Linear Codes and Geometry over Finite Chain Rings

Thomas Honold

Institute of Information and Communication Engineering
Zhejiang University

ZiF Cooperation Group on Finite Projective Ring Geometries

August 2009

Outline

Today's Lecture: Linear codes and projective Hjelmslev geometry over finite chain rings

Speaker

Dr. Thomas Honold (Assoc. Prof.)
Dept. of Information Science and Electronics Engineering
Zhejiang University, Zheda Road
Email: honold@zju.edu.cn

The talk describes joint work with IVAN LANDJEV, MICHAEL KIERMAIER, AXEL KOHNERT, SILVIA BOUMOVA, ...

Disclaimer

In what follows . . .

- rings will be associative with identity $1 \neq 0$ (no rngs, please!)
- modules will be unital (no modls), ring homomorphisms will preserve 1 (no homomorhisms)
- "finite" means "of finite cardinality" (not only "finitely generated")

Algebraic Coding Theory

Suppose A is a finite set of size $|A| = q \geq 2$ ("q-ary alphabet").

Definition

A *(block) code over A* is a nonempty subset $C \subseteq A^n$ for some integer $n \geq 0$.

Parameters of a code

- n *Length*, i.e. $C \subseteq A^n$
- M Number of codewords, i.e. $M = |C|$
- d *Minimum distance*, defined as $\min\{\mathrm{d}_{\mathrm{Ham}}(\mathbf{c}, \mathbf{c}'); \mathbf{c}, \mathbf{c}' \in C, \mathbf{c} \neq \mathbf{c}'\}$

A code with these parameters is said to be a q-ary (n, M, d) code or, using *bracket notation*, an $[n, k, d]$ code, where $k = \log_q M$.

The performance of a communication system using C to transmit information over a noisy channel is determined by k/n (*transmission rate*) and d/n (*error correction rate*), which both should be large.

For complexity reasons n should be small.

Main Problem

- Given two of the parameters (n, M, d), optimize the value of the third parameter.
- Find codes with sufficiently rich structure in order to facilitate (encoding) and decoding.

Classical Linear Codes

Suppose $q > 1$ is a prime power and $A = \mathbb{F}_q = \mathrm{GF}(q)$ is the finite field of order q.

Definition

A *q-ary linear $[n,k,d]$ code* is a code over $\mathbb{F}_q$ with parameters $[n,k,d]$ (or $(n,2^k,d)$), which is also a vector subspace of $\mathbb{F}_q^n$.

Simplifications

- $k = \dim(C)$
- $d = \min\{\mathrm{w}_{\mathrm{Ham}}(\mathbf{c}); \mathbf{c} \in C; \mathbf{c} \neq \mathbf{0}\}$, where $\mathrm{w}_{\mathrm{Ham}}(\mathbf{c})$ is the Hamming weight (number of nonzero entries) of $\mathbf{c}$
- $C = \{\mathbf{xG}; \mathbf{x} \in \mathbb{F}_q^k\}$, where $\mathbf{G} \in \mathbb{F}_q^{k\times n}$ is a matrix having as its rows a basis of C (*generator matrix*).
- $C = \{\mathbf{c} \in \mathbb{F}_q^n; \mathbf{Hc}^{\mathsf{T}} = \mathbf{0}\}$ for some $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ (*parity-check matrix*)

For some families of linear codes (Reed-Muller codes, cyclic codes, algebraic-geometry codes, low-density parity-check codes) efficient encoding and decoding algorithms are known.

The Hexacode

A particularly nice example

The *Hexacode* is the quaternary linear code with generator matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \alpha & \beta \\ 0 & 0 & 1 & 1 & \beta & \alpha \end{pmatrix} \in \mathbb{F}_4^{3\times 6},$$

where $\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ (so $\beta = 1 + \alpha = \alpha^2$).

C has parameters $n = 6$, $k = 3$ (so $|C| = 2^3 = 8$), $d = 4$.

C is an *MDS code*, i.e. it satisfies the Singleton bound $d \leq n - k + 1$ with equality. In terms of **G** this means that every 3×3-submatrix of **G** is invertible.

The Geometric View

Idea: View the columns of **G** as (homogeneous coordinates) of points of $\mathrm{PG}(2,\mathbb{F}_4)$.

The projective plane over $\mathbb{F}_4$

$\mathrm{PG}(2,\mathbb{F}_4)$ is defined as the point-line incidence structure $(\mathcal{P},\mathcal{L},I)$ with

$$\mathcal{P} := \{U \le \mathbb{F}_4^3; \dim U = 1\}, \quad \mathcal{L} := \{U \le \mathbb{F}_4^3; \dim U = 2\}$$

and $I := \subseteq$ (set inclusion).

Thus **G** corresponds to the point set
$\mathfrak{K} = \{\mathbb{F}_4(100), \mathbb{F}_4(010), \mathbb{F}_4(001), \mathbb{F}_4(111), \mathbb{F}_4(1\alpha\beta), \mathbb{F}_4(1\beta\alpha)\}$.

The geometric view is compatible with coding theory:

- Replacing **G** by a different generator matrix **G**′ of the same code corresponds to a collineation of $\mathrm{PG}(2,\mathbb{F}_4)$.
- Changing the order of the points and/or the coordinate vectors corresponds to a code isomorphism of $\mathbb{F}_4^6$.

$d = 4$ (or "all 3×3-submatrices of $\mathbf{G}$ are invertible") translates into the following geometric property:

No three points of $\mathfrak{K}$ are collinear.

Such point sets $\mathfrak{K}$ are known as *maximal* $(6, 2)$-*arcs* or *hyperovals*.

Ovals and hyperovals

An *oval* (*hyperoval*) in a projective plane of order q is a set of $q + 1$ points (resp., $q + 2$ points) meeting every line in at most 2 points.

Ovals have unique tangents (1-lines) in each of their points. Hyperovals have no tangents at all (i.e. meet every line in either 0 or 2 points).

Using geometry to compute the weight distribution of a linear code

Weight distribution of $C \subseteq \mathbb{F}_q^n$

The sequence $(A_0, A_1, \ldots, A_n)$ defined by $A_i := \#\{\mathbf{c} \in C; \mathrm{w}_{\mathrm{Ham}}(\mathbf{c}) = i\}$.

Now suppose $\mathbf{G} = (\mathbf{g}_1|\mathbf{g}_2|\ldots|\mathbf{g}_n)$ and $\mathbf{x} \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}$.

Observation

$\mathrm{w}_{\mathrm{Ham}}(\mathbf{xG}) = \mathrm{w}_{\mathrm{Ham}}\big((\mathbf{x}\cdot\mathbf{g}_1, \ldots, \mathbf{x}\cdot\mathbf{g}_n)\big) = \#\{i; \mathbb{F}_q\mathbf{g}_i \notin \mathbf{x}^\perp\}$,
where $L := \mathbf{x}^\perp = \{\mathbf{y} \in \mathbb{F}_q^n; \mathbf{x}\cdot\mathbf{y} = \mathbf{0}\}$ is a line of $\mathrm{PG}(2, \mathbb{F}_q)$.

In other words, a line L of $\mathrm{PG}(2, \mathbb{F}_q)$ meeting $\mathfrak{K}$ in $n - w$ points contributes exactly $q - 1$ codewords of weight w.

Application

Hyperovals in $\mathrm{PG}(2, \mathbb{F}_4)$ have 15 secants (2-lines) and 6 passants (external or 0-lines). Hence the Hexacode has weight distribution

i	0	1	2	3	4	5	6
A_i	1	0	0	0	45	0	18

The Heptacode over $\mathbb{Z}_4$

Twin brother of the Hexacode

Linear codes over a finite ring R are defined in the same way as for finite fields, except that "vector subspace of $\mathbb{F}_q^n$" is replaced by "submodule of either ${}_RR^n$ ("left linear code") or R_R^n ("right linear code").

"Linear over $\mathbb{Z}_4$" means just "closed under addition mod 4".

Observation

The Gray map $\gamma\colon \mathbb{Z}_4 \to \mathbb{F}_2^2$, $0 \mapsto 00$, $1 \mapsto 10$, $2 \mapsto 11$, $3 \mapsto 01$ maps every linear $[n,k,d]$ code over $\mathbb{Z}_4$ onto a (linear or nonlinear) binary $[2n,2k,d]$ code with essentially the same encoding and decoding complexity. These codes are sometimes better than the best binary linear codes.

Caution

The observation is only true if we use the preimage $\mathrm{w}_{\mathrm{Ham}} \circ \gamma\colon \mathbb{Z}_4^n \to \mathbb{R}$ of the Hamming weight as the corresponding weight for codes over $\mathbb{Z}_4$. This is called the *Lee weight*.

$x \in \mathbb{Z}_4$	0	1	2	3
$\mathrm{w}_{\mathrm{Lee}}(x)$	0	1	2	1

The *Heptacode* is the linear code over $\mathbb{Z}_4$ generated by

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

It is a $[7, 3, 6]$ (or $(7, 4^3, 6)$) code and corresponds (via the Gray map) to a nonlinear binary $[14, 6, 6]$ code. Linear binary codes with these parameters do not exist.

The columns of **G** define a hyperoval in the *projective Hjelmslev plane* $\mathrm{PHG}(2, \mathbb{Z}_4)$ *over* $\mathbb{Z}_4$.

Definition of $\mathrm{PHG}(2, \mathbb{Z}_4)$

The plane $\mathrm{PHG}(2, \mathbb{Z}_4)$ is defined as the incidence structure $(\mathcal{P}, \mathcal{L}, \subseteq)$ with

$$\mathcal{P} := \{U \leq \mathbb{Z}_4^3; U \cong \mathbb{Z}_4\}, \quad \mathcal{L} := \{U \leq \mathbb{Z}_4^3; U \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4\}.$$

The points are thus the cyclic modules $\mathbb{Z}_4(x_1, x_2, x_3)$ with at least one entry x_1, x_2, x_3 equal to ± 1, and the lines are generated by two linearly independent such vectors. Lines can also be described as point sets $\{\mathbb{Z}_4(x, y, z); ax + by + cz = 0\} = (\mathbb{Z}_4(a, b, c))^{\perp}$ for some point $\mathbb{Z}_4(a, b, c)$.

Properties of PHG$(2, \mathbb{Z}_4)$

- Tow distinct points $p_1, p_2 \in \mathcal{P}$ can be incident with either one or two lines. In the latter case the points (as well as the corresponding lines L_1, L_2) are said to be neighbours (written as $p_1 \supset p_2$ resp. $L_1 \supset L_2$).
- Neighborhood corresponds to equality mod 2 and defines an equivalence relation on both $\mathcal{P}$ and $\mathcal{L}$.
- There are 28 points and 28 lines (falling into 7 neighbour classes of size 4). Each line has 6 points, and each point is on 6 lines.
- The quotient structure induced on the neighbour classes $[x]$, $[L]$ of points resp. lines is isomorphic to the Fano plane PG$(2, \mathbb{F}_2)$. We write $x \supset L$ if $[x]$ is incident with $[L]$. (If $L = (a, b, c)^\perp$, this means $ax + by + cz \equiv 0 \pmod 2$.)

Type, Spectrum, Weight Distribution

Definition

(i) The *type* of $\mathbf{x} \in \mathbb{Z}_4^n$ is the integer triple (a_0, a_1, a_2), where a_0, a_1, a_2 count the entries of $\mathbf{x}$ equal to ± 1, 2, resp. 0. (This is sometimes also written as $(\pm 1)^{a_0} 2^{a_1} 0^{a_2}$.

(ii) The (symmetrized) *weight enumerator* of a code $C \subseteq \mathbb{Z}_4^n$ is

$$\mathrm{A}_C(X_0, X_1, X_2) = \sum_{\mathbf{c} \in C} X_0^{a_0(\mathbf{c})} X_1^{a_1(\mathbf{c})} X_2^{a_2(\mathbf{c})}.$$

Remarks

- Clearly A_C encodes all information necessary to compute the Lee weight distribution of C (Hamming weight distribution of the binary image of C).
- As in the classical case, linear codes over $\mathbb{Z}_4$ can be associated with point (multi-)sets in projective Hjelmslev spaces over $\mathbb{Z}_4$, and weight enumerators can be computed from geometric information about the corresponding point sets.

Example (Weight enumerator of the Heptacode)

First we verify that no 3 points of $\mathfrak{K}$, the set of points derived from

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix},$$

are collinear. (Since no two points of $\mathfrak{K}$ are neighbours, the determinant test can be used for this.)

Since $\#\{L; p \in L\} = 6 = |\mathfrak{K}| - 1$, this implies that $\mathfrak{K}$ has only 2-lines and 0-lines. There are $\binom{7}{2} = 21$ secants and hence $28 - 21 = 7$ passants.

Definition

The $\mathfrak{K}$-*type* of a line L is the integer triple (b_0, b_1, b_2) defined by

$$\begin{aligned} b_0 &= \#\{p \in \mathfrak{K}; p \not\subset L\}, \\ b_1 &= \#\{p \in \mathfrak{K}; p \subset L, p \notin L\}, \\ b_2 &= \#\{p \in \mathfrak{K}; p \in L\} = |\mathfrak{K} \cap L|. \end{aligned}$$

If $L = (a, b, c)^\perp$, the $\mathfrak{K}$-type of L is equal to the type of the two codewords $\pm(a, b, c)\mathbf{G}$.

In our case the line types are:

	type
2-line	$(\pm 1)^4 2^1 0^2$
0-line	$(\pm 1)^4 2^3$

This gives a contribution of $2(21X_0^4X_1X_2^2 + 7X_0^4X_1^3)$ to the weight enumerator.

The *torsion code* of the Heptacode has weight enumerator $X_2^7 + 7X_1^4X_2^3$ (Simplex code over $\{0, 2\}$).

Hence the final result is

$$\mathrm{A}_C(X_1, X_2, X_3) = X_2^7 + 7X_1^4X_2^3 + 42X_0^4X_1X_2^2 + 14X_0^4X_1^3.$$

Recall the following facts about a ring R.

- The *(Jacobson) radical* $N = \operatorname{rad} R$ is defined as the intersection of all maximal left ideals of R. The set N is a two-sided ideal of R (and equals the intersection of all maximal right ideals of R).
- If R is finite (or, more generally, left Artinian) then $N^m = 0$ for some integer $m > 0$.
- R is said to be a *local* ring if R has exactly one maximal left ideal. In this case, R/N is a division ring and $R \setminus N$ is the set of units (invertible elements) of R.
- A finite ring R is local iff $R/N \cong \mathbb{F}_q$ is a finite field (by Wedderburn's Theorem).
- R is said to be a *left chain ring* if its lattice of left ideals is a chain (i.e., the left ideals of R are linearly ordered w.r.t. $\subseteq$). *Right chain rings* are defined in an analogous manner.

Theorem

For a finite ring R with radical N the following are equivalent:

(i) *R is a left chain ring.*

(ii) *The principal left ideals of R form a chain.*

(iii) *R is a local ring, and $N = R\theta$ is left principal;*

(iv) *R is a right chain ring.*

Moreover, if R satisfies these conditions, then every proper ideal of R has the form $N^i = R\theta^i = \theta^i R$ for some integer $i > 0$.

Definition (Finite chain ring)

A finite ring R is called a *chain ring* if it satisfies the equivalent properties of the preceding theorem.

Proof of the theorem.

If $N = \{0\}$, then $R \cong \mathbb{F}_q$ is a finite field and satisfies (i)–(iv).
From now on we assume $N \neq \{0\}$ and hence $N^2 \subsetneq N$.

(i)⇒(iii): Clearly R is local.
Consider the quotient module $V := N/N^2$.

$NV = VN = 0$, so V is both a left and a right vector space over $R/N \cong \mathbb{F}_q$ (necessarily of the same dimension).

The left ideals between N and N^2 correspond to subspaces of V.
Since they form a chain, we must have $\dim V = 1$.

Let $\theta \in N \setminus N^2$.

$$\left.\begin{array}{l} R\theta \subseteq N \\ R\theta \nsubseteq N^2 \end{array}\right\} \Longrightarrow R\theta = N$$

(iii)⇒(i),(iv): The crucial step is to show $N = \theta R$.

$$\left.\begin{array}{l} N = R\theta \Longrightarrow \dim_{R/N} V = 1 \\ \theta \in N \setminus N^2 \end{array}\right\} \Longrightarrow N = \theta R + N^2$$

This gives

$$\begin{aligned} N &= \theta R + N^2 = \theta R + (\theta R + N^2)N \\ &= \theta R + N^3 = \cdots = \theta R + N^m = \theta R. \end{aligned}$$

Proof cont'd.

It follows that $N^i = R\theta^i = \theta^i R$ for $i = 1, 2, \ldots$.

We have the chain of two-sided ideals

$$R = N^0 \supsetneq N \supsetneq N^2 \supsetneq \cdots \supsetneq N^{m-1} \supsetneq N^m = \{0\}. \qquad (\star)$$

Suppose now $0 \neq a \in R$. There exists $i \in \{0, 1, \ldots, m-1\}$ such that $a \in N^i \setminus N^{i+1} = R\theta^i \setminus R\theta^{i+1}$, i.e.

$$a = u\theta^i \quad \text{where } u \in R \setminus N \text{ is a unit.}$$

Hence $Ra = R\theta^i$, and thus every left ideal of R belongs to the chain $(\star)$.

We have proved that property (iii) is left-right symmetric and implies (i). Hence (iii)$\Rightarrow$(iv) is true as well.

The remaining implications are trivial. □

Properties of Finite Chain Rings

With every finite chain ring R we associate the following pair (q, m) of integers:

- q The order of the residue class field R/N (i.e. $R/N \cong \mathbb{F}_q$)
- m The index of nilpotency of N (equal to the composition length of the regular module ${}_R R$)

We have the following counting formulas:

- $|R| = q^m, \quad |N| = q^{m-1}, \quad |R^\times| = q^m - q^{m-1} = (q-1)q^{m-1}$
- $\left|N^i\right| = q^{m-i}, \quad \left|R/N^i\right| = q^i \quad$ for $0 \le i \le m$

For the proof it suffices to observe that $N^i/N^{i+1} = R\theta^i/R\theta^{i+1} \cong R/N$ as a vector space over R/N.

Galois Rings

Let $q = p^r > 1$ be a prime power and $h(X) \in \mathbb{Z}_{p^m}[X]$ a monic polynomial of degree r which is irreducible modulo p (a so-called *basic irreducible polynomial* or *Galois polynomial*).

Definition

The ring $\mathrm{GR}(q^m, p^m) := \mathbb{Z}_{p^m}[X]/\big(h(X)\big)$ is called *Galois ring* of order q^m and characteristic p^m.

Properties of $R = \mathrm{GR}(q^m, p^m)$

- R is a finite commutative chain ring with radical $N = Rp$, invariants (q, m) and characteristic p^m.
- The isomorphism type of R does not depend on the particular choice of the polynomial $h(X)$.
- A finite chain ring with invariants (q, m) and characteristic p^m is isomorphic to R.
- Every automorphism of R/N can be lifted in a unique way to an automorphism of R. Thus $\mathrm{Aut}\, R \cong \mathrm{Aut}\, \mathbb{F}_q \cong (\mathbb{Z}_r, +)$.

Remark

For the Galois ring of order $q^m = p^{rm}$ and characteristic p^m two different notations are widely used: $\mathrm{GR}(q^m, p^m)$ (due to Raghavendran [**?**]) and $\mathrm{GR}(p^m, r)$ (due to Janusz [**?**]).

Representation Theorem

Definition

Suppose S is a Galois ring.

(i) For $\sigma \in \operatorname{Aut} S$ the *skew polynomial ring* $S[X;\sigma]$ is defined in the same way as the polynomial ring $S[X]$, except that $Xa = \sigma(a)X$ for $a \in S$.

(ii) A polynomial of the form $g(X) = X^k + p(g_{k-1}X^{k-1} + \cdots + g_1X + g_0) \in S[X;\sigma]$ where $g_0 \in S \setminus pS$ is said to be an *Eisenstein polynomial*.

Theorem

Suppose R is a finite chain ring with invariants (q,m) and characteristic p^s ($1 \le s \le m$). Let $S = \mathrm{GR}(q^s,p^s)$. Then there exist (unique) integers k,t satisfying $m = (s-1)k + t$, $1 \le t \le k$ ($k = t = m$ if $s = 1$), an automorphism $\sigma \in \operatorname{Aut} S$ and a (possibly nonunique) Eisenstein polynomial $g(X) \in S[X;\sigma]$ such that

$$R \cong S[X;\sigma]/\big(g(X), p^{s-1}X^t\big).$$

The Case $m = 2$

Corollary

Suppose R is a finite chain ring with residue class field $\mathbb{F}_q$, $q = p^r$, and nilpotency index $m = 2$. Then $|R| = q^2$, and either

(i) *R has characteristic p^2 and $R \cong \mathrm{GR}(q^2, p^2)$, or*

(ii) *R has characteristic p and there exists $\sigma \in \mathrm{Aut}\,\mathbb{F}_q$ such that $R \cong \mathbb{F}_q[X;\sigma]/(X^2)$.*

Thus there are exactly $r+1$ isomorphism types of such rings. Two of them, $\mathbb{G}_q := \mathrm{GR}(q^2, p^2)$ and $\mathbb{S}_q := \mathbb{F}_q[X;\mathrm{id}]/(X^2) = \mathbb{F}_q[X]/(X^2)$, are commutative.

Example

The chain rings of order ≤ 16 with $m = 2$ are

$|R| = 4$ $\quad \mathbb{G}_2 = \mathbb{Z}_4, \quad \mathbb{S}_2 = \mathbb{Z}_2[X]/(X^2)$

$|R| = 9$ $\quad \mathbb{G}_3 = \mathbb{Z}_9, \quad \mathbb{S}_3 = \mathbb{Z}_3[X]/(X^2)$

$|R| = 16$ $\quad \mathbb{G}_4 = \mathbb{Z}_4[X]/(X^2+X+1)$, $\mathbb{S}_4 = \mathbb{F}_4[X]/(X^2)$, and $\mathbb{T}_4 = \mathbb{F}_4[X; a \mapsto a^2]/(X^2)$ with multiplication $(a_0 + a_1X)(b_0 + b_1X) = a_0b_0 + (a_0b_1 + a_1b_0^2)X$.

Consider first the special case $R = \mathbb{Z}_{p^m}$. A $\mathbb{Z}_{p^m}$-module is the same thing as an Abelian group of exponent dividing p^m (i.e. the additively written abelian group G satisfies $p^m G = \{p^m x; x \in G\} = \{0\}$).

The following is well-known:

Theorem

For every finite abelian p-group G there exists a unique sequence of integers $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r \geq 1$ *such that*

$$G \cong \mathbb{Z}_{p^{\lambda_1}} \oplus \mathbb{Z}_{p^{\lambda_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\lambda_r}}.$$

The group G satisfies $p^m G = \{0\}$ *iff* $\lambda_1 \leq m$.

Now we shall generalize this theorem to modules over arbitrary finite chain rings (and thereby reprove it).

Some Notation

R denotes a finite chain ring with invariants (q, m) and radical $N = R\theta$ (where $\theta \in N \setminus N^2$ is chosen arbitrarily). All modules considered will be finite.

Definition

For a left R-module ${}_RM$ and $x \in M$ we say

(i) x has *period* θ^i, if $i \in \{0, 1, \ldots, m\}$ is the smallest integer satisfying $\theta^i x = 0$;

(ii) x has *height* i, if $i \in \{0, 1, \ldots, m\}$ is the largest integer satisfying $x = \theta^i y$ for some $y \in M$.

We also define $M^\times := \{x \in M; \operatorname{period}(x) = \theta^m\}$ ("units of ${}_RM$").

Remarks

- $0 \in M$ is the only element with period $\theta^0 = 1$ (resp., height m)
- If x has period θ^i, then $R \to Rx$, $r \mapsto rx$ has kernel $R\theta^i = N^i$. Hence $Rx \cong R/N^i$ as left R-modules, and $Rx \cong R$ iff $x \in M^\times$.

Further we define

$$\theta^i M := \{\theta^i x; x \in M\},$$
$$M[\theta^i] := \{x \in M; \theta^i x = 0\},$$
$$V_i := M[\theta] \cap \theta^{i-1} M.$$

All these sets are submodules of ${}_R M$ (since $R\theta^i = \theta^i R$).

We have the submodule chains

$$M = \theta^0 M \supseteq \theta^1 M \supseteq \theta^2 M \supseteq \cdots \supseteq \theta^m M = \{0\},$$
(upper Loewy series of ${}_R M$)

$$M = M[\theta^m] \supseteq M[\theta^{m-1}] \supseteq \cdots \supseteq M[\theta^0] = \{0\},$$
(lower Loewy series of ${}_R M$)

whose successive quotients are vector spaces over $R/N \cong \mathbb{F}_q$ (since they are annihilated by θ),

and the chain of R/N-spaces

$$M[\theta] = V_1 \supseteq V_2 \supseteq \cdots \supseteq V_m \supseteq \{0\}$$
(Ulm-Kaplansky series of ${}_R M$)

Proposition

(i) *For* $1 \le i \le m$ *we have* $\dim_{R/N}\left(\theta^{i-1}M/\theta^{i}M\right) = \dim_{R/N}\left(M[\theta^{i}]/M[\theta^{i-1}]\right) = \dim_{R/N}\left(M[\theta] \cap \theta^{i-1}M\right)$.

(ii) *The integers* $\mu_i := \dim_{R/N}\left(M[\theta] \cap \theta^{i-1}M\right)$, $1 \le i \le m$ *(Ulm-Kaplansky invariants of* ${}_RM$*) satisfy* $\mu_1 \ge \mu_2 \ge \cdots \ge \mu_m$ *and* $\mu_1 + \mu_2 + \cdots + \mu_m = \log_q |M|$.

Proof.

(i) The map $\theta^{i-1}M \to \theta^{i}M$, $x \mapsto \theta x$ induces an (additive) isomorphism $\theta^{i-1}M/\left(M[\theta] \cap \theta^{i-1}M\right) \cong \theta^{i}M$. Hence

$$\frac{\left|\theta^{i-1}M\right|}{\left|M[\theta] \cap \theta^{i-1}M\right|} = \left|\theta^{i}M\right| \quad \text{and} \quad \left|\theta^{i-1}M/\theta^{i}M\right| = \left|M[\theta] \cap \theta^{i-1}M\right|.$$

Similarly, $M[\theta^{i}] \to M[\theta]$, $x \mapsto \theta^{i-1}x$ induces an isomorphism $M[\theta^{i}]/M[\theta^{i-1}] \to M[\theta] \cap \theta^{i-1}M$, proving the second equality.

(ii) The inequality $\mu_i \ge \mu_{i+1}$ follows from $\mu_i = \dim_{R/N}(V_i)$ and $V_i \supseteq V_{i+1}$. Part (i) and the upper Loewy series give $|M| = \prod_{i=1}^{m}\left|\theta^{i-1}M/\theta^{i}M\right| = q^{\mu_1+\cdots+\mu_m}$. □

Example

Let $R = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, $M = \mathbb{Z}_4^n$, $\theta = 2$ (the only choice for θ).

The possible periods (heights) of $\mathbf{x} \in \mathbb{Z}_4^n$ are $1, 2, 4$ (resp. $0, 1, 2$).

$\mathbf{x} \in \mathbb{Z}_4^n$ has period 1 (height 2) iff $\mathbf{x} = \mathbf{0}$
$\mathbf{x}$ has period 2 (height 1) iff $2\mathbf{x} = \mathbf{0} \wedge \mathbf{x} \neq \mathbf{0}$ iff $x_i \in \{0, 2\}$ and at least one $x_i = 2$.
$\mathbf{x}$ has period 4 (height 0) iff at least one $x_i \in \{1, 3\}$.

We have $\mathbb{Z}_4^n[2] = 2\mathbb{Z}_4^n$, so both Loewy series coincide (a property of free modules in general).

The factors are
$2\mathbb{Z}_4^n \cong \mathbb{Z}_2^n$ (divide the entries of $\mathbf{x}$ by 2)
$\mathbb{Z}_4^n / 2\mathbb{Z}_4^n \cong \mathbb{Z}_2^n$ (read the entries of $\mathbf{x}$ modulo 2)

Example

Let C be the linear code of even length n over $\mathbb{Z}_4$ generated by

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 2 & 2 & 0 & \dots & 0 \\ 0 & 2 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 2 & 2 \end{pmatrix}$$

$2C = \{00\dots0, 22\dots2\}$
$C[2]$ is either $2\mathbb{Z}_4^n$ (if n is odd) or the even-weight subcode of $2\mathbb{Z}_4^n$ (if n is even)

So the Loewy series $C \supset 2C \supset \{0\}$ and $C \supset C[2] \supset \{0\}$ are different, but its factors $C/2C \cong C[2]$ and $C/C[2] \cong 2C$ are the same.

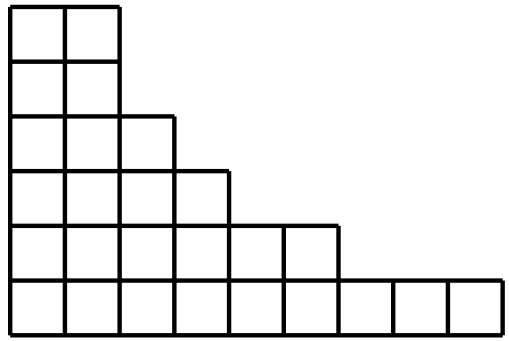
Partitions of integers

Definition

An *(integer) partition* is a sequence $\lambda = (\lambda_1, \lambda_2, \dots)$ with $\lambda_i \in \mathbb{Z}$, $\lambda_1 \geq \lambda_2 \geq \cdots$, and $\lambda_i = 0$ for all but finitely many i. The numbers $\lambda_i > 0$ are called the *parts* of λ, and $|\lambda| = \lambda_1 + \lambda_2 + \cdots$ is called the *weight* of λ. If $|\lambda| = n$, we say that λ is an (unordered) partition of n and write $\lambda \vdash n$.

Trailing zeros are usually suppressed, e.g. $(2, 1, 1, 0, 0, \dots)$ is written as $(2, 1, 1)$, or as $4 = 2 + 1 + 1$.

A partition λ is often visualized by an (empty) *Young tableaux* T_λ, shown here for $\lambda = (6, 6, 4, 3, 2, 2, 1, 1, 1) \vdash 26$:



Think of T_λ as the union of all unit squares in the Euclidean plane whose upper right corners have coordinates (i, j) where $i \geq 1$ and $1 \leq j \leq \lambda_i$.

Definition

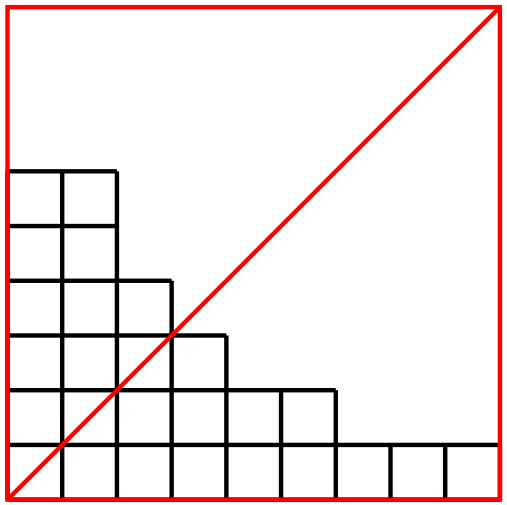
Let λ be a partition. The *conjugate* λ' of λ is the partition whose Young tableaux $T_{\lambda'}$ is obtained from T_λ by a reflection at the line $y = x$.

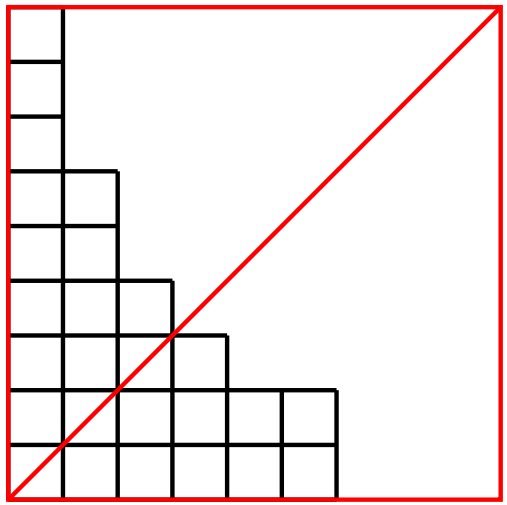
Properties

- If $\lambda \vdash n$ then also $\lambda' \vdash n$.
- The parts of λ' are $\lambda'_i = |\{j; \lambda_j \geq i\}|$.
- The largest part λ'_1 of λ' is equal to the number of parts of λ.

Example

The conjugate of $\lambda = (6, 6, 4, 3, 2, 2, 1, 1, 1)$ is $\lambda' = (9, 6, 4, 3, 2, 2)$.





The Module Classification Theorem

Theorem

For any finite module ${}_RM$ there exists a uniquely determined partition $\lambda \vdash \log_q |M|$ into parts $\lambda_i \leq m$ such that

$$ {}_RM \cong R/N^{\lambda_1} \oplus R/N^{\lambda_2} \oplus \cdots \oplus R/N^{\lambda_r}. $$

(Here r denotes the number of parts of λ.)

Remarks

- The theorem holds mutatis mutandis for right modules M_R.
- The theorem says in particular that every finite R-module is a direct sum of cyclic R-modules.

Proof of the theorem.

Uniqueness part: Suppose ${}_RM \cong \bigoplus_{i=1}^{r} R/N^{\lambda_i}$.
The upper Loewy series of R/N^{λ_i} is clearly

$$R/N^{\lambda_i} \supsetneq N/N^{\lambda_i} \supsetneq N^2/N^{\lambda_i} \supsetneq \cdots \supsetneq N^{\lambda_i}/N^{\lambda_i} = \{0\}$$

with all successive quotients 1-dimensional over R/N.
Hence

$$\dim_{R/N}\left(\theta^{j-1}M/\theta^{j}M\right) = |\{i; \lambda_i \geq j\}| = \lambda'_j$$

This shows that λ' (and hence λ) is uniquely determined by ${}_RM$.

Existence part: Since any cyclic R-module is isomorphic to R/N^i for some $i \leq m$, it suffices to prove that ${}_RM$ is a direct sum of cyclic R-modules. We use induction on $|M|$.

Assume $M \neq \{0\}$ (otherwise the assertion is clear) and choose $x_1 \in M$ of maximal period θ^{λ_1}. By induction,

$$M/Rx_1 = Ry_2 \oplus \cdots \oplus Ry_r. \qquad (\star)$$

Let $x_i \in M$ such that $y_i = x_i + Rx_1$ $(2 \leq i \leq r)$. Then

$$M = Rx_1 + Rx_2 + \cdots + Rx_r. \qquad (\star\star)$$

To make $(\star\star)$ a direct sum decomposition, the x_i's must be chosen in a special way.

Suppose y_i has period θ^{λ_i}, i.e. $\theta^{\lambda_i} x_i \in Rx_1$ and λ_i is the smallest such integer.

There exists $r \in R$ such that $\theta^{\lambda_i} x_i = \theta^{\lambda_i} a x_1$. (Otherwise the period of x_1 would be smaller than the period of x_i.)
Then $\theta^{\lambda_i}(x_i - a x_1) = 0$, and so $x_i - a x_1$ has period θ^{λ_i}.
Replacing x_i by $x_i - a x_1$, we may assume that the x_i's in $(\star\star)$ have the same period θ^{λ_i} as the y_i's in $(\star)$.

Proof cont'd.

Now suppose

$$a_1x_1 + a_2x_2 + \cdots + a_rx_r = 0 \quad \text{where } a_i \in R$$

Modulo Rx_1 this reads $a_2y_2 + \cdots + a_ry_r = 0$, and $(\star)$ gives $a_2y_2 = \cdots = a_ry_r = 0$.

Since x_i has the same period as y_i, we conclude $a_2x_2 = \cdots = a_rx_r = 0$, and further $a_1x_1 = 0$. □

Definition

The partition $\lambda \vdash \log_q |M|$ such that ${}_RM \cong \bigoplus_{i=1}^{r} R/N^{\lambda_i}$ is called the *shape* (or *type*) of ${}_RM$. The conjugate partition λ', which satisfies $\lambda'_i = \dim_{R/N}\left(\theta^{i-1}M/\theta^i M\right)$, is called the *conjugate shape* of ${}_RM$. The integer $r = \lambda'_1$ (number of nonzero summands in a direct sum decomposition of ${}_RM$ into cyclic R-modules) is called the *rank* of ${}_RM$ (and denoted by $\operatorname{rk} M$).

Definition

A sequence $x_1, x_2, \ldots, x_s$ of elements of ${}_RM$ is said to

(i) *independent* if $a_1x_1 + a_2x_2 + \cdots + a_sx_s = 0$ with $a_i \in R$ implies $a_ix_i = 0$ for $1 \le i \le s$;

(ii) a *basis* of ${}_RM$ if $x_1, \ldots, x_r$ are independent and generate ${}_RM$;

(iii) *linearly independent* if $a_1x_1 + a_2x_2 + \cdots + a_sx_s = 0$ with $a_i \in R$ implies $a_i = 0$ for $1 \le i \le s$.

Remarks

- Properties (ii) is equivalent to ${}_RM = Rx_1 \oplus \cdots \oplus Rx_s$.
- Property (iii) is equivalent to (i) and $x_i \in M^\times$ for $1 \le i \le s$.

Example

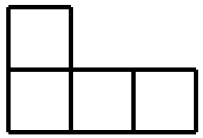
Consider the linear codes C_3, C_4 over $\mathbb{Z}_4$ generated by

$$\mathbf{G}_3 = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix} \quad \text{resp.} \quad \mathbf{G}_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

The rows of $\mathbf{G}_3$ are independent, hence a basis of C_3.

The first 3 rows of $\mathbf{G}_4$ form a basis of C_4 (since they are independent, and the last row is a linear combination of the 1st and 2nd row).

Hence both modules have the same shape $\lambda = (2, 1, 1)$ with Young diagram



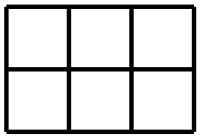
rank equal to 3 and cardinality $|C_3| = |C_4| = 2^{2+1+1} = 16$.

Example

The linear code over $\mathbb{Z}_4$ generated by

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

has shape $\lambda = (2, 2, 2)$ with Young diagram



rank 3 and cardinality $2^{2+2+2} = 64$.

Free Modules

Recall that ${}_RM$ is free if ${}_RM \cong R^k$ for some integer $k \geq 0$. (The integer k is the rank of M.) Equivalently, ${}_RM$ has "rectangular" shape $(m, m, \ldots, m)$.

Free modules are important, since they are the ambient spaces for both linear codes and projective Hjelmslev geometries over R.

Definition

Let ${}_RM$ be free of rank k. The *projective geometry* $\mathrm{PG}({}_RM)$ is the lattice of all submodules of ${}_RM$. A free submodule $U \leq {}_RM$ of rank 1 (rank $k-1$, rank $s+1$) is said to be a *point* (resp. *hyperplane*, *s-flat*) of $\mathrm{PG}({}_RM)$.

Important problems

- Determine the number of points (hyperplanes, s-flats, or in general λ-shaped submodules) of $\mathrm{PG}({}_RM)$.
- How many hyperplanes contain a given point (s-flat, or λ-shaped submodule)?

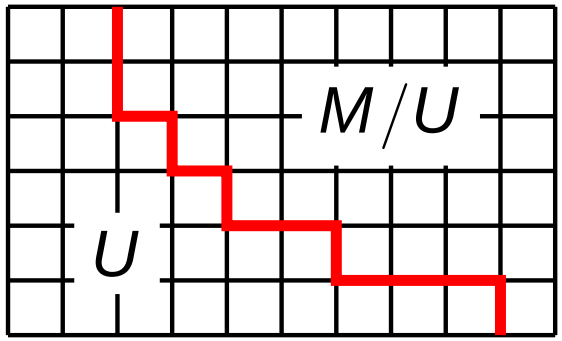
Theorem

Suppose ${}_RM$ is free of rank k, and U is a (not necessarily free) submodule of ${}_RM$ of shape λ and rank s.

1. *For every basis $x_1, \ldots, x_s$ of U there exists a basis $y_1, \ldots, y_k$ of M such that $x_i \in Ry_i$ for $1 \le i \le s$. (Bases of U and M related in this way are called stacked bases.)*
2. *The quotient module M/U has shape $(m - \lambda_k, m - \lambda_{k-1}, \ldots, m - \lambda_1)$.*
3. *If $U^* \neq \emptyset$ then U is the sum of its free rank 1 submodules (i.e., points).*
4. *If $(M/U)^* \neq \emptyset$ then U is the intersection of all free rank $k-1$ submodules of ${}_RM$ (i.e., hyperplanes) containing U.*

Remark

Part (2) says that the shape of M/U is the complement of λ in the $k \times m$-rectangle corresponding to M.



Lemma

If ${}_RM$ is free then $M[\theta^i] = \theta^{m-i}M$ for $0 \le i \le m$.

Proof.

Suppose M is free of rank k. For the shape λ of ${}_RM$ this means

$$\lambda_1 = \cdots = \lambda_k = m, \quad \lambda'_1 = \cdots = \lambda'_m = k.$$

So $\left|M[\theta^i]/M[\theta^{i-1}]\right| = q^{\lambda'_i} = q^k$ for $1 \le i \le m$, and hence $\left|M[\theta^i]\right| = q^{ki}$ for $0 \le i \le m$.

By a similar argument using the upper Loewy series of ${}_RM$ we have $\left|\theta^i M\right| = q^{k(m-i)}$.

Hence $\left|M[\theta^i]\right| = \left|\theta^{m-i}M\right|$ for $0 \le i \le m$. Together with $\theta^{m-i}M \subseteq M[\theta^i]$ this gives $M[\theta^i] = \theta^{m-i}M$ for $0 \le i \le m$. □

Remark

Suppose R is a proper chain ring (i.e. $m \ge 2$). If there exists $i \in \{1, 2, \ldots, m-1\}$ such that $M[\theta^i] = \theta^{m-i}M$, then ${}_RM$ is necessarily free.

Proof of the theorem.

(1) Suppose M is free of rank k, $U \leq M$ has shape λ, and $x_1, \ldots, x_s$ is a basis of U with x_i of period θ^{λ_i}.
$M[\theta^{\lambda_i}] = \theta^{m-\lambda_i} M \Rightarrow \exists y_i \in M$ with $x_i = \theta^{m-\lambda_i} y_i$ $(1 \leq i \leq s)$.
$y_1, \ldots, y_s$ are linearly independent (since their period is θ^m), hence may be extended to a basis $y_1, \ldots, y_k$ of M (e.g., by first extending $\theta^{m-1}y_1, \ldots, \theta^{m-1}y_s$ to a basis of the R/N-space $M[\theta]$ and then proceeding as before).

(2) With y_i as in (1) we have

$$\begin{aligned} M/U &\cong Ry_1/Rx_1 \oplus \cdots \oplus Ry_s/Rx_s \oplus R^{k-s} \\ &\cong R/N^{m-\lambda_1} \oplus \cdots \oplus R/N^{m-\lambda_s} \oplus R/N^m \oplus \cdots \oplus R/N^m \\ &= R/N^{m-\lambda_1} \oplus \cdots \oplus R/N^{m-\lambda_k}. \end{aligned}$$

(3) $U^\times \neq \emptyset$ is equivalent to $\lambda_1 = m$, i.e. $x_1 \in M^\times$.
For $j \geq 2$, if $x_j \notin U^\times$ then $x_1 + x_j \in U^\times$, so U is generated by $U^\times$.

(4) $(M/U)^* \neq \emptyset$ is equivalent to $\lambda_k = 0$. In this case U is contained in the hyperplane $H = Ry_1 + \cdots + Ry_{k-1}$.
For $z \in H \setminus U$, $z = r_1y_1 + \cdots + r_{k-1}y_{k-1}$ with $\theta^{m-\lambda_j} \nmid r_j$, say, let H' be the hyperplane obtained from H by replacing y_j by $y_j + \theta^{\lambda_j} y_k$.
One easily checks that $U \subseteq H'$, but $z \notin H'$. □

Embedding into Free Modules

Definition

Suppose ${}_RM$, ${}_RM'$ are modules over R. A mapping $\phi\colon {}_RM \to {}_RM'$ is said to be *semilinear with associated ring homomorphism* $\sigma\colon R \to R$ if $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(rx) = \sigma(r)\phi(x)$ for all $x, y \in M$ and $r \in R$.

Remarks

- Semilinear mappings are important in geometry ($\longrightarrow$ *Fundamental Theorem of Projective Hjelmslev Geometry*)
- If $M^\times \neq \emptyset$ and ϕ is in an embedding, then $\sigma \in \operatorname{Aut} R$ and σ is uniquely determined by ϕ. In this case ϕ preserves free modules.
- The group of all R-linear (R-semilinear) isomorphisms $\phi\colon {}_RM \to {}_RM$ is denoted by $\mathrm{GL}({}_RM)$ (resp. $\Gamma\mathrm{L}({}_RM)$).

Proposition

For every module ${}_RM$ there exists a minimal free module ${}_RH$ containing ${}_RM$. More precisely, there exists an R-linear embedding $\iota\colon {}_RM \to {}_RH$ such that no proper free submodule of ${}_RH$ contains $\iota(M)$.

Proof.

The minimality of ${}_RH$ is equivalent to $\operatorname{rk} H = \operatorname{rk} M$. In this case ${}_RH$ contains a submodule of the same shape as ${}_RM$. □

Theorem

Let ${}_RM$ be a finite module with $M^\times \neq \emptyset$ 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.*

The theorem allows us to restrict attention to free R-modules in most situations.

Main idea of the proof.

Reduction to the R-linear case:

$\phi\colon {}_RM \to {}_RF$ is semilinear iff ϕ is linear as a map from ${}_RM$ to ${}_RF^\sigma$, where ${}_RF^\sigma$ has scalar multiplication defined by $rx := \sigma(r)x$.

The proof can be completed using either the existence of stacked bbases for ${}_RM$ and ${}_RH$ or the fact that ${}_RH$ is an *injective hull* of ${}_RM$. □

Counting Formulas for Submodules

First recall the following

Fact

An n-dimensional vector space over $\mathbb{F}_q$ has exactly

$$\begin{aligned}\binom{n}{k}_q &:= \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} \\ &= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}\end{aligned}$$

k-dimensional subspaces.
In particular, an $n-1$-dimensional projective geometry over $\mathbb{F}_q$ has $\frac{q^n-1}{q-1}$ points and the same number hyperplanes.

Question

Let R be a finite chain ring with invariants (q,m). How many points (hyperplanes) does the projective geometry $\mathrm{PG}({}_RR^n)$ have?

Answer

A free cyclic submodule of ${}_RR^n$ has the form $R\mathbf{x} = R(x_1, \ldots, x_n)$ where at least one $x_i \in R^\times$.
Normalize $\mathbf{x}$ by setting the first unit coordinate equal to 1.

For fixed $i \in \{1, \ldots, n\}$ there are

$$|N|^{i-1}\,|R|^{n-i} = q^{(m-1)(i-1)+m(n-i)} = q^{mn-m-i+1}$$

choices for $\mathbf{x}$, such that $x_i = 1$ and $x_j \notin R^\times$ for $j < i$.
Hence the number of points of $\mathrm{PG}({}_RR^n)$ is

$$\sum_{i=1}^{n} q^{mn-m-i+1} = q^{(m-1)(n-1)} \sum_{i=1}^{n} q^{n-i} = q^{(m-1)(n-1)} \cdot \frac{q^n - 1}{q - 1}.$$

To count the number of hyperplanes we could

- either use some duality theory to conclude (hopefully) that the number of points and hyperplanes is the same,
- or prove a general counting formula for the number of μ-shaped submodules of a λ-shaped module and specialize this to the case at hand.

The General Counting Formula

For $U \leq {}_RM$ we have $U[\theta] \cap \theta^{i-1}U \subseteq M[\theta] \cap \theta^{i-1}M$.
$\Rightarrow$ The shapes λ, μ of ${}_RM$ resp. ${}_RU$ satisfy $\mu \leq \lambda$ (part-wise).

Theorem

Let ${}_RM$ be a module of shape λ. For every partition μ satisfying $\mu \leq \lambda$ the module ${}_RM$ has exactly

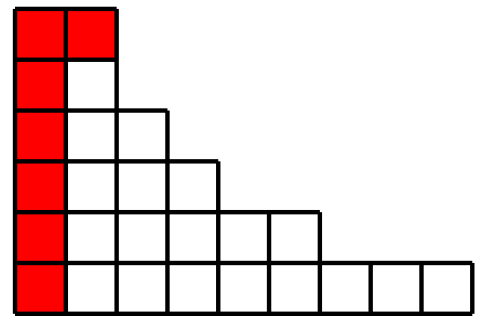
$$\alpha_\lambda(\mu; q) := \prod_{i=1}^{m} q^{\mu'_{i+1}(\lambda'_i - \mu'_i)} \cdot \begin{pmatrix} \lambda'_i - \mu'_{i+1} \\ \mu'_i - \mu'_{i+1} \end{pmatrix}_q$$

submodules of shape μ. In particular, the number of free rank 1 submodules of ${}_RM$ equals

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

Remark

One can memorize the 2nd formula as follows: The top row and first column of λ (consisting of $\lambda'_m + m - 1$ squares) account for $\frac{q^{\lambda'_m}-1}{q-1}$ points. Each further square accounts for a factor q.



Proof.

Let $V_i := M[\theta] \cap \theta^{i-1}M$, and for $U \leq {}_RM$ similarly $U_i := U[\theta] \cap \theta^{i-1}U$ $(1 \leq i \leq m)$.
Then $U_i \subseteq V_i$, $\dim_{R/N}(V_i) = \lambda_i$, and $\dim_{R/N}(U_i) = \mu_i$. $(\star)$

There are $\prod_{j=1}^{m} \binom{\lambda'_i - \mu'_{i+1}}{\mu'_i - \mu'_{i+1}}_q$ possible ways to choose the Ulm-Kaplansky chain $U_1 \supseteq U_2 \supseteq \cdots \supseteq U_m$ for ${}_RU$ subject to $(\star)$.

Let $x_1, \ldots, x_{\mu'_1}$ be a basis of U_1 such that for every i the subsequence $x_1, \ldots, x_{\mu'_i}$ is a basis of U_i.

A basis $y_1, \ldots, y_{\mu'_1}$ for ${}_RU$ such that $\theta^{\mu_j - 1}y_j = x_j$ for all j can be chosen in $\prod_{j=1}^{\mu'_1} \left|M[\theta^{\mu_j - 1}]\right|$ ways. Two such bases (y_j), (y'_j) yield the same submodule U iff $y_j - y'_j \in U[\theta^{\mu_j - 1}]$ for all j.

Now $\left|M[\theta^i]\right| = q^{\lambda'_1 + \cdots + \lambda'_i}$, $\left|U[\theta^i]\right| = q^{\mu'_1 + \cdots + \mu'_i}$, so there are exactly

$$\prod_{j=1}^{\mu'_1} \frac{\left|M[\theta^{\mu_j - 1}]\right|}{\left|U[\theta^{\mu_j - 1}]\right|} = \prod_{j=1}^{\mu'_1} q^{\sum_{i=1}^{\mu_j - 1}(\lambda'_i - \mu'_i)}$$

$$= q^{\sum_{i \geq 1} \left|\{j; \mu_j \geq i+1\}\right| (\lambda'_i - \mu'_i)} = q^{\sum_{i \geq 1} \mu'_{i+1}(\lambda'_i - \mu'_i)}$$

submodules U with Ulm-Kaplansky chain $U_1 \supseteq \cdots \supseteq U_m$. □

Corollary

Let ${}_RM$ be a free module of rank n. The number of submodules of ${}_RM$ with complementary shapes $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ resp. $\overline{\mu} = (m - \mu_n, m - \mu_{n-1} \ldots, m - \mu_1)$ is the same. In particular, $\mathrm{PG}({}_RM)$ *has the same number of points and hyperplanes.*

Proof.

$\overline{\mu}' = (n - \mu'_m, n - \mu'_{m-1}, \ldots, n - \mu'_1)$.

The number of chains $\overline{U_1} \supseteq \overline{U_2} \supseteq \cdots \supseteq \overline{U}_m$ of subspaces of a n-dimensional vector space satisfying $\dim \overline{U_i} = n - \mu'_{m+1-i}$ equals the number of chains $U_1 \supseteq U_2 \supseteq \cdots \supseteq U_m$ of subspaces satisfying $\dim U_i = \mu'_i$ (by duality).

Hence the second factor $\prod_{i=1}^{m} \binom{n-\mu'_{i+1}}{\mu'_i - \mu'_{i+1}}_q$ is invariant under complementation.

Further

$$\sum_{i=1}^{m-1} \mu'_{i+1}(n - \mu'_i) = \sum_{i=1}^{m-1} (n - \overline{\mu}'_{m-i})\overline{\mu}'_{m-i+1} = \sum_{j=1}^{m-1} \overline{\mu}'_{j+1}(n - \overline{\mu}'_j),$$

so the first factor $q^{\sum_{i=1}^{m-1} \cdots}$ is invariant as well. □

Applications

Example

The module ${}_RR^n$ has conjugate shape $\lambda' = (n, n, \ldots, n)$. Using the general formula, the number of points (hyperplanes) of $\mathrm{PHG}({}_RR^n)$ is equal to

$$q^{\lambda'_1-1+\lambda'_2-1+\cdots+\lambda'_{m-1}-1} \cdot \begin{bmatrix} \lambda'_m \\ 1 \end{bmatrix}_q = q^{n-1+\cdots+n-1} \begin{bmatrix} n \\ 1 \end{bmatrix}_q$$
$$= q^{(m-1)(n-1)} \cdot \frac{q^n - 1}{q - 1}.$$

Example

Suppose $R\mathbf{x}$ is a point of $\mathrm{PHG}({}_RR^n)$. A point $R\mathbf{y}$ is an i-th neighbour of $R\mathbf{x}$ iff $R\mathbf{y} \subseteq R\mathbf{x} + \theta^i R^n$.
The module $R\mathbf{x} + \theta^i R^n$ has shape $(m, m-i, \ldots, m-i)$ and conjugate shape $(\underbrace{n, \ldots, n}_{m-i}, \underbrace{1, \ldots, 1}_{i})$.

Hence

$$|[R\mathbf{x}]_i| = q^{(m-i)(n-1)} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}_q = q^{(m-i)(n-1)}.$$

Example

The number of $s-1$-dimensional Hjelmslev subspaces of $\mathrm{PHG}({}_RR^n)$ (free rank s submodules of ${}_RR^n$) is obtained by plugging $\lambda' = (n, n, \ldots, n)$ and $\mu' = (s, s, \ldots, s)$ into the general formula:

$$\prod_{i=1}^{m} q^{\mu'_{i+1}(\lambda'_i - \mu'_i)} \cdot \begin{bmatrix} \lambda'_i - \mu'_{i+1} \\ \mu'_i - \mu'_{i+1} \end{bmatrix}_q = q^{s(n-s)+\cdots+s(n-s)} \cdot \begin{bmatrix} n \\ s \end{bmatrix}_q$$

$$= q^{s(n-s)(m-1)} \cdot \begin{bmatrix} n \\ s \end{bmatrix}_q .$$

Now suppose U is a free rank t submodule of ${}_RR^n$.

A submodule $V \supseteq U$ is free of rank s iff V/U (a submodule of ${}_RR^n/{}_RU \cong {}_RR^{n-t}$ is free of rank $s-t$.

$\Rightarrow$ The number of $s-1$-dimensional Hjelmslev subspaces of $\mathrm{PHG}({}_RR^n)$ of $\mathrm{PHG}({}_RR^n)$ through a fixed $t-1$-dimensional Hjelmslev subspace is equal to

$$q^{(s-t)(n-t-(s-t))(m-1)} \cdot \begin{bmatrix} n-t \\ s-t \end{bmatrix}_q = q^{(s-t)(n-s)(m-1)} \cdot \begin{bmatrix} n-t \\ s-t \end{bmatrix}_q .$$

Remark

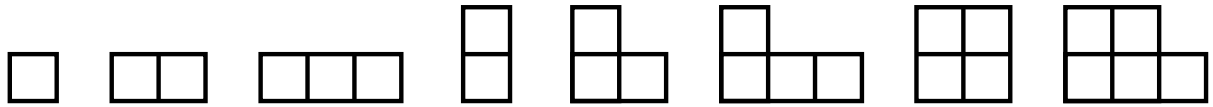
The preceding formula is a special case of the following

Proposition

Let λ, μ partitions with $\mu \le \lambda \le (\underbrace{m, m, \ldots, m}_{n})$. Then every submodule $U \le {}_R R^n$ of shape μ is contained in exactly $\alpha_{\overline{\mu}}(\overline{\lambda}; q)$ submodules $V \le M$ of shape λ, where $\overline{\lambda}$, $\overline{\mu}$ denote the complementary shapes of λ, μ (i.e. the shapes of R^n/U resp. R^n/V).

Example

The $\mathbb{Z}_4$-module $\mathbb{Z}_4^3$ has the following number of submodules of each shape:

shape	
#submodules	7 7 1 28 42 7 28 7

Structure of Linear Codes

For linear codes over R (i.e. submodules $C \leq {}_R R^n$) the structure theorem for R-modules says:
There exists a uniquely determined partition λ into at most n parts, all of which are $\leq m$, such that ${}_R C$ has a basis $\mathbf{c}_1, \ldots, \mathbf{c}_k$ ($k = \lambda'_1 = \operatorname{rk} C$) with corresponding periods $\theta^{\lambda_1}, \ldots, \theta^{\lambda_k}$.

Since ${}_R R^n$ is free, $\mathbf{c}_i$ has height $m - \lambda_i$ in ${}_R R^n$, i.e.

$$\mathbf{c}_i = (\theta^{m-\lambda_i} c_{i1}, \theta^{m-\lambda_i} c_{i2}, \ldots, \theta^{m-\lambda_i} c_{in})$$

with at least one c_{ij} not divisible by θ.

The number of codewords of C is

$$|C| = q^{|\lambda|} = q^{\lambda_1 + \cdots + \lambda_k}.$$

Theorem

Every linear code $C \leq {}_R R^n$ is permutation equivalent to a linear code generated by a matrix of the following form:

$$\mathbf{G} := \begin{pmatrix} \mathbf{I}_{k_0} & \mathbf{A}_{01} & \mathbf{A}_{02} & \dots & \mathbf{A}_{0,m-1} & \mathbf{A}_{0,m} \\ \mathbf{0} & \theta\mathbf{I}_{k_1} & \theta\mathbf{A}_{12} & \dots & \theta\mathbf{A}_{1,m-1} & \theta\mathbf{A}_{1,m} \\ \mathbf{0} & \mathbf{0} & \theta^2\mathbf{I}_{k_2} & \dots & \theta^2\mathbf{A}_{2,m-1} & \theta^2\mathbf{A}_{2,m} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \theta^{m-1}\mathbf{I}_{k_{m-1}} & \theta^{m-1}\mathbf{A}_{m-1,m} \end{pmatrix}$$

Here $k_i \geq 0$ are integers satisfying $k_0 + k_1 + \cdots + k_{m-1} \leq n$, $\mathbf{I}_{k_i}$ denote $k_i \times k_i$ identity matrices over R, and with $k_m := n - \sum_{i=0}^{m-1} k_i$ we have $\mathbf{A}_{ij} \in R^{k_i \times k_j}$ for all $i < j$.

Proof.

Suppose ${}_R C$ has shape λ. Let $k_i := \lambda'_{m-i} - \lambda'_{m-i+1}$ denote the number of parts of λ equal to $m - i$. Then $k = \mathrm{rk}({}_R C) = k_0 + k_1 + \cdots + k_{m-1}$.

Arrange the basis $\mathbf{c}_1, \dots, \mathbf{c}_k$ of ${}_R C$ as rows of a matrix $\mathbf{G} \in R^{k \times n}$ (in that order). Then the first k_0 rows of $\mathbf{G}$ have height 0, the next k_1 rows have height 1, etc.

Performing Gaussian elimination and permuting columns, if necessary, we can transform $\mathbf{G}$ into the required form. □

Remarks

- In terms of $k_0, k_1, \ldots, k_{m-1}$, the number of codewords of C is

$$(q^m)^{k_0}(q^{m-1})^{k_1}\cdots q^{k_{m-1}} = q^{\sum_{i=0}^{m-1}(m-i)k_i}.$$

- The submodules $C_i := C[\theta^i] \cap \theta^{i-1}C$ of the Ulm-Kaplansky series of C are visible in $\mathbf{G}$ as follows: If we define

$$\mathbf{G}' := \theta^{m-1}\begin{pmatrix} \mathbf{I}_{k_0} & \mathbf{A}_{01} & \mathbf{A}_{02} & \cdots & \mathbf{A}_{0,m-1} & \mathbf{A}_{0,m} \\ \mathbf{0} & \mathbf{I}_{k_1} & \mathbf{A}_{12} & \cdots & \mathbf{A}_{1,m-1} & \mathbf{A}_{1,m} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_{k_2} & \cdots & \mathbf{A}_{2,m-1} & \mathbf{A}_{2,m} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{I}_{k_{m-1}} & \mathbf{A}_{m-1,m} \end{pmatrix}, \quad (\star)$$

  then $C_1 = C[\theta]$ is generated by $\mathbf{G}'$ (which has $k_0 + \cdots + k_{m-1}$ rows), $C_2 = C[\theta] \cap \theta C$ by the first $k_0 + \cdots + k_{m-2}$ rows of $\mathbf{G}'$, $\ldots$, and finally $C_m = C[\theta] \cap \theta^{m-1}C$ by the first k_0 rows of $\mathbf{G}'$.

- Using the isomorphism $\theta^{m-1}R = N^{m-1} \cong R/N$, we can consider the C_i's as classical linear codes over $\mathbb{F}_q$. (Simply omit the factor θ^{m-1} in $(\star)$ and read the rest modulo N.) This viewpoint was adopted in [**?**, **?**].

Duality

For $\mathbf{x}, \mathbf{y} \in R^n$ write $\mathbf{x} \cdot \mathbf{y} := x_1 y_1 + \cdots + x_n y_n$.

For $S \subseteq R^n$ define the *left* (resp. *right*) *dual* code of S as

$$^{\perp}S := \{\mathbf{x} \in R^n; \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in S\},$$

$$S^{\perp} := \{\mathbf{x} \in R^n; \mathbf{y} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{y} \in S\}.$$

Remark

We have $^{\perp}S \leq {}_R R^n$ regardless of whether S is (one-sided) linear or not, and similarly for $S^{\perp}$.

Hence we can expect a suitable duality theory only if we define the double dual of $C \leq {}_R R^n$ as $(^{\perp}C)^{\perp}$.

Theorem

Let $C \leq {}_R R^n$ be a left linear code over R of shape λ.

1. *The right linear code $C^\perp$ has complementary shape $(m-\lambda_n, m-\lambda_{n-1}, \ldots, m-\lambda_1)$.*
   In particular we have $|C| \cdot |C^\perp| = |R|^n$, and C is free as an R-module iff $C^\perp$ is free iff $\mathrm{rk}(C) + \mathrm{rk}(C^\perp) = n$.
2. $^\perp(C^\perp) = C$
3. *$C \mapsto C^\perp$ defines an antiisomorphism between the lattices of left resp. right linear codes of length n over R, and hence $(C \cap C')^\perp = C^\perp + C'^\perp$, $(C + C')^\perp = C^\perp \cap C'^\perp$.*

Remark

Parts (2) and (3) are more generally true for quasi-Frobenius rings.

Proof.

Since $C \subseteq {}^\perp(C^\perp)$, Part (2) follows from (1), and clearly implies (3).

(1) It is possible to derive this result working with standard generator matrices, but the following is more conceptual and will be needed later.

Proof cont'd.

Each $\mathbf{y} \in R^n$ induces a linear map ${}_RC \to {}_RR$, $\mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{y}$.
In this way we obtain a homomorphism from R_R^n to $C^\sharp = \mathrm{Hom}({}_RC, {}_RR)_R$ with kernel $C^\perp$.
Any linear map $f : {}_RC \to {}_RR$ can be extended to ${}_RR^n$ (using, for example, stacked bases for ${}_RC$ and ${}_RR^n$) and hence has the form $\mathbf{x} \mapsto \mathbf{x} \cdot \mathbf{y}$.
This proves $R_R^n/C^\perp \cong C^\sharp$ and that the shapes of $C^\perp$, $C^\sharp$ are complementary. The proof of (1) is finished by the following Lemma. □

Lemma

A module ${}_RM$ and its dual $M^\sharp$ have the same shape (and in particular the same number of elements).

Proof.

Write ${}_RM \cong \bigoplus_{i=1}^r R/N^{\lambda_i}$, and let $x_1, \ldots, x_r$ be a basis of ${}_RM$.
A linear map $f : {}_RM \to {}_RR$ is determined once $f(x_1), \ldots, f(x_r)$ have been specified. For $f(x_i)$ we can choose any $a_i \in R$ of period dividing θ^{λ_i}, i.e. any $a_i \in N^{m-\lambda_i}$.

This leads to $M^\sharp \cong \bigoplus_{i=1}^r (N^{m-\lambda_i})_R \cong \bigoplus_{i=1}^r (R/N^{\lambda_i})_R$. □

Remark

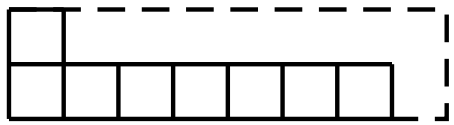
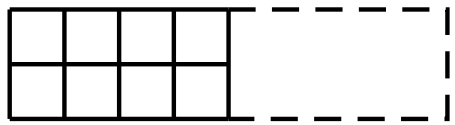
A self-dual linear code over R (i.e. $C = C^{\perp}$) necessarily has self-complementary shape. This gives certain restrictions on the parameters of C.

Examples

The linear codes C_8 and O over $\mathbb{Z}_4$ generated by

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

are both selfdual with shapes

 resp. 

The code O is the famous *Octacode*.

Weight Spectra of Linear Codes

For linear codes over a proper chain ring R the Hamming distance $\mathrm{d}_{\mathrm{Ham}}$ is not a good performance parameter. This is due to the following

Fact

For $C \leq {}_R R^n$ we have $\mathrm{d}_{\mathrm{Ham}}(C) = \mathrm{d}_{\mathrm{Ham}}\big(C[\theta]\big)$.

So C cannot be better than the (usually much smaller) code $C[\theta]$ (which is a classical linear code over $R/N \cong \mathbb{F}_q$).

Proof.

Let $\mathbf{c} \in C$ with $\mathrm{w}_{\mathrm{Ham}}(\mathbf{c}) = \mathrm{d}_{\mathrm{Ham}}(C)$. If $\mathbf{c}$ has period θ^i, then $\theta^{i-1}\mathbf{c} = (\theta^{i-1}c_1, \ldots, \theta^{i-1}c_n) \in C[\theta] \setminus \{\mathbf{0}\}$.
Obviously $\mathrm{w}_{\mathrm{Ham}}(\theta^{i-1}\mathbf{c}) \leq \mathrm{w}_{\mathrm{Ham}}(\mathbf{c})$, so we must have equality and $\mathrm{d}_{\mathrm{Ham}}\big(C[\theta]\big) = \mathrm{w}_{\mathrm{Ham}}(\mathbf{c}) = \mathrm{d}_{\mathrm{Ham}}(C)$. □

Consequence

To produce good linear codes over chain rings, we should assign larger weights to those elements of R which generate small ideals. Hence we must be able to distinguish between elements of R^*, $N \setminus N^2$, $\ldots$, $N^{m-1} \setminus \{0\}$, and $\{0\}$.

For $\mathbf{x} = (x_1, \ldots, x_n) \in R^n$ and $0 \le i \le m$ define

$$a_i(\mathbf{x}) := \left|\{j; 1 \le j \le n \text{ and } x_j \in N^i \setminus N^{i+1}\}\right|.$$

i.e. $a_i(\mathbf{x})$ counts the entries of $\mathbf{x}$ which are "exactly" divisible by θ^i.

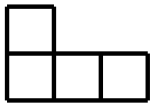
Definition

(i) The *weight composition* of $\mathbf{x} \in R^n$ is the $(m+1)$-tuple of integers $\big(a_0(\mathbf{x}), a_1(\mathbf{x}), \ldots, a_m(\mathbf{x})\big)$.

(ii) The *weight enumerator* of $S \subseteq R^n$ is the polynomial

$$\mathrm{A}_S(X_0, \ldots, X_m) := \sum_{\mathbf{x} \in S} X_0^{a_0(\mathbf{x})} \cdots X_m^{a_m(\mathbf{x})} \in \mathbb{C}[X_0, \ldots, X_m].$$

Example

The $\mathbb{Z}_4$-linear code $C \le \mathbb{Z}_4^4$ of shape  generated by

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}$$

has weight enumerator
$\mathrm{A}_C(X_0, X_1, X_2) = 8X_0^4 + X_1^4 + 6X_1^2X_2^2 + X_2^4$.

Isomorphism of Linear Codes

Definition

(i) Two linear codes $C_1, C_2 \leq {}_R R^n$ are said to be *linearly isomorphic* if there exists a monomial matrix $\mathbf{A} \in R^{n\times n}$ (a matrix having exactly one nonzero entry $a_{ij} \in R^\times$ in each row and column) such that $C_2 = \{\mathbf{xA}; \mathbf{x} \in C_1\}$.

(ii) C_1 and C_2 are said to be *semilinearly isomorphic* if $C_2 = \{\sigma(\mathbf{x})\mathbf{A}; \mathbf{x} \in C_1\}$ with $\mathbf{A}$ as in (i) and $\sigma \in \operatorname{Aut} R$.

Remark

The monomial transformations $R^n \to R^n$, $\mathbf{x} \mapsto \mathbf{xA}$, are exactly those automorphisms of the module ${}_R R^n$ which preserve the weight composition. A similar remark applies to the "semimonomial" transformations of (ii).

Multisets in PG(M_R)

Deviating a little from our previous notation, we denote the lattice of submodules of an arbitrary (not necessarily free) module M_R by $\mathrm{PG}(M_R)$ and the set of nonzero cyclic submodules of $\mathrm{PG}(M_R)$ by $\mathcal{P}$. The elements of $\mathcal{P}$ are called *points*. A point xR is *degenerate* if xR is not free, i.e. $|xR| < |R|$.

Definition

A *multiset in* $\mathrm{PG}(M_R)$ is a mapping $\mathfrak{K}\colon \mathcal{P} \to \mathbb{N}_0$.

The mapping $\mathfrak{K}$ is extended to the power set $2^{\mathcal{P}}$ by defining

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

For $P = xR \in \mathcal{P}$ the integer $\mathfrak{K}(P) \geq 0$ is called the *multiplicity* of P in $\mathfrak{K}$.

The integer $\mathfrak{K}(\mathcal{P}) = \sum_{P \in \mathcal{P}} \mathfrak{K}(P)$ is called the *cardinality* of $\mathfrak{K}$.

The *support* of $\mathfrak{K}$ is defined as $\operatorname{supp} \mathfrak{K} := \{P \in \mathcal{P}; \mathfrak{K}(P) > 0\}$, the *hull* of $\mathfrak{K}$ as the module $\langle \mathfrak{K} \rangle := \sum_{xR \in \operatorname{supp} \mathfrak{K}} Rx \leq M_R$, and the *shape* of $\mathfrak{K}$ as the shape of $\langle \mathfrak{K} \rangle$.

Definition

Two multisets $\mathfrak{K}$, $\mathfrak{K}'$ in PG(M_R) resp. PG(M'_R) are said to be *equivalent* if there exists a semilinear bijection $\phi\colon \langle\mathfrak{K}\rangle \to \langle\mathfrak{K}'\rangle$ satisfying $\mathfrak{K}(P) = \mathfrak{K}'\big(\phi(P)\big)$ for every point $P = xR \leq \langle\mathfrak{K}\rangle$.

Codes Associated to Multisets

Suppose $C \leq {}_R R^n$ is any left linear code of length n over R.

Take any generator matrix $\mathbf{G} \in R^{k\times n}$ of C (i.e. $C = \{\mathbf{xG}; \mathbf{x} \in R^k\}$, but the rows of $\mathbf{G}$ need not be independent).
Write $\mathbf{G} = (\mathbf{g}_1 | \ldots | \mathbf{g}_n)$ and define a multiset $\mathfrak{K}$ in $\mathrm{PG}(R_R^k)$ by setting

$$\mathfrak{K}(P) := |\{j; 1 \leq j \leq n \wedge P = \mathbf{g}_j R\}|$$

for $P = \mathbf{g}R \in \mathcal{P}$.

Definition

We say that the multiset $\mathfrak{K}$ and the code C are *associated*.

Remarks

- If C has *full length* (i.e. no universal zero coordinate), then $\mathfrak{K}(\mathcal{P}) = n$.
- One can restrict the definition to multisets in $\mathrm{PHG}(R_R^k)$ (i.e. allow only nondegenerate points) and so-called *fat* linear codes.
- In general the relation $C \mapsto \mathfrak{K}$ is many-to-many.

The Correspondence Theorem

Theorem

For every multiset $\mathfrak{K}$ of cardinality n in $\mathrm{PG}(R_R^k)$ *there exists an associated linear code* $C \leq {}_R R^n$ *(which is necessarily of full length). Two multisets* $\mathfrak{K}_1$ *in* $\mathrm{PG}(R_R^{k_1})$ *and* $\mathfrak{K}_2$ *in* $\mathrm{PG}(R_R^{k_2})$ *associated with full-length linear codes* C_1 *and* C_2 *over* R*, respectively, are equivalent if and only if the codes* C_1 *and* C_2 *are semilinearly isomorphic.*

Proof.

The first part is easy: Choose a sequence $\mathbf{g}_1, \ldots, \mathbf{g}_n$ over R^k such that the multiplicities in $\mathfrak{K}$ of all points match those in the sequence $\mathbf{g}_1 R, \ldots, \mathbf{g}_n R$, and define $C \leq {}_R R^n$ as the code generated by $(\mathbf{g}_1 | \ldots | \mathbf{g}_n)$.

The proof of the second part is quite technical and can be found in [**?**]. □

Remark

The theorem holds for a more general class of rings (including finite Frobenius rings).

How to Compute the Parameters of C from Properties of $\mathfrak{K}$?

Parameters of C: *length*, *shape* (*cardinality*), weight enumerator

The length of C equals $\mathfrak{K}(\mathcal{P})$).
For the shape use the following

Proposition

A multiset $\mathfrak{K}$ in $\mathrm{PG}(R_R^k)$ *and an associated code C have the same shape. In particular,* $|\langle\mathfrak{k}\rangle| = |C|$.

Proof.

Let $\mathbf{G} \in R^{k\times n}$ be such that

$$C = \{\mathbf{xG}; \mathbf{x} \in R^k\} \qquad \text{(Left row space of } \mathbf{G}\text{)}$$
$$\langle\mathfrak{k}\rangle = D := \{\mathbf{Gy}; \mathbf{y} \in R^n\} \qquad \text{(Right column space of } \mathbf{G}\text{)}$$

Define $f : R^n \to C$, $\mathbf{x} \mapsto \mathbf{xG}$.

$$C = \operatorname{Im} f \cong R^n / \operatorname{Ker} f = R^n /{}^{\perp}D \cong D^{\sharp} \qquad \text{(as left } R\text{-modules)}$$

Hence C, $D^{\sharp}$ and D all have the same shape. □

Remark

The following example shows that the left row space and the left column space of a matrix $\mathbf{G} \in R^{k\times n}$ usually have different shape.

Example

Let $a, b \in R$ such that $ab \neq ba$ and

$$\mathbf{G} = \begin{pmatrix} 1 & a \\ b & ab \end{pmatrix}.$$

Left column space of $\mathbf{G}$: $R\binom{1}{b} + R\binom{a}{ab} = R\binom{1}{b}$

Left row space of $\mathbf{G}$: $R(1,a) + R(b,ab) \supsetneq R(1,a)$.

To compute the weight enumerator

$$\mathrm{A}_C(X_0,\ldots,X_m) = \sum_{\mathbf{i}=(i_0,\ldots,i_m)\in I} \mathrm{A}_{\mathbf{i}} X_0^{i_0}\cdots X_m^{i_m}$$

of C (where I consists of all $m+1$-tuples $\mathbf{i}\in\mathbb{N}_0^{m+1}$ satisfying $i_0+\cdots+i_m=n$), we establish a correspondence between codewords of C and hyperplanes of $\mathrm{PG}(R_R^k)$.

All hyperplanes of $\mathrm{PG}(R_R^k)$ (or $\mathrm{PHG}(R_R^k)$) have the form $H=(Rx)^\perp$ for some $\mathbf{x}\in(R^k)^\times$.

Definition

The *$\mathfrak{K}$-type* of H is the sequence $(a_0,\ldots,a_m)$ where

$$a_i := \sum_{\substack{P\in\mathcal{P}\\ P\subseteq H+\theta^i R^k\\ P\not\subseteq H+\theta^{i+1}R^k}} \mathfrak{K}(P) \quad \text{for } 0\le i\le m.$$

Remark

If $\mathfrak{K}$ is a multiset in $\mathrm{PHG}(R_R^k)$ (i.e. $\operatorname{supp}\mathfrak{K}$ contains only free points), then a_i counts the number of points of $\mathfrak{K}$ which are i-neighbours but not $i+1$-neighbours to H.

Proposition

Let $\mathfrak{K}$ be a multiset in $\mathrm{PG}(R_R^k)$ associated with $C \leq_R R^n$, and suppose the correspondence $C \mapsto \mathfrak{K}$ is given by $\mathbf{G} \in R^{k\times n}$. For each hyperplane $H = (R\mathbf{x})^\perp$ of $\mathfrak{K}$-type

$$(0,\ldots,0,a_j,\ldots,a_m) \quad \text{with } a_j \neq 0$$

the cyclic subcode $R\mathbf{x}\mathbf{G} \leq_R C$ has weight enumerator

$$X_m^n + \sum_{s=j}^{m-1} (q^{m-s} - q^{m-s-1}) X_s^{a_j} X_{s+1}^{a_{j+1}} \cdots X_{m-1}^{a_{j+m-1-s}} X_m^{a_{j+m-s}+\cdots+a_m}$$

Proof.

Let $\mathbf{G} = (\mathbf{g}_1|\ldots|\mathbf{g}_n)$ and $\mathbf{c} = \mathbf{x}\mathbf{G} = (\mathbf{x}\cdot\mathbf{g}_1,\ldots,\mathbf{x}\cdot\mathbf{g}_n)$.

Observation (easy to verify)

$\mathbf{g}_j \in H + \theta^i R^k \setminus (H + \theta^{i+1} R^k)$ is equivalent to $\mathbf{x}\cdot\mathbf{g}_j \in N^i \setminus N^{i+1}$.

Hence $(a_0,\ldots,a_m)$ is the weight composition of $\mathbf{c}$.
The rest follows from $R\mathbf{c} \cong N^j$ (as left R-modules) and the fact that multiplication by θ shifts the weight composition as follows:

$$(b_0,\ldots,b_{m-1},b_m) \mapsto (0,b_0,\ldots,b_{m-2},b_{m-1}+b_m).$$

Remarks

- The weight enumerator of C can be computed from the weight enumerators of the cyclic subcodes of ${}_RC$ using the principle of inclusion and exclusion. In the classical case this is trivial, since $C = \{\mathbf{0}\} \uplus \biguplus_{\mathbf{c}\in S} \big(\mathbb{F}_q\mathbf{c} \setminus \{\mathbf{0}\}\big)$.
- Sometimes (especially in the case $m = 2$) it is easier to compute the weight enumerators of $C^\times$ and $C \setminus C^\times$ separately.
  If $a_0 \neq 0$, H gives rise to $q^m - q^{m-1}$ codewords in $C^\times$ (the words in $R^\times\mathbf{xG}$). All these have weight composition equal to the $\mathfrak{K}$-type of H.

Example (Weight enumerator of the Octacode)

The Octacode O is generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

The associated multiset $\mathfrak{O}$ is an *arc* in $\mathrm{PHG}(3, \mathbb{Z}_4)$ (i.e. no 4 points of $\mathfrak{O}$ are on the same hyperplane).

Since $2O$ is the extended $[8, 4, 4]$ Hamming code over $\{0, 2\}$,

$$A_{2O}(X_0, X_1, X_2) = X_2^8 + 14X_1^4X_2^4 + X_1^8.$$

Let n_i be the number of planes of $\mathrm{PHG}(3, \mathbb{Z}_4)$ meeting $\mathfrak{O}$ in i points ($0 \le i \le 3$).

$$\begin{aligned} n_0 + n_1 + n_2 + n_3 &= 120 \\ n_1 + 2n_2 + 3n_3 &= 8 \cdot 28 \\ n_2 + 3n_3 &= \tbinom{8}{2} \cdot 6 \\ n_3 &= \tbinom{8}{3} \end{aligned}$$

Example (cont'd)

Solving the system gives $n_0 = 8$, $n_1 = n_3 = 56$, $n_2 = 0$.

Since $O/2O$ is the extended Hamming code, there is 1 neighbourhood class of planes of $\mathfrak{O}$-type $(8,0,0)$ (the class containing $\mathbb{Z}_4(1111)^\perp$) and 14 classes of $\mathfrak{O}$-type $(4,*,*)$.

$\mathfrak{O}$-type	#planes	
$(8,0,0)$	8	$H \cap \mathfrak{O} = \emptyset$
$(4,1,3)$	56	$\lvert H \cap \mathfrak{O}\rvert = 3$
$(4,3,1)$	56	$\lvert H \cap \mathfrak{O}\rvert = 1$

This gives

$$A_{O^\times}(X_0,X_1,X_2) = 16X_0^8 + 112X_0^4X_1X_2^3 + 112X_0^4X_1^3X_2,$$

$$A_O(X_0,X_1,X_2) = X_2^8 + 112X_0^4X_1X_2^3 + 14X_1^4X_2^4 + 16X_0^8 + 112X_0^4X_1^3X_2 + X_1^8$$

MacWilliams Identity

Theorem

The weight enumerators of $C \leq_R R^n$ and its dual code $C^\perp \leq R_R^n$ are related by

$$\mathrm{A}_{C^\perp}(X_0, X_1, \ldots, X_m) = \frac{1}{|C|} \cdot \mathrm{A}_C\big(\mathrm{A}_m - X_{m-1}, \mathrm{A}_{m-1} - qX_{m-2}, \ldots, \mathrm{A}_1 - q^{m-1}X_0, \mathrm{A}_0\big),$$

where $\mathrm{A}_i = X_m + (q-1)X_{m-1} + \cdots + (q^{m-i} - q^{m-i-1})X_i$ is the weight enumerator of N^i.

Sketch of proof.

(1) Define $\alpha \in \mathrm{Aut}\,\mathbb{Q}[X_0, \ldots, X_m]$ by

$$(\alpha f)(X_0, X_1, \ldots, X_m) = f\big(\mathrm{A}_m - X_{m-1}, \mathrm{A}_{m-1} - qX_{m-2}, \ldots, \mathrm{A}_1 - q^{m-1}X_0, \mathrm{A}_0\big)$$

Verify the identity $\alpha(\mathrm{A}_C) = |C|\,\mathrm{A}_{C^\perp}$ for the $m+1$ codes N^i ($0 \leq i \leq m$) of length 1, whose weight enumerators A_i form a basis of $\langle X_0, \ldots, X_m \rangle_{\mathbb{Q}}$.

Proof cont'd.

(2) If $C = C_1 \times C_2$ is a decomposable code and $\alpha(\mathrm{A}_{C_i}) = |C_i|\,\mathrm{A}_{C_i^\perp}$ holds for $i = 1, 2$, then $C^\perp = C_1^\perp \times C_2^\perp$, $\mathrm{A}_C = \mathrm{A}_{C_1}\mathrm{A}_{C_2}$, $\mathrm{A}_{C^\perp} = \mathrm{A}_{C_1^\perp}\mathrm{A}_{C_2^\perp}$ and hence

$$\alpha(\mathrm{A}_C) = \alpha(\mathrm{A}_{C_1}\mathrm{A}_{C_2}) = \alpha(\mathrm{A}_{C_1})\alpha(\mathrm{A}_{C_2}) = |C_1|\,|C_2|\,\mathrm{A}_{C_1^\perp}\mathrm{A}_{C_2^\perp} = |C|\,\mathrm{A}_{C^\perp}.$$

It follows that $\alpha(\mathrm{A}_C) = |C|\,\mathrm{A}_{C^\perp}$ also holds for the $\binom{n+m}{m}$ completely decomposable codes

$$C = \underbrace{R \times \cdots \times R}_{n_0} \times \underbrace{N \times \cdots \times N}_{n_1} \times \cdots \times \underbrace{\{0\} \times \cdots \times \{0\}}_{n_m},$$

whose weight enumerators form a basis of $\mathbb{Q}[X_0, \ldots, X_m]_n$.

(3) Show the existence of a $\mathbb{Q}$-linear endomorphism of $\mathbb{Q}[X_0, \ldots, X_m]$ which sends A_C to $|C|\,\mathrm{A}_{C^\perp}$.
If χ is a generating character of R, then the Fourier transform

$$(\mathcal{F}f)(\mathbf{y}) = \sum_{\mathbf{x} \in R^n} f(\mathbf{x})\chi(\mathbf{x} \cdot \mathbf{y}) \quad \text{for } f \in \mathbb{Q}R^n \qquad (n \geq 0).$$

has this property. □

Axiomatic Definition

Following HJELMSLEV, KLINGENBERG, and KREUZER

Let $\Pi = (\mathcal{P}, \mathcal{L}, I)$, $I \subseteq \mathcal{P} \times \mathcal{L}$, be an arbitrary (point-line) incidence structure.

Definition (Neighbour relation)

Points $x, y \in \mathcal{P}$ are said to be *neighbours* (notation: $x \supset y$) if there exist distinct lines S, T incident with both x and y.
Lines $S, T \in \mathcal{L}$ are said to be *neighbours* (notation: $S \supset T$) if there exist distinct points x, y incident with both S and T. (If lines are identified with subsets of $\mathcal{P}$, this means just $|S \cap T| \geq 2$.)

Further notation

For $x, y \in \mathcal{P}$ with $x \not\supset y$ the symbol $\overline{x, y}$ denotes the unique line $S \in \mathcal{L}$ through x and y.

For $x \in \mathcal{P}$, $S \in \mathcal{L}$ the symbol $x \supset S$ denotes "there exists $y \in S$ with $x \supset y$".

Definition (Projective Hjelmslev Space)

An incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, I)$ with neighbour relation $\frown$ is said to be a *projective Hjelmslev space* if it satisfies the following axioms:

(H1) For any two points $x, y \in \mathcal{P}$ there exists a line S with $(x, S) \in I$, $(y, S) \in I$.

(H2) Every line $S \in \mathcal{L}$ contains at least three points which are pairwise non-neighbours.

(H3) For any $x, y, z \in \mathcal{P}$, $x \frown y$ and $y \frown z$ imply $x \frown z$.

(H4) For any two lines S, T and any three points x, y, z with $(x, S) \in I$, $(y, S) \in I$, $(x, T) \in I$, $(z, T) \in I$, $x \not\frown y$, $x \not\frown z$, $y \frown z$, we have $S \frown T$.

(H5) For a point x not incident with $S \in \mathcal{L}$ with $x \frown S$, there always exist $y, z \in \mathcal{P}$ with $y \not\frown S$, $(z, S) \in I$ and $(x, \overline{y, z}) \in I$.

(H6) Let $x \in \mathcal{P}$, $S \in \mathcal{L}$ with $x \not\frown S$ and let $y, z \in S$. For every $(y', \overline{x, y}) \in I$ and every $(z', \overline{x, z}) \in I$ there exists a line T with $(y', T) \in I$, $(z', T) \in I$ and $S \cap T \neq \emptyset$.

Assume that Π is a projective Hjelmslev space.

Remarks

- Axiom (H2) allows us to identify lines with subsets of $\mathcal{P}$.
- Π induces an incidence structure $\overline{\Pi} = (\overline{\mathcal{P}}, \overline{\mathcal{L}}, \bar{I})$, where $\overline{\mathcal{P}} = \{[x]; x \in \mathcal{P}\}$, $\overline{\mathcal{L}} = \{[S]; S \in \mathcal{L}\}$ denote the corresponding partitions into equivalence classes and $[x]\bar{I}[S] :\Longleftrightarrow x \supset S$. The structure $\overline{\Pi}$ forms a classical projective space.

Hjelmslev subspaces

A subset $\mathcal{T} \subseteq \mathcal{P}$ is called a *Hjelmslev subspace* of Π if for every two distinct points $x, y \in \mathcal{T}$ there exists a line $L \in \mathcal{L}$ with $L \subseteq \mathcal{T}$ and $x, y \in L$.

Hjelmslev subspaces form projective Hjelmslev spaces of their own in a natural way.

Subspaces

For $\mathcal{X} \subseteq \mathcal{P}$ define the *hull* $\langle \mathcal{X} \rangle$ as the intersection of all Hjelmslev subspaces containing $\mathcal{X}$. The set $\mathcal{X}$ is said to be a *subspace* if $\mathcal{X} = \langle \mathcal{X} \rangle$.

Independence

$\mathcal{X} \subseteq \mathcal{P}$ is said to be *independent* if for any $x \in \mathcal{X}$ we have $x \notin \langle \mathcal{X} \setminus \{x\} \rangle$

Basis

$\mathcal{B} \subseteq \mathcal{P}$ is said to be a *basis* of Π if $\langle \mathcal{B} \rangle = \mathcal{P}$ and $\mathcal{B}$ is independent.

Dimension

$\dim \Pi := |\mathcal{B}| - 1$ for any basis $\mathcal{B}$ of Π.

The equality $\dim \Pi = \dim \overline{\Pi}$ holds.

Coordinate Hjelmslev Geometries

Suppose R is a finite chain ring and M_R is a free right module over R of rank $k \geq 3$ (i.e. $M_R \cong R_R^k$).

Notation

$\mathrm{PHG}(M_R) := (\mathcal{P}, \mathcal{L}, \subseteq)$, where $\mathcal{P}$ and $\mathcal{L}$ denote the sets of all free rank 1, respectively free rank 2, submodules of M_R

The incidence structure $\mathrm{PHG}(M_R)$ forms a projective Hjelmslev space (i.e., it satisfies Axioms (H1)–(H7))

$M_R \cong M'_R$ as R-modules implies $\mathrm{PHG}(M_R) \cong \mathrm{PHG}(M'_R)$ as incidence structures.

A subset $\mathcal{T} \subseteq \mathcal{P}$ forms a Hjelmslev subspace of $\mathrm{PHG}(M_R)$ iff $\mathcal{T}$ consists of all free rank 1 submodules of a free submodule U of M_R. In this case we have $\dim \mathcal{T} = \mathrm{rk}(U) - 1$.

Definition

$\Pi = \mathrm{PHG}(R_R^k)$ (which has geometric dimension $\dim \Pi = k - 1$) is called the (right) $(k-1)$-dimensional projective Hjelmslev geometry over R.

Coordinatization Theorem

Theorem

For every projective Hjelmslev space Π *of dimension* $s \geq 3$*, having on each line at least 5 points no two of which are neighbours, there exists a chain ring* R *such that* $\mathrm{PHG}(R_R^{s+1})$ *is isomorphic to* Π*.*

Duality

$\mathcal{S}(M_R)$ denotes the set of submodules of the R-module M_R (which in case of $M = R^k$ can be identified with the set of subspaces of $\mathrm{PHG}(R_R^k)$).

Consider the map $\gamma\colon \mathcal{S}({}_RR^k) \to \mathcal{S}(R_R^k)$,

$$U \mapsto U^\perp := \{\mathbf{y} \in R^k; x_1y_1 + \cdots + x_ky_k = 0 \text{ for all } \mathbf{x} \in U\}.$$

Since $U \leq {}_RR^k$ is free of rank s iff $U^\perp \leq R_R^k$ is free of rank $k-s$, the map γ induces a correlation between the geometries $\mathrm{PHG}({}_RR^k)$ and $\mathrm{PHG}(R_R^k)$.

In particular we can view hyperplanes (i.e. $k-2$-dimensional Hjelmslev subspaces) of the right coordinate geometry $\mathrm{PHG}(R_R^k)$ as points of the left coordinate geometry $\mathrm{PHG}({}_RR^k)$ (and vice versa).

In the planar case ($k = 3$) we have $\mathrm{PHG}({}_RR^3) = \mathrm{PHG}(R_R^3)^*$ (dual incidence structure).

Affine Hjelmslev coordinate geometries

AHG$(R_R^k) = (\mathcal{P}, \mathcal{L}, \in)$, where $\mathcal{P} = R^k$ and $\mathcal{L} = \{\mathbf{a} + \mathbf{u}R; \mathbf{a} \in R^k, \mathbf{u} \in (R^k)^\times\}$

In the planar case ($k = 2$) lines have equations

$$y = mx + t \quad (m, t \in R) \quad \text{resp.} \quad x = my + t \quad (m \in N, t \in R)$$

There are q^{2k} points and $q^{3(k-1)} \cdot \frac{q^k-1}{q-1}$ lines

The incidence structure obtained by removing from PHG(R_R^{k+1}) a neighbour class $[H]$ of hyperplanes is isomorphic to AHG(R_R^k).

Simplex Codes

Definition

The linear code C associated with the multiset $\mathfrak{K}$ in $\mathrm{PG}(R_R^k)$, defined by $\mathfrak{K}(P) = 1$ if $P \in \mathcal{P}$ is a free point and $\mathfrak{K}(P) = 0$ otherwise, is called the *k-dimensional simplex code over R and is denoted by* $\mathrm{Sim}(k, R)$.

The code $\mathrm{Sim}(k, R)$ has length $q^{(k-1)(m-1)} \begin{bmatrix} k \\ 1 \end{bmatrix}_q$, shape $(\underbrace{m, \ldots, m}_{k})$, and cardinality $|\mathrm{Sim}(k, R)| = q^{km}$.

All hyperplanes H of $\mathrm{PG}(R_R^k)$ have the same $\mathfrak{K}$-type $(a_0, a_1, \ldots, a_m)$ given by

$$a_0 = q^{(k-1)(m-1)} \left(\begin{bmatrix} k \\ 1 \end{bmatrix}_q - \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q \right) = q^{(k-1)m},$$

$$a_j = q^{(k-2)(m-1)} \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q \left(q^{m-j} - q^{m-j-1} \right), \quad j = 1, \ldots, m-1,$$

$$a_m = q^{(k-2)(m-1)} \begin{bmatrix} k-1 \\ 1 \end{bmatrix}_q.$$

To prove this, observe that $\sum_{s \geq j} a_s$ is the number of free rank 1 submodules contained in $H + \theta^j R^k$, a module of shape $(\underbrace{m, \ldots, m}_{k-1}, m-j)$.

Hence

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

Solving for a_j gives the stated formulas.

Hamming Codes

Definition

The dual code $\mathrm{Sim}(k,R)^{\perp}$ is called the *k-th order Hamming code over R* and is denoted by $\mathrm{Ham}(k,R)$.

$\mathrm{Ham}(k,R)$ is free of rank $q^{(k-1)(m-1)}\begin{bmatrix}k\\1\end{bmatrix}_q - k$.

In particular $|\mathrm{Ham}(k,R)| = q^{mq^{(k-1)(m-1)}\begin{bmatrix}k\\1\end{bmatrix}_q - mk}$.

The weight distribution of $\mathrm{Ham}(k,R)$ can be computed using the MacWilliams identity.

Example

$C := \mathrm{Sim}(2, \mathbb{Z}_4)$ and $C^\perp = \mathrm{Ham}(2, \mathbb{Z}_4)$ are generated by

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 3 & 3 & 1 & 0 & 0 & 0 \\ 3 & 2 & 0 & 1 & 0 & 0 \\ 2 & 3 & 0 & 0 & 1 & 0 \\ 3 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and have weight distributions

$$\begin{aligned} \mathrm{A}_C(X_0, X_1, X_2) &= X_2^6 + 3X_1^4X_2^2 + 12X_0^4X_1X_2, \\ \mathrm{A}_{C^\perp}(X_0, X_1, X_2) &= \frac{1}{16}\mathrm{A}_C(X_2 - X_1, X_1 + X_2 - 2X_0, X_1 + X_2 + 2X_0) \\ &= \cdots \end{aligned}$$

Today's Lecture: Projective Hjelmslev planes over chain rings of length two

Let $\Pi = (\mathcal{P}, \mathcal{L}, I) = \mathrm{PHG}(R_R^k)$ be a coordinate Hjelmslev geometry over a finite chain ring R of length m with $R/N \cong \mathbb{F}_q$.

Definition (Refined neighbourhood relations)

Two points $x = \mathbf{x}R$ and $y = \mathbf{y}R$ are called *i-neighbours* ($0 \le i \le m$, notation: $x \supset_i y$) if $|\mathbf{x}R \cap \mathbf{y}R| \ge q^i$.
Two lines S and T are called i-neighbours (notation: $S \supset_i T$) if for every point x on S there exists a point y on T with $x \supset_i y$.

Remarks

- $\supset_0$ is the universal relation on $\mathcal{P}$ and $\mathcal{L}$, $\supset_1 = \supset$ is the ordinary neighbour relation, and $\supset_m$ is just equality.
- $\supset_i$ can be described as equality modulo N^i.
- $\supset_i$ defines equivalence relations on $\mathcal{P}$ and $\mathcal{L}$. The corresponding classes are denoted by $[x]_i$, $[S]_i$.
- $\supset_i$ is extended to Hjelmslev subspaces (of possibly different dimension) by $\Delta_1 \supset_i \Delta_2$ iff $\pi^{(i)}(\Delta_1) \subseteq \pi^{(i)}(\Delta_2)$ for the corresponding images modulo N^i.

The Structure Theorems

Indispensable for doing Finite Geometry

Let $\mathcal{P}^{(i)} = \{[x]_i; x \in \mathcal{P}\}$, $\mathcal{L}^{(i)} = \{[S]_i; S \in \mathcal{L}\}$.

Theorem

The incidence structure $(\mathcal{P}^{(i)}, \mathcal{L}^{(i)}, \subset_i)$ *is isomorphic to the projective Hjelmslev geometry* $\mathrm{PHG}((R/N^i)^k_{R/N^i})$. *In particular,* $(\mathcal{P}^{(1)}, \mathcal{L}^{(1)}, J^{(1)})$ *is isomorphic to* $\mathrm{PG}(k-1, \mathbb{F}_q)$.

There are further theorems pertaining to the incidence structures induced on $[x]_i$ resp. $[S]_i$ (and, more generally, L-shaped submodules of R^k_R). For simplicity these will be stated only for the special case $m = 2$, $k = 3$.

Definition

Nonempty intersections $S \cap [x]$ (where $x \in \mathcal{P}$, $S \in \mathcal{L}$) are called *line segments* of $\mathrm{PHG}(R^3_R)$.
The neighbour class $\{T \in \mathcal{L}; T \cap [x] = S \cap [x]\} = [S]$ is called the *direction* of the line segment $S \cap [x]$.

Theorem

Let x be a point of $\mathrm{PHG}(R_R^3)$*. The incidence structure induced on* $[x]$ *(with the line segments contained in* $[x]$ *as lines) is isomorphic to the affine plane* $\mathrm{AG}(2,\mathbb{F}_q)$*.*

Theorem

Let S be a line of $\mathrm{PHG}(R_R^3)$*. The incidence structure induced on* $[S]$ *(with the line segments having direction S as lines) is isomorphic to the dual affine plane (or punctured projective plane)* $\mathrm{AG}(2,\mathbb{F}_q)^* \cong \mathrm{PG}(2,\mathbb{F}_q) \setminus p_\infty$*.*

Example

Draw a picture for $\mathrm{PHG}(2,\mathbb{Z}_4)$.

Singer's Classical Theorem

Theorem (Singer 1938)

$\mathrm{PG}(2,\mathbb{F}_q)$ *admits a cyclic collineation group* G *acting regularly (i.e. sharply transitive) on the points (and lines) of* $\mathrm{PG}(2,\mathbb{F}_q)$.

This leads to a simplified representation $\mathrm{PG}(2,\mathbb{F}_q) \cong \mathrm{Dev}(D) := (\mathcal{P}', \mathcal{L}', \in)$ with

$$\mathcal{P}' := G \cong \mathbb{Z}_{q^2+q+1}, \quad \mathcal{L}' := \{D + i; i \in \mathbb{Z}_{q^2+q+1}\},$$

where $D := \{g \in G; g(p_0) \in L_0\}$ for some fixed point-line pair $(p_0, L_0) \in \mathcal{P} \times \mathcal{L}$.

Proof.

Represent the ambient space $\mathbb{F}_q^3$ as $\mathbb{F}_{q^3}$ (the cubic extension field of $\mathbb{F}_q$). Choose a primitive element β of $\mathbb{F}_{q^3}$ and consider the collineation σ induced by $\mathbb{F}_{q^3} \to \mathbb{F}_{q^3}$, $x \mapsto \beta x$ (which has the same order q^2+q+1 as the quotient group $\mathbb{F}_{q^3}^\times/\mathbb{F}_q^\times$). Let $G = \langle\sigma\rangle$. □

Singer's Theorem for Projective Hjelmslev Planes

Theorem (Hale-Jungnickel 1978)

The projective Hjlemslev plane $\mathrm{PHG}(R_R^3)$*, where* R *is either* $\mathbb{G}_q$ *or* $\mathbb{S}_q$*, admits a regular collineation group* $G \cong \mathbb{Z}_{q^2+q+1} \times (\mathbb{F}_q, +) \times (\mathbb{F}_q, +)$.

Proof.

R has a cubic Galois extension S ($S = \mathbb{G}_{q^3}$ if $R = \mathbb{G}_q$, resp. $S = \mathbb{S}_{q^3}$ if $R = \mathbb{S}_q$). The ring S satisfies $S_R \cong R_R^3$.
Hence we can view $\mathrm{PHG}(R_R^3)$ as $\mathrm{PHG}(S_R)$.

- $xR \in \mathcal{P}$ iff $x \in S \setminus \theta S = S^\times$
- $xR = yR$ iff $y \in xR^\times$

This implies that

$$G := S^\times / R^\times \cong \mathbb{Z}_{q^2+q+1} \times (\mathbb{F}_q, +) \times (\mathbb{F}_q, +)$$

acts regularly on $\mathcal{P}$. □

Example

Let $G = \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$.

1. If we set $D = \{1, b, a, ac, a^3b, a^3c\}$, then $\mathrm{Dev}(D) \cong \mathrm{PHG}(2, \mathbb{Z}_4)$ and $\langle a \rangle$ forms a hyperoval in $\mathrm{Dev}(D)$.
2. If $D = \{1, b, a, ac, a^3, a^3bc\}$, then $\mathrm{Dev}(D) \cong \mathrm{PHG}(2, \mathbb{S}_2)$ and $\langle a \rangle$ is a Baer subplane in $\mathrm{Dev}(D)$.

Collineations

Every semilinear automorphism $\phi\colon R_R^3 \to R_R^3$ induces a collineation (i.e. an isomorphism) of $\mathrm{PHG}(R_R^3)$ via $\phi(\mathbf{x}R) = \phi(\mathbf{x})R$ for $\mathbf{x}R \in \mathcal{P}$.

Fundamental Theorem of Projective Hjelmslev Geometry

Every collineation of $\mathrm{PHG}(R_R^3)$ arises in this way, i.e. $\mathrm{Aut}\,\mathrm{PHG}(R_R^3) \cong \mathrm{P\Gamma L}(3,R)$.

Projectivities of $\mathrm{PHG}(2,\mathbb{G}_q)$

$\mathrm{PGL}(3,R) = \mathrm{GL}(3,R)/\mathrm{Z}(R)$

Notes

- A corresponding theorem also holds for $\mathrm{PHG}(R_R^k)$, $k > 3$.
- Collineations preserve the partitions $\overline{\mathcal{P}}$, $\overline{\mathcal{L}}$ of $\mathcal{P}$ resp. $\mathcal{L}$ into neighbour classes, as well as the sets of line segments resp. dual line segments.
- $\mathrm{PGL}(3,R)$ acts regularly on ordered quadrangles of $\mathrm{PHG}(R_R^3)$, i.e. sets of 4 points which form a quadrangle in the quotient plane $\mathrm{PG}(2,\mathbb{F}_q)$

General assumption: $\Pi = \mathrm{PHG}(R_R^3)$, where R has length $m = 2$.

Definition

A multiset $\mathfrak{K}$ in $(\mathcal{P}, \mathcal{L}, I)$ is called a (k, n)-*arc* (or simply an n-arc) if

(i) $\mathfrak{K}(\mathcal{P}) = k$;

(ii) $\mathfrak{K}(L) \leq n$ for every line $L \in \mathcal{L}$;

Definition

A multiset $\mathfrak{K}$ in $(\mathcal{P}, \mathcal{L}, I)$ is called a (k, n)-*blocking multiset* (or an n-blocking multiset) if

(i) $\mathfrak{K}(\mathcal{P}) = k$;

(ii) $\mathfrak{K}(L) \geq n$ for every line $L \in \mathcal{L}$;

Further notes

- If $\mathfrak{K}$ is a set, then $\mathfrak{K}$ is an n-arc iff $\mathcal{P} \setminus \mathfrak{K}$ is a $(q^2 + q - n)$-blocking set. Hence projective arcs and blocking sets are equivalent concepts.
- We are interested in *maximal* arcs (i.e. (k, n)-arcs with the largest possible k) or, more generally, *complete* arcs (i.e. (k, n)-arcs which cannot be extended to a $(k + 1, n)$-arc (and dually in *minimal* resp. *irreducible* blocking multisets).

The Maximal Arc Problem

The maximal arc problem (for coordinate Hjelmslev planes) asks for the determination of the integers

$$\mathrm{m}_n(R_R^3) = \max\{k;\ \text{there exists a } (k,n)\text{-arc in PHG}(R_R^3)\}$$

for $n \in \mathbb{N}$ (or, less ambitious, only for $1 \le n \le q^2+q$).

Remarks

- The maximal arc problem is inherently difficult and has been completely solved so far only for $|R| = 4$. (The completion of the case $|R| = 9$ is to be expected soon.)
- The corresponding problem in classical finite geometry is well-studied. Many results are available and can be used along with the structure theorems for $\overline{\Pi}$, $[x]$, and $[S]$.

The General Upper Bound

Theorem

Let $\mathfrak{K}$ be a (k,n)-arc in $\mathrm{PHG}(R_R^3)$*. Suppose there exists a neighbour class of points $[x]$ with $\mathfrak{K}([x]) = u$ and let u_i, $1 \le i \le q+1$, be the maximum number of points on a line from the i-th parallel class in the affine plane defined on $[x]$. Then*

$$k \le q(q+1)n - q\sum_{i=1}^{q+1} u_i + u.$$

Proof.

For $1 \le i \le q+1$ let ℓ_i be a corresponding line segment in $[x]$ of multiplicity u_i. Count the sum of the multiplicities of the $q(q+1)$ lines through the segments ℓ_i in two different ways, using the fact that these lines partition $\mathcal{P} \setminus [x]$. □

Example

We show that a 5-arc in $\mathrm{PHG}(2, \mathbb{Z}_9)$ or $\mathrm{PHG}(2, \mathbb{S}_3)$ can have at most 40 points.

Case 1: $\mathfrak{K}$ has a 2-point, say x.
Each of the 12 lines through x can contain at most 3 further points of $\mathfrak{K}$. $\quad\Longrightarrow k \le 2 + 12 \cdot 3 = 38$

Case 2: $7 \le u \le 9$
$\mathfrak{K} \cap [x]$ must contain line segments in every direction. Each line through such a line segment can contain at most 2 further points from $\mathfrak{K}$ outside $[x]$. $\quad\Longrightarrow k \le u + 6 + 6 + 6 + 6 = 33$

Case 3: $5 \le u \le 6$
$\mathfrak{K} \cap [x]$ must contain at least one line segment ℓ.
$\Longrightarrow k \le u + 6 + 9 + 9 + 9 \le 39$

Case 4: $u = 4$
If the 4 points in $\mathfrak{K} \cap [x]$ form an oval (quadrangle), we get $k \le 4 + 4 \cdot 9 = 40$, otherwise Case 3 applies and gives $k \le 37$.

Case 5: $u \le 3$
Here $k \le 3 \cdot 13 = 39$.

Remark

Recently we have proved that $\mathrm{m}_5(\mathbb{Z}_9^3) = 39$ and $\mathrm{m}_5(\mathbb{S}_3^3) = 38$. The corresponding maximal arcs have completely different structure. (The first arc consists of 13 properly arranged triangles, one in each point class. The second arc has triangles in 9 point classes, which form an affine subplane of $\overline{\Pi} \cong \mathrm{PG}(2, \mathbb{F}_3)$. The remaining point classes contain 3, 2, 2 and 1 points.

Tables

Online tables of lower bounds (arising from constructions) are maintained by the group in Bayreuth (KIERMAIER, KOHNERT):

`http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/PHG_arc_table/index.html`

Table: Values of $m_n(R_R^3)$ for Hjelmslev planes of order $q^2 = 4$ and $q^2 = 9$

n/R	$\mathbb{Z}_4$	$\mathbb{F}_2[X]/(X^2)$	$\mathbb{Z}_9$	$\mathbb{F}_3[X]/(X^2)$
2	7	6	9	9
3	10	10	19	18
4			30	30
5			39	38
6			48 – 51	48 – 51
7			60 – 62	60 – 62
8			69	69

The Case $q^2 \le n \le q^2 + q$

This case has been solved completely.
It is more convenient to consider (k, n)-blocking multisets with $0 \le n \le q$.

In perfect analogy with the classical case we have

Theorem

The minimum size of a 1*-blocking multiset in* $\mathrm{PHG}(R_R^3)$ *is* $k = q^2 + q$*. A* $(q^2 + q, 1)$*-blocking multiset is necessarily (the characteristic function of) a line.*

The existence part can be generalized to

Theorem

The minimum size of an n-blocking multiset, $1 \le n \le q$*, in* $\mathrm{PHG}(R_R^3)$ *is* $k = n(q^2 + q)$*.*

Examples are provided by sums of n lines (which are not projective if $n \ge 2$). There exist projective examples as well.

The Classical Case

In PG$(2,\mathbb{F}_q)$ the maximum size of a 2-arc (a set of points no three of which are collinear) is given by

$$\mathrm{m}_2(\mathbb{F}_q^3) = \begin{cases} q+2 & \text{if } q = 2^r, \\ q+1 & \text{if } q \text{ is odd.} \end{cases}$$

Examples of $(q+1,2)$-arcs (ovals) are provided by conics:

$$\mathfrak{K} = \{\mathbb{F}_q(x,y,z); y^2 - xz = 0\} = \{(1,y,y^2); y \in \mathbb{F}_q\} \cup \{(0,0,1)\}$$

In the case $q = 2^r$ the tangents to an oval $\mathfrak{K}$ are concurrent in the *nucleus* p ($p = \mathbb{F}_q(0,1,0)$ in the above example), so that $\mathfrak{K} \cup \{p\}$ is a $(q+2,2)$-arc (hyperoval).

In the case q odd every oval is a conic (B. SEGRE'S THEOREM) The tangents to an oval $\mathfrak{K}$ form a dual $(q+1,2)$-arc. (Each point outside $\mathfrak{K}$ is on either 0 or 2 tangents.)

2-Arcs in Hjelmslev planes

We keep the assumption $\Pi = \mathrm{PHG}(R_R^3)$, where R has length $m = 2$.

Theorem

$\mathrm{m}_2(R_R^3) = q^2 + q + 1$ *if* $R = \mathbb{G}_{2^r}$ *(a Galois ring of characteristic* 4*).*

The corresponding $(q^2 + q + 1, 2)$-arcs have exactly one point in each neighbour class and meet every line in 0 or 2 points (*hyperovals*).

Theorem

$q^2 + 2 \le \mathrm{m}_2(R_R^3) \le q^2 + q$ *if* R *has characteristic* 2*.*

Theorem

$\mathrm{m}_2(R_R^3) = q^2$ *if* R *has characteristic* $p > 2$*.*

The corresponding $(q^2, 2)$-arcs have q^2 neighbour classes containing 1 point and $q + 1$ empty neighbour classes which form a line of the quotient plane $\mathrm{PG}(2, \mathbb{F}_q)$.

In the remaining case $R = \mathbb{G}_q$, q odd, we have only the upper bound $\mathrm{m}_2(R_R^3) \le q^2$.

The Upper Bounds

Let us show that

$$\mathrm{m}_2(R_R^3) \le \begin{cases} q^2+q+1 & \text{if } q \text{ is even,} \\ q^2 & \text{if } q \text{ is odd.} \end{cases}$$

Proof.

If there exists a point class $[x]$ with $\mathfrak{K}([x]) \ge 2$, we get the stronger bound

$$\mathrm{m}_2(R_R^3) \le 2 + 1 \cdot 0 + q \cdot q = q^2 + 2.$$

Otherwise of course $\mathrm{m}_2(R_R^3) \le q^2+q+1$.

Now assume q is odd and consider the induced arc in a line neighbour class $[L] \cong \mathrm{PG}(2,\mathbb{F}_q) \setminus \{p_\infty\}$.
Since q is odd, at least one point class $[x]$ on $[L]$ must be empty.
$\Longrightarrow$ The set of empty point neighbour classes forms a blocking set in the quotient plane $\mathrm{PG}(2,\mathbb{F}_q)$. Hence there must be at least $q+1$ empty classes (and if there are exactly $q+1$, they must form a line of the quotient plane). □

The Existence of Hyperovals in PHG$(2, \mathbb{G}_{2^r})$

Idea of the proof

Represent PHG(R_R^3) as PHG(S_R) where $S = \mathbb{G}_{q^3}$ is the cubic Galois extension of $R = \mathbb{G}_q$. Since

$$\left|\mathbb{G}_{q^3}^\times / \mathbb{G}_q^\times\right| = \frac{q^6 - q^3}{q^2 - q} = q^2(q^2 + q + 1),$$

there is a (unique) candidate set $\mathfrak{T}$ of $q^2 + q + 1$ points which forms a subgroup of $\mathbb{G}_{q^3}^\times / \mathbb{G}_q^\times$.

The set $\mathfrak{T}$ is invariant under a lifted Singer cycle
$\Longrightarrow$ it suffices to test the points in one line class $[L]$ for the 2-arc property.

Definition

$\mathfrak{T}$ is called *Teichmüller set* of PHG(R_R^3)

This is due to the fact that $\mathfrak{T} = \{\mathbb{G}_q \eta^i; 0 \le i \le q^2 + q\}$, where η has order $q^3 - 1$ in $\mathbb{G}_{q^3}^\times$ (Teichmüller or Hensel lift of a primitive element β of $\mathbb{G}_{q^3}/p\mathbb{G}_{q^3} = \mathbb{F}_{q^3}$).

For the actual computation one uses the following (with $q = p^r$)

Fact

$\mathbb{G}_q$ is isomorphic to the ring $\mathrm{W}_2(\mathbb{F}_q)$ of (truncated) Witt vectors of length 2 over $\mathbb{F}_q$, which has underlying set $\mathbb{F}_q^2$ and operations

$$(a_0, a_1) + (b_0, b_1) = (a_0 + b_0, a_1 + b_1 - \frac{1}{p}\sum_{j=1}^{p-1} \binom{p}{j} a_0^j b_0^{p-j}),$$

$$(a_0, a_1) \cdot (b_0, b_1) = (a_0 b_0, a_0^p b_1 + b_0^p a_1).$$

This reduces the arithmetic of $\mathbb{G}_q$ to that of $\mathbb{F}_q$ (in a way that only depends on the characteristic p). For example, all Galois rings $\mathbb{G}_{2^r}$ have the "same" operations

$$(a_0, a_1) + (b_0, b_1) = (a_0 + b_0, a_1 + b_1 + a_0 b_0),$$

$$(a_0, a_1) \cdot (b_0, b_1) = (a_0 b_0, a_0^2 b_1 + b_0^2 a_1).$$

With this isomorphism we have $\eta = (\beta, 0)$ and, using $\{a\} := (a, 0)$ (Witt's notation), $p(a_0, a_1) = (0, a_0^p)$, and thus

$$(a_0, a_1) = (a_0, 0) + (0, a_1) = \{a_0\} + p\{a_1^{1/p}\}.$$

The existence of ovals in $\mathrm{PHG}(R_R^3)$, $\mathrm{char}\, R = p$

Idea of proof

Work in the affine Hjelmslev plane $\mathrm{AHG}(R_R^2)$, representing the point set R_R^2 as a quadratic extension ring S of R.

It is rather obvious how to do this. If $R = \mathbb{F}_q[X;\sigma]/(X^2)$ with $\sigma(a) = a^{p^i}$, take $S = \mathbb{F}_q[X;\sigma]/(X^2)$ with the "same" σ.

Points of $\mathrm{AHG}(S_R)$

$p = a_0 + a_1X \in S$, i.e. $a_0, a_1 \in \mathbb{F}_{q^2}$ (q^4 points)

Lines of $\mathrm{AHG}(S_R)$

$L = a + uR = \{a_0 + a_1X + (u_0 + u_1X)(\lambda_0 + \lambda_1X);\, \lambda_0, \lambda_1 \in \mathbb{F}_q\}$, where $u_0 \neq 0$ (since $u \in S^\times$)

Point sets in $\mathrm{AHG}(S_R)$ with exactly 1 point in each neighbour class correspond with functions $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ via

$$p_t = t + f(t)X$$

Choose f as a σ-*quadratic map*.

Quadratic maps of $\mathbb{F}_{q^2}$

Definition

$f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is said to be σ-*quadratic* if $f(\lambda a) = \sigma(\lambda)^2 f(a)$ for $a \in \mathbb{F}_{q^2}$, $\lambda \in \mathbb{F}_q$, and if $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$, $(a,u) \mapsto f(a+u) - f(a) - f(u)$ is a (symmetric) bilinear map.

Theorem

If $\sigma(a) = a^{p^i}$, the σ-quadratic maps of $\mathbb{F}_{q^2}$ are exactly the maps of the form

$$f(x) = Ax^{2p^i} + Bx^{2p^i q} + Cx^{2p^i(q+1)} \quad \text{with } A, B, C \in \mathbb{F}_{q^2},$$

i.e. those represented by a quadratic q-polynomial in x^{p^i}.

Why Does This Work?

Observation

The point set $\mathfrak{K}$ in AHG(S_R) corresponding to $f : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}$ forms an oval iff for any $a \in \mathbb{F}_{q^2}$, $u \in \mathbb{F}_{q^2}^\times$, $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$ the equation

$$p_{a+\lambda u} = p_a + (p_{a+u} - p_a)(\lambda + \mu X)$$

has no solution $\mu \in \mathbb{F}_q$.

For the X-component (only the X-component matters!) this translates into

$$\frac{f(a+\lambda u) - f(a)}{\sigma(\lambda)u} - \frac{f(a+u) - f(a)}{u} = \frac{\mu}{\sigma(\lambda)} \notin \mathbb{F}_q.$$

Consequence

$\mathfrak{K}$ forms in oval in AHG(S_R), provided that f is σ-quadratic and satisfies the condition

$$\frac{f(u)}{u} \notin \mathbb{F}_q \quad \text{for all } u \in \mathbb{F}_{q^2}^\times.$$

The Final Step

Theorem

There exist σ-quadratic maps satisfying this condition.

Proof.

f can be considered as a map of $\mathrm{PG}\big((\mathbb{F}_{q^2})_{\mathbb{F}_q}\big) \cong \mathrm{PG}(1, \mathbb{F}_q)$. For a fixed point $\mathbb{F}_q u$ the complementary condition $\frac{f(u)}{u} \in \mathbb{F}_q$ is linear in f and defines a hyperplane H_u of the projective space over $\mathbb{F}_q$ formed by all σ-quadratic maps of $\mathbb{F}_{q^2}$. This space is a $\mathrm{PG}(5, \mathbb{F}_q)$.

It can be shown that the $q+1$ hyperplanes H_u do not cover all the points of this space. Equivalently they do not contain a common solid (3-dimensional space). □

Remarks

- $(9, 2)$-arcs exist in the planes over both $\mathbb{Z}_9$ and $\mathbb{S}_3$.
- The existence of $(q^2, 2)$-arcs was proved soon after a computer search done earlier this year revealed the first $(25, 2)$-arc in the plane over $\mathbb{Z}_{25}$.
- There is much evidence that $\mathrm{m}_2(\mathbb{Z}_{25}^3) = 21$. If true we would have the first example of chain rings R, S of the same order with $\mathrm{char}(R) < \mathrm{char}(S)$ but $\mathrm{m}_n(R_R^3) > \mathrm{m}_n(S_S^3)$ for some n.