Arcs in Galois ring planes invariant under a Singer cycle

Joint work with Michael Kiermaier

Thomas Honold

Institute of Information and Communication Engineering
Zhejiang University

Fq9
University College Dublin
12. 7.–18. 7. 2009

Outline

Galois Rings

The uniform case $m = 2$

Let $q = p^r > 1$ be a prime power.

Galois rings of length 2

$\mathbb{G}_q := \mathbb{Z}_{p^2}[X]/(h)$, where $h \in \mathbb{Z}_{p^2}[X]$ is monic of degree r and irreducible mod p.

The polynomial h (whose particular choice does not matter) may be chosen as a divisor of $X^{q-1} - 1$.

Basic properties of $\mathbb{G}_q$

- $\mathbb{G}_q \supset (p) \supset \{0\}$ are the ideals of $\mathbb{G}_q$;
- $\mathbb{G}_q/(p) \cong \mathbb{F}_q$ (as rings) and $(p) \cong \mathbb{F}_q$ as $\mathbb{F}_q$-spaces;
- $|\mathbb{G}_q| = q^2$;
- $\mathrm{Char}(\mathbb{G}_q) = p^2$.

The last property characterizes $\mathbb{G}_q$ among the chain rings of length 2 with residue field $\mathbb{F}_q$. (The other r such rings have characteristic p.)

Galois Ring Planes

The projective Hjelmslev plane over $\mathbb{G}_q$

$\mathrm{PHG}(2,\mathbb{G}_q) := (\mathcal{P},\mathcal{L},\subseteq)$, where $\mathcal{P}$ ("points") and $\mathcal{L}$ ("lines") denote the sets of free rank 1 (resp., free rank 2) submodules of $\mathbb{G}_q^3$ (or any other free $\mathbb{G}_q$-module of rank 3).

Since $\mathbb{G}_q$ is commutative, we need not distinguish between left and right projective Hjelmslev planes over $\mathbb{G}_q$.

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

- $\mathrm{PHG}(2,\mathbb{G}_q)$ is a symmetric divisible design with parameters $(m,n,k,\lambda_1,\lambda_2) = (q^2+q+1,q^2,q^2+q,q,1)$.
- Lines intersect point classes in either 0 or q points, and dually points are on either 0 or q lines of each line class.

Thus $\mathrm{PHG}(2,\mathbb{G}_q)$ is an example of a *uniform* projective Hjelmslev plane of order q.

Galois Ring Planes (Cont'd)

$$\overline{\mathcal{P}} = \{[p]; p \in \mathcal{P}\}, \quad \overline{\mathcal{L}} = \{[L]; L \in \mathcal{L}\}$$

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

- $(\overline{\mathcal{P}}, \overline{\mathcal{L}}, \overline{I}) \cong \mathrm{PG}(2, \mathbb{F}_q)$
- $[p] \cong \mathrm{AG}(2, \mathbb{F}_q)$
- $[L] \cong \mathrm{AG}(2, \mathbb{F}_q)^* \cong \mathrm{PG}(2, \mathbb{F}_q) \setminus \{p\}$

Nonempty point sets of the form $L \cap [p]$ are called *line segments*.
All line segments have size q.
The lines of $[p]$, as well as the points of $[L]$ are line segments.

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 $\mathrm{PG}(2,\mathbb{F}_q) \cong (\mathcal{P}', \mathcal{L}', \in)$ 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 $D := \{g \in S; g(p_0) \in L_0\}$ 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 $G = \langle \sigma \rangle$. $\square$

Singer's Theorem for $\mathrm{PHG}(2, \mathbb{G}_q)$

Theorem (Hale-Jungnickel 1978)

$\mathrm{PHG}(2, \mathbb{G}_q)$ *admits a regular collineation group* $G \cong \mathbb{Z}_{q^2+q+1} \times (\mathbb{F}_q, +) \times (\mathbb{F}_q, +)$.

Proof.

Represent the ambient space $\mathbb{G}_q^3$ as $\mathbb{G}_{q^3}$ (the cubic Galois extension of $\mathbb{G}_q$). Here we use the fact that $\mathbb{G}_{q^3}$ is a free $\mathbb{G}_q$-module of rank 3.

- $\mathbb{G}_q x \in \mathcal{P}$ iff $x \in \mathbb{G}_{q^3} \setminus p\mathbb{G}_{q^3} = \mathbb{G}_{q^3}^\times$
- $\mathbb{G}_q x = \mathbb{G}_q y$ iff $y \in \mathbb{G}_q^\times x$

This implies that

$$G := \mathbb{G}_{q^3}^\times / \mathbb{G}_q^\times \cong \mathbb{Z}_{q^2+q+1} \times (\mathbb{F}_q, +) \times (\mathbb{F}_q, +)$$

acts regularly on $\mathcal{P}$. $\square$

Coordinate-Free Representation

In the classical case the trace $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}$ serves this purpose via the trace form

$$\mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \to \mathbb{F}_q, \quad (x,y) \mapsto \mathrm{Tr}(xy)$$

and the associated polarity

$$\mathcal{P} \to \mathcal{L}, \quad \mathbb{F}_q x \mapsto (\mathbb{F}_q x)^{\perp} = \{y \in \mathbb{F}_{q^3}; \mathrm{Tr}(xy) = 0\}.$$

Using Singer's Theorem this simplifies to

$$\begin{aligned}
p_i &= \mathbb{F}_q \beta^i = \sigma^i(p_0),\\
L_i &= \{x \in \mathbb{F}_{q^3}; \mathrm{Tr}(\beta^{-i}x) = 0\} = \sigma^i(L_0),\\
p_i \in L_j \iff i - j \in D &= \{i \in \mathbb{Z}_{q^2+q+1}; p_i \in L_0\}\\
&= \{i \in \mathbb{Z}_{q^2+q+1}; \mathrm{Tr}(\beta^i) = 0\}.
\end{aligned}$$

Coordinate-Free Representation (Cont'd)

Teichmüller coordinates

$$\mathrm{T}_q^* = \{x \in \mathbb{G}_q^*; x^{q-1} = 1\} \qquad \text{(Teichmüller group)}$$
$$\mathrm{T}_q = \{x \in \mathbb{G}_q; x^q = x\} = \mathrm{T}_q^\times \cup \{0\} \qquad \text{(Teichmüller set)}$$

Every $x \in \mathbb{G}_q$ has a unique representation $x = x_0 + px_1$ with $x_0, x_1 \in \mathrm{T}_q$.

Trace of the extension $\mathbb{G}_{q^3}/\mathbb{G}_q$

The trace $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{G}_{q^3}/\mathbb{G}_q} : \mathbb{G}_{q^3} \to \mathbb{G}_q$ is defined by

$$\mathrm{Tr}(x_0 + px_1) = \sum_{i=0}^{2} \left(x_0^{q^i} + px_1^{q^i} \right).$$

Tr is $\mathbb{G}_q$-linear, onto, and $\ker(\mathrm{Tr})$ contains no nonzero ideal of $\mathbb{G}_{q^3}$.

Coordinate-Free Representation (Cont'd)

Theorem

(i) For every line L of $\mathrm{PHG}(\mathbb{G}_{q^3})$ *there exists a unit* $\alpha \in \mathbb{G}_{q^3}^{\times}$ *such that*

$$L = \left\{\mathbb{G}_q x \in \mathcal{P}; \mathrm{Tr}(\alpha x) = 0\right\}.$$

(ii) The equations $\mathrm{Tr}(\alpha x) = 0$ *and* $\mathrm{Tr}(\beta x) = 0$ *(*$\alpha, \beta \in \mathbb{G}_{q^3}^{\times}$*) determine the same line iff* $\alpha = u\beta$ *for some unit* $u \in \mathbb{G}_q^{\times}$*.*

Sketch of proof.

(i) Consider the $\mathbb{G}_q$-module $M = \mathrm{Hom}_{\mathbb{G}_q}(\mathbb{G}_{q^3}, \mathbb{G}_q)$ (the dual of the $\mathbb{G}_q$-module $\mathbb{G}_{q^3}$).

M is also a module over $\mathbb{G}_{q^3}$ relative to the action $(\phi a)(x) := \phi(ax)$ ($\phi \in \mathrm{Hom}_{\mathbb{G}_q}(\mathbb{G}_{q^3}, \mathbb{G}_q)$, $a, x \in \mathbb{G}_{q^3}$).

Show that M is freely generated by Tr as a $\mathbb{G}_{q^3}$-module.

Proof cont'd.

(ii) Since Tr is $\mathbb{G}_q$-linear, $\mathrm{Tr}(\alpha x) = 0$ and $\mathrm{Tr}(\beta x) = 0$ determine the same line whenever $\alpha\mathbb{G}_q^\times = \beta\mathbb{G}_q^\times$.

"Only if" then follows from $|\mathcal{P}| = q^2(q^2 + q + 1) = |\mathbb{G}_{q^3}^\times / \mathbb{G}_q^\times|$. □

Remark

The trace form $(x, y) \mapsto \mathrm{Tr}(xy)$ has an associated orthogonal polarity $\tau\colon \mathcal{P} \cup \mathcal{L} \to \mathcal{P} \cup \mathcal{L}$, sending a free rank 1 or rank 2 submodule U of the $\mathbb{G}_q$-module $\mathbb{G}_{q^3}$ to $U^\perp := \{x \in \mathbb{G}_{q^3}; \mathrm{Tr}(xy) = 0 \text{ for all } y \in U\}$. For any point $\mathbb{G}_q\alpha \in \mathcal{P}$ we have $\tau(\mathbb{G}_q\alpha) = L_\alpha$, where $L_\alpha \in \mathcal{L}$ denotes the line with equation $\mathrm{Tr}(\alpha x) = 0$.

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

Fundamental Theorem of Projective Hjelmslev Geometry

$\operatorname{Aut}\mathrm{PHG}(2, \mathbb{G}_q) \cong \mathrm{P\Gamma L}(3, \mathbb{G}_q)$, a group of order $r \cdot q^{11}(q^3-1)(q^2-1)$.

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

$\mathrm{PGL}(3, \mathbb{G}_q) = \mathrm{GL}(3, \mathbb{G}_q)/\mathbb{G}_q^{\times}$, a group of order $q^{11}(q^3-1)(q^2-1)$.

Notes

- 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.
- $\mathrm{PGL}(3, \mathbb{G}_q)$ acts regularly on ordered quadrangles of $\mathrm{PHG}(2, \mathbb{G}_q)$, i. e. sets of 4 points which form a quadrangle in the quotient plane $\mathrm{PG}(2, \mathbb{F}_q)$

Multisets in $\mathrm{PHG}(2,\mathbb{G}_q)$ Arising from a Singer Cycle

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

A collineation σ of $\mathrm{PHG}(2,\mathbb{G}_q)$ is called a *Singer cycle*, if σ has order q^2+q+1 and permutes the point classes $[p] \in \overline{\mathcal{P}}$ in one cycle.

Example

If $\mathrm{T}_{q^3}^{\times} = \langle\eta\rangle$, then $\sigma\colon \mathcal{P} \to \mathcal{P}$, $\mathbb{G}_q x \mapsto \mathbb{G}_q \eta x$ (and dually for lines) defines a Singer cycle of $\mathrm{PHG}(2,\mathbb{G}_q) = \mathrm{PHG}(\mathbb{G}_{q^3})$.

Proposition

The Singer cycles generate a single conjugacy class of subgroups of $\mathrm{PGL}(3,\mathbb{G}_q)$.

Hence we need only consider a fixed Singer cycle σ.

Multisets Arising from a Singer cycle (Cont'd)

We are interested in multisets (of points) in $\mathrm{PHG}(2,\mathbb{G}_q)$ invariant under a Singer cycle σ.

Observation

A σ-invariant multiset $\mathfrak{K}$ in $\mathrm{PHG}(2,\mathbb{G}_q)$ is complete determined by its restriction $\mathfrak{k}$ to the point class $[\mathbb{G}_q 1] \cong \mathrm{AG}(2,\mathbb{F}_q)$.

Definition

We say that $\mathfrak{K}$ *is induced by* $\mathfrak{k}$.

Proposition

Suppose that the multisets $\mathfrak{K}_1$, $\mathfrak{K}_2$ in $\mathrm{PHG}(2,\mathbb{G}_q)$ are induced by multisets $\mathfrak{k}_1$, resp. $\mathfrak{k}_2$ in $[\mathbb{G}_q 1]$.

(i) *If $\mathfrak{K}_1$ and $\mathfrak{K}_2$ are equivalent then $\mathfrak{k}_1$, $\mathfrak{k}_2$ are equivalent.*

(ii) *If $\mathfrak{k}_1$, $\mathfrak{k}_2$ are translation-equivalent (i. e. there exists a translation τ of $[\mathbb{G}_q 1]$ such that $\mathfrak{k}_2 = \mathfrak{k}_1 \circ \tau$), then $\mathfrak{K}_1$ and $\mathfrak{K}_2$ are equivalent.*

σ-Invariant Arcs

First recall the following

Definition

A multiset $\mathfrak{K}$ in $\mathrm{PHG}(2,\mathbb{G}_q)$ is said to be a (k,n)-*arc* if

(i) $|\mathfrak{K}| := \mathfrak{K}(\mathcal{P}) := \sum_{p\in\mathcal{P}} \mathfrak{K}(p) = k$, and

(ii) $\mathfrak{K}(L) := \sum_{p\in L} \mathfrak{K}(p) \leq n$ for every line $L \in \mathcal{L}$.

Notes and questions

- Our goal is to find *maximal arcs* (i.e. those which maximize k for a given n) or, more generally,*complete arcs* (i.e. those which cannot be extended without increasing n).
- Restricting attention to σ-invariant arcs simplifies the construction problem. (However, we may loose something.)
- Can we compute the line multiplicities $\mathfrak{K}(L)$ from data about the inducing multiset $\mathfrak{k}$? (The answer is a somewhat restricted "yes".)
- Which multisets in $\mathrm{AG}(2,\mathbb{F}_q)$ give rise to good arcs?

The Teichmüller Set

The simplest example of a σ-invariant multiset

Definition

The multiset in $\mathrm{PHG}(2, \mathbb{G}_q)$ induced by $\{\mathbb{G}_q 1\}$ is called *Teichmüller set* and denoted by $\mathfrak{T}$.

We have $\mathfrak{T} = \{\mathbb{G}_q \eta^i ; 0 \leq i \leq q^2 + q\}$.

Up to equivalence $\mathfrak{T}$ is just the multiset induced by a single point in $[\mathbb{G}_q 1] \cong \mathrm{AG}(2, \mathbb{F}_q)$.

Theorem (H.-Landjev, 2005)

$\mathfrak{T}$ is a maximal $(q^2 + q + 1, 2)$-arc ("hyperoval") iff q is even.

Sketch of proof.

σ is transitive on line classes

$\Longrightarrow$ It suffices to check line multiplicities in one particular line class, say $[\mathrm{Tr}(x) = 0]$. This class consists of the lines $\mathrm{Tr}\big((1 + pv)x\big) = 0$, where $v \in (\mathbb{F}_{q^3}, +)/(\mathbb{F}_q, +)$.

A direct computation using the isomorphism $\mathbb{G}_q \cong \mathrm{W}_2(\mathbb{F}_q)$ (*Witt vectors of length* 2 *over* $\mathbb{F}_q$) yields the result. $\square$

Viewing Everything Within $\mathrm{AG}(2,\mathbb{F}_q)$

Consider again fixed line class, say $[L]=[\mathrm{Tr}(x)=0]$.
Define $I\subset\{0,1,\dots,q^2+q\}$ by

$$I:=\{i;\mathrm{Tr}(\eta^i)\equiv 0 \pmod p\}=\{i;[\mathbb{G}_q\eta^i] \text{ is on } [L]\}.$$

σ^i induces an isomorphism $[\mathbb{G}_q 1]\cong[\mathbb{G}_q\eta^i]$ of affine planes $\implies\sigma^i$ maps a unique parallel class of lines in $[\mathbb{G}_q 1]$ onto the parallel class of lines in $[\mathbb{G}_q\eta^i]$ having direction $[L]$.

Observations

- Putting these maps together gives a bijection ι from the set of lines of $[\mathbb{G}_q 1]\cong\mathrm{AG}(2,\mathbb{F}_q)$ to the set of line segments incident with $[L]$ (points of $[L]$).
- Under ι every line $L'\in[L]$ corresponds to a set of $q+1$ lines of $\mathrm{AG}(2,\mathbb{F}_q)$ having different directions. The q^2 sets $\iota^{-1}(L')$, $L'\in[L]$, form a single translation equivalence class.
- Knowing one such set $\iota^{-1}(L)$ enables us to compute the spectrum of $\mathfrak{k}$ w.r.t. to the whole class, and in turn the spectrum of $\mathfrak{K}$.

Observations cont'd

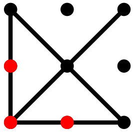
- The spectrum of $\mathfrak{T}$ w.r.t. the lines in $[L]$ equals the spectrum of $\iota^{-1}(L)$ w.r.t. to the points in $[\mathbb{G}_q 1]$.

Example

We give a computer-free proof of the existence of a (maximal) $(39,5)$-arc $\mathfrak{K}$ in the plane over $\mathbb{G}_3 = \mathbb{Z}_9$.

$|\mathfrak{K}| = 3 \cdot 13 = 3 \times \#$points of $\mathrm{PG}(2,\mathbb{F}_3)$
suggests inducing $\mathfrak{K}$ from a triangle in $\mathrm{AG}(2,\mathbb{F}_3)$.

An easy hand computation (omitted) reveals that $\mathfrak{T}$ is a (proper) 3-arc. Hence $\iota^{-1}(L)$ consists of 3 lines L_1, L_2, L_3 in $\mathrm{AG}(2,\mathbb{F}_3)$ passing through a common point p and another line L_4 with $p \notin L_4$ and $L_4 \nparallel L_i$ for $1 \leq i \leq 3$.



There exists a triangle $\mathfrak{k}$ in $\mathrm{AG}(2,\mathbb{F}_3)$ meeting $\iota^{-1}(L)$ in at most 5 points. The multiset in $\mathrm{PHG}(2,\mathbb{Z}_9)$ induced by $\mathfrak{k}$ is the required $(39,5)$-arc.

Generalization

The $(39, 5)$-arc meets every line in either 2 or 5 points.

Theorem

Let q be an odd prime. There exist $\left(\frac{1}{2}(q^4 - q), \frac{1}{2}(q^2 + q - 2)\right)$-arcs in $\mathrm{PHG}(2, \mathbb{G}_q)$ with only two line multiplicities $\frac{1}{2}(q^2 \pm q - 2)$.

Proof.

Use Singer induction from so-called triangle sets in $\mathrm{AG}(2, \mathbb{F}_q)$.

Triangle Sets

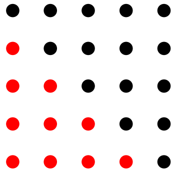
Definition

Suppose q is prime. A set of points of $\mathrm{AG}(2,\mathbb{F}_q)$ is called a *triangle set* if it is affinely equivalent to

$$\Delta := \left\{(x,y)\in\mathbb{F}_q^2; x+y<q-1\right\}.$$

Example

A triangle set in $\mathrm{AG}(2,\mathbb{F}_5)$.



Theorem

(i) *The characteristic function of a triangle set in* $\mathrm{AG}(2,\mathbb{F}_q)$ *is constant on* $q-2$ *parallel classes of lines and takes the values* $0,1,\ldots,q-1$ *exactly once on each of the remaining 3 parallel classes of lines.*

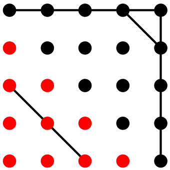
(ii) *If S is a set of points of* $\mathrm{AG}(2,\mathbb{F}_q)$ *with the foregoing properties, then q is necessarily prime and S is a triangle set.*

Observations

- The mod-q-value t of the sum of the multiplicities of any 3 lines in the 3 exceptional directions depends only on the translation equivalence class.
- The sum is 2-valued precisely for $t = q - 2$ (Example on the right) and $t = q - 1$ (3 concurrent lines).

Example

A triangle set in $\mathrm{AG}(2, \mathbb{F}_5)$.



Proof cont'd.

Induct from a triangle set $\mathfrak{k}$ such that the 3 exceptional lines of $\iota^{-1}(L)$ have $t = q - 2$ (i.e. multiplicities $q - 2$ and $2q - 2$). $\square$

Remark

Sets of points whose characteristic function is constant on all but three parallel classes of lines exist also in the affine planes $\mathrm{AG}(2, \mathbb{F}_q)$, $q = 2^r$, and give rise to arcs with two line multiplicities in the corresponding Hjelmslev planes $\mathrm{PHG}(2, \mathbb{G}_q)$.