Integral automorphisms of affine spaces over finite fields

István Kovács

University of Primorska, Slovenia

istvan.kovacs@upr.si

Joint work with Klavdija Kutnar, János Ruff and Tamás Szőnyi

4th Annual Mississippi Discrete Mathematics Workshop
November 14-15, 2015

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

Integral automorphisms

Notations:

- $\mathbb{F}_q$: the finite field with $q = p^h$ elements for an odd prime p.
- $\square_q$: the set of all square elements in $\mathbb{F}_q$.
- d : Euclidean distance

$$d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} (x_i - y_i)^2$$

where $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$.

Integral automorphisms

Two points $\mathbf{x}$ and $\mathbf{y}$ are at integral distance if $d(\mathbf{x}, \mathbf{y}) \in \square_q$.

Definition

An integral automorphism is any permutation γ of $\mathbb{F}_q^n$ satisfying

$$d(\mathbf{x}, \mathbf{y}) \in \square_q \iff d(\mathbf{x}^\gamma, \mathbf{y}^\gamma) \in \square_q$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$,

$\mathrm{Aut}(\mathbb{F}_q^n)$: the group of all integral automorphisms.

The case $n = 2$ and $q \equiv 3 \pmod 4$

Theorem (Kurz, 2007)

If $q \equiv 3 \pmod 4$ *then* $\mathrm{Aut}(\mathbb{F}_q^2)$ *consists of the permutations*

$$\mathbf{x} \mapsto a\mathbf{x}^{\sigma^i}A + \mathbf{b}$$

where $a \in \mathbb{F}_q^\times$, $i \in \{1, \ldots, h\}$, $A \in \mathrm{GL}(2, q)$ *with* $AA^T = I$, *and* $\mathbf{b} \in \mathbb{F}_q^2$.

$\sigma : \mathbb{F}_q^2 \to \mathbb{F}_q^2,\ (x_1, x_2) \mapsto (x_1^p, x_2^p)$.

Every integral automorphism in the above theorem is a semiaffine transformation.

Integral automorphisms which are not semiaffine transformations

Let $q \equiv 1 \pmod 4$ and let $\omega \in \mathbb{F}_q$ with $\omega^2 = -1$.

$x_1^2 + x_2^2 = (x_1 + \omega x_2)(x_1 - \omega x_2)$.

$F : (x_1, x_2) \mapsto (x_1 + \omega x_2, x_1 - \omega x_2)$.

$\sigma_1 : (x_1, x_2) \mapsto (x_1^p, x_2)$.

$\gamma : \mathbf{x} \mapsto (\mathbf{x}F)^{\sigma_1} F^{-1}$.

The permutation γ is an integral automorphism which is not a semiaffine transformation.

Case $n = 2$ and $q \equiv 1 \pmod 4$

Theorem (Kovács–Ruff, 2014)

If $q \equiv 1 \pmod 4$ *and* $q \neq 5, 9$ *then* $\mathrm{Aut}(\mathbb{F}_q^2)$ *consists of the permutations*

$$\mathbf{x} \mapsto a(\mathbf{x}F)^{\sigma_1^i \sigma_2^j} AF^{-1} + \mathbf{b}$$

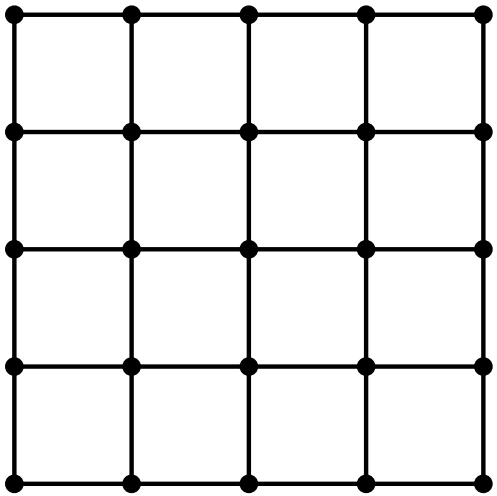
where $a \in \mathbb{F}_q^\times$, $F = \left(\begin{smallmatrix} 1 & 1 \\ \omega & -\omega \end{smallmatrix}\right)$, $i, j \in \{1, \ldots, h\}$, $A \in \left\langle \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle$, α *is a generator of* $\mathbb{F}_q^\times$, ω *is an element of* $\mathbb{F}_q$ *for which* $\omega^2 = -1$, *and* $\mathbf{b} \in \mathbb{F}_q^2$.

$\sigma_1 : (x_1, x_2) \mapsto (x_1^p, x_2)$,

$\sigma_2 : (x_1, x_2) \mapsto (x_1, x_2^p)$.

The exceptional cases $q = 5$ and $q = 9$

If $q = 5$ or 9, then $\mathrm{Aut}(\mathbb{F}_q^2)$ is the the automorphism group of a strongly regular graph.



The lattice graph $L_2(5)$

$$(i,j) \sim (i',j') \iff i = i' \text{ or } j = j'$$

$$\mathrm{Aut}(L_2(5)) = (S_5 \times S_5) : \mathbb{Z}_2.$$

Semiaffine transformations

Theorem (Kurz–Meyer, 2009)

If $n \geq 3$ *then* $\mathrm{Aut}(\mathbb{F}_q^n) \cap A\Gamma L(n,q)$ *consists of the permutations*

$$\mathbf{x} \mapsto a\mathbf{x}^{\sigma^i}A + \mathbf{b}$$

where $a \in \mathbb{F}_q^\times$, $i \in \{1,\ldots,h\}$, $A \in \mathrm{GL}(n,q)$ *with* $AA^T = I$, *and* $\mathbf{b} \in \mathbb{F}_q^n$.

$A\Gamma L(n,q)$: the group of semiaffine transformations.

$\sigma : (x_1,\ldots,x_n) \mapsto (x_1^p,\ldots,x_n^p)$.

Case $n \geq 3$

Theorem (K–Kutnar–Ruff–Szőnyi, 2015)

Every integral automorphism of $\mathrm{AG}(n, q)$ *is a semiaffine transformation if* $n \geq 3$.

Theorem (K–Kutnar–Ruff–Szőnyi, 2015)

If $n \geq 3$ *then* $\mathrm{Aut}(\mathbb{F}_q^n)$ *consists of the permutations*

$$\mathbf{x} \mapsto a\mathbf{x}^{\sigma^i}A + \mathbf{b}$$

where $a \in \mathbb{F}_q^\times$, $i \in \{1, \ldots, h\}$, $A \in \mathrm{GL}(n, q)$ *with* $AA^T = I$, *and* $\mathbf{b} \in \mathbb{F}_q^n$.

Ingrediant no. 1: The socle of $\mathrm{Aut}(\mathbb{F}_q^n)$

The socle $soc(G)$ of a group G is the subgroup of G generated by its minimal normal subgroups.

Let $E = \{\mathbf{x} \mapsto \mathbf{x} + \mathbf{b} : \mathbf{b} \in \mathbb{F}_q^n\}$.

Lemma

If $(n, q) \neq (2, 5)$ *then* $\mathrm{soc}(\mathrm{Aut}(\mathbb{F}_q^n)) = E$.

Corollary

For all $\gamma \in \mathrm{Aut}(\mathbb{F}_q^n)$ *with* $\mathbf{0}^\gamma = \mathbf{0}$, *and for all* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$,

$$(\mathbf{x} + \mathbf{y})^\gamma = \mathbf{x}^\gamma + \mathbf{y}^\gamma.$$

Ingrediant no. 2: The $\mathrm{Aut}(\mathbb{F}_q^n)_{\mathbf{0}}$-orbits

Let $\mathrm{Aut}(\mathbb{F}_q^n)_{\mathbf{0}}$ be the stabiliser of $\mathbf{0}$ in $\mathrm{Aut}(\mathbb{F}_q^n)$ where $\mathbf{0} = (0, \ldots, 0)$.

Let $M = \left\{ \mathbf{x} \mapsto aA\mathbf{x} : a \in \mathbb{F}^\times, AA^T = I \right\}$.

Lemma (Kurz–Meyer, 2015)

The M-orbits are

- $S_0 = \left\{ \mathbf{x} \in \mathbb{F}_q^n : \sum_{i=1}^n x_i^2 = 0, \mathbf{x} \neq \mathbf{0} \right\}$,
- $S_+ = \left\{ \mathbf{x} \in \mathbb{F}_q^n : \sum_{i=1}^n x_i^2 \in \square_q \setminus \{0\} \right\}$,
- $S_- = \left\{ \mathbf{x} \in \mathbb{F}_q^n : \sum_{i=1}^n x_i^2 \notin \square_q \right\}$.

Ingrediant no. 2: The $\mathrm{Aut}(\mathbb{F}_q^n)_{\mathbf{0}}$-orbits

Lemma

If $n \geq 3$, then the $\mathrm{Aut}(\mathbb{F}_q^n)_{\mathbf{0}}$-orbits are

- $S_0 = \left\{\mathbf{x} \in \mathbb{F}_q^n : \sum_{i=1}^n x_i^2 = 0, \mathbf{x} \neq \mathbf{0}\right\}$,
- $S_+ = \left\{\mathbf{x} \in \mathbb{F}_q^n : \sum_{i=1}^n x_i^2 \in \square_q \setminus \{0\}\right\}$,
- $S_- = \left\{\mathbf{x} \in \mathbb{F}_q^n : \sum_{i=1}^n x_i^2 \notin \square_q\right\}$.

Corollary

For all $\gamma \in \mathrm{Aut}(\mathbb{F}_q^n)$ and $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$,

$$d(\mathbf{x}, \mathbf{y}) = 0 \iff d(\mathbf{x}^\gamma, \mathbf{y}^\gamma) = 0.$$

Ingrediant no. 3: The quadric induced by $\sum x_i^2$

Let $\mathcal{Q}$ be the quadric in PG$(n-1,q)$ induced by $\sum x_i^2$:

$$\mathcal{Q} = \left\{ P(\mathbf{x}) : \sum_{i=1}^{n} x_i^2 = 0 \right\} = \left\{ P(\mathbf{x}) : \mathbf{x} \in S_0 \right\}.$$

A generator of $\mathcal{Q}$ is a projective subspace of maximum dimension on $\mathcal{Q}$.

Properties.

1. Every point on $\mathcal{Q}$ can be expressed as the intersection of some generators.
2. Every point outside $\mathcal{Q}$ can be expressed as the intersection of two secants if $(n,q) \neq (3,3)$.

Ingrediant no. 4: Maximal integral point sets

Let $I_0(d, \mathbb{F}_q^n)$ denote the largest cardinality $|X|$ that $X \subset \mathbb{F}_q^n$ and

$$d(\mathbf{x}, \mathbf{y}) = 0 \text{ for all } \mathbf{x}, \mathbf{y} \in X.$$

Theorem (Iosevich–Shparlinski–Xiong, 2010)

The number $I_0(d, \mathbb{F}_q^n) = |U|$ where U corresponds to a generator of $\mathcal{Q}$.

Sketch of proof

Let $\gamma \in \mathrm{Aut}(\mathbb{F}_q^n)_{\mathbf{0}}$. Our goal is to show that γ is a semilinear transformation. By the fundamental theorem of projective geometry, it is sufficient to show that γ induces a collineation of $\mathrm{PG}(n-1, q)$.

This is done in a few steps. Namely, γ maps

- any max. subspace $U \subset S_0$ to a max. subspace $U' \subset S_0$;

- any 1-dim. subspace $U \subset S_0$ to a 1-dim. subspace $U' \subset S_0$;

- any 2-dim. subspace U generated by two vectors from S_0 to a 2-dim. subspace U'.

- any 1-dim. subspace U to a 1-dim. subspace U'.

- any 2-dim. subspace U to a 2-dim. subspace U'.

THANK YOU FOR ATTENTION.