

LABORATOIRE



INFORMATIQUE, SIGNAUX ET SYSTÈMES
DE SOPHIA ANTIPOLIS
UMR 6070

TWO-WEIGHT CODES OVER CHAIN RINGS AND PARTIAL DIFFERENCE SETS

San Ling, Patrick Solé

Projet RECIF

Rapport de recherche
I3S/RR-2002-40-FR

Septembre 2002

Two-Weight Codes over Chain Rings and Partial Difference Sets

San Ling*
Department of Mathematics
National University of Singapore
Singapore 117543
Republic of Singapore
lings@math.nus.edu.sg

and

Patrick Solé
CNRS–I3S
ESSI
Route des Colles
06903 Sophia Antipolis
France
ps@essi.fr

Abstract

The homogeneous weight of chain rings is related here to a special additive character. Two-weight codes for that weight are shown to give rise to partial difference sets on the syndrome space of their dual codes. An infinite family of such codes, which includes the Camion codes over \mathbf{Z}_4 as a special case, is constructed.

1 Introduction

In recent years, Galois rings have proved very useful in the construction of difference sets [2, 6, 7]. They have also led to remarkable advances in algebraic coding theory via the Gray

*The research of this author is partially supported by NUS-ARF research grant R-146-000-029-112 and DSTA research grant R-394-000-011-422. This research was done while this author was visiting ESSI, Sophia Antipolis. He thanks this institution for the invitation and for its hospitality.

map [5], an isometry between Lee weight and Hamming weight spaces. The Gray map was extended recently to the context of chain rings by Greferath and Schmidt [4] as an isometry between homogeneous weight and Hamming weight spaces. We unify these two trends by attaching a partial difference set to a two (homogeneous) weight code over a chain ring. We generalize from Galois rings to chain rings a recent result of Voloch and Walker [8] on the homogeneous weight. This result is instrumental in the Fourier analysis of the said difference set. An infinite family of such codes, which includes the Camion codes over \mathbf{Z}_4 [1] as a special case, is constructed.

2 Finite chain rings

A **chain ring** is a local principal ideal commutative ring. Let R be a finite chain ring with maximal ideal (π) and let its residue field $R/(\pi)$ be \mathbf{F}_q . The only ideals of R are:

$$R \supset (\pi) \supset (\pi^2) \supset \cdots \supset (\pi^{d-1}) \supset (\pi^d) = 0,$$

for some d . This integer d is called the **depth** of R .

It can be easily verified that, for every $0 \leq i \leq d-1$, $(\pi^i)/(\pi^{i+1})$ is an \mathbf{F}_q -vector space of dimension 1 (where $(\pi^0) = R$). Hence, (π^i) has q^{d-i} elements and R has q^d elements.

An additive character of R is a group homomorphism from R to \mathbf{C}^\times , where only the additive group structure of R is considered.

Lemma 2.1 *Let R be a finite chain ring. Then R admits an additive character ψ such that the restriction of ψ to the ideal (π^i) is not the trivial character for all $0 \leq i \leq d-1$.*

Proof. A finite chain ring is a Frobenius ring (cf. [9, Remark 1.3]). From *loc. cit.*, Theorem 3.10 and Lemma 4.1, a finite ring is Frobenius if and only if it admits an additive character ψ such that the kernel of ψ does not contain any nonzero ideal of R . \square

3 A family of two-weight linear codes over finite chain rings

For a finite chain ring R , a homogeneous weight wt_{hom} was introduced in [4]. For $x \in R$, we have:

$$wt_{\text{hom}}(x) = \begin{cases} q^{d-1} & \text{if } x \in (\pi^{d-1}) \setminus \{0\} \\ q^{d-2}(q-1) & \text{if } x \notin (\pi^{d-1}) \\ 0 & \text{if } x = 0. \end{cases}$$

For $\mathbf{x} = (x_1, \dots, x_n) \in R^n$, the homogeneous weight of \mathbf{x} is just $wt_{\text{hom}}(\mathbf{x}) = \sum_{i=1}^n wt_{\text{hom}}(x_i)$. The homogeneous distance d_{hom} is defined as $d_{\text{hom}}(\mathbf{x}, \mathbf{y}) = wt_{\text{hom}}(\mathbf{x} - \mathbf{y})$.

In this section, we generalize a construction given in [1, Section 5.4] to construct a family of two-weight linear codes over finite chain rings, where the weight involved is the homogeneous weight.

Let R be a finite chain ring as in Section 2. For $s \geq 1$, we first define a $s \times n_s$ matrix G_s (where n_s will be made precise later) with entries in R . The matrix G_s will serve as a generator matrix for the code C_s , i.e., $C_s = \{\mathbf{x}G_s \mid \mathbf{x} \in R^s\}$.

Intuitively, the matrix G_s is best described in terms of its columns. Let U_s be the set of all the vectors of R^s such that at least one of the coordinates is a unit. We say that two vectors \mathbf{u}, \mathbf{u}' of U_s are related, denoted $\mathbf{u} \sim \mathbf{u}'$, if and only if there is a unit λ of R such that $\mathbf{u} = \lambda\mathbf{u}'$. It is straight-forward to verify that \sim is an equivalence relation. The columns of G_s are just the equivalence classes of \sim on U_s .

Formally, the matrix G_s can be described in the following inductive manner. First, we order the elements of R in some fixed way, so that $R = \{r_1, r_2, \dots, r_{q^d}\}$. Let $G_1 = (1)$. Then, for all $s \geq 2$,

$$G_s = \begin{pmatrix} G_{s-1} & G_{s-1} & \cdots & G_{s-1} & G'_{s-1} \\ r_1 \cdots r_1 & r_2 \cdots r_2 & \cdots & r_{q^d} \cdots r_{q^d} & 1 \cdots 1 \end{pmatrix}, \quad (1)$$

where G'_{s-1} is just the $(s-1) \times q^{(d-1)(s-1)}$ matrix whose columns are all the vectors in πR^{s-1} .

The following lemma is needed in the proof of Theorem 3.2.

Lemma 3.1 *Let A be an invertible $s \times s$ matrix in $GL(s, R)$. Then there exists a monomial matrix $B \in GL(s, R)$ (i.e., B has exactly one unit entry in each row and each column, while the other entries are all 0) such that $AG_s = G_sB$.*

Proof. Since A is invertible, it follows that, for all $\mathbf{c} \in R^s$, if $\pi^{d-1}A\mathbf{c} = A(\pi^{d-1}\mathbf{c}) = \mathbf{0}$, then $\pi^{d-1}\mathbf{c} = \mathbf{0}$. In other words, if \mathbf{c} contains a unit coordinate, then so does $A\mathbf{c}$.

Let \mathbf{c}, \mathbf{c}' be two columns of G_s . For any two units λ, λ' of R ,

$$\lambda A\mathbf{c} + \lambda' A\mathbf{c}' = \mathbf{0} \text{ implies } \lambda\mathbf{c} + \lambda'\mathbf{c}' = \mathbf{0},$$

which means that \mathbf{c}, \mathbf{c}' are in the same equivalence class under \sim . This contradicts the definition of G_s , so no two columns of AG_s are in the same equivalence class of \sim .

Combining the above two observations, together with the definition of G_s , we conclude that AG_s is a monomial permutation of the columns of G_s , i.e., $AG_s = G_sB$ for some monomial matrix B . \square

Theorem 3.2 *The R -linear code $C_s = \{\mathbf{x}G_s \mid \mathbf{x} \in R^s\}$ has length $q^{(d-1)(s-1)}(q^s - 1)/(q - 1)$, has $q^{ds} - q^s$ codewords of (homogeneous) weight $q^{(d-1)s-1}(q^s - 1)$, $q^s - 1$ codewords of (homogeneous) weight q^{ds-1} and the zero-codeword.*

Proof. Denote the length of C_s by n_s , with $n_1 = 1$. From (1), it is clear that we have the recurrence relation $n_s = q^d n_{s-1} + q^{(d-1)(s-1)}$. It then follows that

$$\begin{aligned} n_s &= q^d n_{s-1} + q^{(d-1)(s-1)} \\ &= q^d (q^d n_{s-2} + q^{(d-1)(s-2)}) + q^{(d-1)(s-1)} \\ &= q^{2d} n_{s-2} + (q^{(d-1)(s-1)+1} + q^{(d-1)(s-1)}) \\ &= \cdots \\ &= q^{(s-1)d} n_1 + q^{(d-1)(s-1)} (1 + q + \cdots + q^{s-2}) \\ &= q^{(s-1)d} + q^{(d-1)(s-1)} (q^{s-1} - 1)/(q - 1) \\ &= q^{(d-1)(s-1)} (q^s - 1)/(q - 1). \end{aligned}$$

Consider the last row of G_s . There are n_{s-1} coordinates that are equal to 0. For each $1 \leq i \leq d-1$, the number of coordinates in $(\pi^i) \setminus (\pi^{i+1})$ is equal to $q^{d-i-1}(q-1)n_{s-1}$, and the number of coordinates that are units is given by $q^{d-1}(q-1)n_{s-1} + q^{(d-1)(s-2)}$.

Consider now the word $\mathbf{x}G_s$, where $\mathbf{x} \in \pi^j R^s \setminus \pi^{j+1} R^s$, where $0 \leq j \leq d-1$. Write $\mathbf{x} = \pi^j \mathbf{x}'$, where $\mathbf{x}' \in R^s$ has at least one unit coordinate.

Since \mathbf{x}' has at least one unit coordinate, there exists an invertible matrix A in $GL(s, R)$ with \mathbf{x}' as the last row. (For example, if x'_ℓ is a unit, then by choosing all the entries in A above x'_ℓ to be 0, and filling up the remaining entries with an invertible matrix A' in $GL(s-1, R)$ will yield an invertible A .) Therefore, by Lemma 3.1, $\mathbf{x}'G_s$ is the last row of $G_s B$, for some monomial matrix B in $GL(s, R)$. In other words, $\mathbf{x}'G_s$ is a monomial permutation of the last row of G_s .

Given the distribution of the coordinates of the last row of G_s mentioned above, it is easy to verify that the distribution of the coordinates of $\mathbf{x}G_s$ is then the following.

If $\mathbf{x} = \pi^{d-1} R^s \setminus \{\mathbf{0}\}$, then there are $q^{d-1}(q-1)n_{s-1} + q^{(d-1)(s-2)}$ coordinates in (π^{d-1}) and the other entries are all 0. It follows that the homogeneous weight of such a codeword is $q^{ds} - 1$ and there are exactly $q^s - 1$ such codewords.

If $\mathbf{x} \in \pi^j R^s \setminus \pi^{j+1} R^s$, where $0 \leq j < d-1$, then the number of coordinates in (π^{d-1}) is exactly $q^j(q-1)n_{s-1}$, the number of 0 is $\sum_{i=d-j}^{d-1} q^{d-i-1}(q-1)n_{s-1} + n_{s-1} = q^j n_{s-1}$, and the number of coordinates not in (π^{d-1}) is

$$\sum_{i=1}^{d-j-2} q^{d-i-1}(q-1)n_{s-1} + q^{d-1}(q-1)n_{s-1} + q^{(d-1)(s-2)} = q^d n_{s-1} + q^{(d-1)(s-1)}.$$

It follows that the homogeneous weight this codeword is $q^{(d-1)s-1}(q^s - 1)$ and there are exactly $q^{ds} - q^s$ such codewords. \square

In [4], a Gray map $\phi : R^n \rightarrow \mathbf{F}_q^{q^d n}$ was defined and it was shown [4, Theorem 1.1] that ϕ is an isometry between (R^n, d_{hom}) and $(\mathbf{F}_q^{q^d n}, d_H)$, where d_{hom} is the homogeneous distance on R^n and d_H is the Hamming distance on $\mathbf{F}_q^{q^d n}$. Therefore, applying the Gray map to the code in Theorem 3.2, we obtain

Corollary 3.3 *The Gray image $\phi(C_s)$ of C_s is a q -ary code of length $q^{(d-1)s}(q^s - 1)/(q-1)$, with $q^{ds} - q^s$ codewords of (Hamming) weight $q^{(d-1)s-1}(q^s - 1)$, $q^s - 1$ codewords of (Hamming) weight q^{ds-1} and the zero-codeword.*

The Gray image $\phi(C_s)$ may or may not be linear, depending on the ring R . For example, when $R = \mathbf{F}_q[X]/(X^d) = \mathbf{F}_q + u\mathbf{F}_q + \cdots + u^{d-1}\mathbf{F}_q$, it is easy to see that $\phi(C_s)$ is linear, while for R equal to the Galois ring $GR(p^d, m)$ ($d > 1$), $\phi(C_s)$ is nonlinear.

Recall that the Griesmer bound says that: if there exists a q -ary linear code of parameters $[N, K, D]$, then the inequality $N \geq \sum_{i=0}^K \lceil D/q^i \rceil$ holds. Using, for example, the Gray image $\phi(C_s)$ for $R = \mathbf{F}_q[X]/(X^d)$, it is easy to see that the following proposition is true.

Proposition 3.4 *When the Gray image $\phi(C_s)$ is linear, it meets the Griesmer bound and is hence an optimal linear code.*

4 Weight and characters

We saw in Lemma 2.1 that a finite chain ring R admits an additive character ψ such that the restriction of ψ to the ideal (π^i) is not the trivial character for all $0 \leq i \leq d-1$. We first prove the following generalization of [8, Theorem 2.1] from Galois rings to finite chain rings.

Theorem 4.1 *Let R be a finite chain ring and let ψ be an additive character of R satisfying Lemma 2.1. For any $x \in R$, the homogeneous weight of x can be written as*

$$wt_{\text{hom}}(x) = (q-1)q^{d-2} - \frac{1}{q} \sum_{a \in R \setminus (\pi)} \psi(ax). \quad (2)$$

Proof. We consider three distinct cases.

Case 1: $x = 0$

When $x = 0$, then $\psi(ax) = 1$ for all $a \in R \setminus (\pi)$. Therefore, the right hand side of (2) becomes

$$(q-1)q^{d-2} - \frac{1}{q}(q^d - q^{d-1}) = 0,$$

which is exactly the homogeneous weight of 0.

Case 2: $x \notin (\pi^{d-1})$

Suppose that $x \in (\pi^i) \setminus (\pi^{i+1})$, where $0 \leq i \leq d-2$. Write $x = \pi^i y$, for some unit y of R . Since a is a unit in R , ay is again a unit, so $ax \in (\pi^i) \setminus (\pi^{i+1})$ again. Moreover, as a runs through the units of R , ax runs through each element of $(\pi^i) \setminus (\pi^{i+1})$ exactly q^i times.

Since $0 \leq i \leq d-2$, the restrictions of ψ to (π^i) and (π^{i+1}) are not the trivial characters. Therefore,

$$\sum_{z \in (\pi^i)} \psi(z) = 0 = \sum_{z \in (\pi^{i+1})} \psi(z)$$

by the orthogonality relations of characters.

In particular, $\sum_{a \in R \setminus (\pi)} \psi(ax) = 0$. Hence, it follows that the right hand side of (2) is equal to $(q-1)q^{d-2}$, which is again exactly the homogeneous weight of x .

Case 3: $x \in (\pi^{d-1}) \setminus \{0\}$

The argument at the beginning of Case 2 still holds, except that now we have

$$\sum_{z \in (\pi^d)} \psi(z) = \psi(0) = 1.$$

It then follows that the right hand side of (2) becomes

$$(q-1)q^{d-2} - \frac{1}{q}q^{d-1} \left(\sum_{z \in (\pi^{d-1})} \psi(z) - \sum_{z \in (\pi^d)} \psi(z) \right) = (q-1)q^{d-2} - q^{d-2}(-1) = q^{d-1},$$

which is again the homogeneous weight of x . \square

Let $K(N, Q, w) := N(Q-1) - Qw$ denote the first order Krawtchouk polynomial attached to the Hamming scheme $H(N, Q)$ [1]. We can now derive the following suggestive corollary.

Corollary 4.2 For all $\mathbf{x} = (x_1, \dots, x_n) \in R^n$, we have that

$$K(nq^{d-1}, q, wt_{\text{hom}}(\mathbf{x})) = \sum_{i=1}^n \sum_{a \in R \setminus (\pi)} \psi(ax_i).$$

5 Strongly regular graphs

An undirected graph on v vertices is **strongly regular** with parameters (v, k, λ, μ) if:

1. it is k -regular; and
2. any pair of adjacent (resp. non-adjacent) vertices admit λ (resp. μ) common neighbors.

Strongly regular graphs (SRG) with parameters (v, k, λ, μ) are known to be equivalent to reversible **partial difference sets** (PDS)[6]. More precisely, a PDS D on a group G is equivalent to an SRG on the Cayley graph of G with the generating set D and the same set of 4 parameters.

Let C denote a code of length n over R , defined by a parity-check matrix H , that is $C = \text{Ker}(H)$. The **syndrome space** of C is defined as $S(C) := HR^n$. Introduce the **syndrome graph** $\Gamma(C)$ of C as the Cayley graph on the additive group of $S(C)$, with generating set

$$D := \{aH\mathbf{e}_i \mid i = 1, \dots, n, a \in R \setminus (\pi)\},$$

where $\mathbf{e}_i = (\delta_{i,j})_j$.

Lemma 5.1 Let ψ be an additive character of R satisfying Lemma 2.1. The eigenvalues of the adjacency matrix of $\Gamma(C)$ are, accounted with their multiplicities, the complex numbers

$$\Lambda_{\mathbf{x}} := \sum_{i=1}^n \sum_{a \in R \setminus (\pi)} \psi(ax_i),$$

for $\mathbf{x} = (x_1, \dots, x_n)$ ranging over C^\perp . Equivalently ,

$$\Lambda_{\mathbf{x}} = K(nq^{d-1}, q, wt_{\text{hom}}(\mathbf{x})).$$

Proof. Let f denote a complex-valued function defined on $S(C)$. Then f is an eigenfunction attached to the eigenvalue Λ if and only if, for all $\mathbf{z} \in S(C)$, we have that

$$\sum_{\mathbf{y} - \mathbf{z} \in D} f(\mathbf{y}) = \Lambda f(\mathbf{z}).$$

We claim that, for all $\mathbf{x} = \mathbf{u}H$ in C^\perp , the function $f_{\mathbf{x}}(\mathbf{y}) := \psi(\mathbf{u} \cdot \mathbf{y})$ is an eigenfunction attached to $\Lambda_{\mathbf{x}}$. Indeed, by the definition of group characters,

$$\sum_{\mathbf{h} \in D} \psi(\mathbf{u} \cdot (\mathbf{z} + \mathbf{h})) = \psi(\mathbf{u} \cdot \mathbf{z}) \sum_{\mathbf{h} \in D} \psi(\mathbf{u} \cdot \mathbf{h}).$$

The first assertion follows then upon observing that

$$\mathbf{u} \cdot aH\mathbf{e}_i = ax_i.$$

The second assertion follows by Corollary 4.2. \square

The main result of this section is the following.

Theorem 5.2 *If C is a two-weight code over R , then $\Gamma(C)$ is a strongly regular graph. Equivalently, $S(C)$ is a reversible partial difference set in the additive group of $S(C)$.*

Proof. A graph is strongly regular if and only if the spectrum of its adjacency matrix contains three distinct eigenvalues [3, Chapter 10, Lemma 1.5]. The result follows then by the preceding Lemma and the hypothesis on the number of weights. \square

The parameters (v, k, λ, μ) can be computed as a function of the two non-trivial eigenvalues by using [3, Chap. 10, Lemma 1.4] or [2, Lemma A].

Example: The graph $\Gamma(C_s^\perp)$ attached to the dual of the generalized Camion code defined in §3 contains q^{ds} vertices. It is regular of degree $q^{s(d-1)}(q^s - 1)$. Its non-trivial eigenvalues are

$$\begin{array}{ll} 0 & \text{with multiplicity } q^{ds} - q^s, \\ -q^{s(d-1)} & \text{with multiplicity } q^s - 1. \end{array}$$

Unfortunately, we see from [3, eq. (3), p.179] that $\mu = k$, a degenerate case for SRG's, and also for PDS (see [6, Proposition 1.5]).

6 Conclusion and Open Problems

In this short paper, we have constructed an infinite family of two-weight codes for the Hamming metric. While being very good codes (meeting the Griesmer bound), they only yield trivial (in the sense of [3]) strongly regular graphs. It would, therefore, be of interest to find examples of two-weight codes for the homogeneous weight attached to non-trivial SRG's.

At the level of rings, extending the above results (including the Gray map of [4]) to the level of quasi-Frobenius finite rings, where a similar character theory exists (as in [9]), would be of great interest.

Another open question, more concerned with association schemes, would be to determine if these two-weight codes are subschemes of the ambient Hamming scheme. The method of [1] fails in the absence of a formal duality in the generalized Gray map of [4].

References

- [1] P. Camion, *Codes and association schemes: Basic properties of association schemes relevant to coding theory*, in *Handbook of Coding Theory, Volume II*, V.S. Pless & W.C. Huffman eds., Elsevier, 1998, pp. 1441–1566

- [2] Y. Chen, D.K. Ray-Chaudhuri & Q. Xiang, *Construction of partial difference sets and relative difference sets using Galois rings II*, J. Combinatorial Th. A **76** (1996), 179–196.
- [3] C. Godsil, *Algebraic Combinatorics*, Chapman and Hall (1993).
- [4] M. Greferath & S.E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code*, IEEE Trans. Inform. Theory **45** (1999), 2522–2524
- [5] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane & P. Solé, *The \mathbf{Z}_4 -linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319
- [6] S.L. Ma, *A survey of partial difference sets*, Designs, Codes, and Cryptography **4** (1994), 221–261
- [7] D.K. Ray-Chaudhuri & Q. Xiang, *Construction of partial difference sets and relative difference sets using Galois rings*, Designs, Codes and Cryptography **8** (1996), 215–227
- [8] J.F. Voloch & J.L. Walker, *Homogeneous weights and exponential sums*, preprint 2001.
- [9] J.A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), 555–575