Enumeration of the Semilinear Isometry Classes of Linear Codes

Harald Fripertinger

Karl-Franzens-Universität Graz

ALCOMA05, Thurnau, April 3 – 10, 2005

Home Page

Title Page

Contents

Page 1 of 21

Go Back

Full Screen

Close

Quit

Enumeration of the Semilinear Isometry Classes of Linear Codes

Harald Fripertinger

Karl-Franzens-Universität Graz

ALCOMA05, Thurnau, April 3 – 10, 2005

In joint papers together with A. Kerber we showed how to enumerate the linear isometry classes of linear codes by certain substitutions into cycle index polynomials for the action of projective linear groups on projective spaces. In my talk I describe how to generalize this approach for the enumeration of the semilinear isometry classes.

Enumeration of the Semilinear Isometry Classes of Linear Codes

Harald Fripertinger
Karl-Franzens-Universität Graz

ALCOMA05, Thurnau, April 3 – 10, 2005

In joint papers together with A. Kerber we showed how to enumerate the linear isometry classes of linear codes by certain substitutions into cycle index polynomials for the action of projective linear groups on projective spaces. In my talk I describe how to generalize this approach for the enumeration of the semilinear isometry classes.

1. Introduction

Enumeration of the Semilinear Isometry Classes of Linear Codes

Harald Fripertinger

Karl-Franzens-Universität Graz

ALCOMA05, Thurnau, April 3 – 10, 2005

In joint papers together with A. Kerber we showed how to enumerate the linear isometry classes of linear codes by certain substitutions into cycle index polynomials for the action of projective linear groups on projective spaces. In my talk I describe how to generalize this approach for the enumeration of the semilinear isometry classes.

1. Introduction
2. The group of semilinear isometries as a generalized wreath product.

Enumeration of the Semilinear Isometry Classes of Linear Codes

Harald Fripertinger
Karl-Franzens-Universität Graz

ALCOMA05, Thurnau, April 3 – 10, 2005

In joint papers together with A. Kerber we showed how to enumerate the linear isometry classes of linear codes by certain substitutions into cycle index polynomials for the action of projective linear groups on projective spaces. In my talk I describe how to generalize this approach for the enumeration of the semilinear isometry classes.

1. Introduction
2. The group of semilinear isometries as a generalized wreath product.
3. Generalized Lehmann's Lemma and applications.

Enumeration of the Semilinear Isometry Classes of Linear Codes

Harald Fripertinger
Karl-Franzens-Universität Graz

ALCOMA05, Thurnau, April 3 – 10, 2005

In joint papers together with A. Kerber we showed how to enumerate the linear isometry classes of linear codes by certain substitutions into cycle index polynomials for the action of projective linear groups on projective spaces. In my talk I describe how to generalize this approach for the enumeration of the semilinear isometry classes.

1. Introduction
2. The group of semilinear isometries as a generalized wreath product.
3. Generalized Lehmann's Lemma and applications.
4. Cycle index polynomials for the actions of $\mathrm{P\Gamma L}_k(q)$ on $\mathrm{PG}_{k-1}(q)$.

Introduction

$\mathbb{F}_q$: finite field of cardinality $q = p^r$, where the prime number p is its characteristic, and r is a positive integer. Differences between linear isometry and semilinear isometry only for $r > 1$.

Introduction

$\mathbb{F}_q$: finite field of cardinality $q = p^r$, where the prime number p is its characteristic, and r is a positive integer. Differences between linear isometry and semilinear isometry only for $r > 1$.

$Gal := Gal[\mathbb{F}_q : \mathbb{F}_p]$: the Galois group is the group of all $\mathbb{F}_p$-automorphisms of $\mathbb{F}_q$. It is a cyclic group of order r and it is generated by the Frobenius-automorphism $\tau : \mathbb{F}_q \to \mathbb{F}_q$, $\tau(\kappa) := \kappa^p$.

Introduction

$\mathbb{F}_q$: finite field of cardinality $q = p^r$, where the prime number p is its characteristic, and r is a positive integer. Differences between linear isometry and semilinear isometry only for $r > 1$.

$Gal := Gal[\mathbb{F}_q : \mathbb{F}_p]$: the Galois group is the group of all $\mathbb{F}_p$-automorphisms of $\mathbb{F}_q$. It is a cyclic group of order r and it is generated by the Frobenius-automorphism $\tau\colon \mathbb{F}_q \to \mathbb{F}_q$, $\tau(\kappa) := \kappa^p$.

C: linear (n,k)-code over $\mathbb{F}_q$, a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, described by a generator matrix which is a $k \times n$-matrix over $\mathbb{F}_q$, the rows of which form a basis of C. Vectors $v \in \mathbb{F}_q^n$ are written as rows, $v = (v_0, v_1, \ldots, v_{n-1})$.

Introduction

$\mathbb{F}_q$: finite field of cardinality $q = p^r$, where the prime number p is its characteristic, and r is a positive integer. Differences between linear isometry and semilinear isometry only for $r > 1$.

$Gal := Gal[\mathbb{F}_q : \mathbb{F}_p]$: the Galois group is the group of all $\mathbb{F}_p$-automorphisms of $\mathbb{F}_q$. It is a cyclic group of order r and it is generated by the Frobenius-automorphism $\tau : \mathbb{F}_q \to \mathbb{F}_q$, $\tau(\kappa) := \kappa^p$.

C: linear (n,k)-code over $\mathbb{F}_q$, a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, described by a generator matrix which is a $k \times n$-matrix over $\mathbb{F}_q$, the rows of which form a basis of C. Vectors $v \in \mathbb{F}_q^n$ are written as rows, $v = (v_0, v_1, \ldots, v_{n-1})$.

If Γ is a generator matrix of C, then $\mathrm{GL}_k(q)(\Gamma) = \{B \cdot \Gamma \mid B \in \mathrm{GL}_k(q)\}$ is the set of all generator matrices of C.

The Hamming-metric on $\mathbb{F}_q^n$ is the mapping

$$d\colon \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{Z}_{\geq 0} : d(v,w) := \left|\{i \in n \mid v_i \neq w_i\}\right|.$$

The number of errors which can be detected or corrected by maximum-likelihood decoding is determined by the minimum distance

$$\operatorname{dist}(C) := \min\{d(c,c') \mid c,c' \in C,\ c \neq c'\} = \min\{d(c,0) \mid c \in C \setminus \{0\}\}.$$

Two linear codes having the same metrical structure have the same coding theoretic properties. They are considered to be equivalent.

The Hamming-metric on $\mathbb{F}_q^n$ is the mapping

$$d\colon \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{Z}_{\geq 0} : d(v,w) := \left|\{i \in n \mid v_i \neq w_i\}\right|.$$

The number of errors which can be detected or corrected by maximum-likelihood decoding is determined by the minimum distance

$$\operatorname{dist}(C) := \min\{d(c,c') \mid c,c' \in C,\ c \neq c'\} = \min\{d(c,0) \mid c \in C \setminus \{0\}\}.$$

Two linear codes having the same metrical structure have the same coding theoretic properties. They are considered to be equivalent.

A mapping $\iota\colon \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ that preserves the Hamming distance

$$d(v,v') = d(\iota(v),\iota(v')) \text{ for all } v,v' \in \mathbb{F}_q^n$$

with $\iota(C) = C'$ is an isometry between C and C'.

Linear isometries

Two linear (n,k)-codes C and C' are said to be *linearly isometric* or *monomially isometric* if there exists a linear isometry of $\mathbb{F}_q^n$ that maps C onto C'.

The group of all linear isometries is described as the wreath product $\mathbb{F}_q^* \wr_n S_n$.

It operates in a canonical way on the set of all functions from n to $\mathbb{F}_q^k \setminus \{0\}$. By an application of Lehmann's Lemma we replaced this action by an action of S_n on the set of functions from n to $\mathrm{PG}_{k-1}(q)$. This is the $k-1$-dimensional projective space. Its elements, the so called points of $\mathrm{PG}_{k-1}(q)$ are the orbits of $\mathbb{F}_q^*$ on $\mathbb{F}_q^k \setminus \{0\}$.

Home Page

Title Page

Contents

Page 5 of 21

Go Back

Full Screen

Close

Quit

Semilinear isometries

A mapping $\sigma\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ is called *semilinear* if for all $u, v \in \mathbb{F}_q^n$, all $\kappa \in \mathbb{F}_q$ and a given automorphism α of $\mathbb{F}_q$ we have

$$\sigma(u+v) = \sigma(u) + \sigma(v), \qquad \sigma(\kappa u) = \alpha(\kappa)\sigma(u).$$

Two linear (n,k)-codes C and C' are said to be *semilinearly isometric* if there exists a semilinear isometry of $\mathbb{F}_q^n$ that maps C onto C'.

Since σ preserves the Hamming distance, the image of a unit vector $e^{(i)}$ must be a vector of weight 1, i.e. a nonzero multiple $\kappa_j e^{(j)}$ of a unit vector $e^{(j)}$ with $\kappa_j \in \mathbb{F}_q^*$. Since this mapping keeps the dimension, different unit vectors are mapped under σ onto nonzero multiples of different unit vectors. In formal terms

$$\sigma(e^{(i)}) = \varphi(\pi(i))e^{(\pi(i))}, \quad \varphi(\pi(i)) \in \mathbb{F}_q^*, \quad \pi \in S_n,$$

where φ is a mapping $n \longrightarrow \mathbb{F}_q^*$ and π a permutation of n.

Since σ preserves the Hamming distance, the image of a unit vector $e^{(i)}$ must be a vector of weight 1, i.e. a nonzero multiple $\kappa_j e^{(j)}$ of a unit vector $e^{(j)}$ with $\kappa_j \in \mathbb{F}_q^*$. Since this mapping keeps the dimension, different unit vectors are mapped under σ onto nonzero multiples of different unit vectors. In formal terms

$$\sigma(e^{(i)}) = \varphi(\pi(i))e^{(\pi(i))}, \quad \varphi(\pi(i)) \in \mathbb{F}_q^*, \quad \pi \in S_n,$$

where φ is a mapping $n \longrightarrow \mathbb{F}_q^*$ and π a permutation of n. In conclusion,

$$\sigma = (\alpha, \varphi, \pi), \quad \alpha \in \mathrm{Aut}(\mathbb{F}_q), \quad \varphi \in (\mathbb{F}_q^*)^n, \quad \pi \in S_n.$$

Since σ preserves the Hamming distance, the image of a unit vector $e^{(i)}$ must be a vector of weight 1, i.e. a nonzero multiple $\kappa_j e^{(j)}$ of a unit vector $e^{(j)}$ with $\kappa_j \in \mathbb{F}_q^*$. Since this mapping keeps the dimension, different unit vectors are mapped under σ onto nonzero multiples of different unit vectors. In formal terms

$$\sigma(e^{(i)}) = \varphi(\pi(i))e^{(\pi(i))}, \quad \varphi(\pi(i)) \in \mathbb{F}_q^*, \quad \pi \in S_n,$$

where φ is a mapping $n \longrightarrow \mathbb{F}_q^*$ and π a permutation of n. In conclusion,

$$\sigma = (\alpha, \varphi, \pi), \quad \alpha \in \mathrm{Aut}(\mathbb{F}_q), \quad \varphi \in (\mathbb{F}_q^*)^n, \quad \pi \in S_n.$$

Operation on the vector $v \in \mathbb{F}_q^n$ yields

$$\sigma(v) = \left(\varphi(0)\alpha(v_{\pi^{-1}(0)}), \ldots, \varphi(n-1)\alpha(v_{\pi^{-1}(n-1)})\right).$$

The group of semilinear isometries

We prefer to write the semilinear isometry σ in the form $(\psi;(\alpha,\pi))$. Applying the two semilinear isometries $\sigma_2 = (\psi_2;(\alpha_2,\pi_2))$ and $\sigma_1 = (\psi_1;(\alpha_1,\pi_1))$ to the vector $v = (v_0,\ldots,v_{n-1}) \in \mathbb{F}_q^n$ and indicating $\sigma_1(v)$ by $v' = (v'_0,\ldots,v'_{n-1})$ we obtain

$$(\psi_2;(\alpha_2,\pi_2))\big((\psi_1;(\alpha_1,\pi_1))(v_0,\ldots,v_{n-1})\big) =$$

$$(\psi_2;(\alpha_2,\pi_2))(v'_0,\ldots,v'_{n-1})$$

The group of semilinear isometries

We prefer to write the semilinear isometry σ in the form $(\psi;(\alpha,\pi))$. Applying the two semilinear isometries $\sigma_2 = (\psi_2;(\alpha_2,\pi_2))$ and $\sigma_1 = (\psi_1;(\alpha_1,\pi_1))$ to the vector $v = (v_0,\dots,v_{n-1}) \in \mathbb{F}_q^n$ and indicating $\sigma_1(v)$ by $v' = (v'_0,\dots,v'_{n-1})$ we obtain

$$(\psi_2;(\alpha_2,\pi_2))\big((\psi_1;(\alpha_1,\pi_1))(v_0,\dots,v_{n-1})\big) =$$

$$(\psi_2;(\alpha_2,\pi_2))(v'_0,\dots,v'_{n-1}) =$$

$$\big(\psi_2(0)\alpha_2(v'_{\pi_2^{-1}(0)}),\dots,\psi_2(n-1)\alpha_2(v'_{\pi_2^{-1}(n-1)})\big)$$

The group of semilinear isometries

We prefer to write the semilinear isometry σ in the form $(\psi;(\alpha,\pi))$. Applying the two semilinear isometries $\sigma_2=(\psi_2;(\alpha_2,\pi_2))$ and $\sigma_1=(\psi_1;(\alpha_1,\pi_1))$ to the vector $v=(v_0,\dots,v_{n-1})\in\mathbb{F}_q^n$ and indicating $\sigma_1(v)$ by $v'=(v'_0,\dots,v'_{n-1})$ we obtain

$$(\psi_2;(\alpha_2,\pi_2))\big((\psi_1;(\alpha_1,\pi_1))(v_0,\dots,v_{n-1})\big)=$$

$$(\psi_2;(\alpha_2,\pi_2))(v'_0,\dots,v'_{n-1})=$$

$$\big(\psi_2(0)\alpha_2(v'_{\pi_2^{-1}(0)}),\dots,\psi_2(n-1)\alpha_2(v'_{\pi_2^{-1}(n-1)})\big)=$$

$$\Big(\psi_2(0)\alpha_2\big(\psi_1(\pi_2^{-1}(0))\alpha_1(v_{\pi_1^{-1}(\pi_2^{-1}(0))})\big),\dots,$$

$$\dots,\psi_2(n-1)\alpha_2\big(\psi_1(\pi_2^{-1}(n-1))\alpha_1(v_{\pi_1^{-1}(\pi_2^{-1}(n-1))})\big)\Big)$$

The group of semilinear isometries

We prefer to write the semilinear isometry σ in the form $(\psi;(\alpha,\pi))$. Applying the two semilinear isometries $\sigma_2=(\psi_2;(\alpha_2,\pi_2))$ and $\sigma_1=(\psi_1;(\alpha_1,\pi_1))$ to the vector $v=(v_0,\ldots,v_{n-1})\in\mathbb{F}_q^n$ and indicating $\sigma_1(v)$ by $v'=(v'_0,\ldots,v'_{n-1})$ we obtain

$$\begin{aligned}
&(\psi_2;(\alpha_2,\pi_2))\big((\psi_1;(\alpha_1,\pi_1))(v_0,\ldots,v_{n-1})\big)=\\
&(\psi_2;(\alpha_2,\pi_2))(v'_0,\ldots,v'_{n-1})=\\
&\big(\psi_2(0)\alpha_2(v'_{\pi_2^{-1}(0)}),\ldots,\psi_2(n-1)\alpha_2(v'_{\pi_2^{-1}(n-1)})\big)=\\
&\Big(\psi_2(0)\alpha_2\big(\psi_1(\pi_2^{-1}(0))\alpha_1(v_{\pi_1^{-1}(\pi_2^{-1}(0))})\big),\ldots,\\
&\ldots,\psi_2(n-1)\alpha_2\big(\psi_1(\pi_2^{-1}(n-1))\alpha_1(v_{\pi_1^{-1}(\pi_2^{-1}(n-1))})\big)\Big)=\\
&\Big(\psi_2(0)\alpha_2(\psi_1(\pi_2^{-1}(0)))(\alpha_2\circ\alpha_1)(v_{(\pi_2\circ\pi_1)^{-1}(0)}),\ldots,\\
&\ldots,\psi_2(n-1)\alpha_2(\psi_1(\pi_2^{-1}(n-1)))(\alpha_2\circ\alpha_1)(v_{(\pi_2\circ\pi_1)^{-1}(n-1)})\Big)
\end{aligned}$$

Lemma The group of all semilinear isometries of $\mathbb{F}_q^n$ is the semidirect product

$$(\mathbb{F}_q^*)^n \ltimes (Gal \times S_n)$$

with the multiplication

$$(\psi_2;(\alpha_2,\pi_2))\cdot(\psi_1;(\alpha_1,\pi_1)) := (\psi_2\psi_{1(\alpha_2,\pi_2)};(\alpha_2\alpha_1,\pi_2\circ\pi_1)),$$

where

$$\psi_{1(\alpha_2,\pi_2)}(i) := \alpha_2(\psi_1(\pi_2^{-1}(i))), \qquad i \in n$$

and

$$\psi_2\psi_1(i) := \psi_2(i)\psi_1(i), \qquad i \in n.$$

This is a generalized wreath product.

Lemma The group of all semilinear isometries of $\mathbb{F}_q^n$ is the semidirect product

$$(\mathbb{F}_q^*)^n \ltimes (Gal \times S_n)$$

with the multiplication

$$(\psi_2;(\alpha_2,\pi_2)) \cdot (\psi_1;(\alpha_1,\pi_1)) := (\psi_2\psi_{1(\alpha_2,\pi_2)};(\alpha_2\alpha_1,\pi_2\circ\pi_1)),$$

where

$$\psi_{1(\alpha_2,\pi_2)}(i) := \alpha_2(\psi_1(\pi_2^{-1}(i))), \qquad i \in n$$

and

$$\psi_2\psi_1(i) := \psi_2(i)\psi_1(i), \qquad i \in n.$$

This is a generalized wreath product.

The identity element is $(1;(\tau^0,\mathrm{id}))$, where 1 is the mapping $i \mapsto 1$, $i \in n$.

The inverse of $(\psi;(\alpha,\pi))$ is $(\psi^{-1}_{(\alpha^{-1},\pi^{-1})};(\alpha^{-1},\pi^{-1}))$ where $\psi^{-1}(i) := (\psi(i))^{-1}$, $i \in n$, and $\psi^{-1}_{(\alpha,\pi)} := (\psi_{(\alpha,\pi)})^{-1} = (\psi^{-1})_{(\alpha,\pi)}$.

The group of semilinear isometries is the generalized wreath product of $\mathbb{F}_q^*$ and $Gal \times S_n$ which we indicate by $\mathbb{F}_q^* \wr\wr_n (Gal \times S_n)$.

The group of semilinear isometries is the generalized wreath product of $\mathbb{F}_q^*$ and $Gal \times S_n$ which we indicate by $\mathbb{F}_q^* \wr_n (Gal \times S_n)$.

Order $\left|\mathbb{F}_q^* \wr_n (Gal \times S_n)\right| = (q-1)^n \cdot r \cdot n!$.

Home Page

Title Page

Contents

Go Back

Full Screen

Close

Quit

The group of semilinear isometries is the generalized wreath product of $\mathbb{F}_q^*$ and $Gal \times S_n$ which we indicate by $\mathbb{F}_q^* \wr_n (Gal \times S_n)$.

Order $\left|\mathbb{F}_q^* \wr_n (Gal \times S_n)\right| = (q-1)^n \cdot r \cdot n!$.

The generalization of the natural action of a wreath product yields

$$\mathbb{F}_q^* \wr_n (Gal \times S_n) \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$

$$((\psi;(\alpha,\pi)),v) \mapsto \left(\psi(0)\alpha(v_{\pi^{-1}(0)}),\ldots,\psi(n-1)\alpha(v_{\pi^{-1}(n-1)})\right).$$

This is the action of the semilinear isometry on $\mathbb{F}_q^n$.

Operation on the set of all (n,k)-codes

We denote the set of all $k \times n$-matrices over $\mathbb{F}_q$ of rank k by $\mathbb{F}_q^{k\times n,k}$.

Describing codes by their generator matrices we obtain that the set of semilinear isometry classes of (n,k)-codes is equal to the set of orbits

$$\mathbb{F}_q^* \wr_n (Gal \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash \mathbb{F}_q^{k\times n,k} \right),$$

Operation on the set of all (n,k)-codes

We denote the set of all $k \times n$-matrices over $\mathbb{F}_q$ of rank k by $\mathbb{F}_q^{k\times n,k}$.

Describing codes by their generator matrices we obtain that the set of semilinear isometry classes of (n,k)-codes is equal to the set of orbits

$$\mathbb{F}_q^* \wr_n (Gal \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash \mathbb{F}_q^{k\times n,k} \right),$$

where the operation of $(\psi;(\alpha,\pi)) \in \mathbb{F}_q^* \wr_n (Gal \times S_n)$ on the orbit $\mathrm{GL}_k(q)(\Gamma)$ is given by

$$\Big((\psi;(\alpha,\pi)),\mathrm{GL}_k(q)(\Gamma)\Big) \mapsto \mathrm{GL}_k(q)(\hat{\Gamma}) \text{ where } \hat{\Gamma}(i) = \psi(i)\alpha(\Gamma(\pi^{-1}(i))).$$

Here we identify the matrix Γ with the function $\Gamma\colon n \to \mathbb{F}_q^k$ where the transposed vector $\Gamma(i)$ is the i-th column of Γ.

Again, similarly as with the linear isometry classes we eliminate the rank condition on the $k \times n$-matrices and consider the set of *all* $k \times n$-matrices over $\mathbb{F}_q$ which do not contain zero columns. They can be expressed as functions $n \to \mathbb{F}_q^k \setminus \{0\}$. Thus our task is to determine the cardinality of

$$\mathbb{F}_q^* \wr_n (Gal \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^k \setminus \{0\})^n \right).$$

Again, similarly as with the linear isometry classes we eliminate the rank condition on the $k \times n$-matrices and consider the set of *all* $k \times n$-matrices over $\mathbb{F}_q$ which do not contain zero columns. They can be expressed as functions $n \to \mathbb{F}_q^k \setminus \{0\}$. Thus our task is to determine the cardinality of

$$\mathbb{F}_q^* \wr\wr_n (Gal \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^k \setminus \{0\})^n \right).$$

In the situation of linear isometries the actions of the isometry group and of the linear group were commuting and we obtained an action of the direct product of these two groups on $\mathbb{F}_q^{k \times n,k}$. In general, the action of the semilinear isometry group does not commute with the action of $\mathrm{GL}_k(q)$.

Again, similarly as with the linear isometry classes we eliminate the rank condition on the $k \times n$-matrices and consider the set of *all* $k \times n$-matrices over $\mathbb{F}_q$ which do not contain zero columns. They can be expressed as functions $n \longrightarrow \mathbb{F}_q^k \setminus \{0\}$. Thus our task is to determine the cardinality of

$$\mathbb{F}_q^* \wr_n (Gal \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^k \setminus \{0\})^n\right).$$

In the situation of linear isometries the actions of the isometry group and of the linear group were commuting and we obtained an action of the direct product of these two groups on $\mathbb{F}_q^{k \times n,k}$. In general, the action of the semilinear isometry group does not commute with the action of $\mathrm{GL}_k(q)$. For $A \in \mathrm{GL}_k(q)$, $(\psi; (\alpha, \pi)) \in \mathbb{F}_q^* \wr_n (Gal \times S_n)$ and $\Gamma \in (\mathbb{F}_q^k \setminus \{0\})^n$:

$$A \cdot (\psi; (\alpha, \pi))\Gamma =$$
$$\left(\psi(0)A \cdot \alpha(\Gamma(\pi^{-1}(0))), \ldots, \psi(n-1)A \cdot \alpha(\Gamma(\pi^{-1}(n-1)))\right)$$

Home Page

Title Page

Contents

◀◀ ▶▶

◀ ▶

Go Back

Full Screen

Close

Quit

Again, similarly as with the linear isometry classes we eliminate the rank condition on the $k \times n$-matrices and consider the set of *all* $k \times n$-matrices over $\mathbb{F}_q$ which do not contain zero columns. They can be expressed as functions $n \longrightarrow \mathbb{F}_q^k \setminus \{0\}$. Thus our task is to determine the cardinality of

$$\mathbb{F}_q^* \wr_n (Gal \times S_n) \backslash\backslash \left(\mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^k \setminus \{0\})^n \right).$$

In the situation of linear isometries the actions of the isometry group and of the linear group were commuting and we obtained an action of the direct product of these two groups on $\mathbb{F}_q^{k\times n,k}$. In general, the action of the semilinear isometry group does not commute with the action of $\mathrm{GL}_k(q)$. For $A \in \mathrm{GL}_k(q)$, $(\psi;(\alpha,\pi)) \in \mathbb{F}_q^* \wr_n (Gal \times S_n)$ and $\Gamma \in (\mathbb{F}_q^k \setminus \{0\})^n$:

$$A \cdot (\psi;(\alpha,\pi))\Gamma =$$

$$\left(\psi(0)A \cdot \alpha(\Gamma(\pi^{-1}(0))), \ldots, \psi(n-1)A \cdot \alpha(\Gamma(\pi^{-1}(n-1)))\right)$$

$$(\psi;(\alpha,\pi))A \cdot \Gamma =$$

$$\left(\psi(0)\alpha(A) \cdot \alpha(\Gamma(\pi^{-1}(0))), \ldots, \psi(n-1)\alpha(A) \cdot \alpha(\Gamma(\pi^{-1}(n-1)))\right).$$

Generalization of Lehmann's Lemma

If $\varphi\colon \mathrm{GL}_k(q)\backslash\backslash(\mathbb{F}_q^k \setminus \{0\})^n \to \mathrm{GL}_k(q)\backslash\backslash\left(\mathbb{F}_q^* \backslash\backslash(\mathbb{F}_q^k \setminus \{0\})\right)^n$ is given by $\mathrm{GL}_k(q)(\Gamma) \mapsto \mathrm{GL}_k(q)(\bar{\Gamma})$ where $\bar{\Gamma}(i) = \mathbb{F}_q^*(\Gamma(i))$, then

$$\Phi\colon \left(\mathbb{F}_q^* \wr_n (Gal \times S_n)\right)\backslash\backslash\left(\mathrm{GL}_k(q)\backslash\backslash(\mathbb{F}_q^k \setminus \{0\})^n\right) \to (Gal \times S_n)\backslash\backslash\left(\mathrm{GL}_k(q)\backslash\backslash\left(\mathbb{F}_q^* \backslash\backslash(\mathbb{F}_q^k \setminus \{0\})\right)^n\right)$$

defined by

$$\left(\mathbb{F}_q^* \wr_n (Gal \times S_n)\right)(\mathrm{GL}_k(q)(\Gamma)) \mapsto (Gal \times S_n)(\varphi(\mathrm{GL}_k(q)(\Gamma)))$$

is a bijection.

Home Page

Title Page

Contents

Page 12 of 21

Go Back

Full Screen

Close

Quit

Generalization of Lehmann's Lemma

If $\varphi\colon \mathrm{GL}_k(q)\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})^n \to \mathrm{GL}_k(q)\backslash\backslash\left(\mathbb{F}_q^*\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})\right)^n$ is given by $\mathrm{GL}_k(q)(\Gamma)\mapsto \mathrm{GL}_k(q)(\overline{\Gamma})$ where $\overline{\Gamma}(i)=\mathbb{F}_q^*(\Gamma(i))$, then

$$\Phi\colon \left(\mathbb{F}_q^*\wr_n(Gal\times S_n)\right)\backslash\backslash\left(\mathrm{GL}_k(q)\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})^n\right)\to$$

$$(Gal\times S_n)\backslash\backslash\left(\mathrm{GL}_k(q)\backslash\backslash\left(\mathbb{F}_q^*\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})\right)^n\right)$$

defined by

$$\left(\mathbb{F}_q^*\wr_n(Gal\times S_n)\right)(\mathrm{GL}_k(q)(\Gamma))\mapsto(Gal\times S_n)(\varphi(\mathrm{GL}_k(q)(\Gamma)))$$

is a bijection. On the right hand side we have an operation of $(Gal\times S_n)$ on the set of orbits $\mathrm{GL}_k(q)\backslash\backslash\left(\mathbb{F}_q^*\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})\right)^n$ of the form

$$(\alpha,\pi)\,\mathrm{GL}_k(q)(\overline{\Gamma})=\mathrm{GL}_k(q)(\hat{\Gamma})$$

where $\hat{\Gamma}(i)=\alpha(\overline{\Gamma}(\pi^{-1}(i)))=\alpha(\mathbb{F}_q^*(\Gamma(\pi(i))))=\mathbb{F}_q^*(\alpha(\Gamma(\pi(i))))$, $i\in n$.

The set of orbits $\mathbb{F}_q^* \backslash\backslash \mathbb{F}_q^k \setminus \{0\}$ is the $(k-1)$-dimensional projective space $\mathrm{PG}_{k-1}(q)$.

The set of orbits $\mathbb{F}_q^* \backslash\backslash \mathbb{F}_q^k \setminus \{0\}$ is the $(k-1)$-dimensional projective space $\mathrm{PG}_{k-1}(q)$.

The action of $\mathrm{GL}_k(q)$ on $\mathrm{PG}_{k-1}(q)$ corresponds to the natural action of the projective group $\mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}(q)$. Thus

$$\left|\left(\mathbb{F}_q^* \wr_n (Gal \times S_n)\right) \backslash\backslash\, \mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^k \setminus \{0\})^n\right| = \left|(Gal \times S_n) \backslash\backslash \left(\mathrm{PGL}_k(q) \backslash\backslash\, \mathrm{PG}_{k-1}(q)^n\right)\right|$$

The set of orbits $\mathbb{F}_q^* \backslash\backslash \mathbb{F}_q^k \setminus \{0\}$ is the $(k-1)$-dimensional projective space $\mathrm{PG}_{k-1}(q)$.

The action of $\mathrm{GL}_k(q)$ on $\mathrm{PG}_{k-1}(q)$ corresponds to the natural action of the projective group $\mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}(q)$. Thus

$$\left|\left(\mathbb{F}_q^* \wr_n (Gal \times S_n)\right) \backslash\backslash \mathrm{GL}_k(q) \backslash\backslash (\mathbb{F}_q^k \setminus \{0\})^n\right| =$$
$$\left|(Gal \times S_n) \backslash\backslash \left(\mathrm{PGL}_k(q) \backslash\backslash \mathrm{PG}_{k-1}(q)^n\right)\right| =$$
$$\left|Gal \backslash\backslash \left((\mathrm{PGL}_k(q) \times S_n) \backslash\backslash \mathrm{PG}_{k-1}(q)^n\right)\right|$$

The set of orbits $\mathbb{F}_q^*\backslash\backslash\mathbb{F}_q^k\setminus\{0\}$ is the $(k-1)$-dimensional projective space $\mathrm{PG}_{k-1}(q)$.

The action of $\mathrm{GL}_k(q)$ on $\mathrm{PG}_{k-1}(q)$ corresponds to the natural action of the projective group $\mathrm{PGL}_k(q)$ on $\mathrm{PG}_{k-1}(q)$. Thus

$$\begin{aligned}
\left|\left(\mathbb{F}_q^*\wr_n(Gal\times S_n)\right)\backslash\backslash\,\mathrm{GL}_k(q)\backslash\backslash(\mathbb{F}_q^k\setminus\{0\})^n\right| &=\\
\left|(Gal\times S_n)\backslash\backslash\left(\mathrm{PGL}_k(q)\backslash\backslash\,\mathrm{PG}_{k-1}(q)^n\right)\right| &=\\
\left|Gal\backslash\backslash\left((\mathrm{PGL}_k(q)\times S_n)\backslash\backslash\,\mathrm{PG}_{k-1}(q)^n\right)\right| &=\\
\left|(\mathrm{P\Gamma L}_k(q)\times S_n)\backslash\backslash\,\mathrm{PG}_{k-1}(q)^n\right|&,
\end{aligned}$$

since

$$\alpha(\mathbb{F}_q^*(w))=\mathbb{F}_q^*(\alpha(w)),\qquad w\in\mathbb{F}_q^k,$$

and

$$\mathrm{P\Gamma L}_k(q)(y)=\bigcup_{\alpha\in Gal}\mathrm{PGL}_k(q)(\alpha(y)),\qquad y\in\mathrm{PG}_{k-1}(q).$$

Linear isometry classes — semilinear isometry classes

Linear isometry classes

$$(\mathrm{PGL}_k(q) \times S_n) \backslash\backslash \mathrm{PG}_{k-1}(q)^n$$

Linear isometry classes — semilinear isometry classes

Linear isometry classes

$$(\mathrm{PGL}_k(q) \times S_n) \backslash\backslash \, \mathrm{PG}_{k-1}(q)^n$$

Semilinear isometry classes

$$(\mathrm{P\Gamma L}_k(q) \times S_n) \backslash\backslash \, \mathrm{PG}_{k-1}(q)^n$$

Home Page

Title Page

Contents

Go Back

Full Screen

Close

Quit

Cycle index polynomials – generating functions

Let ${}_HY$ be a finite group action. Then the generating function for the number of $(H \times S_n)$-orbits on Y^n, respectively Y^n_{inj}, is equal to

$$\sum_{n\geq 0} |(H \times S_n)\backslash\backslash Y^n| \cdot x^n = C(H,Y)\Big|_{z_i := \sum_{j=0}^{\infty} x^{i\cdot j}}$$

Cycle index polynomials – generating functions

Let ${}_HY$ be a finite group action. Then the generating function for the number of $(H \times S_n)$-orbits on Y^n, respectively Y^n_{inj}, is equal to

$$\sum_{n\geq 0} |(H\times S_n)\backslash\backslash Y^n| \cdot x^n = C(H,Y)\big|_{z_i:=\sum_{j=0}^{\infty} x^{i\cdot j}}$$

$$\sum_{n\geq 0} |(H\times S_n)\backslash\backslash Y^n_{\mathrm{inj}}| \cdot x^n = C(H,Y)\big|_{z_i:=1+x^i}.$$

Cycle index polynomials – generating functions

Let ${}_HY$ be a finite group action. Then the generating function for the number of $(H \times S_n)$-orbits on Y^n, respectively Y^n_{inj}, is equal to

$$\sum_{n\geq 0} |(H\times S_n)\backslash\backslash Y^n| \cdot x^n = C(H,Y)\Big|_{z_i:=\sum_{j=0}^{\infty} x^{i\cdot j}}$$

$$\sum_{n\geq 0} |(H\times S_n)\backslash\backslash Y^n_{\mathrm{inj}}| \cdot x^n = C(H,Y)\Big|_{z_i:=1+x^i}.$$

The cycle index for the action of H on Y is the polynomial

$$C(H,Y) := \frac{1}{|H|}\sum_{g\in H}\prod_{i=1}^{|Y|} z_i^{a_i(\bar{g})} \in \mathbb{Q}[z_1,z_2,\ldots,z_{|Y|}],$$

where $(a_1(\bar{g}),\ldots,a_{|Y|}(\bar{g}))$ is the cycle type of the permutation $\bar{g}$ of Y induced by g.

Let

$$T_{nkq} := \left|(\mathrm{PGL}_k(q) \times S_n) \backslash\backslash \, \mathrm{PG}_{k-1}(q)^n\right|,$$

then $V_{nkq} := T_{nkq} - T_{n,k-1,q}$ is the number of linear isometry classes of nonredundant linear (n,k)-codes over $\mathbb{F}_q$. The generating function for T_{nkq} is obtained by substitution into the cycle index

$$C(\mathrm{PGL}_k(q), \mathrm{PG}_{k-1}(q)).$$

Let

$$T_{nkq} := \left|(\mathrm{PGL}_k(q) \times S_n) \backslash\backslash \mathrm{PG}_{k-1}(q)^n\right|,$$

then $V_{nkq} := T_{nkq} - T_{n,k-1,q}$ is the number of linear isometry classes of nonredundant linear (n,k)-codes over $\mathbb{F}_q$. The generating function for T_{nkq} is obtained by substitution into the cycle index

$$C(\mathrm{PGL}_k(q), \mathrm{PG}_{k-1}(q)).$$

Let

$$t_{nkq} := \left|(\mathrm{P\Gamma L}_k(q) \times S_n) \backslash\backslash \mathrm{PG}_{k-1}(q)^n\right|,$$

then $v_{nkq} := t_{nkq} - t_{n,k-1,q}$ is the number of semilinear isometry classes of nonredundant linear (n,k)-codes over $\mathbb{F}_q$. The generating function for t_{nkq} is obtained by substitution into the cycle index

$$C(\mathrm{P\Gamma L}_k(q), \mathrm{PG}_{k-1}(q)).$$

Numerical results

We have described how to compute the cycle index of the projective linear group. So far only for $q = 4, 8$ and small values of k the cycle index polynomials of the projective semilinear groups are determined.

Numerical results

We have described how to compute the cycle index of the projective linear group. So far only for $q = 4, 8$ and small values of k the cycle index polynomials of the projective semilinear groups are determined.

For $q = 4$ the first differences between the linear and semilinear isometry classes occur for $n = 8$ and $k = 3$.

Table of V_{nk4} and v_{nk4}

$n \backslash k$	1	2	3	4	5	6
1	1	0	0	0	0	0
2	1	1	0	0	0	0
3	1	2	1	0	0	0
4	1	4	3	1	0	0
5	1	6	9	4	1	0
6	1	9	24	17	5	1
7	1	12	55	70	28	6

Home Page

Title Page

Contents

Page 18 of 21

Go Back

Full Screen

Close

Quit

Comparison of V_{nk4} and v_{nk4}

$n \backslash k$	1	2	3	4	5	6
8	1	17	131	323	189	44
8	1	17	**126**	**301**	**184**	44
9	1	22	318	1 784	1 976	490
9	1	22	**286**	**1 419**	**1 594**	**453**
10	1	30	772	12 094	36 477	13 752
10	1	**29**	**640**	**7 970**	**22 405**	**9 278**
11	1	37	1 881	89 437	923 978	948 361
11	1	**36**	**1 431**	**51 456**	**490 138**	**504 573**
12	1	48	4 568	668 922	25 124 571	91 149 571
12	1	**46**	**3 204**	**357 222**	**12 746 664**	**45 963 661**
13	1	59	10 857	4 843 901	665 246 650	9 163 203 790
13	1	**56**	**7 099**	**2 496 031**	**333 787 936**	**4 586 461 981**
14	1	74	25 276	33 456 545	16 677 221 922	887 802 519 854
14	1	**69**	**15 595**	**16 961 133**	**8 345 700 799**	**443 959 979 727**

Comparison of V_{nk8} and v_{nk8}

$n \backslash k$	1	2	3	4
1	1	1	1	1
2	1	2	2	2
3	1	3	4	4
4	1	5	8	9
5	1	7	16	20
6	1	14	57	78
6	1	**12**	**43**	**62**
7	1	21	273	555
7	1	**17**	**143**	**289**
8	1	39	2 034	13 931
8	1	**27**	**792**	**4 979**
9	1	64	16 668	714 573
9	1	**40**	**5 806**	**239 355**
10	1	109	132 237	40 746 243
10	1	**61**	**44 619**	**13 586 393**

Home Page
Title Page
Contents
Page 20 of 21
Go Back
Full Screen
Close
Quit

$n\backslash k$	1	2	3	4
11	1	173	986 453	2 188 928 772
11	1	**89**	**329 959**	**729 659 322**
12	1	286	6 876 180	108 587 171 103
12	1	**136**	**2 294 446**	**36 195 786 755**
13	1	439	44 880 936	4 985 542 976 595
13	1	**197**	**14 965 218**	**1 661 847 901 869**
14	1	686	275 497 786	212 944 610 369 565
14	1	**292**	**91 842 474**	**70 981 537 714 473**
15	1	1 028	1 597 385 468	8 503 511 406 384 359
15	1	**420**	**532 481 348**	**2 834 503 805 580 423**
16	1	1 534	8 784 375 366	318 881 061 522 362 625
16	1	**606**	**2 928 163 108**	**106 293 687 186 817 717**
17	1	2 222	45 985 791 002	11 273 378 553 997 847 510
17	1	**854**	**15 328 669 468**	**3 757 792 851 378 389 530**
18	1	3 208	229 921 910 074	377 031 845 513 665 669 846
18	1	**1 206**	**76 640 772 664**	**125 677 281 838 050 117 086**

Contents