \frac{1}{n}\underline{h}$. Let $q = |\mathbf{F}\ |$ and suppose that q has odd order mod every prime r which divides n. Then $\underline{f} \neq \underline{f}\mu_{-1}$.*

Proof: Let the non-roots of $\underline{f}$ be the characters of X_g. Since $\underline{f} \neq \frac{1}{n}\underline{h}$, $g \neq 0$. The set of non-roots of $\underline{f}\mu_{-1}$ is X_{-g}. It suffices then to show that $\mathrm{X}_g \neq \mathrm{X}_{-g}$.

Let r be a prime dividing n. Since q has odd order mod r, it has odd order mod any power of r. The size of a cyclotomic coset must divide the least common multiple of all orders of q mod each prime power which is the order of a cyclic subgroup of G. In particular, the length of each cyclotomic coset is odd. If $\mathrm{X}_g = \mathrm{X}_{-g}$, then the length of X_g would be even. The result is then shown.

♣◇

Ex. 2-1: We illustrate the above concepts when G is the cyclic group $\mathbb{Z}_{31}$ and $\mathbf{F}$ is the binary field GF(2). These are the nonzero cyclotomic cosets:

$$\begin{aligned}
\mathrm{C}_1 &= \{1, 2, 4, 6, 16\} \\
\mathrm{C}_3 &= \{3, 6, 12, 24, 17\} \\
\mathrm{C}_9 &= \{9, 18, 5, 10, 20\} \\
\mathrm{C}_{27} &= \{27, 24, 15, 30, 29\} \\
\mathrm{C}_{19} &= \{19, 7, 14, 28, 25\} \\
\mathrm{C}_{26} &= \{26, 21, 11, 22, 13\}.
\end{aligned}$$

Each of these cyclotomic cosets supports an idempotent. By Lemma 2.3, any idempotent of $\mathbf{F}[G]$ is a sum of some of these 6 idempotents and $\underline{1}$. There are then 128 ideals of $\mathbf{F}[G]$. This shows that there must be 7 primitive idempotents. There is one minimal ideal of dimension 1, namely H, and 6 of dimension 5. The latter follows from looking at the automorphism μ_3. That is, any nontrivial sum of idempotents from cyclotomic cosets has six images from action by powers of μ_3; in particular, all *minimal ideals must have the same dimension and the sum of these dimensions is* 30. Calculation shows that one of these minimal ideals is generated by the primitive idempotent

$$\underline{1} + \mathrm{C}_1(x) + \mathrm{C}_9(x) + \mathrm{C}_{27}(x)\,.$$

All minimal ideals are then found by images of this one under μ_3.

♣◇

3. Definition of Generalized Q-Codes

Definition: Let $\underline{e}_1$ and $\underline{e}_2$ be two idempotents of $\mathbf{F}[G]$ and $\mu \in \mathrm{Aut}(G)$ such that *the following two equations are satisfied:*

$$\underline{e}_2 = \underline{e}_1\,\mu \tag{3a}$$

$$\underline{e}_1 + \underline{e}_2 - \underline{1} = \frac{1}{n}\underline{h}\,. \tag{3b}$$

Then the four codes,

$$\begin{aligned} C_1 &= \langle \underline{e}_1 \rangle\,, & C_1' &= \langle \underline{1} - \underline{e}_2 \rangle\,, \\ C_2 &= \langle \underline{e}_2 \rangle\,, \quad \text{and} & C_2' &= \langle \underline{1} - \underline{e}_1 \rangle\,, \end{aligned}$$

are the *generalized Q-codes* defined by $\underline{e}_1$, $\underline{e}_2$, and μ.

When $\mathbf{F}$ is the binary field, these are the duadic codes of [L,M,&Pl] and [Pl,M,&L]. When $\mathbf{F}$ is GF(4), these are the Q-codes of [Pl2]. For simplicity we speak of Q-codes and drop the qualifier "generalized." We stay as consistent as possible with the notation of these references. A set of four Q-codes is called a *quartet.* The automorphism μ is called a *splitter* and we say that μ gives the *splitting.* The facts stated in section 2 give the following fundamental theorem about Q-codes; the results and proofs are analogous to those given in [Pl2].

Theorem 3.1. *Let* $\underline{e}_1$ *and* $\underline{e}_2$ *be two odd-like idempotents of* $\mathbf{F}[G]$ *and* $\mu \in \mathrm{Aut}(G)$ *which together generate Q-codes. Then, for* $i = 1, 2$,

a). $C_1 \sim C_2$ and $C_1' \sim C_2'$

b). $C_1 \cap C_2 = H$ and $C_1 + C_2 = \mathbf{F}[G]$

b′). $C_1' \cap C_2' = \mathbf{0}$ and $C_1' + C_2' = E$

c). $dim(C_i) = \frac{n+1}{2}$ and $\dim(C_i') = \frac{n-1}{2}$

d). C_i' *is the even-like subcode of* C_i and $C_i = H \oplus C_i'$

e). $C_1^* \sim C_2^*$ and $\dim(C_i^*) = \frac{n+1}{2}$

f). If δ_o *is the minimum odd-like weight of* C_1, *then* $\delta_o^2 \geq n$.

Proof: From $C_2 = C_1 \mu$ and remarks in section 2, a) is clear . Multiply (3*b*) by $\underline{e}_2$ to conclude that $\underline{e}_2 \, \underline{e}_1 = \frac{1}{n} \underline{h}$. We then have that $\underline{e}_1 + \underline{e}_2 - \underline{e}_1 \, \underline{e}_2 - \underline{1}$. These calculations show b). A similar calculation shows b′). Let k be the dimension of C_1 and so also of C_2. From elementary linear algebra and b),

$$\begin{aligned} \dim(\mathbf{F}[G]) &= \dim(C_1) + \dim(C_2) - \dim(C_1 \cap C_2) \\ \text{or} \qquad\qquad n &= k + k - 1 \, . \end{aligned}$$

This shows the first half of c). The second half is similar working from b′) or from Lemma 2.1. Notice that C_i' is even-like ($i = 1, 2$), and by the respective dimensions, C_i' must be the even-like sub-code of C_i. Computing the idempotent for $H + C_i'$ and the fact that $\underline{h}$ is odd-like shows the rest of d). From d) we see that $C_i^* = H^* \oplus C_i'^*$. This shows that the dimension of C_i^* is $\frac{n+1}{2}$. The equivalence follows from the fact that since C_i' is even-like, the codewords of $C_i'^*$ are just the codewords of C_i' preceded by a zero. Hence the permutation which leaves the first coordinate fixed and is induced by the action of μ on the last n coordinates is seen to be a permutation which shows that $C_1^* \sim C_2^*$. Finally, let $a(x)$ be an odd-like codeword of C_1 of weight δ_o. Then $b(x) = a(x)\mu \in C_2$ and also has weight δ_o. Since $a(x)b(x) \in C_1 \cap \mathrm{C}_2 = H$, we see that $a(x)b(x) = \alpha\underline{h}$ for some $\alpha \in \mathbf{F}$. Since $a(1)b(1) \neq 0$, $\alpha \neq 0$. In particular, the n nonzero coordinates of $\alpha\underline{h}$ must come from the δ_o^2 nonzero cross products in $a(x)b(x)$. This shows that $\delta_o^2 \geq n$. The proof is then completed.

♡♠

In the next section we give some more interesting results on the structure of these codes. We first finish with some examples to illustrate the definitions. All of these examples were previously known; new ones appear in later sections.

Ex. 3-1: This is in [Pl2]. Let $G = \mathbb{Z}_3 = \{0,1,2\}$. Let $\mathbf{F} = \mathrm{GF}(4)$, defined as $\{0,1,\omega,\omega^2\}$, where $\omega^2+\omega+1 = 0$. We wish to determine all possible Q-codes by finding all possible odd-like idempotents and automorphisms satisfying $(3a)$ and $(3b)$. By brute force,

$$\underline{e}_1 = \alpha_0\underline{1} + \alpha_1 x^1 + \alpha_2 x^2 \qquad \text{and} \qquad \underline{e}_2 = \beta_0\underline{1} + \beta_1 x^1 + \beta_2 x^2 ,$$

where all of the coefficients are in $\mathbf{F}$. Since $\underline{e}_1^2 = \underline{e}_1$,

$$\alpha_0 = 0 \text{ or } 1 \qquad \text{and} \qquad \alpha_2 = \alpha_1 .$$

From (3*b*) we see that

$$\alpha_0 = \beta_0, \ \alpha_1 = 1 + \beta_1, \text{ and } \alpha_2 = 1 + \beta_2 .$$

The only nontrivial automorphism of G is $\mu_2 = \mu_{-1}$. Therefore, we may assume that μ_{-1} gives the splitting. This implies that

$$\alpha_1 = \beta_2 \qquad \text{and} \qquad \alpha_2 = \beta_1 .$$

We conclude that

$$\underline{e}_1 \ = \omega x^1 + \omega^2 x^2 \qquad \text{and} \qquad \underline{e}_2 \ = \omega^2 x^1 + \omega x^2 .$$

Notice that C_1 is a two dimensional code which must then have minimum weight at least 2. Hence the minimum weight is 2, and so this code is MDS. We will see that many Q-codes of small length are MDS.

♣◇

Ex. 3-2: We continue with Ex. 2-1. Again we construct all possible binary Q-codes of length 31 (the duadic codes of [L,M,&PL]). That is, we search for automorphisms μ of $\mathbb{Z}_{31}$ and idempotents $\underline{e}_1$ and $\underline{e}_2$ which satisfy (3*a*) and (3*b*). Since the coefficients are 0's and 1's, and since the weight of $\underline{e}_1$ must be the same as $\underline{e}_2$, we see that $\underline{e}_1$ and $\underline{e}_2$ must each have weight 15. From Lemma 2.3 and the calculations in Ex. 1-1, the support of $\underline{e}_1$ is then the union of three cyclotomic cosets, each of which has size 5. Let C_1 be one of these cyclotomic cosets for $\underline{e}_1$. $\mathrm{Aut}(\mathbb{Z}_{31})$ is cyclic of order 30 generated by μ_3. When considered as acting on the 6 nonzero cyclotomic cosets, μ_3 becomes a permutation of order 6 with cycle structure

$$(C_1, C_3, C_9, C_{27}, C_{19}, C_{26})\,.$$

By testing the 10 $(=\binom{5}{2})$ possibilities for $\underline{e}_1$, we arrive at the following four sets which support idempotents of Q-codes:

$$C_1 \cup C_2 \cup C_3,\ C_1 \cup C_2 \cup C_6,\ C_1 \cup C_3 \cup C_5, \text{ and } C_1 \cup C_5 \cup C_6\,.$$

In every case the splitting is given by $\mu_3^3 = \mu_{27} = \mu_{-1}$. Considering the idempotent $\underline{e}_2$ associated by $(3a)$ with each of these $\underline{e}_1$'s, we get the 8 duadic codes of length 31 mentioned in [L,M,&Pl]. The third one listed is the quadratic residue code; the other three are Reed-Muller codes. By Theorem 3.1, the dimension of each of these is 16.

♣◇

Ex. 3-3: *Generalized Quadratic Residue Codes*

We show that the generalized quadratic residue codes of [vL&MW] are Q-codes.

Let r be a prime power and G the additive group of $\mathrm{GF}(r)$. As always, $\mathbf{F}$ is the finite field $\mathrm{GF}(q)$ with q and r relatively prime. We further assume that r and q are both odd. The former restriction is to avoid degeneracy, while the latter restriction will be handled as a special case later on in this chapter. Let S be the set of nonzero squares in G and N be the set of nonzero squares. Then, in particular,

$$\underline{h} = \underline{1} + S(x) + N(x)\,.$$

The generalized quadratic residue codes in [vL&MW] are the four codes whose non-roots are the characters indexed by the sets S,N,$\{0\} \cup S$, and $\{0\} \cup N$. When r is a prime and $\mathbf{F}$ has prime order, these are the quadratic residue codes (see [MW&Sl]), which are cyclic.

We define G-codes which are fixed by μ_ℓ where $\ell \in S$. Here we mean by μ_ℓ the automorphism which sends $g \in G$ to ℓg, where the multiplication takes place in GF(r). This is the same as the μ_ℓ of section 2 if r is a prime. Using the same reasoning as Lemma 2.3, any idempotent of such a code must be a linear sum of $\underline{1}$, $S(x)$, and $N(x)$. Therefore we construct Q-codes whose idempotents are such linear sums. The splitting for any such code will be given by μ_ℓ where ℓ is now any nonzero nonsquare of G. Comparing the idempotents constructed with the idempotents for the codes in [vL&MW], we see that generalized quadratic residue codes are Q-codes.

We need to break the problem into two similar cases.

Case 1: $r \equiv 3 \pmod 4$

Let $\nu = \frac{r+1}{4}$ and $\lambda = \nu - 1$. We record the following computations, proofs of which can be found, for example, in the problems in [La]:

$$\begin{aligned} S(x)S(x) &= \lambda S(x) + \nu N(x) \\ N(x)S(x) = S(x)N(x) &= \nu \underline{1} + \lambda \underline{h} \\ N(x)N(x) &= \nu S(x) + \lambda N(x)\,. \end{aligned}$$

(The middle computation shows that the squares in G form an $(r, \frac{r-1}{2}, \lambda)$ difference set.) Suppose then that $\underline{e}_1$ is given by

$$\underline{e}_1 = \alpha\underline{1} + \beta S(x) + \gamma N(x)\,, \tag{3c}$$

so that

$$\underline{e}_2 = \alpha\underline{1} + \gamma S(x) + \beta N(x)\,. \tag{3d}$$

From (3b) it is immediate that

$$2\alpha - 1 = \frac{1}{r} \qquad \text{and} \qquad \beta + \gamma = \frac{1}{r}\,. \tag{3e}$$

Therefore $\alpha = \frac{r+1}{2r}$. From the fact that $\underline{e}_1$ is an idempotent we have the following sequence of equations:

$$\begin{aligned} \alpha\underline{1} + \beta S(x) + \gamma N(x) &= \big(\alpha\underline{1} + \beta S(x) + \gamma N(x)\big)^2 \\ &= \alpha^2\underline{1} + \beta^2\big(\lambda S(x) + \nu N(x)\big) + \gamma^2\big(\lambda N(x) + \nu S(x)\big) \\ &\quad + 2\alpha\beta S(x) + 2\alpha\gamma N(x) + 2\beta\gamma\big(\nu\underline{1} + \lambda\underline{h}\big) \\ &= \big(\alpha^2 + 2(2\nu - 1)\beta\gamma\big)\underline{1} \\ &\quad + \big(2\alpha\beta + \nu(\beta + \gamma)^2 - \beta(2\gamma + \beta)\big)S(x) \\ &\quad + \big(2\alpha\gamma + \nu(\beta + \gamma)^2 - \gamma(2\beta + \gamma)\big)N(x)\,. \end{aligned}$$

Comparing the first coordinates and using the first half of $(3e)$, we have

$$\beta\gamma = \frac{r+1}{4r^2}\,. \tag{3f}$$

Now $(3f)$ and the second half of $(3e)$ imply that

$$\{\beta,\gamma\} = \left\{\frac{1+\sqrt{-r}}{2r}, \frac{1-\sqrt{-r}}{2r}\right\}. \tag{3g}$$

Hence we need that $-r$ is a square in $\mathbf{F}$. Conversely, if $-r$ is a square in $\mathbf{F}$, then all of the above calculations are valid and the resulting quantities α, β, and γ make $\underline{e}_1$ and $\underline{e}_2$ idempotents for Q-codes. Notice that the resulting quartet is unique. Furthermore, a simple calculation shows that the idempotents are odd-like.

Case 2: $r \equiv 1 \pmod 4$

Let $\nu = \frac{r-1}{4}$ and $\lambda = \nu - 1$. We record the following analogous computations, which again can be derived from [La]:

$$\begin{aligned} S(x)S(x) &= 2\nu\underline{1} + \lambda S(x) + \nu N(x) \\ N(x)S(x) = S(x)N(x) &= \nu S(x) + \nu N(x) \\ N(x)N(x) &= 2\nu\underline{1} + \nu S(x) + \lambda N(x)\,. \end{aligned}$$

Define $\underline{e}_1$ and $\underline{e}_2$ by $(3c)$ and $(3d)$. Rather than repeat the same details, we just state the results:

$$\alpha = \frac{r+1}{2r} \tag{3h}$$

$$\{\beta,\gamma\} = \left\{\frac{1+\sqrt{r}}{2r}, \frac{1-\sqrt{r}}{2r}\right\}. \tag{3i}$$

Hence the Q-codes exist iff r is a square in $\mathbf{F}$.

As an illustration, let $r = 5$ and $\mathbf{F}$ be of characteristic 3. Since $r \equiv 1 \pmod 4$, we need that $5 \equiv 2$ is a square in $\mathbf{F}$. Hence we cannot take $\mathbf{F}$ to be GF(3); the smallest $\mathbf{F}$ of characteristic 3 which will work is GF(9). Let β and γ satisfy

$$y^2 + y - 1 = 0 .$$

Then β and γ are seen to be given by $(3g)$. Also, $\alpha = 0$ for this case, so that we can take

$$\underline{e}_1 = \beta x + \gamma x^2 + \gamma x^3 + \beta x^4 .$$

The weight distribution for the resulting code was computed and is

$$(1, 0, 0, 80, 240, 408) .$$

Notice that the resulting code is MDS.

♣◇

4. Q-Codes,Duality, and Projective Planes

We digress from the discussion on Q-codes to give some general definitions and results about G-codes. Let $\underline{a}, \underline{b} \in \mathbf{F}[G]$ with respective coefficients α_g and β_g, for $g \in G$.

Definition: The *ordinary inner product* or *dot product* of $\underline{a}$ and $\underline{b}$ is

$$(\underline{a}, \underline{b}) = \sum_{g \in G} \alpha_g \beta_g .$$

Let $q = r^2$ for some prime power r. Then the *unitary inner product* of $\underline{a}$ and $\underline{b}$ is

$$(\underline{a}, \underline{b})_{\mathrm{U}} = \sum_{g \in G} \alpha_g \beta_g^r .$$

It is straightforward to check that these satisfy all of the usual conditions for inner products. The *dual* of a code C with respect to some given inner product is the set of all codewords whose inner product is zero with every codeword of C. We denote the dual of C with respect to the dot product as $C^\perp$; with respect to the unitary inner product we use C^{U} for the dual of C. We say that C is $\perp$ *self-orthogonal* ($\perp$s.o.) if $C \leq C^\perp$ and that it is $\perp$ *self-dual* ($\perp$s.d.) if $C = C^\perp$. We have the analogous concepts of U *self-orthogonal* (Us.o.) and U *self-dual* (Us.d.). Notice that the former is called *strictly self-orthogonal*, etc., in [Pl] and the latter is simply called *self-orthogonal*, etc. We begin by describing the idempotents of these dual codes.

Lemma 4.1. *Let $\underline{a}$,$\underline{b} \in \mathbf{F}[G]$ be as above. Then*

$$\underline{a}\,\underline{b} = \sum_{g \in G} \left((\underline{a}x^g) \, , \, (\underline{b}\mu_{-1}) \right) x^g .$$

Proof: This follows from the definition of multiplication of two elements in $\mathbf{F}[G]$.

♣◇

Lemma 4.2. *Let $\underline{e}$ be an idempotent of $\mathbf{F}[G]$ and $C = \langle \underline{e} \rangle$.*

a). *The idempotent for $C^\perp$ is $\underline{1} - \underline{e}\mu_{-1}$.*

b). The idempotent for C^{U} is $\underline{1} - \underline{e}\mu_{-r}$, where $\mathbf{F}$ *is $GF(r^2)$.*

Remmark: Part a) can be found in [vL]; part b) is similar to the GF(4) case in [Pl2].

Proof of lemma: Since $\underline{e}(\underline{1}-\underline{e}) = \underline{0}$, we apply Lemma 4.1 to $\underline{e}$ and $\underline{1}-\underline{e}$ to conclude that $(\underline{1}-\underline{e})\mu_{-1} = \underline{1}-\underline{e}\mu_{-1}$ is orthogonal to all shifts of $\underline{e}$. Therefore $\underline{1}-\underline{e}\mu_{-1} \in C^{\perp}$. If k is the dimension of C, then by Lemma 2.1, $n-k$ is the dimension of $\langle \underline{1} - \underline{e} \rangle$. Hence the dimension of $\langle \underline{1} - \underline{e}\mu_{-1} \rangle$ is $n-k$, which shows that $C^{\perp} = \langle \underline{1} - \underline{e}\mu_{-1} \rangle$. This shows a).

For b), assume that $\mathbf{F}$ is GF(r^2). Notice that

$$\underline{a} \in C^{\mathrm{U}} \qquad \text{iff} \qquad \underline{a}_r = \sum_{g \in G} \alpha_g^r \in C^{\perp} .$$

Since $C^{\perp}$ is an ideal and raising elements of $\mathbf{F}[G]$ to the rth power is an automorphism of $\mathbf{F}[G]$, we have

$$\underline{a}_r \in \mathrm{C}^{\perp} \qquad \text{iff} \qquad \underline{a}_r^r \in \mathrm{C}^{\perp} .$$

But $\underline{a}_r^r = \underline{a}\mu_r$. In particular, the idempotent $\underline{1}-\underline{e}\mu_{-r} \in C^{\mathrm{U}}$. Comparing dimensions finishes the proof.

♣◇

As an application, we have the following three theorems and corollary. Their statements and proofs are analogous to those in [Pl,M,&L] and [Pl2]. For the remainder of the section, $\underline{e}_1$ and $\underline{e}_2$ are odd-like idempotents generating Q-codes.

Theorem 4.3.

a). *These are equivalent.*

1). μ_{-1} *gives the splitting.*

2). $C_i = C_i'^{\perp}$ *for* $i = 1, 2$.

3). C_i^* *is* $\perp$*s.d.*

b). μ_{-1} *is a multiplier for* C_1 *iff* $C_1^* = C_2^{*\perp}$.

Proof: Observe that from Lemma 4.2, μ_{-1} gives the splitting iff $\underline{e}_2 = \underline{e}_1\mu_{-1}$ iff $\underline{1} + \underline{e}_2 = \underline{1} + \underline{e}_1\mu_{-1}$ iff $C_1' = C_1^{\perp}$. This shows that 1) and 2) are equivalent. Fix $i = 1, 2$. From Theorem 3.1, $C_i = H + C_i'$ and C_i' is even-like. If C_i^* is $\perp$s.d., then these facts show that $C_i' \leq C_i^{\perp}$. Comparing dimensions shows that $C_i' = C_i^{-}$. Conversely, if $C_i' = C_i^{\perp}$, then the same reasoning shows shows that C_i^* is $\perp$s.o., and comparing dimensions shows that it is $\perp$s.d. Therefore 2) is equivalent 3), which completes a).

For b), $C_1\mu_{-1} = C_1$ iff $\underline{1} + \underline{e}_1 = \underline{1} + \underline{e}_1\mu_{-1}$ iff $C_2' = C_1^{\perp}$. Working again from the facts that $C_i = H + C_i'$ and C_i' is even-like, we see that $C_2' = C_1^{-}$ iff $C_1^* = C_2^{*\perp}$.

♡♠

Theorem 4.4. *Let* $\mathbf{F}$ *be* $GF(r^2)$.

a). *These are equivalent.*

1). μ_{-r} *gives the splitting.*

2). $C_i = C_i'^{\mathrm{U}}$ *for* $i = 1, 2$.

3). C_i^* *is* U*s.d.*

b). μ_{-r} *is a multiplier for* C_1 *iff* $C_1^* = C_2^{*\,\mathrm{U}}$.

Proof: The proof is completely analogous to Theorem 3.4 using the other half of Lemma 4.2.

♡♠

It is clear that the existence of self-dual codes with respect to any inner product requires that the dimension of $\mathbf{F}[G]$ be even, which is contrary to our assumption about the order of G. Notice that it is the extended codes which are sometime self-dual. Instead, we introduce a concept of a code which is as "self-dual" as possible. We say that a code C is $\perp$ *almost self-orthogonal* ($\perp$a.s.o.) if $C \leq H + C^{\perp}$. If equality holds, C is said to be $\perp$ *almost self-dual* ($\perp$a.s.d.). The similar concepts for the unitary product can, of course, be defined, but we will have no special use for them.

Corollary 4.5. C_1 *and* C_2 *are* $\perp$*a.s.d. iff* μ_{-1} *gives the splitting.*

Proof: For $i = 1, 2$, Theorem 4.3 says that μ_{-1} gives the splitting iff $C_i = C_i'^{\perp}$ iff $C_i^{\perp} = C_i'$. But Theorem 3.1 says that $C_i = H + C_i'$, and the result quickly follows.

♡♠

The converse of Corollary 4.5 is also true, which records as the following.

Theorem 4.6. *Let* C *be an* $\perp$*a.s.d. of* $\mathbf{F}[G]$. *Then* C *is a Q-code with the splitting given by* μ_{-1}.

Proof: Let $\underline{e}$ be the idempotent for C. By hypothesis,

$$C = H + C^{\perp}.$$

From the facts of section 2 and Lemma 4.2,

$$\underline{e} = \frac{1}{n}\underline{h} + (\underline{1} - \underline{e}\mu_{-1}) - \frac{1}{n}\underline{h}\,(\underline{1} - \underline{e}\mu_{-1}). \tag{4a}$$

Now $\frac{1}{n}\underline{h}\,(\underline{1} - \underline{e}\mu_{-1}) = \frac{1}{n}\underline{h}$ or $\underline{0}$. If the former, then $\underline{e}$ is even-like, which means that C is even-like. Therefore, $\underline{h} \in C^{\perp}$. But this implies that $C = C^{\perp}$, which is a contradiction. Therefore $\underline{e}$ is odd-like, and so from $(4a)$,

$$\underline{e} + \underline{e}\mu_{-1} - \underline{1} = \frac{1}{n}\underline{h}.$$

Hence C is a Q-code.

♡♠

From these two results we see that $\perp$ almost self-dual codes are precisely Q-codes where μ_{-1} gives the splitting, and so their extensions are self-dual. In section 6, we will develop techniques to construct such codes when $\mathbf{F}$ has characteristic 2. The next result is a non-constructive existence theorem for these codes. It is analogous to the GF(4) case of [Pl2].

Theorem 4.7. *There exists a G-code which is $\perp$a.s.d. iff for every prime r which divides n, the order of q mod r is odd. If this occurs, then if D is an $\perp$a.s.o. code of $\mathbf{F}[G]$, there is an $\perp$a.s.d. code C of $\mathbf{F}[G]$ such that $D \leq C$.*

Proof: $\Longrightarrow$ Let C be a $\perp$a.s.d. code in $\mathbf{F}[G]$. By Theorem 4.6, C is a Q-code with splitter μ_{-1}. Let $\underline{e}_1$ and $\underline{e}_2$ be the idempotents generating the quartet of Q-codes. Suppose that there exists a prime r dividing n such that the order of q mod r is even. We derive a contradiction, which shows the result.

Let R be a subgroup of G of order r, and let ρ be the canonical homomorphism from G to R. We claim that there are Q-codes in $\mathbf{F}[R]$ with splitting given by μ_{-1} and idempotents $\underline{e}_1\rho$ and $\underline{e}_2\rho$. Since $\underline{e}_1\rho = \underline{e}_1^2\rho = (\underline{e}_1\rho)^2$, we see that $\underline{e}_1\rho$ and $\underline{e}_2\rho$ are idempotents. Since $(-g)\rho = -(g\rho)$ for $g \in G$, we see that $(\underline{e}_1\rho)\mu_{-1} = (\underline{e}_1\mu_{-1})\rho = \underline{e}_2\rho$. Finally, applying ρ to eqaution $(3b)$, we see

$$\underline{e}_1\rho + \underline{e}_2\rho - \underline{1} \;=\; \frac{1}{n}\,\frac{|G|}{|R|}\,R(x) \;=\; \frac{1}{|R|}\,R(x)\,.$$

Hence $\underline{e}_1\rho$ and $\underline{e}_2\rho$ generate Q-codes in $\mathbf{F}[R]$ with splitter μ_{-1}. By Lemma 2.2, μ_q is a multiplier of these codes. By assumption, the order of q mod r is even. In particular, some power of q is congruent to -1 mod r. But this says that μ_{-1} is a multiplier for these Q-codes, which is a contradiction.

$\Longleftarrow$ By Lemma 2.4, we can find an indexing set $\Im$ such that the set of primitive idempotents of $\mathbf{F}[G]$ is

$$\{\frac{1}{n}\underline{h}\} \cup \{\underline{f}_i, \underline{f}_i\mu_{-1}\}_{i\in\Im}\,.$$

Define the idempotents

$$\underline{e}_1 \;=\; \frac{1}{n}\underline{h} + \sum_{i\in\Im}\underline{f}_i \qquad \text{and} \qquad \frac{1}{n}\underline{h} + \sum_{i\in\Im}\underline{f}_i\mu_{-1}\,.$$

Clearly $\underline{e}_2 = \underline{e}_1 \mu_{-1}$. Furthermore,

$$\underline{e}_1 + \underline{e}_2 - \underline{1} \; = \; \left(\sum_{i \in \Im} (\underline{f}_i + \underline{f}_i \mu_{-1}) + \frac{1}{n} \underline{h} \right) - \underline{1} + \frac{1}{n} \underline{h} \; = \; \frac{1}{n} \underline{h} .$$

Therefore we have constructed Q-codes in $\mathbf{F}[G]$ with splitting given by μ_{-1}. By Corollary 4.5, these codes are $\perp$a.s.d.

Let D be an $\perp$a.s.o. code in $\mathbf{F}[G]$ and assume the hypotheses of the above result. Using the notation of the above proof, suppose that $\underline{f}_i \neq \frac{1}{n} \underline{h}$ is in D. Suppose that $\underline{f}_i \mu_{-1}$ is in D. Then

$$\underline{f}_i \; = \; \underline{f}_i^2 \; = \; \sum_{g \in G} (\underline{f}_i x^g \, , \underline{f}_i \mu_{-1}) \; = \; 0 ,$$

since D is $\perp$a.s.o. This contradiction shows that for any $i \in \Im$, at most one of the pair $\{\underline{f}_i, \underline{f}_i \mu_{-1}\}$ is in D. Out of each unrepresented pair, pick one primitive idempotent and add it to the idempotent of D. In this manner one, one splits the primitive idempotents into two halves, and each half generates a Q-code as in the above proof. One of these Q-codes contains D. This completes the proof.

♡♠

The above results seem to indicate the importance of μ_{-1} as a splitter for Q-codes. The rest of this section is devoted to a special subset of such codes, namely those where the supports of the minimum weight vectors form a projective plane with regular automorphism group G. We first give sufficient conditions for this to happen, and follow with a converse of sorts. As in Theorem 3.1, let $\delta_\circ$ denote the minimum weight of odd-like codewords in C_1. This next result and proof are analogous to those given in [L,M,&Pl] when $\mathbf{F}$ is binary and in [Pl2] when $\mathbf{F}$ is GF(4).

Theorem 4.8. *Suppose that μ_{-1} gives the splitting. Then*

$$\delta_\circ^2 - \delta_\circ + 1 \geq n\,.$$

If $n = \delta_\circ^2 - \delta_\circ + 1$, then the supports of the odd-like codewords of weight $\delta_\circ$ are the blocks of a projective plane of order $\delta_\circ - 1$. These codewords are precisely the elements of $\mathbf{F}$ multiplied by the characteristic functions of these blocks. Finally, $\delta_{C_1} = \delta_\circ$.

Remark: Notice that the inequality is slightly stronger than the one in Theorem 3.1, part f).

Proof of theorem: Let $b(x)$ be an odd-like codeword in C_1 of weight $\delta_\circ$. Let $B \subseteq G$ be the set of the nonzero coordinates of $b(x)$ and let these coordinates be β_g for $g \in B$. Set $\tilde{b}(x) = b(x)\mu_{-1}$. From the proof of Theorem 3.1, there is some $\alpha \neq 0$ with

$$\begin{aligned} \alpha \underline{h} &= b(x)\tilde{b}(x) \\ &= \left(\sum_{g\in B} \beta_g^2\right)\underline{1} + \sum_{\substack{g,k\in B\\ g\neq k}} \beta_g\beta_k\, x^{g-k}\,. \end{aligned} \tag{4b}$$

Therefore

$$1 + \delta_\circ(\delta_\circ - 1) \geq n\,, \tag{4c}$$

which is the result.

Now assume that we have equality. From the equation

$$(\delta_\circ - 1)^2 + (\delta_\circ - 1) + 1 \; = \; n\,,$$

we see that the projective plane would have order $\delta_\circ - 1$. We first show that the n shifts of $b(x)$ support the blocks of such a plane. It suffices to show that for $g \neq k \in G$, there is exactly one shift of $b(x)$ with a nonzero coefficient for x^g and x^k. But this is clear from $(4b)$ and the fact that we have equality in $(4c)$. Furthermore, for $g, k, l \in B$, we have from $(4b)$ that

$$\beta_g\beta_k \; = \; \beta_g\beta_l \; = \; \beta_k\beta_l\,.$$

This says that $b(x)$ is a scalar multiple of $B(x)$.

Let $a(x)$ be another odd-like codeword of C_1 with weight $\delta_\circ$ and supporting set A. By Theorem 4.3, C_1^* is $\perp$s.d., so that the extended codewords for $a(x)$ and $b(x)$ are orthogonal. This means that $A \cap B$ has size at least one. In fact, the same is true for every shift of $b(x)$. In other words, A is a set in G of size $\delta_\circ$ which intersects every block of a projective plane in at least one point. It is well-known (see [La]) that this implies that A must be one of these blocks. The above reasoning then shows that $a(x)$ is a multiple of a shift of $b(x)$. In this way, we have completely characterized the minimum weight codewords of C_1.

Finally, let $c(x)$ be any nonzero even-like codeword of C_1. We show that the weight of $c(x)$ is greater than or equal to δ_o. This would complete the theorem. Again C_1^* is $\perp$s.d., so that $c(x)$ is orthogonal to every shift of $b(x)$. Let $c(x)$ be nonzero in the k_0 spot, and let $B_1, \ldots, B_{\delta_o}$ be the δ_o blocks of the projective plane which contain k_0. By the _ self-duality, the support of $c(x)$ must have at least two coordinates in common with each of these B_j, where one of these is k_0. None of these other coordinates can be shared in commmon between the B_j's since they are blocks of a projective plane. Therefore the support of $c(x)$ has size at least $1 + \delta_o$, which is what was to be shown.

♡♠

Theorem 4.9. *Let p be a prime and G be an abelian group of order $n = p^{2s} + p^s + 1$. Suppose that there exists a projective plane P with regular automorphism group G. Let $s = 2^r s'$ where s' is odd and set $q = p^{2^r}$. Let $\mathbf{F} = \mathrm{GF}(q)$. Then the points of P can be considered to be elements of G and the blocks of P to be the minimum weight codewords of a Q-code in $\mathbf{F}[G]$ with μ_{-1} giving the splitting.*

Proof: Let $\nu = p^s$. Then the parameters of P are $(\nu^2 + \nu + 1, \nu + 1, 1)$. From the theory of difference sets ([La]), we can take the points of P to be the elements of G and the blocks of P to be all shifts of one block $B \subseteq G$.

We define the code D to be the ideal generated by all shifts of $\underline{h} - B(x)$ in $\mathbf{F}[G]$. The support of one of these shifts has size ν^2 and two such shifts have $\nu^2 - \nu$ nonzero coordinates in common. In particular, D is $\perp$ self-orthogonal. Trivially then it must be $\perp$a.s.o.

Let π be any prime dividing n and set t to be the order of p mod π. Let $d = \gcd(t, 2^r)$. Then the order of q mod π is $\frac{t}{d}$. We show that this is odd. Multiply the congruence

$$p^{2s} + p^s + 1 \equiv 0 \pmod{\pi}$$

by $p - 1$ to conclude that

$$p^{3s} \equiv 1 \pmod{\pi}.$$

Hence, $t \mid 3s$ and we must then have that $\frac{t}{d}$ is odd.

We are now in the position to apply Theorem 4.7 to conclude that there is an $\perp$a.s.d. C which contains D. By Theorem 4.6, C is a Q-code with μ_{-1} giving the splitting. From the fact that $\underline{h} \in C$, we see that all of the shifts of $B(x)$ are in C. By Theorem 4.8, we see that these shifts and their scalar multiples are the minimum weight codewords of C.

♡♠

Theorem 4.8 shows how to recognize when the minimum weight codewords of certain Q-codes form a projective plane, while Theorem 4.9 says that every *known* projective plane which comes from an abelian difference set must lie in such a Q-code. Suppose that the characteristic of $\mathbf{F}$ is 2 and that G is cyclic. If s is odd, then $r = 0$ and by Theorem 4.9 we can take $\mathbf{F}$ to be the binary field ($q = 2$). This is in [P11]. If s is exactly divisible by 2, then $q = 2^2 = 4$, and so we can take $\mathbf{F}$ to be GF(4). This is in [P12]. In general, we may get by with a smaller value of q than the one of the theorem. However, Ex. 4-3 will give an example when q so defined is necessary.

Ex. 4-1: The smallest example is the cyclic plane of order 2. G is the group $\mathbb{Z}_7$ and by Theorem 4.9, $\mathbf{F}$ is the binary field GF(2). There are two nonzero cyclotomic cosets, namely

$$\mathrm{C}_1 = \{1,2,4\} \qquad \text{and} \qquad \mathrm{C}_3 = \{3,6,5\}\,.$$

Inspection shows that the the quartet of Q-codes has $\underline{e}_1 = \mathrm{C}_1(x)$ and $\underline{e}_2 = \mathrm{C}_3(x)$. The splitting is given by $\mu_{-1} = \mu_6$. This is the (7,3) Hamming code.

♣◇

Ex. 4-2: *This next example concerns the projective plane of order 3. Here we* have $G = \mathbb{Z}_{13}$ and $\mathbf{F}$ the ternary field GF(3). The nonzero elements of G split up into 4 cyclotomic cosets:

$$\{1,3,9\}, \quad \{2,6,5\}, \quad \{4,12,10\}, \quad \text{and} \quad \{8,11,7\}\,.$$

By looking at the multiplication table of the elements supported by these cosets, it is straightforward, but nontrivial, to find combinations which give idempotents. Using the fact that μ_{-1} must give the splitting, one can show that up to equivalence, there is only one choice for $\underline{e}_1$:

$$\underline{e}_1 \;=\; \underline{1} + \mathrm{C}_1(x) + 2\mathrm{C}_2(x) + 2\mathrm{C}_8(x)\,.$$

The weight distribution was calculated and is

$$(1,0,0,0,26,0,156,624,0,494,780,78,28)\,.$$

The supports of the 26 minimum weight codewords must be the blocks of the plane.

There is another way to find the above idempotent. From the theory of difference sets ([La]), the projective plane of order 3 has as its blocks the supports of the shifts of $\underline{1} + \mathrm{C}_1(x)$, and the square of this element must be the idempotent of the code which it spans. Computing,

$$\left(\underline{1} + \mathrm{C}_1(x)\right)^2 = \underline{1} + 2\mathrm{C}_1(x) + \mathrm{C}_2(x) + 2\mathrm{C}_4(x)\,.$$

The image of this idempotent under μ_8 is the $\underline{e}_1$ of above.

It turns out that, up to equivalence, there is only one other Q-code of length 13. This is the quadratic residue code (see Ex. 3.3) and the idempotent is calculated to be

$$\underline{e}_1 = \underline{1} + \mathrm{C}_1(x) + \mathrm{C}_4(x)\,.$$

The weight distribution was calculated to be

$$(1,0,0,0,0,78,182,286,390,520,442,234,26,28)\,.$$

♣◇

Ex. 4-3: Our last example is to show that there are projective planes with order a power of 2 which require **F** to be larger than GF(2) or GF(4); this shows that our results extend the results stated above from [Pl1] and [Pl2]. Let $\nu = 16$. Then $n = 16^2 + 16 + 1 = 273$. Factoring gives $n = 3 \cdot 7 \cdot 13$. We need **F** to be a field of order 2^r such that the order of 2^r is odd for each of these primes. Considering the prime 13 shows us that we need $r = 4$. Theorem 4.9 says that this would work, and so the cyclic plane of order 16 must lie in a Q-code where $G = \mathbb{Z}_{273}$ and $\mathbf{F}$ is GF(16). In section 6 we show how this Q-code perhaps is constructed; because of the sizes involved we have not done so.

♣◇

5. Existence for Characteristic 2

From the examples considered so far in this chapter, it is apparent that the construction of Q-codes when the characteristic of $\mathbf{F}$ is 2 is much easier than for odd characteristics. This is because it is simple to construct all idempotents from cyclotomic cosets. When $\mathbf{F}$ has characteristic 2, one can completely determine from elementary numerical conditions for which G Q-codes can exist. This is our goal. Observe that equation (3b) becomes

$$\underline{1} + \underline{e}_1 + \underline{e}_2 \;=\; \underline{h}\,. \qquad (5a)$$

For the remainder of the chapter, let $\mathbf{F}$ be the finite field GF(q), where $q = 2^m$. For every divisor l of m, we consider GF(2^l) to be a subfield of $\mathbf{F}$. Our only restriction on G now is that n is odd. We will always let p be an odd prime. The order of 2 mod p is denoted by t_p, or t, if p is clear from context.

The first lemma is a natural generalization of Lemma 2.3. We extend the notation of cyclotomic cosets by denoting the orbits of a given automorphism μ_ℓ, $\ell \in \mathbb{Z}$ by $\mathrm{C}_g^{(\ell)}$ for $g \in G$.

Lemma 5.1. *Let $\underline{e}$ be an idempotent of* $\mathbf{F}[G]$ *and* $\ell \in \mathbb{Z}$ *such that* μ_ℓ *is a multiplier of* $\langle \underline{e} \rangle$. *Let* $\Im$ *be a complete set of orbit representatives for* $G \setminus \{0\}$. *Then for some* $\beta_0, \beta_g \in \mathbf{F}$, $g \in \Im$,

$$\underline{e} \; = \; \beta_0 \underline{1} + \sum_{g \in \Im} \beta_g \mathrm{C}_g^{(\ell)}(x) \, . \tag{5b}$$

Proof: This is immediate from the fact that, for $g \in G$, x^g and $x^{\ell g}$ have the same coefficient in $\underline{e}$. Notice that we did not need the characteristic of $\mathbf{F}$ to be 2.

♣◇

The next lemma is a simple observation about cyclic codes of prime length.

Lemma 5.2. *Let* $G = \mathbb{Z}_p$ *and* $d = \gcd(m, t)$, *where* t *is the order of 2 mod* p *and* $\mathbf{F}$ *is* $GF(2^m)$. *Then the coefficients of any idempotent in* $\mathbf{F}[G]$ *are in* $GF(2^d)$. *In particular,* μ_{2^d} *is a multiplier of any code of* $\mathbf{F}[G]$.

Proof: Let $\underline{e}$ be an idempotent of $\mathbf{F}[G]$ with coefficients β_g for $g \in G$. By the calculation

$$\sum_{g \in G} \beta_g \, x^g \; = \; \left(\sum_{g \in G} \beta_g \, x^g \right)^2 \; = \; \sum_{g \in G} \beta_g^2 \, x^{2g} \, ,$$

we see that for all nonzero $g \in G$,

$$\beta_{2g} \; = \; \beta_g^2 \, . \tag{5c}$$

Fix nonzero $g \in G$. Repeating (5c) m times gives

$$\beta_{2^m g} \; = \; \beta_g^{2^m} \; = \; \beta_g \, . \tag{5d}$$

The last equality is just the fact that $\beta_g \in \mathbf{F}$; this is Lemmas 2.2 and 2.3. Repeating $(5c)$ t times gives

$$\beta_g^{2^t} = \beta_{2^t g} = \beta_g . \tag{5e}$$

The last equality holds since the order of 2 mod p is t. From $(5e)$ it follows that $\beta_g \in \mathrm{GF}(2^t)$. Therefore β_g is in the intersection of $\mathbf{F}$ and $\mathrm{GF}(2^t)$, which is $\mathrm{GF}(2^d)$. This shows the first conclusion. It is then immediate from this that μ_{2^d} is a multiplier of $\langle \underline{e} \rangle$.

♣◇

Now fix p, $G = \mathbb{Z}_p$, and set $d = \gcd(m, t)$, where, as always, t is the order of 2 mod p and $\mathbf{F}$ is $\mathrm{GF}(2^r)$. The following is the existence theorem for cyclic Q-codes of prime length.

Theorem 5.3. *There exist Q-codes in* $\mathbf{F}[G]$ *iff* $\frac{p-1}{t}d$ *is even.*

Proof: $\Longrightarrow$ Suppose that there are Q-codes in $\mathbf{F}[G]$. Then there exists idempotents $\underline{e}_1$ and $\underline{e}_2$ and $\mu \in \mathrm{Aut}(G)$ which satisfy $(3a)$ and $(3b)$. Notice that these equations also imply that $\underline{e}_1 = \underline{e}_1 \mu^2$. In particular, the order of μ must be even, since otherwise we would have $\underline{e}_1 = \underline{e}_2$.

Motivated by Lemma 5.2, let $\Im$ be a complete set of orbit representatives of μ_{2^d} on $G \setminus \{0\}$. Observe that the size of $\Im$ is $\frac{p-1}{t}d$. Pick $g \in \Im$ and look at the cycle of $\mathrm{C}_g^{(2^d)}$ under μ. We assert that the length of this cycle is even; this would complete the result. Now some power of μ is an involution, since μ has even order. If the length of the cycle is odd, then at least one of its orbits must be fixed by this involution. Since the characteristic is 2, the coefficients in $\underline{e}_1$ and $\underline{e}_2$ associated with this fixed orbit would cancel in equation $(5a)$. This is a contradiction, and so the result is shown.

$\Longleftarrow$ There are two cases.

Case 1: Let $\frac{p-1}{t}$ be even. Let U be the nonzero elements in G, S the set of squares in G (when G is considered as a field), and T the subgroup of U generated by 2. From the equation

$$t \cdot \frac{p-1}{t} = \frac{p-1}{2} \cdot 2 ,$$

it follows that $t \mid \frac{p-1}{2}$. Since U is cyclic, it then follows that $T \leq S$. That is, 2 is a square mod p. In particular, $S(x)$ is an idempotent. Let ℓ be any nonsquare, and set $\underline{e}_1 = S(x)$ and $\underline{e}_2 = \underline{e}_1\mu_\ell$. These produce Q-codes with splitting given by μ_ℓ.

Case 2: Let d be even. Then GF(4) is a subfield of GF(2^d). Let this subfield be generated by ω with $\omega^2 + \omega + 1 = 0$.

Let $s = \frac{p-1}{t}$ and pick elements $g_1, \ldots, g_s \in G$ such that the set

$$\left\{2^j g_i \ : \ i = 1, \ldots, s \quad j = 0, \ldots, d-1\right\}$$

is a complete set of orbit repesentatives for the orbits of μ_{2^d}. Form the elements

$$\underline{e}_1 = \sum_{i=1}^{s} \sum_{j=0}^{\frac{d}{2}-1} \left(\omega x^{2^{2j} g_i} + \omega^2 x^{2^{2j+1} g_i}\right) \mathrm{C}_1^{(2^d)}(x) ,$$

and

$$\underline{e}_2 = \sum_{i=1}^{s} \sum_{j=0}^{\frac{d}{2}-1} \left(\omega^2 x^{2^{2j} g_i} + \omega x^{2^{2j+1} g_i}\right) \mathrm{C}_1^{(2^d)}(x) .$$

It is straightforward to see that $\underline{e}_1$ and $\underline{e}_2$ are idempotents which satisfy $(5a)$ and that $\underline{e}_2 = \underline{e}_1\mu_2$. This completes the proof.

♡♠

Corollary 5.4. *If $\frac{p-1}{t}d$ is even, then we can always construct Q-codes in* $\mathbf{F}[G]$ *with idempotents whose coefficients are either binary or quaternary.*

Proof: This is immediate from the proof of Theorem 5.3.

♡♠

Corollary 5.5.

a). If m is odd, then Q-codes exist in $\mathbf{F}[G]$ *iff 2 is a square mod p iff $p \equiv \pm 1$* (mod 8).

b). If m is even, then Q-codes always exist in $\mathbf{F}[G]$.

Proof: If m is odd, then by Theorem 5.3, Q-codes exist iff $\frac{p-1}{t}$ is even. But from the proof of Theorem 5.3, $\frac{p-1}{t}$ is even iff 2 is a square mod p. The last statement is well-known from number theory.

Let m be even. If t is even, then d is even. If t is odd, then $\frac{p-1}{t}$ is even. In either case, $\frac{p-1}{t}d$ is even, so Q-codes exist.

♡♠

Suppose that G has prime order. Then Corollary 5.5 implies Theorem 2 of [L,M,&Pl] when $m = 1$ and it implies Corollary 1 of [Pl2] when $m = 2$. Indeed, we used precisely their constructions in our proof. In the next section, however, we will see different constructions for larger m, especially $m = 3$ and 4.

In order to classify all groups G for which Q-codes can exist, we need to know how existence for G relates to existence for subgroups of G. The next two results concern half of this, namely how one can piece together Q-codes from smaller groups.

Theorem 5.6. *Let K and L be two finite abelian groups of odd order such that Q-codes exist in $\mathbf{F}[K]$ and $\mathbf{F}[L]$. Let $G = K \oplus L$. Then there are Q-codes in $\mathbf{F}[G]$.*

Proof: By the hypothesis, let $\underline{u}_1$ and $\underline{u}_2$ be idempotents in $\mathbf{F}[K]$ which generate Q-codes and let the splitting be given by μ_K. Similarly, let idempotents $\underline{v}_1$ and $\underline{v}_2$ generate Q-codes in $\mathbf{F}[L]$ with splitter μ_L. We thus have the equations

$$\underline{1} + \underline{u}_1 + \underline{u}_2 = K(x) \qquad \text{and} \qquad \underline{u}_2 = \underline{u}_1\mu_K \,,$$

$$\underline{1} + \underline{v}_1 + \underline{v}_2 = L(x) \qquad \text{and} \qquad \underline{v}_2 = \underline{v}_1\mu_L \,.$$

Consider the natural imbedding of K and L into G. In particular, all of the above equations can be taken to be in $\mathbf{F}[G]$. For $g \in G$, g can be uniquely written as $g_K + g_L$ where $g_K \in K$ and $g_L \in L$. Then we define μ for $g \in G$ by

$$\mu : \qquad g \quad \longmapsto \quad g_K\mu_K + g_L\mu_L \,.$$

It is easy to see that $\mu \in \mathrm{Aut}(G)$. We define the elements

$$\underline{e}_1 \;=\; \underline{u}_1 + \underline{v}_1 + \underline{u}_1\underline{v}_1 + \underline{u}_1\underline{v}_2$$

and

$$\underline{e}_2 \;=\; \underline{u}_2 + \underline{v}_2 + \underline{u}_2\underline{v}_2 + \underline{u}_2\underline{v}_1 \,.$$

Then $\underline{e}_1$ and $\underline{e}_2$ are idempotents with $\underline{e}_2 = \underline{e}_1\mu$. Furthermore,

$$\underline{1} + \underline{e}_1 + \underline{e}_2 \;=\; (\underline{1} + \underline{u}_1 + \underline{u}_2)(\underline{1} + \underline{v}_1 + \underline{v}_2) \;=\; K(x)L(x) \;=\; G(x)\,.$$

Hence $\underline{e}_1$ and $\underline{e}_2$ generate Q-codes in $\mathbf{F}[G]$ with splitter μ.

♡♠

Theorem 5.7. *Suppose that there is a Q-code in $\mathbf{F}[\mathbb{Z}_p]$ with splitter μ_ℓ, $\ell \in \mathbb{Z}$. Then for any $s \geq 1$ and $G = \mathbb{Z}_{p^s}$, there is a Q-code in $\mathbf{F}[G]$ with splitter μ_ℓ.*

Proof: We proceed by induction on s; the hypothesis is the case $s = 1$. Let $G = \mathbb{Z}_{p^s}$ for $s > 1$. Let $P = \langle p^{s-1}\rangle$ and $K = \langle p\rangle$ be the subgroups of G with respective orders p and p^{s-1}. By the induction hypotheses, there are Q-codes in both $\mathbf{F}[P]$ and $\mathbf{F}[K]$ with splitting given by μ_ℓ. Let

$$\underline{u} \;=\; \sum_{i=0}^{p-1} \alpha_i x^{ip^{s-1}}$$

be an idempotent for a Q-code in $\mathbf{F}[P]$ and

$$\underline{v} \;=\; \sum_{j=0}^{p^{s-1}-1} \beta_j x^{jp}$$

be an idempotent for a Q-code in $\mathbf{F}[K]$, where both splittings are given by μ_ℓ. Let

$$\underline{e} \;=\; \left(\sum_{j=0}^{p^{s-1}-1} \beta_j x^{jp}\right) + \left(\sum_{i=1}^{p-1} \alpha_i\, x^i K(x)\right)\,.$$

Pick $g = i + jp \in G$ where $0 \leq i \leq p - 1$ and $0 \leq j \leq p^{s-1} - 1$. Let γ_g be the coefficient of x^g. If $i = 0$, then $\gamma_g = \beta_j$; if $i \neq 0$, then $\gamma_g = \alpha_i$. From this it follows that $\gamma_{2g} = \gamma_g^2$ and, if $g \neq 0$, $\gamma_g + \gamma_{\ell g} = 1$. It is immediate that $\underline{e}$ is an idempotent of $\mathbf{F}[G]$ and that $1 + \underline{e} + \underline{e}\mu_\ell = \underline{h}$. Therefore $\underline{e}$ generates the desired Q-code.

♡♠

Our next result shows how the existence of Q-codes in $\mathbf{F}[G]$ can sometimes imply the existence of Q-codes in the group ring $\mathbf{F}[K]$, where K is a subgroup of G.

Theorem 5.8. *Let $\underline{e}$ generate a Q-code in $\mathbf{F}[G]$ with splitting μ. Suppose that K is a subgroup of G which is invariant under μ. Then there are Q-codes in $\mathbf{F}[K]$ and $\mathbf{F}[G/K]$.*

Proof: Define the element $\underline{u} \in \mathbf{F}[K]$ by having the coefficient of x^k for $k \in K$ to be the same as in $\underline{e}$. It is easy to see that $\underline{u}$ is an idempotent, and if μ_K is the restriction of μ to K, then $1 + \underline{u} + \underline{u}\mu_K = K(x)$. This constructs the Q-code in $\mathbf{F}[K]$.

Let $L = G/K$ and set φ to be the canonical map from G to L with kernel K. Our reasoning is analogous to the proof of Theorem 4.7. Observe that $\underline{e}\varphi$ is an idempotent of $\mathbf{F}[L]$ since

$$\underline{e}\varphi \;=\; (\underline{e}^2)\varphi \;=\; (\underline{e}\varphi)^2 .$$

Furthermore, from $1 + \underline{e} + \underline{e}\mu = \underline{h}$ it follows that

$$1 + \underline{e}\varphi + (\underline{e}\mu)\varphi \;=\; |K| \cdot L(x) \;=\; L(x) .$$

As K is invariant under μ, μ induces an automorphism of L given by $g + K$ being mapped to $g\mu + K$. Call this automorphism ρ. Then

$$(\underline{e}\mu)\varphi = (\underline{e}\varphi)\rho .$$

In particular, $\underline{e}\varphi$ generates a Q-code in $\mathbf{F}[L]$ with the splitting given by ρ.

♡♠

Recall that a subgroup K of G is called *characteristic* if K is invariant under every automorphism of G. Hence Theorem 5.8 says that the existence of Q-codes in $\mathbf{F}[G]$ implies the existence of Q-codes in the group ring of any characteristic subgroup of G.

Corollary 5.9. *A Q-code exists in* $\mathbf{F}[G]$ *iff a Q-code exists in* $\mathbf{F}[K]$ *for every p-Sylow subgroup K of G.*

Proof: If there is a Q-code in $\mathbf{F}[G]$, then there is one in $\mathbf{F}[K]$ for any p-Sylow subgroup K of G since p-Sylow subgroups are characteristic subgroups of G. The converse follows from repeated application of Theorem 5.6.

♡♠

Corollary 5.10. *Let G be cyclic. Then there is a Q-code in* $\mathbf{F}[G]$ *iff for every prime p dividing n, $\frac{p-1}{t}d$ is even.*

Proof: For any prime p dividing n, there is a unique (and so characteristic) cyclic subgroup of order p. One direction of this result is then immediate from Theorems

5.8 and 5.3. The other direction follows from Theorem 5.3, and repeated application of Theorems 5.6 and 5.7.

♡♠

When $m = 1$, Corollary 5.10 and Corollary 5.4 imply Theorem 2 of [L,M,&Pl]. When $m = 2$, they imply Theorem 12 of [Pl2].

In order to finish the existence question, we need to handle the case for those primes such that $\frac{p-1}{t}d$ is odd. We introduce some notation from the theory of finite abelian groups (see [Ca] for these concepts). Let G be an abelian p-group. Then

$$G \cong \bigoplus_{i=1}^{s} (\mathbb{Z}_{p^i})^{\pi_i} .$$

The π_i's are uniquely determined. Define

$$G_{(i)} = \{g \in G \ : \ \text{order of } g \ \big| \ p^i\}$$

and

$$G^{(i)} = \{p^i g \ : \ g \in G\} .$$

These turn out to be characteristic subgroups of G. We assume the notation of the above in the following.

Theorem 5.11. *Let G be a p-group with $\frac{p-1}{t}d$ odd. If there is a Q-code in $\mathbf{F}[G]$, then π_i is even for $i = 1, \ldots, s$.*

Proof: We first deal with a special case. Suppose that $G = (\mathbb{Z}_p)^{\pi}$. Then by the reasoning of Theorem 5.3, we need the number of nonzero orbits of μ_{2^d} ("cyclotomic cosets") to be even. One computes that in this special case, this number is

$$\frac{p^{\pi}-1}{t}d = \frac{p-1}{t}d\,(p^{\pi-1}+\cdots+1)\,.$$

Since p is odd and by the hypothesis, we must have π even.

We prove the general result by induction on i, starting with $i = s$. By Theorem 5.8, there is a Q-code for the group ${}^{G}\!\big/{}_{G_{(s-1)}}$. But

$${}^{G}\!\big/{}_{G_{(s-1)}} \cong (\mathbb{Z}_p)^{\pi_s}\,.$$

Therefore, by the above special case, π_s is even.

Suppose that $\pi_{i+1}, \ldots, \pi_s$ are known to be even. Again by Theorem 5.8 there is a Q-code for

$$K = {}^{G}\!\big/{}_{G_{(i-1)}} \cong (\mathbb{Z}_p)^{\pi_i} \oplus \cdots \oplus (\mathbb{Z}_{p^{s-i+1}})^{\pi_s}\,.$$

There then is a Q-code for

$${}^{K}\!\big/{}_{K^{(1)}} \cong (\mathbb{Z}_p)^{\pi_i+\cdots+\pi_s}\,.$$

In particular, $\pi_i + \cdots + \pi_s$ is even, which implies that π_i is even. This completes the induction and the proof.

♡♠

Theorem 5.12. *Suppose that G is as in Theorem 5.11. If π_i is even for $i = 1, \ldots, s$, then there is a Q-code in $\mathbf{F}[G]$.*

Proof: From repeated application of Theorem 5.6, it would suffice to prove the result when $G = \mathbb{Z}_{p^s} \oplus \mathbb{Z}_{p^s}$. We construct a Q-code with binary coefficients in such a G.

For $g = (i, j) \in G$, define the map

$$\mu : \qquad g \quad \longmapsto \quad (i + j, i - j) \,.$$

It is easy to see that $\mu \in \mathrm{Aut}(G)$. Observe that $g\mu^2 = 2g$ for all $g \in G$. We claim that the cycle $(g, g\mu, g\mu^2, \ldots)$ has even length for every nonzero g. But if it had odd length, then $\mu^2 = \mu_2$ would produce the same cycle. In particular, 2 would have odd order mod some power of p. But this contradicts the fact that $\frac{p-1}{t}$ is odd.

Since every such cycle has even length, we can take every other element in each cycle and give it a coefficient of 1 and give a zero coefficient to the other half of the nonzero elements of G. The resulting element of G is an idempotent which generates a Q-code with splitter μ.

♡♠

Ex. 5-1: We illustrate the construction in Theorem 5.12. Let $G = (\mathbb{Z}_3)^2$ and **F** be binary. The hypotheses of the theorem apply, so we let $\mu \in \mathrm{Aut}(G)$ be the matrix

$$\mu = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} .$$

There are two cycles on the nonzero elements of G from the action of μ:

$$\Big((0,1)\,,\, (1,-1)\,,\, (0,2)\,,\, (2,-2) \Big) \qquad \text{and} \qquad \Big((1,0)\,,\, (1,1)\,,\, (2,0)\,,\, (2,2) \Big) \,.$$

Therefore we can take for an odd-like idempotent for a Q-code

$$\underline{e} \;=\; \underline{1} + x^{(0,1)} + x^{(0,2)} + x^{(1,0)} + x^{(2,0)}\,.$$

In general, if G is an elementary p-group of rank r, then all automorphisms of G are nonsingular $r \times r$ matrices with entries in the field $\mathbb{Z}_p$. If $\frac{p-1}{t}d$ is odd, then a matrix giving the splitting cannot have any eigenvalues in $\mathbb{Z}_p$, since the span of an eigenvector is an invariant subgroup of G isomorphic to $\mathbb{Z}_p$ which contradicts Theorems 5.3 and 5.8. Notice that this is true in the above example.

♣◇

The next theorem and Corollary 5.9 complete the existence theorem for Q-codes in $\mathbf{F}[G]$.

Theorem 5.13. *Let G be a p-group.*

a). If $\frac{p-1}{t}d$ is even, then a Q-code always exists in $\mathbf{F}[G]$.

b). If $\frac{p-1}{t}d$ is odd, then a Q-code exists in $\mathbf{F}[G]$ iff the π_i's defined above are all even.

Proof: Part a) follows from Theorem 5.3 and repeated applications of Theorems 5.6 and 5.7. Part b) is just Theorems 5.11 and 5.12 combined.

♡♠

Ex. 5-2: We extend Ex. 3-3 to the case of characteristic 2. Let G be the additive group of $\mathrm{GF}(p^r)$ for $r \geq 1$, S be the nonzero squares in G, and N be the nonzero nonsquares.

If 2 is a square mod p, then $S(x)$ and $N(x)$ are idempotents which generate Q-codes; the splitting is given by μ_ℓ where $\ell \in N$. In particular, for any $\mathbf{F}$, Q-codes exist which are invariant under μ_ℓ where $\ell \in S$.

If 2 is a nonsquare and if d is odd, then no Q-codes can exist by Theorem 5.13. If d is even, then GF(4) is in $\mathbf{F}$; let it be defined as in the proof of Theorem 5.3. Then the idempotents

$$\omega S(x) + \omega^2 N(x) \qquad \text{and} \qquad \omega^2 S(x) + \omega N(x)$$

generate Q-codes with splitting μ_2. When G has prime order, these were constructed in [Pl2].

♣◇

We should stress that no attempt was made in the above to give a complete description of *all* Q-codes which exist for a given G and $\mathbf{F}$. Such questions depend on the values of the parameters involved, and so general statements are difficult. We have always picked the easiest idempotents to use in our constructions; these are usually binary or quaternary. In the next section we give some construction techniques which we hope will indicate how one may go about in a specific case to classify all Q-codes in $\mathbf{F}[G]$.

6. Construction Techniques for Characteristic 2

All of the constructions for the characteristic 2 case have involved binary or quaternary idempotents. Many of these codes are interesting, as [L,M,&Pl], [Pl,M,&L],

and [P12] would indicate. We wish to finally offer construction techniques which will apply to larger fields and which, we hope, yield additional interesting codes. This section concerns numerical splitters and multipliers.

Fix an odd prime p and define t as in section 5. Set $G = \mathbb{Z}_p$ and recall that all of the automorphisms of G are numerical. Let $\mathbf{F}$ be $\mathrm{GF}(2^d)$ where $d \mid t$. Notice that from Lemma 5.2 no generality is lost by this restriction. We record the following lemma without proof; all of the results have been stated explicitly or implicitly in the above discussion.

Lemma 6.1. *Let $\underline{e}$ an idempotent generating a Q-code in $\mathbf{F}[G]$ with splitter μ_ℓ and multiplier $\mu_\jmath$. Let the coefficients of $\underline{e}$ be β_i for $0 \le i \le p-1$. Then*

a). *For $i \neq 0$, $\qquad \beta_i + \beta_{\ell i} = 1$.*

b). *For all i, $\qquad \beta_i = \beta_{\jmath i}$.*

c). *$\mu_\ell^2 = \mu_{\ell^2}$ is a multiplier of $\langle \underline{e} \rangle$.*

d). *The number of orbits of $\mu_\jmath$ on the nonzero elements of G is even.*

♣◇

The construction of Q-codes, in particular finding the splitter μ_ℓ, is dependent on the specific prime p. There are, however, three cases when we can state general results on when μ_ℓ can be a splitting. These are when ℓ is a power of 2, -1, or the negative of a power of 2. We handle these separately.

Theorem 6.2. *Let $\ell = 2^s$ and $r = \gcd(2s, d)$. Then these are equivalent:*

a). *There exists a Q-code in $\mathbf{F}[G]$ given by splitting μ_ℓ.*

b). The polynomial $y^\ell + y + 1$ *has a root in* $GF(2^r)$*.*

Proof: a) $\Longrightarrow$ b) Let $\underline{e}$ be an idempotent for a Q-code in $\mathbf{F}[G]$ with coefficients β_i for $0 \le i \le p-1$. From Lemma 6.1 and the fact that $\underline{e}$ is an idempotent we have for all i

$$\beta_i \;=\; \beta_{\ell^2 i} \;=\; \beta_{2^{2s} i} \;=\; (\beta_i)^{2^{2s}} .$$

Hence $\beta_i \in \mathrm{GF}(2^r)$ since $r = \gcd(2s, d)$. Furthermore, for any $i \neq 0$,

$$\beta_{\ell i} + \beta_i = 1 \qquad \text{so that} \qquad \beta_i^\ell + \beta_i + 1 = 0 .$$

This shows that the required polynomial has a root in $\mathrm{GF}(2^r)$.

b) $\Longrightarrow$ a) Let β be a root of $y^\ell + y + 1$. Let U be the nonzero elements of G considered as a group under multiplication. Let T be the subgroup of U generated by 2 and $\Im$ be a set of coset representaives of T in U. Define the two elements

$$\underline{e}_1 \;=\; \sum_{i \in \Im} \sum_{j=0}^{t-1} \beta^{2^j} \, x^{i2^j}$$

and

$$\underline{e}_2 \;=\; \sum_{i \in \Im} \sum_{j=0}^{t-1} \beta^{2^{j+s}} \, x^{i2^j} .$$

We assert that these generate Q-codes with splitting μ_ℓ.

First we show $\underline{e}_2 = \underline{e}_1 \mu_\ell$. Pick $i \in \Im$ and $j = 0, \ldots, t-1$. Let $g = i2^j \in U$. Then the coefficient of x^g in $\underline{e}_1$ is β^{2^j} while the coefficient of $x^{\ell g}$ in $\underline{e}_2$ is $\beta^{2^{j+2s}}$. We need to show that these are equal. But since $r \mid 2s$,

$$\beta^{2^j} = \left(\beta^{2^j}\right)^{2^{2s}} = \beta^{2^{j+2s}}.$$

A similar calculation shows that $\underline{e}_1$ and $\underline{e}_2$ are idempotents, since we just need to show that the coefficient of x^{2g} is the square of the coefficient of x^g. It remains to show that $\underline{1} + \underline{e}_1 - \underline{e}_2 = \underline{h}$. For a given g as above we add the coefficient of x^g in both $\underline{e}_1$ and $\underline{e}_2$:

$$\beta^{2^{j+s}} + \beta^{2^j} = \left(\beta^{2^s} + \beta\right)^{2^j} = 1.$$

This completes the construction.

Notice that in either case of this theorem, the coefficients for nonzero $g \in G$ are roots of the polynomial in the statement of the theorem.

♡♠

Corollary 6.3. *If* $2s \mid d$, *then there exists a Q-code in* $\mathbf{F}[G]$ *for which* μ_{2^s} *gives the splitting.*

Proof: From Theorem 6.2, it suffices to show that the polynomial

$$\rho(x) = y^{2^s} + y + 1$$

has a root in $\mathrm{GF}(2^s)$. Now let β be a root of $\rho(x)$ in some field of characteristic 2. From $\beta^{2^s} = \beta + 1$ we have

$$\beta^{2^{2s}} = \left(\beta^{2^s}\right)^{2^s} = \beta^{2^s} + 1 = \beta.$$

In particular, β is in GF(2^s).

♡♠

Ex. 6-1: We illustrate the above results.

$s = 1$: From Corollary 6.3, we need that y^2+y+1 has a root in $\mathbf{F}$. This occurs iff $2 \mid d$ iff GF(4) is a sub-field of of $\mathbf{F}$. This is precisely the quaternary construction of [P12]. As an example, let $\mathbf{F}$ be GF(4) generated by ω with $\omega^2 + \omega + 1 = 0$. Let $p = 5$. The construction of the theorem gives the idempotent

$$\underline{e} \;=\; \underline{1} + \omega x^1 + \omega^2 x^2 + \omega^2 x^3 + \omega x^4 \,.$$

We give properties of this code in section 7; notice that μ_{-1} is a multiplier of this code.

$s = 2$: We need y^4+y+1 to have a root in $\mathbf{F}$. Since this polynomial is irrreducible, we need GF(16) to be a subfield of $\mathbf{F}$, i.e. $4 \mid d$. As an example of this construction, let α be a root of this polynomial and again $p = 5$. One idempotent would then be

$$\underline{e} \;=\; \underline{1} + \alpha x^1 + \alpha^2 x^2 + \alpha^8 x^3 + \alpha^4 x^4 \,.$$

Notice that since $4 \equiv -1 \pmod 5$, μ_{-1} gives the splitting.

$s = 3$: From Theorem 6.2, let $r = \gcd(6, d)$. Since we have the factorization

$$y^8 + y + 1 \;=\; (y^2 + y + 1)\,(y^6 + y^5 + y^3 + y^2 + 1)\,.$$

Therefore there are two possibilities for r: 2 or 6. If $r = 2$, then we just need that d is even. Then since we can construct an idempotent with splitting μ_2, the same

Q-codes are given with splitting $(\mu_2)^3 = \mu_8$. If 6 $\bigm|$ d, then we can also find Q-codes with splitting given by μ_8 and not by μ_2 by taking a root of the 6th degree factor. The smallest such example would be length 13.

In general, in order to describe such splittings completely we need the factorization of $y^{2^s} + y + 1$.

♣◇

We next consider when μ_{-1} gives the splitting. We will need the following technical lemma.

Lemma 6.4. *Let $\frac{t}{d}$ be odd and t be even. Then for all $\alpha \in \mathbf{F}$,*

$$\alpha^{2^{\frac{t}{2}}} = \alpha^{2^{\frac{d}{2}}} .$$

Proof: As $\frac{t}{d}$ is odd and t is even, $t = d(2r+1)$ for some r. Then for every $\alpha \in \mathbf{F}$,

$$\alpha^{2^{\frac{t}{2}}} = \alpha^{2^{\frac{d}{2}(2r+1)}} = \alpha^{2^{\frac{d}{2}}2^{rd}} = \alpha^{2^{\frac{d}{2}}} .$$

The last equality is just the fact that $\beta^{2^d} = \beta$ for all $\beta \in \mathbf{F}$.

♣◇

Theorem 6.5. *There exists a Q-code in $\mathbf{F}[G]$ with splitting given by μ_{-1} iff $\frac{t}{d}$ is odd.*

Proof: Since $\frac{t}{d}$ is the order of 2^d mod p, this is just Theorem 4.7. We wish to give two general constructions rather than just stating this existence result. Therefore let $\frac{t}{d}$ be odd.

t is odd: Pick any α and β in $\mathbf{F}$ with $\alpha + \beta = 1$. As t is odd, $2^s \not\equiv -1 \pmod{p}$ for all $s \geq 1$. Let U be the group of nonzero elements of G and T be the subgroup of U generated by 2. Then μ_{-1} fixes no coset of T in U. This means we can find a set $\Im$ in U such that the set $\{i, -i\}_{i \in \Im}$ is a complete set of coset representatives of T in U. Define the two elements

$$\underline{e}_1 = \sum_{i \in \Im} \sum_{j=0}^{t-1} \left(\alpha^{2^j} x^{i2^j} + \beta^{2^j} x^{-i2^j} \right)$$

and

$$\underline{e}_2 = \sum_{i \in \Im} \sum_{j=0}^{t-1} \left(\beta^{2^j} x^{i2^j} + \alpha^{2^j} x^{-i2^j} \right).$$

It is straightforward to see that $\underline{e}_1$ and $\underline{e}_2$ are idempotents generating Q-codes with splitting given by μ_{-1}; the calculation is similar to that in Theorem 6.2.

t is even: Since $\frac{t}{d}$ is odd, d is even. From Corollary 6.3, there is a Q-code given by splitting $\mu_{2^{\frac{d}{2}}}$. We claim that μ_{-1} also gives the splitting. Let $\underline{e}$ be the idempotent for this Q-code with coefficients β_i for $0 \leq i \leq p-1$. It then would suffice to show for all nonzero i,

$$\beta_{2^{\frac{d}{2}} i} = \beta_{-i}.$$

Notice that $2^{\frac{t}{2}} \equiv -1 \pmod{p}$. Then

$$\beta_{2^{\frac{t}{2}} i} = \beta_{-i}.$$

From Lemma 6.4 and the fact that $\underline{e}$ is an idempotent, we have

$$\beta_{2^{\frac{d}{2}}i} = \beta_i^{2^{\frac{d}{2}}} = \beta_i^{2^{\frac{t}{2}}} = \beta_{2^{\frac{t}{2}}i},$$

which is what was to be shown.

♡♠

Ex. 6-2: If d is odd, then Theorem 6.5 says that there is a Q-code with splitter μ_{-1} iff t is odd. This is the duadic case of [L,M,&Pl]. If $d = 2$, we need that 2 exactly divides t. This is the quaternary case of [Pl2]. In general, if 2^s exactly divides t, we need that 2^s exactly divides d.

We offer the following family of examples which generalize the length 5 code with coefficients in GF(16) in Ex. 6-1. Let $d = t = p - 1$ and let ω be a root of $y^{2^{\frac{t}{2}}} + y + 1$ in $\mathbf{F}$. Then the above constructions offer the Q-codes with splitter μ_{-1} generated by the idempotent

$$\underline{e} = \sum_{j=0}^{p-2} \omega^{2^j} x^{2^j} .$$

The small examples from this family that have been examined (see the last section) suggest that these codes have many interesting properties.

♣◇

The last splitters which we investigate are those μ_{-2^s}. Unfortunately, the results are a little more detailed.

Theorem 6.6. *Let $\ell = -2^s$ and $r = \gcd(2s, d)$. Then these are equivalent.*

a). There is a Q-code in $\mathbf{F}[G]$ with splitting given by μ_ℓ

b). There is a Q-code in $\mathbf{F}[G]$ with the coefficients of the idempotent in $GF(2^r)$.

The splitting is given by $\mu_\jmath$, where

1). If $\frac{t}{d}$ is even, $\jmath - 2^s$.

2). If $\frac{t}{d}$ is odd and t is odd, $\jmath = -1$.

3). If $\frac{t}{d}$ is odd and t is even, $\jmath = 2^{\frac{r}{2}}$ and $\frac{2s+t}{r}$ is odd.

Proof: a) $\Longrightarrow$ b) As usual, let $\underline{e}$ be the idempotent for a Q-code with splitter μ_ℓ. Let the coefficients of $\underline{e}$ be β_i for $0 \leq i \leq p-1$. From Lemma 6.1, μ_{ℓ^2} is a multiplier of the Q-code, so in particular, for any i,

$$\beta_i = \beta_{2^{2s}i} = (\beta_i)^{2^{2s}}.$$

This shows that the β_i's are in GF(2^r).

If $\frac{t}{d}$ is even, then some power of 2^d is congruent to -1 mod p. Hence μ_{-1} is a multiplier and so the splitting is given by μ_{2^s}.

Let $\frac{t}{d}$ be odd. If t is odd, then d is odd, so that r is odd. This implies that $r \mid s$, and so μ_{2^s} must be a multiplier. This means that the splitting is given by μ_{-1}.

So let t be even, so that d is even and hence r is even. As $2^{\frac{t}{2}} \equiv -1 \pmod{p}$, we see that

$$-2^s \equiv 2^{s+\frac{t}{2}} \pmod{p}.$$

That is, $\mu_{2^{s+\frac{t}{2}}}$ gives the splitting. Notice that

$$\mu_{2^{s+\frac{t}{2}}} = (\mu_{2^{\frac{r}{2}}})^{\frac{2s+t}{r}} .$$

If $\frac{2s+t}{r}$ is odd, then $\mu_{2^{\frac{r}{2}}}$ gives the splitting. If $\frac{2s+t}{r}$ is even, we get a contradiction since the splitter would then be a power of the multiplier μ_{2^r}.

b) $\Longrightarrow$ a) All of the above reasoning reverses. That is, for each of 1), 2), and 3), a Q-code with the given splitting would also be given by the splitter μ_ℓ.

♡♠

Ex. 6-3: In order to apply Theorem 6.6, we need to appeal to both Corollary 6.3 and Theorem 6.5. We illustrate by discussing when μ_{-4} gives the splitting (so $s = 2$). If $\frac{t}{d}$ is even, then we need μ_4 to give the splitting, i.e., $4 \mid d$. Let $\frac{t}{d}$ be odd. If t is odd, r is 1 and so we need a binary idempotent with splitting given by μ_{-1}. If t is even, then we need $\frac{4+t}{4}$ to be odd, so that $8 \mid t$. Hence $8 \mid d$ and since $r = \gcd(4, d)$, $r = 4$. Thus μ_4 gives the splitting. We observe that the case $s = 1$ was investigated in [P12].

♣◇

Hidden in the above results is the following theorem about multipliers. We omit the proof.

Theorem 6.7. *Let $\underline{e}$ be an idempotent of $\mathbf{F}[G]$ which generates a Q-code.*

a). The coefficients of $\underline{e}$ are in $GF(2^s)$ iff μ_{2^s} is a multiplier.

b). If $\frac{t}{d}$ is even, then μ_{-1} is a multiplier.

c). Suppose that $\frac{t}{d}$ *is odd and* t *is even. Let* $r = \gcd(2s, d)$. *If the coefficients of* $\underline{e}$ *are in* $GF(2^r)$ *and* $\frac{2s+t}{r}$ *is even, then* μ_{-2^s} *is a multiplier.*

♡♠

7. More Examples

In this final section we wish to present some new and old Q-codes. Relations to the above results and constructions will be given when applicable. We do not intend for these examples to be exhaustive, merely illustrative.

All of the examples will be for characteristic 2, and so we define the following fields:

1). $\mathbf{F}_2 = \{0, 1\}$ is the ordinary binary field.

2). $\mathbf{F}_4 = \{0, 1, \omega, \omega^2\}$ is the quaternary field, defined by $\omega^2 + \omega = 1$.

3). $\mathbf{F}_8 = \{0, 1, \beta, \beta^2, \ldots, \beta^6\}$ is the field of size 8 defined by $\beta^3 + \beta^2 = 1$.

4). $\mathbf{F}_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ is the field of size 16 defined by $\alpha^4 + \alpha = 1$. Observe that $\{0, 1, \alpha^5, \alpha^{10}\}$ is the subfield of $\mathbf{F}_{16}$ of size 4.

Throughout we use the notation of sections 3 and 6. In particular, 2^d is the size of the given field $\mathbf{F}$, and for a given prime p, t is the order of 2 mod p. We take the natural notation for the given abelian group G. All idempotents will be odd-like. The next result will be useful in the establishment of inequivalence in some cases.

Theorem 7.1. *Let* $G = \mathbb{Z}_p$. *Then two* G*-codes are equivalent iff they are equivalent by the permutation induced by some* μ_ℓ.

Proof: This is Theorem 1 of [L,M,&Pl].

♡♠

Ex. 7-1: $n = p = 3$

Since $t = 2$, $\frac{p-1}{t}d = d$. Therefore from section 5, we need d to be even in order for Q-codes to exist.

A): Let $\mathbf{F} = \mathbf{F}_4$ and set

$$\underline{e}_1 = \omega x^1 + \omega^2 x^2 .$$

This is Ex. 4-1, and as mentioned, they are in [Pl2]. Observe that this is an example from the family mentioned at the end of Ex. 6-2. Since the splitting is given by $\mu_2 = \mu_{-1}$, C_1^* is self-dual. The weight distribution for C_1 is

$$(1,0,9,6)$$

and for C_1^* is

$$(1,0,0,12,3) .$$

Both codes are MDS.

B): Let $\mathbf{F} = \mathbf{F}_{16}$ and set

$$\underline{e}_1 = \alpha^5 x^1 + \alpha^{10} x^2 .$$

This is just example A) considered over $\mathbf{F}_{16}$, so all of the above comments apply. The weight distributions are

$$(1,0,45,210)$$

for C_1 and

$$(1,0,0,60,195)$$

for C_1^*. They are both MDS.

♣◇

Ex. 7-2: $n = p = 5$

Again, since $t = 4$, $\frac{p-1}{t}d = d$, and so we must have that d is even.

A): Let $\mathbf{F} = \mathbf{F}_4$ and set

$$\underline{e}_1 = \underline{1} + \omega x^1 + \omega^2 x^2 + \omega^2 x^3 + \omega x^4 .$$

The splitting is given by μ_2 and μ_{-1} is a multiplier. Hence C_1^* is the dual of C_2^*. The weight distribution for C_1 is

$$(1,0,0,30,15,18)$$

and for C_1^* is

$$(1,0,0,0,45,0,18) .$$

Both codes are MDS. These are found in [Pl2]; the extended code is known as the *hexacode*.

B): Consider example A) over $\mathbf{F}_{16}$, so that

$$\underline{e}_1 = \underline{1} + \alpha^5 x^1 + \alpha^{10} x^2 + \alpha^{10} x^3 + \alpha^5 x^4 .$$

The resulting codes have the same properties as in A). Both codes are MDS, since the weight distributions are

$$(1,0,0,150,975,2970)$$

for C_1 and

$$(1,0,0,0,225,1080,2790)$$

for C_1^*.

C): Let $\mathbf{F} = \mathbf{F}_{16}$ again and define

$$\underline{e}_1 = \underline{1} + \alpha x^1 + \alpha^2 x^2 + \alpha^8 x^3 + \alpha^4 x^4 .$$

This was given in Ex. 6-1. Observe that this code is another example from the family discussed at the end of Ex. 6-2. The splitting is given by $\mu_4 = \mu_{-1}$. Therefore the extended codes are self-dual. C_1 and C_1^* are MDS with the same weight distributions as in example B).

From Theorem 7.1, the codes in B) and C) are inequivalent.

♣◇

Ex. 7-3: $n = p = 7$

Here $t = 3$, and so $\frac{p-1}{t}d = 2d$. Hence Q-codes exist for all fields. Notice though that from Lemma 6.1, we may assume that $d \mid t$. Hence, the coefficients of the any idempotent must lie in $\mathbf{F}_2$ or $\mathbf{F}_8$.

A): Consider the binary idempotent:

$$\underline{e}_1 = x^1 + x^2 + x^4 .$$

The splitting is given by μ_{-1} and so the extensions are self-dual. The minimum weight vectors are always multiples of the blocks of the projective plane of order 2. The weight distributions for the codes are as follows:

$\mathbf{F}$	C_1	C_1^*
$\mathbf{F}_2$	(1,0,0,7,7,0,0,1)	(1,0,0,0,14,0,0,0,1)
$\mathbf{F}_4$	(1,0,0,21,21,126,42,45)	(1,0,0,0,42,0,168,0,45)
$\mathbf{F}_8$	(1,0,0,49,49,882,1470,1645)	(1,0,0,0,98,0,1176,1344,1477)
$\mathbf{F}_{16}$	(1,0,0,105,105,4410,19110,41805)	(1,0,0,0,210,0,5880,20160,39285)

B): Set $\mathbf{F} = \mathbf{F}_8$. Suppose that we wished to construct an idempotent for a Q-code such that the coefficient of x^1 is β. Then checking the idempotent conditions, we see that for some $\gamma \in \mathbf{F}$,

$$\underline{e}_1 = (\beta x^1 + \beta^2 x^2 + \beta^4 x^4) + (\gamma x^3 - \gamma^4 x^5 + \gamma^2 x^6).$$

There are three possible automorphisms which could be splitters: μ_3, μ_5, and μ_{-1}. By using the equation $\underline{1} + \underline{e}_1 + \underline{e}_2 = \underline{h}$, one finds that the only time one can solve for γ is when the splitter is μ_{-1}. The resulting idempotent is then

$$\underline{e}_1 = \beta x^1 + \beta^2 x^2 + \beta^6 x^3 + \beta^4 x^4 + \beta^3 x^5 + \beta^5 x^6 ; \tag{7a}$$

the calculations use that $\beta^3 = \beta^2 + 1$. The extended code is self-dual, since the splitter is μ_{-1}. The weight distributions are

$$(1,0,0,0,245,588,1666,1596)$$

for C_1 and

$$(1,0,0,0,0,392,588,1736,1379)$$

for C_1^*. In particular, these codes are MDS. There are already known MDS codes of length 7 over GF(8), namely the Reed-Solomon codes (see [MW&Sl]). We take as a given that the idempotent for such codes is given by

$$\underline{e} = \sum_{i=0}^{6} \gamma^i x^i , \tag{7b}$$

for some nonzero $\gamma \in \mathbf{F}$. Therefore, by Theorem 7.1, the above Q-code is equivalent to the Reed-Solomon code iff there is some $\gamma \in \mathbf{F}$ and $\mu_\ell \in \mathrm{Aut}(G)$ such that the image under μ_ℓ of the idempotent in (7*a*) is the idempotent in (7*b*). But a simple calculation shows that this is impossible. Hence the above MDS Q-code is not a Reed-Solomon code.

♣◇

Ex. 7-4: $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3$

A): Set $\mathbf{F} = \mathbf{F}_2$. There are 4 nonzero cyclotomic cosets:

$$\{(0,1)\,,\,(0,2)\}\;;\;\{(1,0)\,,\,(2,0)\}\;;\;\{(1,1)\,,\,(2,2)\}\;;\;\{(1,2)\,,\,(2,1)\}\,.$$

Any combination of these supports an idempotent. In fact, any pair gives an idempotent which can be sent into the idempotent for the other pair by an automorphism of G. In general, this splitting is given by at least one of the following matrices:

$$M_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} . \quad .$$

This gives $\binom{4}{2}/2 = 3$ sets of idempotents; representatives for each set are

$$\underline{1} + \mathrm{C}_{(0,1)}(x) + \mathrm{C}_{(1,0)}(x) \; , \quad \underline{1} + \mathrm{C}_{(0,1)}(x) + \mathrm{C}_{(1,1)}(x) \; ,$$

$$\text{and} \quad \underline{1} + \mathrm{C}_{(0,1)}(x) + \mathrm{C}_{(1,2)}(x) \, .$$

The first was given in Ex. 5-1. All of the resulting codes are equivalent. In fact, we can find an automorphism of G sending each idempotent to another. This is because it is well-known that the set of nonsingular 2×2 matrices acts 2-transitively on the lines of affine 2-space, and observe that each cyclotomic coset is the set of nonzero vectors in a line. The weight distribution for each C_1 is

$$(1,0,0,6,9,9,6,0,0,1) \, .$$

The weight distribution for each C_1^* is

$$(1,0,0,4,7,8,7,4,0,0,1) \, .$$

D): Set $\mathbf{F} = \mathbf{F}_4$. Then since $4 \equiv 1 \pmod 3$, we get 8 singelton nonzero cyclotomic cosets. Pick any representative from each of the cyclotomic cosets from example A), say $\{g_1, g_2, g_3, g_4\}$. Then it is clear that any idempotent must be given by

$$\underline{e} \; = \; \gamma_0 \underline{1} + \sum_{i=1}^{4} \left(\gamma_i x^{g_i} + \gamma_i^2 x^{2g_i} \right) , \qquad (7c)$$

where the coefficients are in $\mathbf{F}_4$. Clearly γ_0 is 0 or 1; suppose that the other coefficients are not 0 or 1 so that for $i \neq 0$, $\gamma_i \in \{\omega, \omega^2\}$. Let $\gamma_1 = \omega$ for $\underline{e}_1$. There are eight possible choices for $\underline{e}_1$. All of these work for Q-codes by looking at the splitter $\mu_2 = \mu_{-1}$. The resulting codes have the same weight distributions, namely

$$(1,0,0,9,81,54,198,405,216,60)$$

for C_1 and

$$(1,0,0,9,0,81,162,171,351,219,30)$$

for C_1^*. Notice that all of these can be constructed from Ex. 7-1 A) above using the "product" construction of Theorem 5-6.

C): We have dealt with all binary coefficients in A) and with "strictly" quaternary coefficients in B). What about mixtures of these two? For a 2 × 2 matrix $M \in \mathrm{Aut}(G)$, we let μ_M be the automorphism it induces on $\mathbf{F}[G]$. Notice that if μ_M gives a splitting for a Q-code with idempotent $\underline{e}$, then $\mu_{P^{-1}AP}$ gives a splitting for the idempotent $\underline{e}\mu_P$; this follows from the fact that $\mu_{AB} = \mu_A\mu_B$. In this way, we only need examine a matrix from each similarity class.

Suppose that μ_M gives a splitting, and that the idempotent $\underline{e}$ is in the form of $(7c)$. Clearly M cannot have 1 as an eigenvalue, since the coefficient of the resulting eigenvector g would cancel in the left side of the equation $\underline{1} + \underline{e} + \underline{e}\mu_M = \underline{h}$. If 2 is an eigenvalue, then we must have that 2 is also the other eigenvalue. Hence either $\mu = \mu_2$, i.e., case A), or M is the matrix

$$M = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} .$$

A simple calculation then shows that the latter case does work, but that the resulting Q-codes are those in B).

So suppose that the eigenvalues are not in $\mathbb{Z}_3$. The minimum polynomial of M must then be a second degree polynomial irreducible over $\mathbb{Z}_3$. There are three such polynomials, and so there are three M's to check. In each case, a Q-code exists with μ_M as a splitter. These are, however, the codes of part A).

In this way, we have classified all of the Q-codes for this G.

♣◇

Ex. 7-5: $G = \mathbb{Z}_5 \oplus \mathbb{Z}_5$

Set $\mathbf{F} = \mathbf{F}_2$. The cyclotomic cosets are again the nonzero vectors of the lines in affine space. There are 6 such cosets, and so we need to take 3 of them in order to possibly construct an idempotent for a Q-code. Since we may assume that the coset for $(0,1)$ is used, there are $\binom{5}{2} = 10$ idempotents to check. Indeed, all of these are Q-codes.

In order to show this, we construct a splitter for each pair of idempotents. Our method is to find a matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{where} \qquad M^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Since 2 is not a square mod 5, one sees that all such M are given by

$$M = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \qquad \text{where} \qquad a^2 + bc = 2\,.$$

It is a straightforward calculation to show that each of the 10 splittings is given by at least one such M.

In every case the minimum weight is 5 for both C_1 and C_1^*. Every such C_1 has the same weight distribution, but there were two different weight distributions among the extended codes. In particular, not all of the resulting codes are equivalent.

♣◇

It is not difficult to go on and, for a given G and $\mathbf{F}$, to list essentially **Q**-codes. We strongly believe that some of the resulting codes would be interesting. As evidence, we note the two inequivalent MDS codes discovered above. As another example, the constructions for binary G-codes when $G = \mathbb{Z}_7 \oplus \mathbb{Z}_7$ were seen to yield codes with larger minimum weight than the generalized quadratic residue codes. Of course, in order to handle the larger groups, one needs methods to calculate the minimum weight which are different than the purely computational methods used here.

References

[B&M] I.F. Blake & R.C. Mullin, *The Mathematical Theory of Codes*, Academic Press,New York,1975

[Ca] R.D. Carmichael, *Groups of Finite Order*,Dover,1937

[La] E.S. Lander,*Symmetric Designs: An Algebraic Approach*, Cambridge University Press,Cambridge,1983

[L,M,&Pl] J.S. Leon, J.M. Masley, & V. Pless, Duadic Codes,*IEEE Trans. on Information Theory*, **IT-30**,no.5(1984),709–714

[vL] J.H. van Lint,*Introduction to Coding Theory*,Springer-Verlag, New York,1982

[vL&MW] J.H. van Lint & F.J. MacWilliams, Generalized Quadratic Residue Codes, *IEEE Trans. on Information Theory*,**IT-24**, no.6(1978),730–737

[MW] F.J. MacWilliams,Binary Codes Which Are Ideals in the Group Algebra of an Abelian Group,*Bell Sys. Tech. J.*, ?(1970),987–1011

[MW&Sl] F.J. MacWilliams & N.A. Sloane, *The Theory of Error Correcting Codes*,North-Holland, Amsterdam,1977

[Pl1] V. Pless, Cyclic Projective Planes and Binary, Extended Cyclic Self-Dual Codes,*J. Combinatorial Theory A*,*to appear*

[Pl2] V. Pless, Q-Codes,*pre-print*

[Pl,M,&L] V. Pless, J.M. Masley, & J.S. Leon, On Weights in Duadic Codes,*J. Combinatorial Theory Ser. A*, *to appear*