Linear Codes over Finite Chain Rings

Thomas Honold
Zentrum Mathematik
Technische Universität München
D-80290 München, Germany
honold@ma.tum.de

Ivan Landjev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 Acad. G. Bonchev str.
1113 Sofia, Bulgaria
ivan@moi.math.bas.bg

Submitted: December 20, 1998; Accepted: December 18, 1999

AMS Subject Classification: Primary 94B27; Secondary 94B05, 51E22, 20K01.

Abstract

The aim of this paper is to develop a theory of linear codes over finite chain rings from a geometric viewpoint. Generalizing a well-known result for linear codes over fields, we prove that there exists a one-to-one correspondence between so-called fat linear codes over chain rings and multisets of points in projective Hjelmslev geometries, in the sense that semilinearly isomorphic codes correspond to equivalent multisets and vice versa. Using a selected class of multisets we show that certain MacDonald codes are linearly representable over nontrivial chain rings.

1 Introduction

In the past decade, a substantial research has been done on linear codes over finite rings. Traditionally authors used to focus their research on codes over integer residue rings, especially $\mathbb{Z}_4$. Nowadays quite a few papers are concerned with linear codes over other classes of rings (cf. e. g. [2, 7, 11, 12, 16, 17, 21, 24, 42, 43, 44, 50]).

The aim of this paper is to develop the fundamentals of the theory of linear codes over the class of finite chain rings. There are several reasons for choosing this class of rings. First of all, it contains rings, whose properties lie closest to the properties of finite fields. Hence a theory of linear codes over finite chain rings is expected to resemble the theory of linear codes over finite fields. Secondly, the class of finite chain rings contains important representatives like integer residue rings of prime power order and Galois rings. Codes over such rings appeared in various contexts in recent coding theory research. In third place, nontrivial linear codes over finite chain rings can be considered as multisets of points in finite projective Hjelmslev geometries thus extending the familiar interpretation of linear codes over finite fields as multisets of points in classical projective geometries $\mathrm{PG}(k,q)$ [10]. However, there are some differences between linear codes over finite fields and linear codes over finite chain rings. For instance, as a consequence of the existence of noncommutative finite chain rings, one is forced to distinguish between left and right linear codes, between the left and right orthogonal of a given code etc.

In Sect. 2 we give some basic results on finite modules over chain rings. In Sect. 3, we define the notion of a linear code over a finite chain ring R, along with some basic concepts like orthogonal code, code automorphism etc. We introduce regular partitions of R^n and prove MacWilliams-type identities for the spectra of linear codes w. r. t. such partitions. Section 4 contains a brief introduction to projective Hjelmslev geometries. In Sect. 5, we prove that there is a one-to-one correspondence between equivalence classes of so-called fat left linear codes over a chain ring and equivalence classes of multisets of points in right projective Hjelmslev geometries over the same ring. In Sect. 6, we investigate codes which belong to a selected class of multisets. We obtain chain ring analogues of the Simplex and Hamming codes and—as q-ary images with respect to a generalized Gray map—codes with the same parameters as the MacDonald codes.

An outline of some of the results of this paper appeared in [20].

2 Basic Facts on Finite Modules over Chain Rings

A ring[1] is called a left (right) chain ring if its lattice of left (right) ideals forms a chain. The following result describes some properties of finite left chain rings (see e. g. [8, 38, 40]).

Theorem 2.1. *For a finite ring R with radical $N \neq 0$ the following conditions are equivalent:*

(i) R is a left chain ring;

(ii) the principal left ideals of R form a chain;

[1]By the term 'ring' we always mean an associative ring with identity $1 \neq 0$; ring homomorphisms are assumed to preserve the identity.

(iii) R is a local ring, and $N = R\theta$ for any $\theta \in N \setminus N^2$;

(iv) R is a right chain ring.

Moreover, if R satisfies the above conditions, then every proper left (right) ideal of R has the form $N^i = R\theta^i = \theta^i R$ for some positive integer i.

In the sequel, we shall use the term *chain ring* to denote a finite left (and thus right) chain ring. We shall always assume that for a chain ring R the letters N, θ have the same meaning as in Th. 2.1. In addition we denote by $q = p^r$ the cardinality of the finite field R/N (thus $R/N \cong \mathbb{F}_q$) and by m the index of nilpotency of N. Since for $0 \le i \le m-1$ the module N^i/N^{i+1} is a vector space of dimension 1 over R/N, we have $|N^i/N^{i+1}| = q$ for $0 \le i \le m-1$, and in particular $|R| = q^m$.

The structure of chain rings can be very complicated, but the following two special cases are worth to note: (i) If R has characteristic p then $R \cong \mathbb{F}_q[X;\sigma]/(X^m)$ for some $\sigma \in \operatorname{Aut}\mathbb{F}_q$, i. e. R is a truncated skew polynomial ring, and (ii) if R has (maximal) characteristic p^m then $R \cong \mathrm{GR}(q^m, p^m)$ is a Galois ring; cf. [25, 38, 45]. Thus the smallest noncommutative chain ring has cardinality 16. It may be represented as $R = \mathbb{F}_4 \oplus \mathbb{F}_4$ with operations $(a,b)+(c,d) = (a+c, b+d)$, $(a,b)\cdot(c,d) = (ac, ad+bc^2)$.[2]

The *upper Loewy series* of a left R-module ${}_RM$ is the chain

$$M = \theta^0 M \supseteq \theta^1 M \supseteq \cdots \supseteq \theta^{m-1} M \supseteq \theta^m M = 0 \tag{1}$$

of submodules $\theta^i M = N^i M \le {}_RM$. Every quotient $\theta^{i-1}M/\theta^i M$ $(i \ge 1)$ is a vector space over the field $R/N \cong \mathbb{F}_q$. Similarly, the *lower Loewy series* of ${}_RM$ is the chain

$$M = M[\theta^m] \supseteq \cdots \supseteq M[\theta^2] \supseteq M[\theta] \supseteq M[1] = 0 \tag{2}$$

of submodules $M[\theta^i] = \{x \in M \mid \theta^i x = 0\}$. Again every quotient $M[\theta^i]/M[\theta^{i-1}]$ is a vector space over $R/N \cong \mathbb{F}_q$. We say that θ^i is the *period* of $x \in M$ if i is the smallest nonnegative integer such that $\theta^i x = 0$, and we write $M^* = \big\{x \in M \mid x \text{ has period } \theta^m\big\}$. Similarly, the *height* of x is the largest integer $i \le m$ such that $x \in \theta^i M$. If x has height i we write $\theta^i \parallel x$.

For $i \in \mathbb{N}$ let $\mu_i = \dim_{R/N}(\theta^{i-1}M/\theta^i M)$. Multiplication by θ (i. e. the map $M \to M$, $x \to \theta x$) induces additive isomorphisms

$$\theta^{i-1}M/\big(M[\theta] + \theta^i M\big) \cong \theta^i M/\theta^{i+1}M. \tag{3}$$

Thus we have $\log_q|M| = \mu_1 + \mu_2 + \cdots + \mu_m$ with $\mu_i \ge \mu_{i+1}$, i. e. $\mu = (\mu_1, \mu_2, \ldots)$ is a partition of $\log_q|M|$ (into at most m parts) which we abbreviate as $\mu \vdash \log_q|M|$. In the sequel we shall write $\mu = (\mu_1, \ldots, \mu_r)$ if $\mu_i = 0$ for $i > r$ and sometimes $\mu = 1^{s_1}2^{s_2}3^{s_3}\cdots$ if exactly s_j parts of μ are equal to j.

[2]This example is due to Kleinfeld [26].

The following theorem generalizes the structure theorem for finite $\mathbb{Z}/p^m\mathbb{Z}$-modules or equivalently, finite Abelian p-groups of exponent not exceeding p^m, to the case of an arbitrary finite chain ring R.[3]

Theorem 2.2. *Every finite module ${}_RM$ over a chain ring R is a direct sum of cyclic R-modules. The partition $\lambda = (\lambda_1, \ldots, \lambda_r) \vdash \log_q|M|$ satisfying*

$$ {}_RM \cong R/N^{\lambda_1} \oplus \cdots \oplus R/N^{\lambda_r} \tag{4}$$

is uniquely determined by ${}_RM$. More precisely, $\lambda = \mu'$ is conjugate to the partition $\mu = (\mu_1, \mu_2, \ldots) \vdash \log_q|M|$ defined by $\mu_i = \dim \theta^{i-1}M/\theta^i M$.

Definition 2.1. The partitions λ, μ defined in Th. 2.2 are called the *shape* resp. *conjugate shape* of ${}_RM$. The integer $\lambda'_1 = \mu_1 = \dim_{R/N}(M/\theta M) = \dim_{R/N} M[\theta]$ is called the *rank* of ${}_RM$ and denoted by $\operatorname{rk} M$.

Theorem 2.2 implies that any finite module ${}_RM$ and its dual $\operatorname{Hom}({}_RM, {}_RR)_R$ have the same shape.

A sequence $x_1, \ldots, x_r$ of elements of ${}_RM$ is said to be *independent* (resp., *linearly independent*) if $a_1x_1 + \cdots + a_rx_r = 0$ with $a_j \in R$ implies $a_jx_j = 0$ (resp., $a_j = 0$) for every j. A *basis* of ${}_RM$ is an independent set of generators which does not contain 0. By Th. 2.2 the cardinality of any basis of ${}_RM$ is equal to $k = \operatorname{rk} M$, and the periods of its elements are $\theta^{\lambda_1}, \ldots, \theta^{\lambda_k}$ in some order. Note that ${}_RM$ is a free module if and only if ${}_RM$ has shape m^k.

Recall that a module ${}_RM$ is projective (resp., injective) if ${}_RM$ is a direct summand of a free module (resp., a direct summand of every module containing ${}_RM$).

Theorem 2.3. *For a finite module ${}_RM$ over a chain ring R the following properties are equivalent:*

(i) ${}_RM$ is free;

(ii) ${}_RM$ is projective;

(iii) ${}_RM$ is injective;

(iv) There exists $i \in \{1, 2, \ldots, m-1\}$ such that $M[\theta^i] = \theta^{m-i}M$.

Proof. Since R is local, (i) and (ii) are equivalent. The equivalence of (ii) and (iii) is due to the fact that R is a quasi-Frobenius ring; cf. [9, §58]. Clearly (i) implies $M[\theta^i] = \theta^{m-i}M$ for $0 \le i \le m$ and thus in particular (iv). Conversely, suppose that (iv) holds. The R-module $M[\theta^i]$ has conjugate shape $(\lambda'_1, \ldots, \lambda'_i)$ while $\theta^{m-i}M$ has conjugate shape $(\lambda'_{m-i+1}, \ldots, \lambda'_m)$. Since both modules are equal and $m - i \ge 1$, we have $\lambda'_s = \lambda'_{m-i+s} \le \lambda'_{s+1}$ for $1 \le s \le i-1$ and hence $\lambda'_1 = \lambda'_2 = \cdots = \lambda'_i = \lambda'_m$. □

[3]The proof in [35, Ch. 15, § 2] is easily adapted to the present situation. Theorem 2.2 holds, more generally, for matrix rings over finite chain rings—one only has to replace ${}_RR$ by its unique indecomposable direct summand; cf. [1, 15, 28].

For partitions λ, μ with $\mu \leq \lambda$ define

$$\alpha_\lambda(\mu; x) = \prod_{j \geq 1} x^{\mu'_{j+1}(\lambda'_j - \mu'_j)} \cdot \begin{bmatrix} \lambda'_j - \mu'_{j+1} \\ \mu'_j - \mu'_{j+1} \end{bmatrix}_x \tag{5}$$

where $\begin{bmatrix} n \\ k \end{bmatrix}_x = \prod_{s=1}^{k} \frac{x^{n-s+1}-1}{x^s-1}$ denotes a Gaussian polynomial.

Theorem 2.4. *Let R be a finite chain ring with residue field of order q, and let ${}_RM$ be a finite R-module of shape λ. For every partition μ satisfying $\mu \subseteq \lambda$ the module ${}_RM$ has exactly $\alpha_\lambda(\mu; q)$ submodules of shape μ. In particular, the number of free rank 1 submodules of ${}_RM$ equals*

$$q^{\lambda'_1 - 1 + \lambda'_2 - 1 + \cdots + \lambda'_{m-1} - 1} \cdot \begin{bmatrix} \lambda'_m \\ 1 \end{bmatrix}_q . \tag{6}$$

Proof. The theorem is well-known in the special case $R = \mathbb{Z}_{p^m}$, cf. e. g. [6]. The general case follows from the results in [36, Ch. II] which remain valid for arbitrary (even noncommutative) chain rings. $\square$

Theorem 2.5. *Let ${}_RH$ be a free module of rank n over the chain ring R, and let ${}_RM$ be a submodule of ${}_RH$ of shape λ and rank $\lambda'_1 = k$.*

(i) For every basis $x_1, \dots, x_k$ of M there exists a basis $y_1, \dots, y_n$ of H such that $x_j \in Ry_j$ for $1 \leq j \leq k$.

(ii) The quotient module H/M has shape $(m - \lambda_n, m - \lambda_{n-1}, \dots, m - \lambda_1)$ and conjugate shape $(n - \lambda'_m, n - \lambda'_{m-1}, \dots, n - \lambda'_1)$. In particular, M is free if and only if H/M is free if and only if $\mathrm{rk}(H/M) = n - k$.

(iii) If $M^* \neq \emptyset$ (e. g. $\lambda_1 = m$) then M is the sum of its free rank 1 submodules.

(iv) Dually, if $(H/M)^* \neq \emptyset$ (e. g. $k < n$) then M is the intersection of the free rank $n - 1$ submodules of ${}_RH$ containing M.

Proof. Let $\{x_1, \dots, x_k\}$ be a basis of M. We may assume the ordering is such that x_j has period θ^{λ_j}. Since $H[\theta^i] = \theta^{m-i}H$ $(0 \leq i \leq m)$, there exist $y_1, \dots, y_k \in H^*$ such that $x_j = \theta^{m-\lambda_j} y_j$ $(1 \leq j \leq k)$. The sequence $y_1, \dots, y_k$ is linearly independent. By Th. 2.3, it can be extended to a (free) basis $y_1, \dots, y_n$ of H proving (i). The isomorphism $H/M \cong \bigoplus_{j=1}^{n} R/N^{m-\lambda_j}$ then gives (ii). If $z \in M^*$ and $x_j \notin M^*$ then $z + x_j \in M^*$ and $x_j = (z + x_j) - z$, whence (iii) holds. Finally, if $z \notin M$ but $z \in Ry_1 + \cdots + Ry_{n-1}$ we have $z = r_1 y_1 + \cdots + r_{n-1} y_{n-1}$ with r_j not divisible by $\theta^{m-\lambda_j}$, say. Let $y'_j = y_j + \theta^{\lambda_j} y_n$, $y'_t = y_t$ if $t \neq j$. The free rank $n - 1$ module $H' = Ry'_1 + \cdots + ry'_{n-1}$ contains M since $\theta^{m-\lambda_j} y'_j = \theta^{m-\lambda_j} y_j = x_j$. But $z = r_1 y'_1 + \cdots + r_{n-1} y'_{n-1} - r_j \theta^{\lambda_j} y_n \notin M$, proving (iv). $\square$

Recall that a mapping $\phi\colon {}_RM \to {}_RM'$ is *semilinear* if there exists a ring homomorphism $\sigma\colon R \to R$ such that $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(rx) = \sigma(r)\phi(x)$ for $x, y \in M$, $r \in R$. If ϕ is an isomorphism (i. e. The set of all semilinear isomorphisms (i. e. bijective semilinear mappings) $\phi\colon {}_RM \to {}_RM$ is denoted by $\Gamma\mathrm{L}({}_RM)$.

By Th. 2.3 the injective envelope of a finite module ${}_RM$ (cf. [9, §17]) can be characterized as a minimal free module ${}_RH$ containing ${}_RM$. To be precise, we require the existence of an R-linear embedding (injective map) $\iota\colon {}_RM \to {}_RH$ such that no proper free submodule of ${}_RH$ contains $\iota(M)$. The minimality of ${}_RH$ is equivalent to $\operatorname{rk} H = \operatorname{rk} M$.

Theorem 2.6. *Let ${}_RM$ be a finite module with $M^* \neq \emptyset$ and ${}_RH$ a minimal free module containg ${}_RM$.*

(i) Any semilinear embedding of ${}_RM$ into a free module ${}_RF$ can be extended to a semilinear embedding of ${}_RH$ into ${}_RF$.

(ii) If $\phi\colon {}_RM \to {}_RM'$ is a semilinear isomorphism and ${}_RH'$ a minimal free module containing ${}_RM'$, then there exists a semilinear isomorphism $\widetilde{\phi}\colon {}_RH \to {}_RH'$ which extends ϕ.

Proof. Given an R-semilinear map $\phi\colon {}_RM \to {}_RF$ with associated ring homomorphism σ, define a new operation of R on F by $rx := \sigma(r)x$, and denote the resulting module by ${}_RF^\sigma$. Then $\phi\colon {}_RM \to {}_RF^\sigma$ is linear. Since $M^* \neq \emptyset$ and ϕ is an embedding, we have $\sigma \in \operatorname{Aut} R$. Hence ${}_RF^\sigma$ is free, and (i) reduces to a well-known property of the injective envelope of an R-module. Assertion (ii) follows from (i). $\square$

3 Linear Codes over Finite Chain Rings

In this section, we introduce the basic notions of the theory of linear codes over finite chain rings. With respect to component-wise addition and left/right multiplication, the set R^n all n-tuples over R has the structure of an (R, R)-bimodule.

Definition 3.1. A *code $\mathcal{C}$ of length n over R* is a nonempty subset of R^n. The vectors of $\mathcal{C}$ are called *codewords*. The code $\mathcal{C}$ is *left* (resp., *right*) *linear* if it is an R-submodule of ${}_RR^n$ (resp., of R^n_R). A *linear* code is one which is either left or right linear.

In places where this sounds ambiguous we make it precise by writing e. g. $\mathcal{C} \leq {}_RR^n$ if $\mathcal{C}$ is left linear. We formulate our results with a bias towards left modules, omitting obvious right module counterparts.

By Th. 2.1 the periods of $\mathbf{x} = (x_1, \ldots, x_n) \in R^n$ in ${}_RR^n$ and R^n_R coincide, whence the sets $\mathcal{C}[\theta^i]$ in the lower Loewy series (2) of a linear code $\mathcal{C}$ are defined unambiguously even for *bicodes*, i. e. bimodules $\mathcal{C} \leq {}_RR^n{}_R$. The same holds a forteriori for the shape of $\mathcal{C}$.

For two vectors $\mathbf{u} = (u_1, \ldots, u_n) \in R^n$ and $\mathbf{v} = (v_1, \ldots, v_n) \in R^n$ we define their inner product $\mathbf{u} \cdot \mathbf{v}$ by

$$\mathbf{u} \cdot \mathbf{v} := u_1 v_1 + u_2 v_2 + \cdots + u_n v_n. \tag{7}$$

Sending each $\mathbf{v} \in R^n$ to the R-linear mapping $\Phi_r(\mathbf{v})\colon {}_RR^n \to {}_RR$, $\mathbf{u} \to \mathbf{u} \cdot \mathbf{v}$ defines an R-isomorphism $R^n_R \cong \mathrm{Hom}({}_RR^n, {}_RR)_R$.

For a code $\mathcal{C} \subseteq {}_RR^n$ we define

$$\begin{aligned} \mathcal{C}^\perp &= \{\mathbf{y} \in R^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ for every } \mathbf{x} \in \mathcal{C}\} \\ {}^\perp\mathcal{C} &= \{\mathbf{y} \in R^n \mid \mathbf{y} \cdot \mathbf{x} = 0 \text{ for every } \mathbf{x} \in \mathcal{C}\}. \end{aligned} \tag{8}$$

The linear code $\mathcal{C}^\perp \leq R^n_R$ (resp., ${}^\perp\mathcal{C} \leq {}_RR^n$) is called the *right* (resp., *left*) *orthogonal code* of $\mathcal{C}$.

Theorem 3.1. *Let $\mathcal{C}, \mathcal{C}' \leq {}_RR^n$ be left linear codes over R. Further, let $\mathcal{C}$ be of shape $\lambda = (\lambda_1, \ldots, \lambda_n)$ and rank $\lambda'_1 = k$. Then*

(i) $\mathcal{C}^\perp$ has shape $(m - \lambda_n, m - \lambda_{n-1}, \ldots, m - \lambda_1)$ and conjugate shape $(n - \lambda'_m, n - \lambda'_{m-1}, \ldots, n - \lambda'_1)$. In particular, $\mathcal{C}$ is free as an R-module if and only if $C^\perp$ is free if and only if $\mathrm{rk}(C^\perp) = n - k$.

(ii) ${}^\perp(\mathcal{C}^\perp) = \mathcal{C}$;

(iii) the map Φ_r induces an isomorphism $R^n_R/\mathcal{C}^\perp \cong \mathrm{Hom}({}_R\mathcal{C}, {}_RR)_R$;

(iv) $(\mathcal{C} \cap \mathcal{C}')^\perp = \mathcal{C}^\perp + \mathcal{C}'^\perp$, $(\mathcal{C} + \mathcal{C}')^\perp = \mathcal{C}^\perp \cap \mathcal{C}'^\perp$.

Proof. We prove (iii) first. Restricting $\Phi_r(\mathbf{y})$ to the code $\mathcal{C}$ induces an isomorphism from $R^n_R/\mathcal{C}^\perp$ onto a submodule W of $\mathrm{Hom}({}_R\mathcal{C}, {}_RR)_R$. Since ${}_RR$ is injective, every $\phi \in \mathrm{Hom}({}_R\mathcal{C}, {}_RR)$ can be extended to $\widetilde{\phi} \in \mathrm{Hom}({}_RR^n, {}_RR)$, whence $\widetilde{\phi} = \Phi_r(\mathbf{y})$ for some $\mathbf{y} \in R^n$. This implies $W = \mathrm{Hom}({}_R\mathcal{C}, {}_RR)$ proving (iii).

Since $\mathrm{Hom}({}_R\mathcal{C}, {}_RR)_R$ has shape equal to that of ${}_R\mathcal{C}$, assertion (i) follows from the isomorphism in (iii) and Th. 2.5.(ii). Assertions (ii) and (iv) hold for any quasi-Frobenius ring; cf. [9, §58], [18]. □

Theorem 3.1 shows in particular that $\mathcal{C} \mapsto \mathcal{C}^\perp$ defines an antiisomorphism between the lattices of left resp., right linear codes of length n over R.

Definition 3.2 (cf. [34]). A family $\mathcal{S} = (S_i \mid i \in I)$ of nonempty subsets of R^n is called a *regular partition of* R^n if the following conditions are satisfied:

(i) $R^n = \bigcup_{i \in I} S_j$;

(ii) $S_i \cap S_j = \emptyset$ for all pairs $i \neq j$;

(iii) for any two elements $i, j \in I$ and any $\alpha \in R$ there exist constants $\lambda_{ij}^{\alpha}, \rho_{ij}^{\alpha}$ such that for each $\mathbf{x} \in S_i$ there are exactly λ_{ij}^{α} elements $\mathbf{y} \in S_j$ with $\mathbf{x} \cdot \mathbf{y} = \alpha$, and for each $\mathbf{y} \in S_j$ exactly ρ_{ij}^{α} elements $\mathbf{x} \in S_i$ with $\mathbf{x} \cdot \mathbf{y} = \alpha$.

If $\mathbf{x} \in S_i$ we say that $\mathbf{x}$ has *$\mathcal{S}$-type i*. We call a permutation $\phi \in \mathrm{Sym}(R^n)$ an *$\mathcal{S}$-automorphism of R^n* if $\mathbf{x} - \mathbf{y} \in S_i$ implies $\phi(\mathbf{x}) - \phi(\mathbf{y}) \in S_i$ $(i \in I)$.

Regular partitions of R^n can be obtained as the set of orbits from certain subgroups G of $\Gamma\mathrm{L}({}_RR^n)$. Note that for every $\phi \in \Gamma\mathrm{L}({}_RR^n)$ there exist a uniquely determined ring automorphism $\sigma \in \mathrm{Aut}\, R$ and an invertible matrix $A \in \mathrm{GL}(n, R)$ such that

$$\phi(\mathbf{x}) = \sigma(\mathbf{x}) \cdot A \quad (\mathbf{x} \in R^n). \tag{9}$$

In Sections 5 and 6 the following special case will be important: The orbits of the group of all left semimonomial transformations of R^n, i. e. all maps $\phi \in \Gamma\mathrm{L}({}_RR^n)$ whose associated matrix A in (9) is monomial, form a regular partition. They are in one-to-one correspondence with the elements of the set I of $m + 1$-tuples $\mathbf{w} = (w_0, w_1, \ldots, w_m)$ of nonnegative integers satisfying $\sum_{i=0}^{m} w_i = n$. For $\mathbf{x} = (x_1, \ldots, x_n) \in R^n$ and $0 \leq i \leq m$ let

$$a_i(\mathbf{x}) = |\{j \mid 1 \leq j \leq n \text{ and } \theta^i \parallel x_j\}| \tag{10}$$

and define

$$S_{\mathbf{w}} = \bigl\{\mathbf{x} \in R^n \mid a_i(\mathbf{x}) = w_i \text{ for } 0 \leq i \leq m\bigr\} \qquad \bigl(\mathbf{w} \in I\bigr). \tag{11}$$

For brevity we omit the letter '$\mathcal{S}$' when referring to the special regular partition $\mathcal{S} = (S_{\mathbf{w}})_{\mathbf{w} \in I}$ defined in (11). Thus the sequence $\bigl(a_0(\mathbf{x}), \ldots, a_m(\mathbf{x})\bigr)$ is simply the *type* of the word $\mathbf{x}$, and a *(code) automorphism* of R^n is a permutation $\phi \in \mathrm{Sym}(R^n)$ satisfying $a_i(\mathbf{x} - \mathbf{y}) = a_i\bigl(\phi(\mathbf{x}) - \phi(\mathbf{y})\bigr)$ for $\mathbf{x}, \mathbf{y} \in R^n$, $0 \leq i \leq m$.

Definition 3.3. Two codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq R^n$ are said to be *isomorphic* (resp., *semilinearly isomorphic*) if there exists a code automorphism (resp., semilinear code automorphism) ϕ of R^n with $\phi(\mathcal{C}_1) = \mathcal{C}_2$.

Thus two linear codes $\mathcal{C}_1, \mathcal{C}_2 \leq {}_RR^n$ are semilinearly isomorphic if and only if there exists a left semimonomial transformation ϕ of R^n with $\phi(\mathcal{C}_1) = \mathcal{C}_2$.

In the sense of [50] the type of $\mathbf{x}$ is essentially the symmetrized weight composition of $\mathbf{x}$ with respect to the full group of units of R. A result in [48] implies that every semilinear permutation $\phi\colon \mathcal{C} \to \mathcal{C}$ of a linear code $\mathcal{C} \leq {}_RR^n$ which preserves the type of codewords $\mathbf{x} \in \mathcal{C}$ extends to a left semimonomial transformation of R^n. Extensions of this result to general weight functions on finite rings—with particular emphasis on the case of commutative chain rings—have been investigated in [51].

Given a code $\mathcal{C} \subseteq R^n$ and a regular partition $\mathcal{S} = (S_i \mid i \in I)$ of R^n we define integers A_i ($i \in I$) by $A_i = |\mathcal{C} \cap S_i|$. The family $(A_i)_{i\in I}$ is called the *$\mathcal{S}$-spectrum of $\mathcal{C}$*. We write $(B_i^{(s)})_{i\in I}$ for the $\mathcal{S}$-spectra of the codes

$$\mathcal{C}^{\perp}_{(s)} = \{\mathbf{y} \in R^n \mid \mathbf{x} \cdot \mathbf{y} \in N^s \text{ for every } \mathbf{x} \in \mathcal{C}\} \quad (0 \leq s \leq m)$$

and abbreviate $B_i^{(m)} = |\mathcal{C}^{\perp} \cap S_i|$ as B_i.

The $\mathcal{S}$-spectra of a linear code $\mathcal{C} \leq {}_R R^n$ and its dual codes $\mathcal{C}^{\perp}_{(s)}$ are related by identities which are similar to the MacWilliams identities (cf. [19] or [37]). In order to formulate this result, we define functions $\omega_s \colon R \to \mathbb{R}$, $0 \leq s \leq m$, by

$$\omega_s(x) = \begin{cases} 1 & \text{if } x \in N^s, \\ -1/(q-1) & \text{if } x \in N^{s-1} \setminus N^s, \\ 0 & \text{if } x \notin N^{s-1}. \end{cases} \tag{12}$$

These functions satisfy the following "orthogonality relations" for ideals A of R:

$$\frac{1}{|A|} \cdot \sum_{x\in A} \omega_s(x) = \begin{cases} 1 & \text{if } A \leq N^s, \\ 0 & \text{if } A \not\leq N^s. \end{cases} \tag{13}$$

Theorem 3.2 (MacWilliams identities). *Let $S = (S_i \mid i \in I)$ be a regular partition of R^n, and let $\mathcal{C} \leq {}_R R^n$ be a linear code. The $\mathcal{S}$-spectrum of the orthogonal codes $\mathcal{C}^{\perp}_{(s)}$ is obtained from the $\mathcal{S}$-spectrum of $\mathcal{C}$ by*

$$B_j^{(s)} = \frac{1}{|\mathcal{C}|} \cdot \sum_{i\in I} A_i \cdot \Big(\sum_{\alpha\in R} \lambda_{ij}^{\alpha} \cdot \omega_s(\alpha)\Big). \tag{14}$$

Proof. Using (13) we have

$$\sum_{\mathbf{x}\in\mathcal{C}} \omega_s(\mathbf{x}\cdot\mathbf{y}) = \begin{cases} |C| & \text{if } \mathbf{y} \in \mathcal{C}^{\perp}_{(s)}, \\ 0 & \text{if } \mathbf{y} \in R^n \setminus \mathcal{C}^{\perp}_{(s)}, \end{cases} \tag{15}$$

since the set $\{\mathbf{x}\cdot\mathbf{y} \mid \mathbf{x} \in \mathcal{C}\}$ is a left ideal of R which is contained in N^s if and only if $\mathbf{y} \in \mathcal{C}^{\perp}_{(s)}$. Thus

$$\begin{aligned} B_j^{(s)} &= |\mathcal{C}^{\perp}_{(s)} \cap S_j| \\ &= \frac{1}{|\mathcal{C}|} \cdot \sum_{\mathbf{y}\in S_j} \sum_{\mathbf{x}\in\mathcal{C}} \omega_s(\mathbf{x}\cdot\mathbf{y}) \\ &= \frac{1}{|\mathcal{C}|} \cdot \sum_{i\in I} \sum_{\mathbf{x}\in\mathcal{C}\cap S_i} \sum_{\mathbf{y}\in S_j} \omega_s(\mathbf{x}\cdot\mathbf{y}) \\ &= \frac{1}{|\mathcal{C}|} \cdot \sum_{i\in I} |\mathcal{C}\cap S_i| \cdot \Big(\sum_{\alpha\in R} \lambda_{ij}^{\alpha} \cdot \omega_s(\alpha)\Big) \\ &= \frac{1}{|\mathcal{C}|} \cdot \sum_{i\in I} A_i \cdot \Big(\sum_{\alpha\in R} \lambda_{ij}^{\alpha} \cdot \omega_s(\alpha)\Big). \end{aligned} \tag{16}$$

□

Regular partitions of R^n are Fourier-invariant partitions (F-partitions) of the abelian group $(R^n, +)$ in the sense of [13, 14]. The link is provided by an additive character $\psi\colon R \to \mathbb{C}$ satisfying $N^{m-1} \nsubseteq \ker\psi$. The pairing $R^n \times R^n \to \mathbb{C}$, $(\mathbf{x}, \mathbf{y}) \mapsto \psi(\mathbf{x} \cdot \mathbf{y})$ can be used to define a suitable Fourier transform $\mathcal{F}\colon \mathbb{C}R^n \to \mathbb{C}R^n$.

For the special case $R = \mathbb{F}_q$ of Th. 3.2 see [34]. MacWilliams identities for F-partitions are proved in [14]. Other types of MacWilliams identities for codes over finite rings can be found e. g. in [23, 27, 41, 50].

4 The projective Hjelmslev geometries $\mathrm{PHG}(R_R^k)$

In this section, we introduce the projective Hjelmslev geometries $\mathrm{PHG}(R_R^k)$ and give some results on their basic structure. For a rigorous approach to projective Hjelmslev spaces the reader is referred to [29, 30, 31, 47]. Consider a finite free right module H_R where R is a chain ring. The elements of $\mathcal{P} = \mathcal{P}(H_R) = \{xR \mid x \in H^*\}$ are called *points* of H_R, those of $\mathcal{L} = \mathcal{L}(H_R) = \bigl\{xR + yR \mid x, y \text{ linearly independent}\bigr\}$ are called *lines* of H_R. The incidence relation $I \subseteq \mathcal{P} \times \mathcal{L}$ is defined in a natural way by set-theoretical inclusion. As usual we identify lines with subsets of $\mathcal{P}$.[4] Note that any two different points are joined by at least one line.

Definition 4.1. The incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, I)$ together with the neighbour relation $\bigcirc$, defined by

(N1) the points X, Y are *neighbours* (notation $X \bigcirc Y$) if and only if there exist different lines $s, t \in \mathcal{L}$ with $X, Y \in s \cap t$;
(N2) the lines $s, t \in \mathcal{L}$ are *neighbours* if and only if for every point $X \in s$ there is a point $Y \in t$ with $X \bigcirc Y$ and, conversely, for every $Y \in t$ there is an $X \in s$ with $Y \bigcirc X$;

is called a *projective Hjelmslev space* and denoted by $\mathrm{PHG}(H_R)$.[5]

The relation $\bigcirc$ induces an equivalence relation on $\mathcal{P}$ as well as on $\mathcal{L}$. The class $[X]$ of all points which are neighbours to the point $X = xR$ consists of all free rank 1 submodules contained in $xR + H\theta$. Similarly, the class $[s]$ of all lines which are neighbours to $s = xR + yR$, consists of all free rank 2 submodules contained in $xR + yR + H\theta$.

The point set $\mathcal{T} \subseteq \mathcal{P}$ is called a *Hjelmslev subspace* of Π if for every two points $X, Y \in \mathcal{T}$, there exists a line $s \subseteq \mathcal{T}$ with $X, Y \in s$. We write $X \bigcirc \mathcal{T}$ if there exists a point $Y \in \mathcal{T}$ with $X \bigcirc Y$. Every Hjelmslev subspace is a projective Hjelmslev space

[4] A line $s \in \mathcal{L}$ is uniquely determined by $\{X \in \mathcal{P} \mid XIs\}$.

[5] If R is noncommutative, $\mathrm{PHG}(H_R)$ and $\mathrm{PHG}({}_RH)$ are in general not isomorphic. Working with right instead of left modules will be justified in Section 5.

and consists of the points contained in some free submodule of H_R.[6] For every $\mathcal{X} \subseteq \mathcal{P}$ we define the *closure* $\overline{\mathcal{X}}$ as the intersection of all Hjelmslev subspaces containing $\mathcal{X}$. The set $\mathcal{X} \subseteq \mathcal{P}$ is said to be *independent* if for any $X \in \mathcal{X}$ we have $X \not\subset \overline{\mathcal{X} \setminus \{X\}}$, and a *basis of* Π if $\mathcal{X}$ is independent and $\overline{\mathcal{X}} = \mathcal{P}$. The *dimension* of Π is defined as $\dim \Pi = |\mathcal{B}| - 1$ where $\mathcal{B}$ is any basis of Π. Equivalently, $\dim \Pi = \mathrm{rk}(H_R) - 1$.

An isomorphism between two projective Hjelmslev spaces $\Pi = \mathrm{PHG}(H_R)$ and $\Pi' = \mathrm{PHG}(H'_R)$ is a bijection $\beta\colon \mathcal{P} \to \mathcal{P}'$ which satisfies $\beta(\mathcal{L}) = \mathcal{L}'$. The spaces Π and Π' are isomorphic if and only if $\mathrm{rk}(H_R) = \mathrm{rk}(H'_R)$. Every semilinear isomorphism $\phi\colon H_R \to H'_R$ induces such an isomorphism since it maps $xR \in \mathcal{P}$ onto $\phi(xR) = \phi(x)R \in \mathcal{P}'$. The following theorems can be found in [30, 32]:

Theorem 4.1. *If* $\mathrm{rk}(H_R) = \mathrm{rk}(H'_R) \geq 3$ *then for any isomorphism* $\beta\colon \Pi \to \Pi'$ *there exists a semilinear isomorphism* $\phi\colon H_R \to H'_R$ *inducing* β.

Theorem 4.2. *Let* $\{P_1, P_2, \dots, P_{k+1}\} \subseteq \mathcal{P}$ *and* $\{Q_1, Q_2, \dots, Q_{k+1}\} \subseteq \mathcal{P}'$ *be subsets ("frames") such that any* k *of the points in each of the sets form a basis of* Π *resp.,* Π'. *Then there exists exactly one isomorphism* $\beta\colon \Pi \to \Pi'$ *with* $\beta(P_i) = Q_i$, $1 \leq i \leq k+1$.

Projective Hjelmslev spaces can be defined axiomatically as incidence structures $\pi = (\mathcal{P}, \mathcal{L}, I)$ with a neighbour relation $\bigcirc$ on $\mathcal{P}$ and on $\mathcal{L}$ which satisfy certain conditions. Without going into details we mention the following

Theorem 4.3 ([30, 33]). *For every projective Hjelmslev space* Π *of dimension at least 3, having on each line at least 5 points no two of which are neighbours, there exists a free module* H_R *over a chain ring* R *such that* $\mathrm{PHG}(H_R)$ *is isomorphic to* Π.

Remark 4.1. The incidence structure $(\mathcal{P}, \mathcal{L}, I)$ and Def. 4.1 make sense for an arbitrary finite module M_R which is not a priori a submodule of some finite free module. We can embed M_R into a finite free module H_R of rank $\mathrm{rk}(H_R) \geq \mathrm{rk}(M_R)$ and view $(\mathcal{P}, \mathcal{L}, I)$ as a substructure of the geometry $\mathrm{PHG}(H_R)$. By Th. 2.5.(iii) a submodule $M_R \leq H_R$ is determined by its set of points, and if $\mathrm{rk}(H_R) > \mathrm{rk}(M_R)$ then M is closed by Th. 2.5.(iv). According to Theorems 2.3, 2.6 and 4.1 two finite modules ${}_RM$ and ${}_RM'$ of rank at least 3 are semilinearly isomorphic if and only if they are isomorphic as substructures of $\mathrm{PHG}(H_R)$ and $\mathrm{PHG}(H'_R)$, respectively, assuming of course that $\mathrm{rk}(H_R) = \mathrm{rk}(H'_R)$. Thus both viewpoints are essentially equivalent.

For simplicity we take $H_R = R_R^k$ in the sequel. The incidence structure $\mathrm{PHG}(R_R^k)$ is called the (right) $k-1$-dimensional projective Hjelmslev geometry over R.

We shall need the following refinement of the neighbour relation:

Definition 4.2. Let Δ_1, Δ_2 be Hjelmslev subspaces of $\mathrm{PHG}(R_R^k)$ and $0 \leq i \leq m$. We say that Δ_1 *is an i-neighbour to* Δ_2, and write $\Delta_1 \bigcirc_i \Delta_2$ in this case, if $\Delta_1 \subseteq \Delta_2 + R^k\theta^i$.

---

[6] Needless to say, we identify Hjelmslev subspaces of $\mathrm{PHG}(H_R)$ with the corresponding free submodules of H_R.

Denoting by $\pi^{(i)}\colon R^k \to R^k/R^k\theta^i$ the natural projection, we have $\Delta_1 \frown_i \Delta_2$ if and only if $\pi^{(i)}(\Delta_1) \subseteq \pi^{(i)}(\Delta_2)$. The relation $\frown_i$ induces an equivalence relation on Hjelmslev subspaces of equal dimension. The *i-neighbour class of* Δ is $[\Delta]_i = \{\Delta' \mid \dim \Delta' = \dim \Delta \text{ and } \Delta' \frown_i \Delta\}$.

For points $X = \mathbf{x}R$, $Y = \mathbf{y}R$ we have $X \frown_i Y$ but $X \not\frown_{i+1} Y$ if and only if $|X \cap Y| = q^i$ if and only if $\mathbf{x}R + \mathbf{y}R$ has shape $(m, m-i)$. The neighbour class $[X]_i$ coincides with the set of all free rank 1 submodules of $\mathbf{x}R + R^k\theta^i$. Similarly, for a line $s = \mathbf{x}R + \mathbf{y}R$ the neighbour class $[s]_i$ coincides with the set of all free rank 2 submodules of $\mathbf{x}R + \mathbf{y}R + R^k\theta^i$. Furthermore, lines s and t are *i-neighbours* if and only if for every $X \in s$ there is a point $Y \in t$ with $X \frown_i Y$ and, conversely, for every $Y \in t$ there is an $X \in s$ with $Y \frown_i X$. Clearly $\frown_1$ coincides on points and on lines with the neighbour relation $\frown$ introduced at the beginning of this section.

Let $\mathcal{P}^{(i)}$ (resp. $\mathcal{L}^{(i)}$) be the set of all i-neighbour classes of points (resp. of lines) in $(\mathcal{P}, \mathcal{L}, I)$.

Theorem 4.4. *The incidence structure* $\Pi^{(i)} = (\mathcal{P}^{(i)}, \mathcal{L}^{(i)}, I^{(i)})$ *with* $I^{(i)}$ *defined by*

$$[X]_i \, I^{(i)} \, [s]_i \iff \exists X' \in [X]_i, \exists s' \in [s]_i \ : \ X' \, I \, s' \tag{17}$$

is isomorphic to $\mathrm{PHG}\left((R^k/\theta^i R^k)_{R/N^i}\right)$ *for all* $i \in \{1, \dots, m\}$*. In particular,* $\Pi^{(1)}$ *is isomorphic to the projective geometry* $\mathrm{PG}(k-1, q)$.

Proof. The image under $\pi^{(i)}$ of every free submodule of R^k_R is a free module over R/N^i of the same rank. Hence, if we define $[X]_i I' [s]_i$ by $\pi^{(i)}(X) \subseteq \pi^{(i)}(s)$ then $(\mathcal{P}^{(i)}, \mathcal{L}^{(i)}, I')$ is isomorphic to $\mathrm{PHG}\left((R^k/\theta^i R^k)_{R/N^i}\right)$. Let $X = \mathbf{x}R \in \mathcal{P}$, $s = \mathbf{y}R + \mathbf{z}R \in \mathcal{L}$ with $\pi^{(i)}(X) \subseteq \pi^{(i)}(s)$, i.e. $\mathbf{x}R \subseteq \mathbf{y}R + \mathbf{z}R + R^k\theta^i$. Since $\mathbf{x}R$ is free and hence a direct summand of $\mathbf{y}R + \mathbf{z}R + R^k\theta^i$, it is contained in some free rank 2 submodule of $\mathbf{y}R + \mathbf{z}R + R^k\theta^i$. This gives $I' = I^{(i)}$ as desired. $\square$

5 Multisets in Projective Hjelmslev Geometries and Linear Codes over Chain Rings

Let $\Pi = \mathrm{PHG}(H_R) = (\mathcal{P}, \mathcal{L}, I)$ be a finite dimensional projective Hjelmslev geometry over the chain ring R.

Definition 5.1. A *multiset in* Π is a mapping $\mathfrak{k}\colon \mathcal{T} \to \mathbb{N}_0$ where $\mathcal{T} \subseteq \mathcal{P}$.[7]

Often we tacitly assume $\mathcal{T} = \mathcal{P}$, defining $\mathfrak{k}(P) = 0$ for $P \in \mathcal{P} \setminus \mathcal{T}$.

[7] A multiset $\mathfrak{k}\colon \mathcal{T} \to \mathbb{N}_0$ is called a *set* if $\mathfrak{k}(P) \in \{0, 1\}$ for any $P \in \mathcal{T}$.

The mapping $\mathfrak{k}$ is extended to the power set of $\mathcal{P}$ by

$$\mathfrak{k}(\mathcal{Q}) = \sum_{P\in\mathcal{Q}} \mathfrak{k}(P) \quad \text{for } \mathcal{Q} \subseteq \mathcal{P}. \tag{18}$$

The integer $\mathfrak{k}(P)$ is called the *multiplicity* of the point P. The integer $\mathfrak{k}(\mathcal{P}) = \sum_{P\in\mathcal{T}} \mathfrak{k}(P)$ is called the *cardinality* or *length* of the multiset $\mathfrak{k}$ and is denoted by $|\mathfrak{k}|$. The *support* of $\mathfrak{k}$ is defined as $\operatorname{Supp}\mathfrak{k} = \{P \in \mathcal{T} | \mathfrak{k}(P) > 0\}$ and the *hull* of $\mathfrak{k}$ as the module

$$\langle \mathfrak{k} \rangle = \sum_{\mathbf{x}R\in\operatorname{Supp}\mathfrak{k}} \mathbf{x}R \leq H_R. \tag{19}$$

The *shape of* $\mathfrak{k}$ is the shape of its hull $\langle \mathfrak{k} \rangle_R$.

Definition 5.2. Two multisets $\mathfrak{k}$ in Π and $\mathfrak{k}'$ in Π' are said to be *equivalent* if there exists a bijective R-semilinear mapping $\psi\colon \langle \mathfrak{k} \rangle \to \langle \mathfrak{k}' \rangle$ such that $\mathfrak{k}(P) = \mathfrak{k}'\big(\psi(P)\big)$ for every point $P = \mathbf{x}R \leq \langle \mathfrak{k} \rangle$.

If $\dim \Pi \leq \dim \Pi'$, say, then in view of Remark 4.1 the multisets $\mathfrak{k}, \mathfrak{k}'$ are equivalent if and only if there exists an embedding $\beta\colon \Pi \to \Pi'$ such that $\mathfrak{k}$ and $\mathfrak{k}'\beta$ coincide on the points of Π.

Definition 5.3. A linear code $\mathcal{C} \leq {}_RR^n$ is said to be *fat* if for every $i \in \{1, \dots, n\}$ there exists a codeword $\mathbf{c} = (c_1, c_2, \dots, c_n) \in \mathcal{C}$ with $c_i \in R^*$.

Thus $\mathcal{C} \leq {}_RR^n$ is fat if and only if the restriction to $\mathcal{C}$ of every projection map $\Phi_r(\mathbf{e}_j)\colon {}_RR^n \to {}_RR$, $\mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{e}_j = x_j$ is onto.

Let $\mathcal{C} \leq {}_RR^n$ be a fat linear code. We intend to associate with $\mathcal{C}$ a certain multiset of points in a projective Hjelmslev geometry over R which generalizes the familiar correspondence between full-length linear $[n, k]$-codes over $\mathbb{F}_q$ and multisets of points in $\mathrm{PG}(k-1, q)$ of cardinality n obtained as columns of a generator matrix of the $[n, k]$-code. Since the dual $\operatorname{Hom}({}_R\mathcal{C}, {}_RR)_R$ of ${}_R\mathcal{C}$ need not be a free R-module, some extra work is necessary. Let $S = (\mathbf{c}_1, \dots, \mathbf{c}_k)$ be a sequence of (not necessarily independent) generators for ${}_R\mathcal{C}$ and $\mathbf{G} \in \mathrm{M}_{k,n}(R)$ be the $k \times n$-matrix with rows $\mathbf{c}_1, \dots, \mathbf{c}_k$. Denote the columns of $\mathbf{G}$ by $\mathbf{g}_1, \dots, \mathbf{g}_n$, i. e. $\mathbf{g}_j = \big(\Phi_r(\mathbf{e}_j)(\mathbf{c}_1), \dots, \Phi_r(\mathbf{e}_j)(\mathbf{c}_k)\big)$. Note that $\mathbf{g}_j$ has period θ^m since $\Phi(\mathbf{e}_j)$ is onto and $\mathbf{c}_1, \dots, \mathbf{c}_k$ generate ${}_R\mathcal{C}$, and thus defines a point in the projective (right) Hjelmslev geometry $(\mathcal{P}, \mathcal{L}, \mathcal{I}) = \mathrm{PHG}(R^k_R)$. We define the *multiset* $\mathfrak{k}_S$ *induced by the generating sequence* S *of* $\mathcal{C}$ as

$$\mathfrak{k}_S\colon \left\{ \begin{array}{ll} \mathcal{P} & \to \mathbb{N}_0 \\ P & \mapsto |\{j \mid P = \mathbf{g}_jR\}|. \end{array} \right. \tag{20}$$

We say that the *multiset* $\mathfrak{k}_S$ *and the code* $\mathcal{C} = \sum_{\mathbf{c}\in S} R\mathbf{c}$ *are associated.* By definition of $\mathfrak{k}_S$ we have $|\mathfrak{k}_S| = n$. The following theorem is a generalization of a similar result by Dodunekov and Simonis [10] about linear codes over finite fields.

Theorem 5.1. *For every multiset* $\mathfrak{k}$ *of length* n *in* $\mathrm{PHG}(R^k_R)$ *there exists a fat linear code* $\mathcal{C} \le {}_R R^n$ *and a generating sequence* $S = (\mathbf{c}_1, \cdots, \mathbf{c}_k)$ *of* ${}_R\mathcal{C}$ *which induces* $\mathfrak{k}$. *Two multisets* $\mathfrak{k}_1$ *in* $\mathrm{PHG}(R^{k_1}_R)$ *and* $\mathfrak{k}_2$ *in* $\mathrm{PHG}(R^{k_2}_R)$ *associated with fat (left) linear codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *over* R, *respectively, are equivalent if and only if the codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *are semilinearly isomorphic.*

Proof. To prove the first assertion, choose a list $(\mathbf{g}_1, \ldots, \mathbf{g}_n)$ of vectors $\mathbf{g}_j \in R^k$ such that for every point P of $PHG(R^k_R)$

$$\mathfrak{k}(P) = |\{j \mid 1 \le j \le n \text{ and } P = \mathbf{g}_j R\}|. \tag{21}$$

Define $\mathcal{C} \le {}_R R^n$ to be the code generated by the rows of the $k \times n$-matrix $\mathbf{G} \in \mathrm{M}_{k,n}(R)$ with columns $\mathbf{g}_1, \ldots, \mathbf{g}_n$. Every column of $\mathbf{G}$ contains at least one entry $r \in R^*$. Hence the code $\mathcal{C}$ is fat. Clearly, the sequence $S = (\mathbf{c}_1, \ldots, \mathbf{c}_k)$ of rows of $\mathbf{G}$ induces $\mathfrak{k}$ in the sense of (20), i. e. $\mathfrak{k}_S = \mathfrak{k}$.

To prove the second assertion, assume first that two semilinearly isomorphic codes $\mathcal{C}_1, \mathcal{C}_2 \le {}_R R^n$ are associated with multisets $\mathfrak{k}_1$ in $\mathrm{PHG}(R^{k_1}_R)$ and $\mathfrak{k}_2$ in $\mathrm{PHG}(R^{k_2}_R)$, respectively. Let $\mathbf{G}_1 \in \mathrm{M}_{k_1,n}(R)$ and $\mathbf{G}_2 \in \mathrm{M}_{k_2,n}(R)$ be matrices whose sequences S_1 and S_2 of rows generate $\mathcal{C}_1$ (resp., $\mathcal{C}_2$) and induce $\mathfrak{k}_1$ (resp., $\mathfrak{k}_2$), i. e. $\mathfrak{k}_{S_i} = \mathfrak{k}_i$ for $i = 1, 2$. Let $\phi\colon R^n \to R^n$ be a semilinear code automorphism of ${}_R R^n$ with $\phi(\mathcal{C}_1) = \mathcal{C}_2$. The sequence $S_2' = \phi(S_1)$ also generates $\mathcal{C}_2$. Let $\mathbf{G}_2' \in \mathrm{M}_{k_1,n}(R)$ be the matrix associated with S_2' and $\mathfrak{k}_2'$ the multiset in $\mathrm{PHG}(R^{k_1}_R)$ induced by S_2'. There exist $\mathbf{U} \in \mathrm{M}_{k_1,k_2}(R)$, $\mathbf{V} \in \mathrm{M}_{k_2,k_1}(R)$ with $\mathbf{G}_2' = \mathbf{U}\mathbf{G}_2$, $\mathbf{G}_2 = \mathbf{V}\mathbf{G}_2'$. Let $\psi_{\mathbf{U}}\colon R^{k_2}_R \to R^{k_1}_R$, $\mathbf{g} \to \mathbf{U}\mathbf{g}$ and $\psi_{\mathbf{V}}\colon R^{k_1}_R \to R^{k_2}_R$, $\mathbf{g} \to \mathbf{V}\mathbf{g}$ be the corresponding R-linear mappings. Then $\mathfrak{k}_2 = \mathfrak{k}_2'\psi_{\mathbf{U}}$ and $\mathfrak{k}_2' = \mathfrak{k}_2\psi_{\mathbf{V}}$. From $\mathbf{G}_2' = \mathbf{U}\mathbf{V}\mathbf{G}_2'$, $\mathbf{G}_2 = \mathbf{V}\mathbf{U}\mathbf{G}_2$ we conclude that $\psi_{\mathbf{U}}\psi_{\mathbf{V}}$ fixes $\mathfrak{k}_2'$ and $\psi_{\mathbf{V}}\psi_{\mathbf{U}}$ fixes $\mathfrak{k}_2$, whence the restrictions of $\psi_{\mathbf{U}}$ and $\psi_{\mathbf{V}}$ to $\langle\mathfrak{k}_2\rangle$ and $\langle\mathfrak{k}_2'\rangle$, respectively, are mutually inverse R-isomorphisms. Thus $\mathfrak{k}_2$ and $\mathfrak{k}_2'$ are equivalent. Moreover, there exists a monomial matrix $\mathbf{M}$ and a ring automorphism σ such that $\phi(\mathbf{x}) = \sigma(\mathbf{x})\mathbf{M}$ for $\mathbf{x} \in R^n$. This shows $\mathbf{G}_2' = \sigma(\mathbf{G}_1)\mathbf{M}$. The columns of $\mathbf{G}_2'$ and $\sigma(\mathbf{G}_1)$ represent the multisets $\mathfrak{k}_2'$ and $\mathfrak{k}_1\sigma^{-1}$, respectively. Since $\mathbf{M}$ is monomial we have $\mathfrak{k}_2' = \mathfrak{k}_1\sigma^{-1}$ and thus $\mathfrak{k}_1 = \mathfrak{k}_2'\sigma$ proving the equivalence of $\mathfrak{k}_1$ and $\mathfrak{k}_2$.

Conversely, suppose that $\mathfrak{k}_1$ and $\mathfrak{k}_2$ are equivalent and associated with $\mathcal{C}_1$ and $\mathcal{C}_2$. Let $\mathbf{G}_1, \mathbf{G}_2$ have the same meaning as above, and let $\psi\colon \langle\mathfrak{k}_1\rangle \to \langle\mathfrak{k}_2\rangle$ be a bijective semilinear mapping with $\mathfrak{k}_1 = \mathfrak{k}_2\psi$. Let $H_1 \le R^{k_1}_R$ and $H_2 \le R^{k_2}_R$ be minimal free R-modules containing $\langle\mathfrak{k}_1\rangle$ and $\langle\mathfrak{k}_2\rangle$, respectively. By Th. 2.6 ψ can be extended to a bijective semilinear mapping $\widetilde{\psi}\colon H_1 \to H_2$. Since H_1 and H_2 are direct summands of $R^{k_1}_R$ and $R^{k_2}_R$, respectively, we can extend $\widetilde{\psi}$ to a mapping from $R^{k_1}_R$ into $R^{k_2}_R$ and $\widetilde{\psi}^{-1}$ to a mapping from $R^{k_2}_R$ into $R^{k_1}_R$, i. e. there exist matrices $\mathbf{U} \in \mathrm{M}_{k_1,k_2}(R)$, $\mathbf{V} \in \mathrm{M}_{k_2,k_1}(R)$ and a ring automorphism σ of R such that $\psi(\mathbf{g}) = \sigma(\mathbf{V}\mathbf{g})$ for every $\mathbf{g} \in \langle\mathfrak{k}_1\rangle$ and $\psi^{-1}(\mathbf{h}) = \mathbf{U}\sigma^{-1}(\mathbf{h})$ for every $\mathbf{h} \in \langle\mathfrak{k}_2\rangle$. The matrix $\mathbf{G}_1' = \mathbf{V}\mathbf{G}_1 \in \mathrm{M}_{k_2,n}(R)$ generates $\mathcal{C}_1$ since $\mathbf{U}\mathbf{G}_1' = \mathbf{G}_1$, and for every point P of $\mathrm{PHG}(R^{k_1}_R)$ it contains exactly $\mathfrak{k}_1(P) = \mathfrak{k}_2\big(\psi(P)\big)$ columns $\mathbf{h} \in R^{k_2}$ with $\sigma(\mathbf{h})R = \psi(P)$. Thus the columns of $\sigma(\mathbf{G}_1')$ and $\mathbf{G}_2$ represent the same points of $\mathrm{PHG}(R^{k_2}_R)$ when counted with their multiplicities. This clearly implies the existence of a monomial matrix $\mathbf{M}$ with $\mathbf{G}_2 = \sigma(\mathbf{G}_1')\mathbf{M}$ which in turn yields that $\mathcal{C}_1$ and $\mathcal{C}_2$ are semilinearly isomorphic. $\square$

Remark 5.1. If one defines $\mathrm{PHG}(R_R^k)$ as a point-line incidence structure as we did in Section 4, the restriction to fat linear codes in Th. 5.1 is a natural consequence. Non-fat linear codes, however, do appear in some situations, for example in the classification of $\mathbb{Z}_4$-linear codes of constant Lee or Euclidean weight [49]. It is possible to circumvent the restriction to fat linear codes by viewing $\mathrm{PHG}(R_R^k)$ as a projective lattice geometry [4] having additional non-free points. Theorem 5.1 can be proved in this more general setting.

Definition 5.4. Let $\mathfrak{k}\colon \mathcal{P} \to \mathbb{N}_0$ be a multiset in $\Pi = \mathrm{PHG}(R_R^k)$. A hyperplane Δ in Π is said to have the $\mathfrak{k}$*-type* $(a_0, a_1, \ldots, a_m)$, where $a_i = \sum_{P\colon P \subset {}_i\Delta,\, P \not\subset {}_{i+1}\Delta} \mathfrak{k}(P)$, for $i = 0, 1, \ldots, m$.

We shall often say 'type' instead of '$\mathfrak{k}$-type', if there is no doubt about the multiset $\mathfrak{k}$ we are referring to. By duality (Th. 3.1) every hyperplane Δ in $\mathrm{PHG}(R_R^k)$ can be considered as the set of points, whose homogeneous coordinates $(x_1, \ldots, x_k)$ satisfy a linear equation

$$r_1x_1 + r_2x_2 + \ldots + r_kx_k = 0,$$

where at least one of the r_i's is a unit in R. Let $\mathcal{C}$ be a fat linear code associated with $\mathfrak{k}$, and let $\mathbf{G}_S$ be a $k \times n$-matrix whose sequence S of rows generates $\mathcal{C}$ and satisfies $\mathfrak{k}_S = \mathfrak{k}$. All codewords of $\mathcal{C}$ which belong to the cyclic submodule $R(r_1, \ldots, r_k)\mathbf{G}_S \le {}_R\mathcal{C}$ are called *codewords associated with the hyperplane* Δ (relative to the choice of the generating sequence S). For different generating sequences S, S' of $\mathcal{C}$ with $\mathfrak{k}_S = \mathfrak{k}_{S'}$ the matrices $\mathbf{G}_S$ and $\mathbf{G}_{S'}$ can differ only by the ordering and scaling of their columns. Thus as far as the number and type (10) of codewords associated with a hyperplane is concerned, we may safely omit from now on any reference to the generating sequence. There is a connection between the type of a hyperplane in Π and the number of codewords of a given type in $\mathcal{C}$ associated with that hyperplane.

Theorem 5.2. *Let $\mathfrak{k}$ be a multiset in $\mathrm{PHG}(R_R^k)$ and $\mathcal{C}$ a fat linear code over R associated with $\mathfrak{k}$. For each hyperplane Δ of $\mathfrak{k}$-type*

$$(0, \ldots, 0, a_j, a_{j+1}, \ldots, a_m) \qquad \text{with } a_j \neq 0 \quad (0 \le j \le m)$$

there exist exactly $q^{m-s} - q^{m-s-1}$ codewords in $\mathcal{C}$ of type

$$(\underbrace{0, \ldots, 0}_{s}, a_j, \ldots, a_{m+j-s-1}, \sum_{i=m+j-s}^{m} a_i) \qquad (j \le s \le m-1) \tag{22}$$

which are associated with Δ.

Proof. Fix a generating sequence S of $\mathcal{C}$ and let $\mathbf{G} = \mathbf{G}_S$ be as above. Let $\Delta = (R\mathbf{r})^\perp$ with $\mathbf{r} = (r_1, \dots, r_k) \in {}_RR^k$. The codeword $\mathbf{c} = (r_1 \dots r_k)\mathbf{G}$ has exactly the same type $(0, \dots, 0, a_j, a_{j+1}, \dots, a_m)$ as the hyperplane Δ. Since $\mathbf{c}$ has period θ^{m-j}, we have $|R\mathbf{c}| = q^{m-j}$. The words in $R\mathbf{c}$ with type as in (22) are exactly those which generate the cyclic submodule $R\mathbf{c}[\theta^{m-s}] \le R\mathbf{c}$ of order q^{m-s}. Their number is therefore $q^{m-s} - q^{m-s-1}$ as asserted. □

Theorem 5.3. *A multiset* $\mathfrak{k}$ *in* $\mathrm{PHG}(R_R^k)$ *and its associated code have the same shape. In particular,* $|\langle \mathfrak{k} \rangle| = |\mathcal{C}|$.

Proof. Choose a $k \times n$-matrix $\mathbf{G}$ whose sequence S of rows generate $R_{\mathcal{C}}$ and whose columns $\mathbf{g}_1, \dots, \mathbf{g}_n$ represent the points P as in (21). Since S generates ${}_R\mathcal{C}$, the linear map $\mathrm{Hom}({}_R\mathcal{C}, {}_RR)_R \to \langle \mathfrak{k} \rangle_R$ which sends the restriction $\Phi_r(\mathbf{e}_j)|_{\mathcal{C}}$ to $\mathbf{g}_j$ is an isomorphism. Thus $\langle \mathfrak{k} \rangle_R$, $\mathrm{Hom}({}_R\mathcal{C}, {}_RR)_R$ and ${}_R\mathcal{C}$ all have the same shape; cf. the remark following Def. 2.1. □

6 Linear Codes from Selected Multisets in $\mathrm{PHG}(R_R^k)$

In this section we discuss some classes of linear codes over chain rings which arise from certain multisets of points in projective Hjelmslev geometries.

6.1 Simplex and Hamming Codes over Chain Rings

In [3] Blake introduced a generalization of the class of Hamming codes to the ring of integers modulo $q = p^r$, where p is prime. Below we suggest another definition, which reflects the geometric nature of the usual Hamming codes.

Consider the Hjelmslev geometry $\Pi = (\mathcal{P}, \mathcal{L}, I) = \mathrm{PHG}(R_R^k)$. The linear code $\mathcal{C}$ associated with the multiset $\mathfrak{k}$ defined by $\mathfrak{k}(P) = 1$ for all $P \in \mathcal{P}$, is called the *k-dimensional simplex code over R* and is denoted by $\mathrm{Sim}(k, R)$. By Th. 2.4 the code $\mathrm{Sim}(k, R)$ has length $q^{(k-1)(m-1)} \begin{bmatrix} k \\ 1 \end{bmatrix}_q$, and by Th. 5.3 it has shape m^k, in particular $|\mathrm{Sim}(k, R)| = q^{km}$. All hyperplanes Δ in Π have the same $\mathfrak{k}$-type $(a_0, a_1, \dots, a_m)$, where

$$\begin{aligned} a_0 &= q^{(k-1)(m-1)} \left(\begin{bmatrix} k \\ 1 \end{bmatrix}_q - \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q \right) = q^{(k-1)m}, \\ a_j &= q^{(k-2)(m-1)} \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q \left(q^{m-j} - q^{m-j-1} \right), \quad j = 1, \dots, m-1, \qquad (23) \\ a_m &= q^{(k-2)(m-1)} \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q . \end{aligned}$$

These numbers are obtained e. g. by observing that $\sum_{s\geq j} a_s$ is the number of free rank 1 submodules contained in $\Delta + \theta^j R^k$ which has shape $m^{k-1}(m-j)^1$. Thus

$$\sum_{s\geq j} a_s = \alpha_{m^{k-1}(m-j)^1}(m^1;q) = \begin{cases} q^{(k-1)(m-1)} \begin{bmatrix} k \\ 1 \end{bmatrix}_q & \text{if } j=0, \\ q^{(k-1)(m-1)} \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q \cdot q^{1-j} & \text{if } 1 \leq j \leq m.^8 \end{cases}$$

The dual code $\mathrm{Sim}(k,R)^\perp$ is called the *k-th order Hamming code over R* and is denoted by $\mathrm{Ham}(k,R)$. It is free of rank $q^{(k-1)(m-1)} \begin{bmatrix} k \\ 1 \end{bmatrix}_q - k$, in particular $|\mathrm{Ham}(k,R)| = q^{mq^{(k-1)(m-1)} \begin{bmatrix} k \\ 1 \end{bmatrix}_q - mk}$. For example, $\mathrm{Ham}(k,\mathbb{Z}_4)$ has parameters $(n, M, w_{\mathrm{Lee}}) = \big(2^{2k-1} - 2^{k-1}, 2^{2^{2k}-2^k-2k}, 3\big)$.

6.2 The Linearity of the MacDonald Codes

Let us fix a Hjelmslev subspace Σ of Π with $\mathrm{rk}\,\Sigma = u$, $1 \leq u \leq k-1$. Let $\mathcal{C}$ be associated with $\mathfrak{k}\colon \mathcal{P} \to \mathbb{N}_0$ defined by

$$\mathfrak{k}(P) = \begin{cases} 1 & \text{if } P \bigcirc_i \Sigma, \\ 0 & \text{otherwise,} \end{cases} \tag{24}$$

where $i \geq 1$ is fixed. Since $\mathfrak{k}$ is the set of points of the R-module $\Sigma + R^k\theta^i$ of conjugate shape $k^{m-i}u^i$, we have by Th. 2.4 and Th. 5.3

$$\mathfrak{k}(\mathcal{P}) = q^{(k-1)(m-i)+(u-1)(i-1)} \cdot \begin{bmatrix} u \\ 1 \end{bmatrix}_q, \qquad |\mathcal{C}| = q^{k(m-i)+ui}. \tag{25}$$

Consider the mapping $\psi\colon R \to \mathbb{F}_q^m$ (cf. [22, Section 3]) defined by the matrix

$$\mathbf{G} = \mathbf{G}^{(m)} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \mathbf{a}_1 & \mathbf{a}_2 & \dots & \mathbf{a}_{q^{m-1}} \end{bmatrix}, \tag{26}$$

where $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{q^{m-1}}$ are the elements of $\mathbb{F}_q^{m-1}$ taken in some order. By [17, Th. 1.1] or [24, Prop. 11],

$$w_{\mathrm{Ham}}\big(\psi(x) - \psi(y)\big) = \begin{cases} 0 & \text{if } x = y, \\ q^{m-1} & \text{if } x - y \in N^{m-1} \setminus \{0\}, \\ q^{m-1} - q^{m-2} & \text{if } x - y \notin N^{m-1}. \end{cases}$$

Thus the q-ary image $\psi(\mathcal{C})$ is a (possibly nonlinear) distance invariant code with parameters $N = q^{m-1}\mathfrak{k}(P) = q^{(k-u)(m-i)+u(m-1)} \begin{bmatrix} u \\ 1 \end{bmatrix}_q$, $M = |\mathcal{C}| = q^{(k-u)(m-i)+um}$.

The hyperplanes of Π can be divided into $i+1$ disjoint nonempty classes, which we denote by (A_j), $0 \leq j \leq i$:

[8] Note that $\alpha_\lambda(m^1;q)$ is already determined by λ'_m and $|\lambda| = \sum \lambda_i$.

(A_j) hyperplanes Δ with $\Sigma \subset\!\supset_j \Delta$, and $\Sigma \not\subset\!\supset_{j+1} \Delta$, $0 \leq j < i$;

(A_i) hyperplanes Δ with $\Sigma \subset\!\supset_i \Delta$.

Denote by $\lambda^{(t)}$ (resp., $\mu^{(t)}$) the shape (resp., conjugate shape) of the module $(\Delta + R^k\theta^t) \cap (\Sigma + R^k\theta^i)$, $0 \leq t \leq m$. The nonzero Hamming weights of $\psi(\mathcal{C})$ are

$$\begin{aligned}
&\sum_{s=0}^{t-2} a_s(q^{m-1} - q^{m-2}) + a_{t-1}q^{m-1} = \\
&\qquad = \alpha_{\lambda^{(0)}}(m^1, q)(q^{m-1} - q^{m-2}) - \alpha_{\lambda^{(t)}}(m^1, q)q^{m-1} + \alpha_{\lambda^{(t-1)}}(m^1, q)q^{m-2},
\end{aligned}$$

where $(a_0, \dots, a_m)$ is one of the possible $\mathfrak{k}$-types of hyperplanes of Π and $j+1 \leq t \leq m$ if Δ is of class (A_j), $0 \leq j \leq i$. If Δ is of class (A_i) then

$$\mu^{(t)} = \begin{cases} k^{m-i}u^i = \mu^{(0)} & \text{if } 0 \leq t \leq i, \\ k^{m-t}(k-1)^{t-i}u^i & \text{if } i \leq t \leq m. \end{cases} \tag{27}$$

Hence $\alpha_{\lambda^{(t)}}(m^1, q) = \alpha_{\lambda^{(t-1)}}(m^1, q)/q$ if $i+1 \leq t \leq m$, and Δ produces codewords of single nonzero weight

$$\alpha_{\lambda^{(0)}}(m^1, q)(q^{m-1} - q^{m-2}) = q^{(k-u)(m-i)+u(m-1)-1}(q^u - 1). \tag{28}$$

If Δ is of class (A_j), $0 \leq j \leq i-1$, then

$$\mu^{(t)} = \begin{cases} k^{m-i}u^i & \text{if } 0 \leq t \leq j, \\ k^{m-i}u^{i-t+j}(u-1)^{t-j} & \text{if } j \leq t \leq i, \\ k^{m-t}(k-1)^{t-i}u^j(u-1)^{i-j} & \text{if } i \leq t \leq m. \end{cases} \tag{29}$$

Equation (29) is derived e.g. using the formula $|U \cap V| = |U||V|/|U+V|$ with $U = \Delta + R^k\theta^t$, $V = \Sigma + R^k\theta^i$, and observing that $\Delta + \Sigma$ has shape $m^{k-1}(m-j)^1$. Hence we have $\alpha_{\lambda^{(t)}}(m^1, q) = \alpha_{\lambda^{(t-1)}}(m^1, q)/q$ if $j+2 \leq t \leq m$, and thus Δ produces nonzero codewords of weights (28) and

$$\begin{aligned}
\alpha_{\lambda^{(0)}}(m^1, q)(q^{m-1} - q^{m-2}) &- \alpha_{\lambda^{(j+1)}}(m^1, q)q^{m-1} + \alpha_{\lambda^{(j)}}(m^1, q)q^{m-2} = \\
&= \big(\alpha_{\lambda^{(0)}}(m^1, q) - \alpha_{\lambda^{(j+1)}}(m^1, q)\big)q^{m-1} \\
&= q^{(k-u)(m-i)+u(m-1)+u-1}.
\end{aligned} \tag{30}$$

Let $K = (k-u)(m-i) + um$, $U = (k-u)(m-i) + u(m-1)$ (whence $K - U = u$). The code $\psi(\mathcal{C})$ is a two-weight code over a q-ary alphabet of length N, minimum distance D, and with weights W_1 and W_2, where

$$N = \frac{q^K - q^U}{q-1}, \ |\psi(\mathcal{C})| = q^K, \ D = W_1 = q^{K-1} - q^{U-1}, \ W_2 = q^{K-1}. \tag{31}$$

Now we assume that R is one of the chain rings $\mathbb{F}_q[X;\sigma]/(X^m)$ of characteristic p. By Th. 5 from [22], the code $\psi(\mathcal{C})$ is linear over $\mathbb{F}_q$, and it has the parameters (31) of a MacDonald code. Since MacDonald codes are uniquely determined by their parameters (cf. [10, 46]), we get that $\psi(\mathcal{C})$ is semilinearly isomorphic to a MacDonald code. Choosing k, u, i appropriately, we can get all MacDonald codes with parameters $U \geq K(1-1/m)$. Hence we have the following theorem (cf. [22] for the special case $m = 2$):

Theorem 6.1. *A q-ary MacDonald code whose parameters K, U satisfy the condition $U \geq K(1-1/m)$ is linearly representable over any of the chain rings $\mathbb{F}_q[X;\sigma]/(X^m)$.*

Acknowledgements. The authors wish to thank S. Dodunekov, W. Heise, A. Kreuzer, A. Nechaev, J. Simonis, J. Wood, and V. Zinoviev for comments/references. They are indebted to the referee for valuable suggestions which helped to improve the paper. The research of the second author was financially supported by the Alexander-von-Humboldt Stiftung.

References

[1] K. Asano. Über verallgemeinerte Abelsche Gruppen mit hyperkomplexem Operatorenring und ihre Anwendungen. *Japanese Journal of Mathematics*, 15:231–253, 1938/39.

[2] C. Bachoc. Applications of coding theory to the construction of modular lattices. *Journal of Combinatorial Theory, Series A*, 78:92–119, 1997.

[3] I. F. Blake. Codes over integer residue rings. *Information and Control*, 29:295–300, 1975.

[4] U. Brehm, M. Greferath, and S. E. Schmidt. Projective geometry on modular lattices. In Buekenhout [5], chapter 21, pages 1115–1142.

[5] F. Buekenhout, editor. *Handbook of Incidence Geometry—Buildings and Foundations.* Elsevier Science Publishers, 1995.

[6] L. M. Butler. *Subgroup Lattices and Symmetric Functions.* Number 539 in Memoirs of the American Mathematical Society. American Mathematical Society, 1994.

[7] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Designs, Codes and Cryptography*, 6:21–35, 1995.

[8] W. E. Clark and D. A. Drake. Finite chain rings. *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, 39:147–153, 1974.

[9] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. John Wiley & Sons, Wiley Classics Library edition, 1988.

[10] S. Dodunekov and J. Simonis. Codes and projective multisets. *Electronic Journal of Combinatorics*, 5(#R37), 1998.

[11] S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, and P. Solé. Type IV self-dual codes over rings. *IEEE Transactions on Information Theory*, 45(7):2345–2360, Nov. 1999.

[12] S. T. Dougherty, P. Gaborit, M. Harada, and P. Solé. Type II codes over $\mathbb{F}_2+u\mathbb{F}_2$. *IEEE Transactions on Information Theory*, 45(1):32–45, Jan. 1999.

[13] T. Ericson, J. Simonis, H. Tarnanen, and V. A. Zinoviev. F-partitions of cyclic groups. *AAECC*, 8:387–393, 1997.

[14] T. Ericson and V. A. Zinoviev. On Fourier-invariant partitions of finite abelian groups and the MacWilliams identity for group codes. *Problems of Information Transmission*, 32(1):117–122, 1996.

[15] C. Faith. On Köthe rings. *Mathematische Annalen*, 164:207–212, 1966.

[16] P. Gaborit. Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$-rings. *IEEE Transactions on Information Theory*, 42:1222–1228, 1996.

[17] M. Greferath and S. E. Schmidt. Gray isometries for finite chain rings. *IEEE Transactions on Information Theory*, 45(7):2522–2524, Nov. 1999.

[18] M. Hall, Jr. A type of algebraic closure. *Annals of Mathematics*, 40:360–369, 1939.

[19] W. Heise and P. Quattrocchi. *Informations- und Codierungstheorie*. Springer-Verlag, Berlin, 3rd edition, 1995.

[20] T. Honold and I. Landjev. Linear codes over finite chain rings. In *Optimal Codes and Related Topics*, pages 116–126, Sozopol, Bulgaria, 1998.

[21] T. Honold and I. Landjev. All Reed-Muller codes are linearly representable over the ring of dual numbers over $\mathbb{Z}_2$. *IEEE Transactions on Information Theory*, 45(2):700–701, Mar. 1999.

[22] T. Honold and I. Landjev. Linearly representable codes over chain rings. *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, 69:187–203, 1999.

[23] T. Honold and I. Landjev. MacWilliams identities for linear codes over finite Frobenius rings. Submitted for publication, Oct. 1999.

[24] T. Honold and A. A. Nechaev. Weighted modules and representations of codes. *Problems of Information Transmission*, 35(3):205–223, 1999.

[25] S. K. Jain, J. Luh, and B. Zimmermann-Huisgen. Finite uniserial rings of prime characteristic. *Communications in Algebra*, 16(10):2133–2135, 1988.

[26] E. Kleinfeld. Finite Hjelmslev planes. *Illinois Journal of Mathematics*, 3:403–407, 1959.

[27] M. Klemm. Über die Identität von MacWilliams für die Gewichtsfunktion von Codes. *Archiv der Mathematik*, 49:400–406, 1987.

[28] G. Köthe. Verallgemeinerte Abelsche Gruppen mit hyperkomplexem Operatorenring. *Mathematische Zeitschrift*, 39:31–44, 1935.

[29] A. Kreuzer. Hjelmslev-Räume. *Resultate der Mathematik*, 12:148–156, 1987.

[30] A. Kreuzer. *Projektive Hjelmslev-Räume*. Dissertation, Technische Universität München, 1988.

[31] A. Kreuzer. Hjelmslevsche Inzidenzgeometrie - Ein Bericht. Bericht TUM-M9001, Technische Universität München, Jan. 1990. Beiträge zur Geometrie und Algebra Nr. 17.

[32] A. Kreuzer. Fundamental theorem of projective Hjelmslev spaces. *Mitteilungen der Mathematischen Gesellschaft in Hamburg*, 12(3):809–817, 1991.

[33] A. Kreuzer. A system of axioms for projective hjelmslev spaces. *Journal of Geometry*, 40:125–147, 1991.

[34] I. Landjev. A note on the MacWilliams identities. *Compt. Rend. Bulg. Acad. Sci.*, 52, 1999.

[35] S. Lang. *Algebra*. Addison-Wesley Publishing Company, 2nd edition, 1984.

[36] I. G. MacDonald. *Symmetric Functions and Hall Polynomials*. Oxford University Press, 2nd edition, 1995.

[37] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, Amsterdam, 1977.

[38] B. R. McDonald. *Finite Rings with Identity*. Marcel Dekker, New York, 1974.

[39] T. Mora and H. F. Mattson, Jr., editors. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC) 12*, number 1255 in Lecture Notes in Computer Science. Springer-Verlag, 1997.

[40] A. A. Nechaev. Finite principal ideal rings. *Russian Academy of Sciences. Sbornik. Mathematics*, 20:364–382, 1973.

[41] A. A. Nechaev. Linear codes over modules and over spaces. MacWilliams' identity. In *Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl.*, pages 35–38, Victoria B.C., Canada, 1996.

[42] A. A. Nechaev and A. S. Kuzmin. Linearly presentable codes. In *Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl.*, pages 31–34, Victoria B.C., Canada, 1996.

[43] A. A. Nechaev and A. S. Kuzmin. Formal duality of linear presentable codes over a Galois field.

[44] A. A. Nechaev, A. S. Kuzmin, and V. T. Markov. Linear codes over finite rings and modules. Preprint N 1995-6-1, Center of New Information Technologies, Moscow State University, 1995.

[45] R. Raghavendran. Finite associative rings. *Compositio Mathematica*, 21:195–229, 1969.

[46] F. Tamari. On linear codes which attain the Solomon-Stiffler bound. *Discrete Mathematics*, 49:179–191, 1984.

[47] F. D. Veldkamp. Geometry over rings. In Buekenhout [5], chapter 19, pages 1033–1084.

[48] J. A. Wood. Extension theorems for linear codes over finite rings. In Mora and Mattson [39], pages 329–340.

[49] J. A. Wood. Codes of constant Lee or Euclidean weight. Extended Abstract for the Workshop on Coding and Cryptography (WCC 99), Paris 1999.

[50] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121(3):555–575, 1999.

[51] J. A. Wood. Weight functions and the extension theorem for linear codes over finite rings. In G. L. M. Ronald C. Mullin, editor, *Finite Fields: Theory, Applications, and Algorithms*, volume 225 of *Contemporary Mathematics*, pages 231–243. American Mathematical Society, 1999.