Cycle indices of linear, affine and projective groups

Harald Fripertinger [1]

Institut für Mathematik, Karl-Franzens-Universität Graz, Heinrichstr. 36/4, A–8010 Graz. e-mail: `harald.fripertinger@kfunigraz.ac.at`

Abstract

The Pólya cycle indices for the natural actions of the general linear groups and affine groups (on a vector space) and for the projective linear groups (on a projective space) over a finite field are computed. Finally it is demonstrated, how to enumerate isometry classes of linear codes by using these cycle indices.

1 Preliminaries

This section contains all the basic notions and facts about finite group actions necessary for the following. For more details the reader is referred to the book [11], from which we take the notation.

Let G be a multiplicative group and X a nonempty set. An *action* of G on X from the left is denoted by ${}_GX$, and X is called a G-set. If both the group G and the set X are finite, then ${}_GX$ is called a *finite group action*. It induces a group homomorphism ϕ from G into the *symmetric group* S_X on X:

$$\phi\colon G \to S_X, \qquad g \mapsto \phi(g),$$

where $\phi(g)x = gx$ for all $x \in X$. The *orbit* of x will be indicated as $G(x)$, the *stabilizer* of x by G_x. The set of all G-orbits will be denoted by

$$G\backslash\backslash X := \{G(x) \mid x \in X\}.$$

Let G be a permutation group of X (if necessary take the homomorphic image

[1] Supported by a Forschungsstipendium of the University of Graz and by the Fond zur Förderung der wissenschaftlichen Forschung P10189 - PHY.

of G under $\phi: G \to S_X$). The *cycle index* of G acting on X is the following polynomial $Z(G,X)$ in the indeterminates $x_1, x_2, \ldots, x_{|X|}$ over $\mathbb{Q}$, defined by

$$Z(G,X) := \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} x_i^{a_i(g)},$$

where $(a_1(g), \ldots, a_{|X|}(g))$ is the cycle type of the permutation $g \in G$. This means, g decomposes into $a_i(g)$ disjoint cycles of length i for $i = 1, \ldots, |X|$. All elements of a conjugacy class have the same cycle type, so the cycle index can be rephrased in the following way:

$$Z(G,X) = \frac{1}{|G|} \sum_{C \in \mathcal{C}} |C| \prod_{i=1}^{|X|} x_i^{a_i(g_C)}, \tag{1}$$

where $\mathcal{C}$ is the set of all conjugacy classes C of G with representatives $g_C \in C$.

The finite field of q elements will be denoted by F_q, q is assumed to be a power of the prime p, the *characteristic* of F_q, and the multiplicative group of F_q will be indicated by F_q^*. The set of all regular $n \times n$-matrices over F_q will be denoted by $\mathrm{GL}(n, F_q)$, which is the *general linear group*. The *affine group*

$$\mathrm{Aff}(n, F_q) := \left\{ (A, b) \mid A \in \mathrm{GL}(n, F_q),\ b \in F_q^n \right\}$$

is the semidirect product of $\mathrm{GL}(n, F_q)$ and F_q^n with the following multiplication

$$(A_1, b_1)(A_2, b_2) = (A_1 A_2, b_1 + A_1 b_2).$$

The group F_q^* acts on the vector space F_q^n by scalar multiplication

$$F_q^* \times F_q^n \to F_q^n, \qquad (\alpha, v) \mapsto \alpha v.$$

The orbit $F_q^*(v)$, $v \neq 0$, is a point in the *projective space* $\mathrm{PG}(n-1, F_q) := F_q^* \backslash\backslash (F_q^n \setminus \{0\})$. Furthermore F_q^* acts on $\mathrm{GL}(n, F_q)$ by

$$F_q^* \times \mathrm{GL}(n, F_q) \to \mathrm{GL}(n, F_q), \qquad (\alpha, A) \mapsto \alpha A.$$

The set $F_q^* \backslash\backslash \mathrm{GL}(n, F_q)$ of all orbits is the *projective linear group* $\mathrm{PGL}(n, F_q)$. In the present paper we will show how to compute the cycle indices for the natural actions of the linear, affine and of the projective groups. These actions are:

$$\mathrm{GL}(n, F_q) \times F_q^n \to F_q^n, \qquad (A, v) \mapsto Av,$$

$$\mathrm{Aff}(n, F_q) \times F_q^n \to F_q^n, \qquad ((A,b),v) \mapsto Av + b$$

and

$$\mathrm{PGL}(n, F_q) \times \mathrm{PG}(n-1, F_q) \to \mathrm{PG}(n-1, F_q),$$

$$(F_q^*(A), F_q^*(v)) \mapsto F_q^*(Av).$$

The orders of these groups are

$$|\mathrm{GL}(n, F_q)| = [q]_n := (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}),$$

$$|\mathrm{Aff}(n, F_q)| = [q]_n q^n, \qquad |\mathrm{PGL}(n, F_q)| = [q]_n/(q-1).$$

The idea for computing these cycle indices according to (1) is the following: First determine the conjugacy classes in $\mathrm{GL}(n, F_q)$, which can be done by using the theory of normal forms of matrices. Then determine the number of elements in these conjugacy classes and for each class compute the cycle type of an arbitrary representative. In the case $q = 2$ Slepian [16] and Harrison [7,8] computed the cycle indices of $\mathrm{GL}(n, F_2)$ and $\mathrm{Aff}(n, F_2)$. They applied them for the enumeration of isometry classes of linear (n, k)-codes over F_2 and for the classification of switching functions. These two authors referred to Elspas [2], who determined the cycle type of $A \in \mathrm{GL}(n, F_p)$, where p is a prime.

In the next section a short introduction into the theory of normal forms of linear operators in vector spaces over arbitrary fields is given. Since this theory can be found in many textbooks of algebra, we only present some definitions and final results. In the case of finite fields the size of these conjugacy classes can be evaluated using a formula of Kung [12], which goes back to a formula of Green [6].

2 The classical normal form of a linear operator

In this section K denotes an arbitrary field, V is an n-dimensional vector space over K and A is a linear operator on V. A polynomial $\varphi(x) \in K[x]$ is called *annihilating polynomial* of $v \in V$, if and only if $\varphi(A)v = 0$. In order to understand what is meant by $\varphi(A)$, let Φ_A be the ring homomorphism $\Phi_A : K[x] \to \mathrm{End}(V)$ defined by $x \mapsto A$, and $a \mapsto a\,\mathrm{id}_V$ for all $a \in K$. Then the image of $\varphi(x) := \sum_{i=0}^{d} a_i x^i$ under Φ_A is given by

$$\varphi(A) := \Phi_A(\varphi(x)) = \sum_{i=0}^{d} a_i A^i, \text{ where } A^0 = \mathrm{id}_V\,.$$

Furthermore $K[A] := \{\varphi(A) \,|\, \varphi \in K[x]\}$ is a subring of $\mathrm{End}(V)$, and V is a $K[A]$-*module* with the following multiplication

$$K[A] \times V \to V, \qquad (\varphi(A), v) \mapsto \varphi(A)v.$$

In the same way a polynomial $\varphi(x) \in K[x]$ is called *annihilating polynomial* of V, if and only if $\varphi(x)$ is an annihilating polynomial of each $v \in V$, and such a polynomial of minimal degree, which is monic as well, is called the *minimal polynomial* of V. If the minimal polynomial $\varphi(x)$ of V can be written as

$$\varphi(x) = \prod_{i=1}^{s} \varphi_i(x)^{c_i},$$

where $\varphi_i(x)$ are pairwise distinct, monic, irreducible polynomials over K, then the *primary decomposition* of V yields a representation of V as a direct sum of invariant subspaces U_i, such that $\varphi_i(x)^{c_i}$ is the minimal polynomial of U_i. Each of these invariant subspaces U_i is a direct sum of cyclic subspaces $W_{i,j}$, such that the minimal polynomial of $W_{i,r(i)}$ is $\varphi_i(x)^{c_i}$ and the minimal polynomial of $W_{i,j}$ is a divisor of the minimal polynomial of $W_{i,j+1}$ for $j = 1, \ldots, r(i) - 1$.

$$V = \bigoplus_{i=1}^{s} U_i \qquad \text{and} \qquad U_i = \bigoplus_{j=1}^{r(i)} W_{i,j}.$$

Let U be a cyclic subspace of dimension d with basis $(v, Av, \ldots, A^{d-1}v)$ and minimal polynomial $\varphi(x) := \sum_{i=0}^{d} a_i x^i$, $a_d = 1$, then the restriction of A to U can be represented as the *companion matrix* $C(\varphi)$ of $\varphi(x)$, which is given by

$$C(\varphi) := \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -a_{d-2} \\ 0 & 0 & \ldots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

In the case that U is a cyclic subspace of V of dimension kd with minimal polynomial $\varphi(x)^k$, there is a basis of U such that the restriction of A to U can be represented as the *hypercompanion matrix* $H(\varphi^k)$ of $\varphi(x)^k$, which is given by

$$H(\varphi^k) := \left.\begin{pmatrix} C(\varphi) & 0 & 0 & \dots & 0 & 0 \\ E_{1d} & C(\varphi) & 0 & \dots & 0 & 0 \\ 0 & E_{1d} & C(\varphi) & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & C(\varphi) & 0 \\ 0 & 0 & 0 & \dots & E_{1d} & C(\varphi) \end{pmatrix}\right\} k\text{-times},$$

where

$$E_{1d} = (e_{ij})_{1 \le i,j \le d} \text{ is given by } e_{ij} = \begin{cases} 1 & \text{if } (i,j) = (1,d) \\ 0 & \text{else.} \end{cases}$$

The hypercompanion matrix $H(\varphi^k)$ is a $kd \times kd$-matrix and in the case that $k = 1$ it is the companion matrix $C(\varphi)$. If the vector space V with minimal polynomial

$$\varphi(x) = \prod_{i=1}^{s} \varphi_i(x)^{c_i}$$

decomposes into a direct sum of $\lambda_j^{(i)}$ cyclic subspaces with minimal polynomial $\varphi_i(x)^j$ (for $1 \le j \le c_i$ and for $1 \le i \le s$), then the classical normal form of A is a block diagonal matrix

$$\operatorname{diag}\left(D(\varphi_1, \lambda^{(1)}), \dots, D(\varphi_s, \lambda^{(s)})\right). \tag{2}$$

The matrices $D(\varphi, \lambda)$ are again block diagonal matrices defined by:

$$D(\varphi, \lambda) = \operatorname{diag}(\underbrace{C(\varphi), \dots, C(\varphi)}_{\lambda_1}, \underbrace{H(\varphi^2), \dots, H(\varphi^2)}_{\lambda_2}, \dots).$$

Then the characteristic polynomial of A is

$$\chi_A(x) = \prod_{i=1}^{s} \varphi_i(x)^{\gamma_i},$$

where $\gamma_i = \sum_j j\lambda_j^{(i)}$. In other words $\lambda^{(i)}$ is a cycle type of γ_i, which will be indicated as $\lambda^{(i)} \vdash\!\dashv \gamma_i$. In the special case that K is a finite field F_q KUNG [12] determined the size of a conjugacy class in $\mathrm{GL}(n, F_q)$ by the following formula: Let $\varphi(x) \in F_q[x]$ be a monic, irreducible polynomial of degree d and let $\lambda = (\lambda_1, \lambda_2, \ldots)$ be a cycle type of γ. The size of the centralizer of $D(\varphi, \lambda)$ in $\mathrm{GL}(\gamma d, F_q)$ is

$$b(d, \lambda) := \prod_{i=1}^{\gamma} \prod_{j=1}^{\lambda_i} (q^{d\mu_i} - q^{d(\mu_i - j)}), \tag{3}$$

where

$$\mu_i := \sum_{k=1}^{i} k\lambda_k + \sum_{k=i+1}^{\gamma} i\lambda_k.$$

Especially this number only depends on the degree of the polynomial. The size of the conjugacy class of a matrix given by (2), where the $\varphi_i(x)$ are polynomials of degree d_i, is given by

$$\frac{[q]_n}{\prod_{i=1}^{s} b(d_i, \lambda^{(i)})}.$$

3 The cycle index of $\mathrm{GL}(n, F_q)$

In [9] the following definition of a product operator for two polynomials A and B in indeterminates $x_1, x_2, \ldots$ over $\mathbb{Q}$ is given. Let

$$A(x_1, x_2, \ldots, x_n) = \sum_{(j)} a_{(j)} \prod_{i=1}^{n} x_i^{j_i},$$

$$B(x_1, x_2, \ldots, x_m) = \sum_{(k)} b_{(k)} \prod_{i=1}^{m} x_i^{k_i},$$

then

$$A(x_1, \ldots, x_n) \times B(x_1, \ldots, x_m) := \sum_{(j)} \sum_{(k)} a_{(j)} b_{(k)} \left(\prod_{i=1}^{n} x_i^{j_i} \right) \times \left(\prod_{i=1}^{m} x_i^{k_i} \right),$$

where

$$\left(\prod_{i=1}^{n} x_i^{j_i} \right) \times \left(\prod_{i=1}^{m} x_i^{k_i} \right) := \prod_{i=1}^{n} \prod_{l=1}^{m} (x_i^{j_i} \times x_l^{k_l})$$

and

$$x_i^{j_i} \times x_l^{k_l} := x_{\mathrm{lcm}(i,l)}^{j_i k_l \gcd(i,l)}. \tag{4}$$

The k-th power of A according to this product will be indicated as

$$A(x_1, \ldots, x_n)^{\times k}.$$

It was already PÓLYA [15], who realized that the cycle index of the induced action

$$(G \times H) \times (X \times Y) \to X \times Y, \qquad ((g,h),(x,y)) \mapsto (gx, hy)$$

of the direct product of two group actions ${}_GX$ and ${}_HY$ can be expressed as

$$Z(G \times H, X \times Y) = Z(G, X) \times Z(H, Y).$$

A matrix $A \in \mathrm{GL}(n, F_q)$ given in normal form is a block diagonal matrix of companion and hypercompanion matrices of monic, irreducible polynomials over F_q. The natural action of A given by (2), where $\lambda^{(i)}$ is a cycle type of γ_i and $\sum_{i=1}^{s} \gamma_i = n$, can be expressed as the direct product $\times_{i=1}^{s} \times_{j=1}^{\gamma_i} \times_{k=1}^{\lambda_j^{(i)}} H(\varphi_i^j)$ acting on $\times_{i=1}^{s} \times_{j=1}^{\gamma_i} \times_{k=1}^{\lambda_j^{(i)}} F_q^{j d_i}$. For that reason we only have to know the cycle types of companion and hypercompanion matrices of monic, irreducible polynomials over F_q. (Applying the product operator of (4) yields the cycle type of the matrix A.) It is important to realize that the cycle type of a hypercompanion matrix of a monic, irreducible polynomial $\varphi(x) \in F_q[x]$ can be computed from its exponent $\exp(\varphi)$.

In [14] the *period*, the *order* or the *exponent* of a polynomial $\varphi(x) \in F_q[x]$, $\varphi(0) \neq 0$, is defined to be the least positive integer e such that $\varphi(x)$ is a divisor of $x^e - 1$. We will need the following facts about the exponent: Let $\varphi(x) \in F_q[x]$ be a monic, irreducible polynomial of degree d over F_q. If $\varphi(x)$ can be expressed as $\varphi(x) = \prod_{i=1}^{d}(x - \alpha_i)$, where the α_i are distinct elements in F_{q^d}, then

$$\exp(\varphi) = \min\left\{t \in \mathbb{N} \,\middle|\, \alpha_i^t = 1\right\}.$$

The exponent of $\varphi(x)$ is a divisor of $q^d - 1$ but it is not a divisor of $q^r - 1$ for all $1 \leq r < d$. So the set $E(d,q)$ of all possible exponents of monic, irreducible polynomials of degree d over F_q can be computed as

$$E(d,q) = \left\{e \,\middle|\, e \mid q^d - 1 \text{ and } e \nmid q^r - 1 \text{ for } 1 \leq r < d\right\}.$$

In the case $d = e = 1$ there is exactly one monic, irreducible polynomial of degree d and of exponent e such that $\varphi(0) \neq 0$, namely $\varphi(x) = x - 1$. (Actually, when extending the definition of exponents of polynomials for polynomials with $\varphi(0) = 0$, there is another polynomial $\varphi(x) = x$ of degree 1 and of exponent 1.) Otherwise, if e is a divisor of $q^d - 1$ and e does not divide $q^r - 1$ for $1 \leq r < d$, then there are $\phi(e)/d$ monic, irreducible polynomials of degree d and of exponent e in $F_q[x]$, where ϕ is the EULER-ϕ-function. For $e \in E(d,q)$ we define

$$\nu(d,e) := \begin{cases} 1 & \text{if } e = d = 1 \\ \phi(e)/d & \text{else.} \end{cases}$$

The exponent of the power $\varphi(x)^k$ for an integer $k \geq 1$ is given by $\exp(\varphi)p^t$, where p is the characteristic of F_q and $t := \min\{r \in \mathbb{N}_0 \mid p^r \geq k\}$.

Let A be the hypercompanion matrix $H(\varphi^k)$ of a monic, irreducible polynomial $\varphi(x) \neq x$ of degree d and of exponent e. Then the cycle inventory of A acting on F_q^{kd} is

$$x_1 \prod_{i=1}^{k} x_{e_i}^{(q^{id} - q^{(i-1)d})/e_i},$$

where $e_i = \exp(\varphi^i)$ for $1 \leq i \leq k$.

For computing the cycle index of $\mathrm{GL}(n, F_q)$ we have to determine all normal forms (2) in $\mathrm{GL}(n, F_q)$ which can be done in the following way: It is well known [14] that there are

$$N_q(d) = \frac{1}{d} \sum_{t \mid d} \mu(t) q^{\frac{d}{t}}$$

monic, irreducible polynomials of degree d over F_q, where μ is the classical Möbius function. Each monic, irreducible polynomial of degree $\leq n$, except the polynomial $\varphi(x) = x$, can occur as a divisor of the characteristic polynomial of some regular matrix $A \in \mathrm{GL}(n, F_q)$. These $t_n := \sum_{i=1}^{n} N_q(i) - 1$ polynomials will be labelled as $\varphi_1(x), \varphi_2(x), \ldots, \varphi_{t_n}(x)$. Furthermore let d_i be the degree of $\varphi_i(x)$. At first we have to find all solutions $(\gamma_1, \ldots, \gamma_{t_n}) \in \mathbb{N}_0^{t_n}$ of

$$\sum_{i=1}^{t_n} \gamma_i \cdot d_i = n. \tag{5}$$

Then for each solution $(\gamma_1, \ldots, \gamma_{t_n})$ the set of all cycle types of γ_i

$$CT(\gamma_i) := \{\lambda \mid \lambda \vdash \gamma_i\}$$

must be computed. Finally the representatives of the conjugacy classes of matrices A with characteristic polynomial

$$\chi_A(x) = \prod_{i=1}^{t_n} \varphi_i(x)^{\gamma_i}$$

are given as diagonal matrices

$$\operatorname{diag}\left(D(\varphi_1, \lambda^{(1)}), \ldots, D(\varphi_{t_n}, \lambda^{(tn)})\right),$$

where

$$(\lambda^{(1)}, \ldots, \lambda^{(t_n)}) \in \mathop{\times}_{i=1}^{t_n} CT(\gamma_i).$$

All these results can be collected in the following

Theorem 1 *The cycle index $Z(\mathrm{GL}(n, F_q), F_q^n)$ can be computed as*

$$\frac{1}{[q]_n} \sum_\gamma \sum_\lambda \frac{[q]_n}{\prod_{i=1}^{t_n} b(d_i, \lambda^{(i)})} \mathop{\times}_{i=1}^{t_n} \mathop{\times}_{j=1}^{\gamma_i} \left(x_1 \prod_{k=1}^{j} x_{e_{ik}}^{a_{ik}} \right)^{\times \lambda_j^{(i)}},$$

where e_{ik} is the exponent of $\varphi_i(x)^k$. Furthermore a_{ik} is given as

$$a_{ik} = \frac{q^{kd_i} - q^{(k-1)d_i}}{e_{ik}}.$$

$[q]_n$ is the order of $\mathrm{GL}(n, F_q)$ and $b(d_i, \lambda^{(i)})$ is the size of the centralizer of $D(\varphi_i, \lambda^{(i)})$ computed by (3). The first sum is running over all $\gamma = (\gamma_1, \ldots, \gamma_{t_n})$ which are solutions of (5). The second sum is running over all t_n-tuples $\lambda = (\lambda^{(1)}, \ldots, \lambda^{(t_n)}) \in \times_{i=1}^{t_n} CT(\gamma_i)$.

Something should be said about possibilities to compute this cycle index without knowing the monic, irreducible polynomials of degree $\leq n$ over F_q. As was pointed out above, the set $E(d, q)$ of all exponents of monic, irreducible polynomials of degree d over F_q and for each $e \in E(d, q)$ the number $\nu(d, e)$ of these polynomials of exponent e can easily be computed. Careful scrutiny of the formula above leads to:

$$Z(\mathrm{GL}(n, F_q), F_q^n) =$$

$$\sum_{c \vdash n} \mathop{\times}_{d=1}^{n} \left(\sum_r \mathop{\times}_{e \in E(d,q)} \left(\sum_s \xi(\nu(d, e), s) \mathop{\times}_{j=1}^{\nu(d,e)} \left(\sum_{\lambda \vdash s_j} \frac{1}{b(d, \lambda)} z(d, e, \lambda) \right) \right) \right),$$

where $z(d, e, \lambda)$ is the cycle inventory of a matrix $D(\varphi, \lambda)$, with $\varphi(x)$ a polynomial of degree d and exponent e. It can be computed as

$$\sum_{\ell=1}^{s_j} \left(x_1 \prod_{k=1}^{\ell} x_{e_k}^{a_k} \right)^{\sum \lambda_\ell}$$

where $e_k = ep^t$, p is the characteristic of F_q, t is the least non negative integer such that $p^t \geq k$ and a_k is given by

$$a_k = \frac{q^{kd} - q^{(k-1)d}}{e_k}.$$

The numbers c_d of $c = (c_1, \ldots, c_n) \vDash n$ can be interpreted as the sum of the multiplicities of all irreducible factors of degree d of the characteristic polynomial of a linear mapping. The second sum is running over all functions r from $E(d, q)$ to $\mathbb{N}_0$, which satisfy $\sum_{e \in E(d,q)} r(e) = c_d$. Then the sum of the multiplicities of all irreducible factors of degree d and exponent e is given by $r(e)$. The third sum must be taken over all cycle types $s \vDash r(e)$, which satisfy $\sum_j s_j \leq \nu(d, e)$. Such a cycle type s defines types of partitions of the set $\{1, \ldots, r(e)\}$ into at most $\nu(d, e)$ parts. The number of all combinations of $\nu(d, e)$ different polynomials (of exponent e and of degree d) forming a product of degree $r(e)d$, where exactly s_i polynomials occur with multiplicity i, can be computed as the multinomial coefficient

$$\xi(\nu(d, e), s) := \binom{\nu(d, e)}{s_1, s_2 \ldots, \nu(d, e) - \sum_j s_j}.$$

4 The cycle index of the affine group

The following Lemma holds in a more general concept for affine mappings over an R-module.

Lemma 2 *Let R be a commutative ring with 1, then R^n is an R-module. Furthermore let $A: R^n \to R^n$ be a regular linear mapping, and $b \in R^n$. If the mapping $v \mapsto Av - v$ is bijective, then the mapping $v \mapsto B(v) := Av + b$ has the same cycle type as $v \mapsto Av$.*

Proof. Since $A - \mathrm{id}$ is bijective, $c := (A - \mathrm{id})^{-1}(b)$ is well defined. The mapping $T: R^n \to R^n, v \mapsto v - c$ is a permutation of R^n and $(T^{-1} \circ B \circ T)(v) = A(v - c) + b + c = Av$, so the two mappings $v \mapsto B(v)$ and $v \mapsto Av$ are conjugated in the symmetric group of R^n, which means that they have the same cycle type. $\square$

Theorem 3 *Using the same notation as in the previous section the cycle index of* $\mathrm{Aff}(n, F_q)$ *is given by*

$$\frac{1}{[q]_n q^n} \sum_{\gamma} \sum_{\lambda} \frac{[q]_n}{\prod_{i=1}^{t_n} b(d_i, \lambda^{(i)})} \bigtimes_{i=1}^{t_n} \bigtimes_{j=1}^{\gamma_i} u_{ij}^{\times \lambda_j^{(i)}},$$

where

$$u_{ij} = \begin{cases} q^{jd_i} x_1 \prod_{k=1}^{j} x_{e_{ik}}^{a_{ik}} & \text{if } \varphi_i(x) \neq x - 1 \\ q^{j-1} x_1 \prod_{k=1}^{j} x_{e_{ik}}^{a_{ik}} + q^{j-1}(q-1) x_{e_{i,j+1}}^{q^j/e_{i,j+1}} & \text{if } \varphi_i(x) = x - 1. \end{cases}$$

Proof. The action of $(A, b) \in \mathrm{Aff}(n, F_q)$ on F_q^n can be considered as the direct product of actions (A', b') on subspaces of F_q^n, where A' is a hypercompanion matrix of a monic, irreducible polynomial $\varphi_i(x) \in F_q[x]$. If $\varphi_i(x) \neq x - 1$, then the mapping $v \mapsto H(\varphi_i^j)v - v$ is a regular linear mapping. According to 2 Lemma the cycle type of $(H(\varphi_i^j), b)$ does not depend on b, and it is equal to the cycle type of $(H(\varphi_i^j), 0)$.

Now let $\varphi_i(x)$ be the polynomial $x - 1$, then

$$A := H(\varphi_i^j) = \begin{pmatrix} 1 & 0 & & 0 & 0 \\ 1 & 1 & \ddots & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & & 1 & 1 \end{pmatrix}.$$

Let $b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_j \end{pmatrix} \in F_q^j$, $b' = \begin{pmatrix} b_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in F_q^j$ and $T(v) := v + \begin{pmatrix} -b_2 \\ -b_3 \\ \vdots \\ -b_j \\ 0 \end{pmatrix}$. Then T is a permutation of F_q^j and the two mappings $v \mapsto Av + b$ and $v \mapsto Av + b'$ are conjugated via T in $S_{F_q^j}$, (i.e. $T^{-1}(AT(v) + b) = Av + b'$). For all $b \in F_q^j$ with $b_1 = 0$ — these are q^{j-1} vectors — the affine mappings (A, b) and $(A, 0)$ are of the same cycle type. Finally, when $b_1 \neq 0$, we have to compute the cycle type of $v \mapsto B(v) := Av + b'$. For doing this, let $A' := H(\varphi_i^{j+1}) \in \mathrm{GL}(j+1, F_q)$, then

$$A' \begin{pmatrix} b_1 \\ v \end{pmatrix} = \begin{pmatrix} b_1 \\ B(v) \end{pmatrix}.$$

Since $b_1 \neq 0$, all elements $\begin{pmatrix} b_1 \\ v \end{pmatrix} \in F_q^{j+1}$ have the same minimal polynomial $\varphi_i^{j+1}(x)$ (with respect to A'), so they all lie in $q^j/e_{i,j+1}$ cycles of A' of length $e_{i,j+1}$, and the proof is completed. $\square$

5 The cycle index of the projective group

Before computing the cycle index of $\mathrm{PGL}(n, F_q)$ acting on $\mathrm{PG}(n-1, F_q)$ we want to determine the so called *subcycle index* of $\mathrm{GL}(n, F_q)$ acting on $F_q^n \setminus \{0\}$. We start by defining the *subcycle type* of $A \in \mathrm{GL}(n, F_q)$. The vector $v \in F_q^n \setminus \{0\}$ lies in a *subcycle* of A of length s, if and only if

$$s = \min \left\{ t \in \mathbb{N} \mid \exists \alpha \in F_q^* \text{ such that } A^t v = \alpha v \right\}.$$

Let v be in a subcycle of A of length s, and $A^s v = \alpha_0 v$ then α_0 is called the *integral element* of v. The set

$$\langle A \rangle (F_q^*(v)) = \left\{ A^i \alpha v \mid i \in \mathbb{N}, \alpha \in F_q^* \right\}$$

can be written as a disjoint union of sets consisting of $q-1$ elements each,

$$\langle A \rangle (F_q^*(v)) = \dot{\bigcup_{i=0}^{s-1}} A^i F_q^*(v) = \dot{\bigcup_{i=0}^{s-1}} \left\{ A^i \alpha v \mid \alpha \in F_q^* \right\} =$$

$$\dot{\bigcup_{i=0}^{s-1}} \left\{ \alpha A^i v \mid \alpha \in F_q^* \right\} = \dot{\bigcup_{i=0}^{s-1}} F_q^*(A^i v),$$

so $\left| \langle A \rangle (F_q^*(v)) \right| = s(q-1)$. All these $s(q-1)$ elements can be identified with s elements in $\mathrm{PG}(n-1, F_q)$, which form the cycle $(F_q^*(v), \ldots, F_q^*(A^{s-1}v))$ of length s of the projectivity $F_q^*(A)$. Furthermore each $v' \in \langle A \rangle (F_q^*(v))$ lies in a subcycle of A of length s with integral element α_0. Using indeterminates with two indices — the first is the length of the subcycle, the second is the integral element — we identify the action of A on $\langle A \rangle (F_q^*(v))$ with the subcycle expression x_{s,α_0}^{q-1} of $\langle A \rangle (F_q^*(v))$. Since $F_q^n \setminus \{0\}$ is a disjoint union of $\langle A \rangle (F_q^*(v))$ the subcycle type of A is defined to be the product of the subcycle expressions of all $\langle A \rangle (F_q^*(v))$. A term of the form x_{s,α_0}^i in the subcycle type of A means that the cardinality of the set

$$\left\{ v \in F_q^n \setminus \{0\} \mid s = \min \left\{ t \in \mathbb{N} \mid \exists \alpha \in F_q^*, \ A^t v = \alpha v \right\} \text{ and } A^s v = \alpha_0 v \right\}$$

equals is. Especially the exponent i is a multiple of $q-1$. The subcycle index of $\mathrm{GL}(n, F_q)$ on $F_q^n \setminus \{0\}$ is the sum of the subcycle types of all $A \in \mathrm{GL}(n, F_q)$

divided by the order of $\mathrm{GL}(n, F_q)$. Then the cycle index of the projective group can be computed from the subcycle index by omitting the second index of all indeterminates and by dividing the exponents by $q-1$. So the main task is the computation of the subcycle index of $\mathrm{GL}(n, F_q)$. Since all elements in a conjugacy class of $\mathrm{GL}(n, F_q)$ have the same subcycle type it is enough to determine the subcycle type for matrices of the form (2), with monic, irreducible polynomials $\varphi_i(x) \in F_q[x]$. As in the case of the computation of the cycle index of $\mathrm{GL}(n, F_q)$ we first want to determine the subcycle type of a hypercompanion matrix $H(\varphi^j)$ and then we have to define a product, with which the subcycle type of the direct product action of two hypercompanion matrices can be computed. In [10] HIRSCHFELD gave the following definition for the *subexponent* of a polynomial $\varphi(x) \in F_q[x]$, $\varphi(0) \neq 0$,

$$\mathrm{subexp}(\varphi) := \min\left\{t \in \mathbb{N} \,\middle|\, \exists \alpha_0 \in F_q^* \text{ such that } \varphi(x) \mid x^t - \alpha_0\right\}.$$

The element $\alpha_0 \in F_q^*$ is called the *integral element* of φ. Let $\varphi(x) \in F_q[x] \setminus \{x\}$ be a monic, irreducible polynomial of degree d. If $\varphi(x)$ can be expressed as $\varphi(x) = \prod_{i=1}^{d}(x - \alpha_i)$, where the α_i are distinct elements in F_{q^d}, then

$$\mathrm{subexp}(\varphi) = \min\left\{t \in \mathbb{N} \,\middle|\, \alpha_i^t \in F_q^*\right\}.$$

The subexponent of $\varphi(x)$ is a divisor of $q^d - 1/(q-1)$. The subexponent of the power $\varphi(x)^k$ for an integer $k \geq 1$ is given by $\mathrm{subexp}(\varphi)p^t$, where p is the characteristic of F_q and $t := \min\{r \in \mathbb{N}_0 \mid p^r \geq k\}$. The subexponent of $\varphi(x)$ is a divisor of the exponent of $\varphi(x)$, especially

$$h := \frac{\exp(\varphi)}{\mathrm{subexp}(\varphi)}$$

is a divisor of $q-1$. Furthermore h is the multiplicative order of the integral element of $\varphi(x)$ in F_q^*, and $h = \gcd(q-1, \exp(\varphi))$. So the subexponent can be derived from the exponent by

$$\mathrm{subexp}(\varphi) = \frac{\exp(\varphi)}{\gcd(q-1, \exp(\varphi))}.$$

For $e \in E(d,q)$ let $h := \gcd(q-1, e)$, then for each $\alpha \in F_q^*$ with multiplicative order h there are $\phi(e)/(d\phi(h))$ monic irreducible polynomials $\varphi(x) \in F_q[x]$ of degree d with exponent e subexponent e/h and integral element α. The number of monic, irreducible polynomials of degree d and subexponent f in $F_q[x]$ is given by

$$\sum_{e} \frac{\phi(e)}{d},$$

where we have to sum over all $e \in E(d,q)$ which fulfil $e/\gcd(e,q-1) = f$. In the case $q = 2$ the subexponent and the exponent of a monic, irreducible polynomial are the same. Let A be the hypercompanion matrix $H(\varphi^k)$ of a monic, irreducible polynomial $\varphi(x) \neq x$ of degree d of subexponent f with integral element α. Then the subcycle type of A acting on $F_q^{kd} \setminus \{0\}$ is

$$\prod_{i=1}^{k} x_{f_i,\alpha^{f_i/f}}^{(q^{id}-q^{(i-1)d})/f_i},$$

where $f_i = \mathrm{subexp}(\varphi^i)$ for $1 \leq i \leq k$.

Finally we have to define a product formula for the direct product of two subcycle types, which is similar to the direct product formula of (4). Let A_1 be in $\mathrm{GL}(n_1, F_q)$ and let A_2 be in $\mathrm{GL}(n_2, F_q)$, then $\mathrm{diag}(A_1, A_2)$ is in $\mathrm{GL}(n_1 + n_2, F_q)$. Furthermore $F_q^{n_1+n_2} \setminus \{0\}$ can be written as

$$F_q^{n_1+n_2} \setminus \{0\} =$$

$$F_q^{n_1} \setminus \{0\} \times \{0\}^{n_2} \,\dot\cup\, \{0\}^{n_1} \times F_q^{n_2} \setminus \{0\} \,\dot\cup\, F_q^{n_1} \setminus \{0\} \times F_q^{n_2} \setminus \{0\}\,.$$

Since F_q^* is a cyclic group, each element $\alpha \in F_q^*$ can be expressed as $\alpha = \beta^r$, where β is a generator of F_q^* and $0 \leq r < q-1$. With the multiplicative and linear extension of the following multiplication defined by

$$x_{i_1,\beta^{r_1}}^{j_1} \otimes x_{i_2,\beta^{r_2}}^{j_2} := x_{i_1,\beta^{r_1}}^{j_1} x_{i_2,\beta^{r_2}}^{j_2} x_{i_3,\beta^{r_3}}^{j_3},$$

where

$$i_3 = \mathrm{lcm}(i_1,i_2) \frac{q-1}{\gcd\left(q-1, \mathrm{lcm}(i_1,i_2)r_1/i_1 - \mathrm{lcm}(i_1,i_2)r_2/i_2\right)},$$

$$r_3 \equiv \frac{r_1 i_3}{i_1} \equiv \frac{r_2 i_3}{i_2} \bmod q-1,$$

and

$$j_3 = \frac{i_1 j_1 i_2 j_2}{i_3},$$

the subcycle type of $\mathrm{diag}(A_1, A_2)$ can be computed as the $\otimes$-product of the subcycle types of A_1 and A_2.

Proof. Consider $v \in F_q^{n_1} \setminus \{0\}$ lies in a subcycle of A_1 of length i_1 with integral element β^{r_1} then $(v, 0)$ lies in a subcycle of $\mathrm{diag}(A_1, A_2)$ of length i_1

with integral element β^{r_1} as well. In the same way the subcycles of $(0, y)$ of $\mathrm{diag}(A_1, A_2)$ for $y \in F_q^{n_2} \setminus \{0\}$ correspond with the subcycles of y of A_2. For the rest of the proof it is enough to investigate pairs (v, y) such that $v \neq 0$ and $y \neq 0$. If v lies in a subcycle of A_1 of length i_1 with integral element β^{r_1} and y in a subcycle of A_2 of length i_2 with integral element β^{r_2}, then

$$\mathrm{lcm}(i_1, i_2) = \min\left\{t \in \mathbb{N} \,\middle|\, \exists \alpha_1, \alpha_2 \in F_q^* : \mathrm{diag}(A_1^t, A_2^t)(v, y) = (\alpha_1 v, \alpha_2 y)\right\}.$$

Especially

$$\alpha_l = (\beta^{r_l})^{\mathrm{lcm}(i_1,i_2)/i_l} = \beta^{r_l \,\mathrm{lcm}(i_1,i_2)/i_l}.$$

In the next step both

$$i_3 = \min\left\{t \in \mathbb{N} \,\middle|\, \exists \alpha \in F_q^* : \ \mathrm{diag}(A_1^t, A_2^t)(v, y) = \alpha(v, y)\right\}$$

and the integral element α must be computed. So we have to find the least positive integer t such that $\alpha_1^t = \alpha_2^t$. This however is the same as the multiplicative order of $\alpha_1 \alpha_2^{-1}$ which can be computed as

$$\mathrm{ord}(\alpha_1 \alpha_2^{-1}) = \frac{\mathrm{ord}(\beta)}{\gcd(\mathrm{ord}(\beta), r_1 \,\mathrm{lcm}(i_1, i_2)/i_1 - r_2 \,\mathrm{lcm}(i_1, i_2)/i_2)}.$$

Then $i_3 = \mathrm{lcm}(i_1, i_2)\,\mathrm{ord}(\alpha_1 \alpha_2^{-1})$ and

$$\beta^{r_3} = \alpha_l^{\mathrm{ord}(\alpha_1 \alpha_2^{-1})} = \beta^{r_l \,\mathrm{lcm}(i_1,i_2)\,\mathrm{ord}(\alpha_1\alpha_2^{-1})/i_l} = \beta^{r_l i_3/i_l}.$$

Since there are $i_l j_l$ elements in subcycles of length i_l with integral element β^{r_l} for $l = 1, 2$, there are $i_1 j_1 i_2 j_2$ elements in subcycles of $\mathrm{diag}(A_1, A_2)$ of length i_3 with integral element β^{r_3}, and the exponent of $x_{i_3, \beta^{r_3}}$ is given by $i_1 j_1 i_2 j_2 / i_3$. This finishes the proof. □

Theorem 4 *The subcycle index of* $\mathrm{GL}(n, F_q)$ *acting on* $F_q^n \setminus \{0\}$ *can be computed as*

$$\frac{1}{[q]_n} \sum_{\gamma} \sum_{\lambda} \frac{[q]_n}{\prod_{i=1}^{t_n} b(d_i, \lambda^{(i)})} \bigotimes_{i=1}^{t_n} \bigotimes_{j=1}^{\gamma_i} \left(\prod_{k=1}^{j} x_{f_{ik}, \alpha_{ik}}^{a_{ik}} \right)^{\otimes \lambda_j^{(i)}}$$

where f_{ik} *is the subexponent of* $\varphi_i(x)^k$. *The integral element of* $\varphi_i(x)$ *will be denoted by* α_i, *and* α_{ik} *is the integral element of* $\varphi_i(x)^k$ *computed as*

$$\alpha_{ik} = \alpha_i^{f_{ik}/f_{i1}}.$$

Furthermore a_{ik} is given as

$$a_{ik} = \frac{q^{kd_i} - q^{(k-1)d_i}}{f_{ik}}.$$

$[q]_n$ is the order of $\mathrm{GL}(n, F_q)$ and $b(d_i, \lambda^{(i)})$ is the size of the centralizer of $D(\varphi_i, \lambda^{(i)})$ computed by (3). The first sum is running over all $\gamma = (\gamma_1, \dots, \gamma_{t_n})$ which are solutions of (5). The second sum is running over all t_n-tuples $\lambda = (\lambda^{(1)}, \dots, \lambda^{(t_n)}) \in \times_{i=1}^{t_n} CT(\gamma_i)$. Omitting the second index of all variables and dividing the exponents by $q-1$ the cycle index of $\mathrm{PGL}(n, F_q)$ acting on $\mathrm{PG}(n-1, F_q)$ can be computed.

For the actual computation of the subcycle index of $\mathrm{GL}(n, F_q)$ we want to determine all pairs (f, α) of subexponents f and integral elements α of monic, irreducible polynomials $\varphi(x) \in F_q[x]$ of degree d. The set of these pairs can be described as:

$$S(d, q) := \bigcup_{e \in E(d,q)} \left\{ (f, \alpha) \mid f = \frac{e}{\gcd(e, q-1)},\ \mathrm{ord}(\alpha) = \gcd(e, q-1) \right\}.$$

For $(f, \alpha) \in S(d, q)$ the number of monic, irreducible polynomials in $F_q[x]$ of degree d, with subexponent f and integral element α is

$$\mu(d, f, \alpha) := \frac{\nu(d, f\,\mathrm{ord}(\alpha))}{\phi(\mathrm{ord}(\alpha))}.$$

Now the following formula yields the subcycle index of $\mathrm{GL}(n, F_q)$ acting on $F_q^n \setminus \{0\}$.

$$\sum_{c \dashv n} \bigotimes_{d=1}^{n} \left(\sum_{r} \bigotimes_{(f,\alpha) \in S(d,q)} \left(\sum_{s} \xi(\mu(d, f, \alpha), s) \bigotimes_{j=1}^{\mu(d,f,\alpha)} \left(\sum_{\lambda \dashv s_j} \frac{1}{b(d, \lambda)} z(d, f, \alpha, \lambda) \right) \right) \right),$$

where $z(d, f, \alpha, \lambda)$ is the subcycle type of a matrix $D(\varphi, \lambda)$, with $\varphi(x)$ a monic, irreducible polynomial of degree d subexponent f and integral element α. It can be computed as

$$\bigotimes_{\ell=1}^{s_j} \left(\prod_{k=1}^{\ell} x_{f_k, \alpha_k}^{a_k} \right)^{\otimes \lambda_\ell}$$

where $f_k = fp^t$, p is the characteristic of F_q, t is the least non negative integer such that $p^t \geq k$, the integral element α_k is computed by $\alpha^{f_k/f}$, and a_k is given by

$$a_k = \frac{q^{kd} - q^{(k-1)d}}{f_k}.$$

The numbers c_d of $c = (c_i, \dots, c_n) \vdash n$ can be interpreted as the sum of the multiplicities of all irreducible factors of degree d of the characteristic polynomial of a linear mapping. The second sum is running over all functions r from $S(d,q)$ to $\mathbb{N}_0$, which satisfy $\sum_{(f,\alpha)\in S(d,q)} r(f,\alpha) = c_d$. Then the sum of the multiplicities of all irreducible factors of degreed d subexponent f and integral element α is given by $r(f,\alpha)$. The third sum must be taken over all cycle types $s \vdash r(f,\alpha)$, which satisfy $\sum_j s_j \leq \mu(d,f,\alpha)$. Such a cycle type s defines types of partitions of the set $\{1,\dots,r(f,\alpha)\}$ into at most $\mu(d,f,\alpha)$ parts. The number of all combinations of $\mu(d,f,\alpha)$ different polynomials (of subexponent f, integral element α and of degree d) forming a product of degree $r(f,\alpha)d$, where exactly s_i polynomials occur with multiplicity i, can be computed as the multinomial coefficient

$$\xi(\mu(d,f,\alpha),s) := \binom{\mu(d,f,\alpha)}{s_1, s_2 \dots, \mu(d,f,\alpha) - \sum_j s_j}.$$

6 Applications

When generalizing Slepians method [16] for counting isometry classes of linear (n,k)-codes over F_q from $q=2$ to arbitrary q the author [5] realized that the number of orbits under the following group action must be computed. (In this section the set $\{1,\dots,n\}$ will be abbreviated by $\underline{n}$. Using this notation the *symmetric group* of $\underline{n}$ will be indicated as $S_{\underline{n}}$. When we want to replace the indeterminate x_i in the cycle index $Z(G,X)$ by an expression $f(i)$ we will write $Z(G,X|x_i = f(i))$.)

$$\left(S_{\underline{n}} \times \mathrm{GL}(k,F_q)\right) \times \left(F_q^* \backslash\backslash (F_q^k \setminus \{0\})\right)^{\underline{n}} \to \left(F_q^* \backslash\backslash (F_q^k \setminus \{0\})\right)^{\underline{n}}$$

$$\left((\pi, A), \bar{\Gamma}\right) \mapsto A(\bar{\Gamma} \circ \pi^{-1}).$$

This is just the group action of $S_{\underline{n}} \times \mathrm{PGL}(k,F_q)$ acting on the set of all functions from $\underline{n}$ to $\mathrm{PG}(k-1,F_q)$. According to [1] a generating function for these numbers (we call them T_{nkq}) can be derived as

$$\sum_{n=0}^{\infty} T_{nkq} x^n = Z\left(\mathrm{PGL}(k,F_q), \mathrm{PG}(k-1,F_q) | x_i = \sum_{j=0}^{\infty} x^{ij}\right) =$$

$$= Z\left(\mathrm{PGL}(k, F_q), \mathrm{PG}(k-1, F_q) | x_i = \frac{1}{1-x^i}\right).$$

When enumerating linear codes over F_q for $q \neq 2$ we have to compute the cycle index for the action of a projective group. Then the number of isometry classes of linear (n, k)-codes over F_q with no columns of zeros is given by $T_{nkq} - T_{n,k-1,q}$. When counting only orbits of injective functions the number of classes of so called "injective" linear (n, k)-codes (i.e. codes without any proportional columns) with no columns of zeros can be computed.

For example tables 1 and 2, giving the numbers of classes of linear (n, k)-codes and of injective linear (n, k)-codes for $q = 5$, were computed with SYMMETRICA [17].

Table 1
Number of isometry classes of linear (n, k)-codes over F_5, where columns of zeros are not allowed.

$n\backslash k$	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	11	28	19	5	1
7	1	14	81	98	32	6
8	1	22	253	774	337	53
9	1	30	851	8595	9116	1166
10	1	43	2883	118566	493440	126831
11	1	56	9760	1.678533	32.284551	32.659425
12	1	79	32359	22.865614	2081.311042	9903.862799
13	1	100	103564	293.232423	126195.756981	2.933556.753888
14	1	134	319235	3529.984582	7.145719.133836	817.792688.298269
15	1	170	946611	39964.715420	378.561532.692888	213504.876729.763324
16	1	220	2.701708	426952.413242	18831.255937.967044	52.309680.228011.475650
17	1	273	7.435209	4.319069.402516	882825.589984.276846	12067.473900.919649.779357
18	1	348	19.769246	41.508414.582734	39.138258.211050.467183	2.630003.988084.389247.724482
19	1	424	50.885804	380.119696.621896	1645.862734.742940.014521	543.163334.129150.960709.567991

Extending these tables in n is no problem, but as it is indicated in table 3 both the computing time (and the usage of memory) are growing rapidly when k becomes larger. (In table 3 you can find the time used for computing the cycle indices of $\mathrm{GL}(k, F_q)$, $\mathrm{Aff}(k, F_q)$ and $\mathrm{PGL}(k, F_q)$ evaluated with the SYMMETRICA routine `print_time()` on a HP-UX 9.0 workstation. The corresponding SYMMETRICA routines are `zykelind_glkq`, `zykelind_affkq` and `zykelind_pglkq`.)

These cycle index methods can be applied for the computation of the numbers of classes of q-nary matroids as well. Wild [18,19] applied the Cauchy–Frobenius Lemma for enumerating classes of binary and ternary matroids.

Table 2
Number of isometry classes of injective linear (n,k)-codes over F_5, where columns of zeros are not allowed.

$n\backslash k$	1	2	3	4	5	6
1	1	0	0	0	0	0
2	0	1	0	0	0	0
3	0	1	1	0	0	0
4	0	1	2	1	0	0
5	0	1	4	3	1	0
6	0	1	11	12	4	1
7	0	0	22	58	23	5
8	0	0	42	460	255	42
9	0	0	92	5001	7659	1019
10	0	0	174	64508	428928	120463
11	0	0	296	818669	27.835871	31.538685
12	0	0	476	9.757050	1753.691821	9557.206823
13	0	0	669	107.557544	103274.780465	2.817242.794112
14	0	0	832	1096.838553	5.659059.348470	780.447912.679009
15	0	0	948	10377.098235	289.285392.795863	202321.035985.581414
16	0	0	948	91427.918120	13848.548789.245809	49.191770.712964.929451
17	0	0	832	752869.839421	623173.264672.168315	11255.693730.501677.363863
18	0	0	669	5.813629.740101	26.450117.442738.201150	2.431828.164135.538350.110169
19	0	0	476	42.224711.823579	1062.179716.246420.445710	497.627566.565645.258069.997134

For enumerating matroids the cycle index of $\mathrm{GL}(n,F_q)$ acting on $F_q^*\backslash\backslash F_q^n$ must be known, which is

$$x_1 \cdot Z(\mathrm{PGL}(n,F_q),\mathrm{PG}(n-1,F_q)).$$

The numbers of n-element matroids of rank k can be interpreted as numbers of classes of linear (n,k)-codes, where columns of zeros are allowed. The numbers of loopless matroids correspond to the numbers of classes of codes with no columns of zeros, and the simple matroids correspond to classes of injective codes. For $q=2$ tables of these numbers can be found in [16] and in [13]. For $q=2,3$ the numbers of matroids can be found in [18]. In [5] the authors give numbers of classes of indecomposable codes for $q=2,3,4,5,7$, from which the numbers of all classes of codes can be computed. Some further tables for $q=3,4$ can be found in [4]. In [3] tables for $q=8$ are given, and some details about enumeration of isometry classes of linear (n,k)-codes in SYMMETRICA using the cycle indices of projective linear groups can be found.

Table 3
Computing time for some cycle indices in seconds

q	k	$\mathrm{GL}(k, F_q)$	$\mathrm{Aff}(k, F_q)$	$\mathrm{PGL}(k, F_q)$	q	k	$\mathrm{GL}(k, F_q)$	$\mathrm{Aff}(k, F_q)$	$\mathrm{PGL}(k, F_q)$
2	9	0.75	1.34		4	5	0.56	0.63	1.73
	10	1.57	2.46			6	1.98	2.22	9.01
	11	2.78	4.43			7	10.06	11.33	65.72
	12	5.22	8.88			8	36.32	39.46	420.01
	13	11.35	18.68			9	232.76	274.63	2984.37
	14	23.37	33.87		5	2	0.04	0.05	0.05
	15	41.40	57.83			3	0.12	0.15	0.24
	16	68.32	107.18			4	0.53	0.62	1.64
	17	167.95	262.13			5	1.73	2.02	15.83
3	5	0.32	0.39	0.35		6	9.48	10.76	167.94
	6	0.72	0.98	1.08	9	2	0.08	0.09	0.19
	7	1.47	2.60	3.55		3	0.36	0.44	2.72
	8	5.77	7.27	12.73		4	3.34	3.36	96.77
	9	17.24	21.1	45.81		5	33.76	35.38	3647.17
	10	46.28	57.20	166.04		6	758.30	757.99	
	11	168.20	198.99	672.75					
	12	623.42	734.34	2971.00					

References

[1] N.G. de Bruijn. Pólya's Theory of Counting. In E.F. Beckenbach, editor, *Applied Combinatorial Mathematics*, chapter 5, pages 144 – 184. Wiley, New York, 1964.

[2] B. Elspas. The Theory of Autonomous Linear Sequential Networks. *IRE Transactions on Circuit Theory*, **CT–6** (1959) 45 – 60.

[3] H. Fripertinger. Enumeration of isometry classes of linear (n, k)-codes over $GF(q)$ in SYMMETRICA. *Bayreuther Mathematische Schriften*, **49** (1995) 215 – 223. ISSN 0172-1062.

[4] H. Fripertinger. Zyklenzeiger linearer Gruppen und Abzählung linearer Codes. *Séminaire Lotharingien de Combinatoire*, **Actes 33** (1995) 1 – 10. ISSN 0755-3390.

[5] H. Fripertinger and A. Kerber. Isometry Classes of Indecomposable Linear Codes. In G. Cohen, M. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 11th International Symposium, AAECC-11, Paris, France, July 1995*, volume 948 of *Lecture Notes in Computer Science*, pages 194–204. Springer, 1995.

[6] J.A. Green. The characters of the finite general linear groups. *Trans. Amer. Math. Soc.*, **80** (1955) 402 – 447.

[7] M.A. Harrison. On the classification of Boolean functions by the general linear and affine groups. *J. Soc. Appl. Ind. Math.*, **12** (1964) 285 – 299.

[8] M.A. Harrison. Counting Theorems and their Applications to Switching Theory. In A. Mukhopadyay, editor, *Recent Developments in Switching Functions*, chapter 4, pages 85 – 120. Academic Press, 1971.

[9] M.A. Harrison and R.G. High. On the Cycle Index of a Product of Permutation Groups. *Journal of Combinatorial Theory*, **4** (1968) 277 – 299.

[10] J.W.P. Hirschfeld. *Projective Geometries over Finite Fields.* Clarendon Press, Oxford, 1979. ISBN 0-19-853526-0.

[11] A. Kerber. *Algebraic Combinatorics via Finite Group Actions.* B.I. Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991. ISBN 3-411-14521-8.

[12] J.P.S. Kung. The Cycle Structure of a Linear Transformation over a Finite Field. *Linear Algebra and its Applications*, **36** (1981) 141 – 155.

[13] D. Lattermann. Computerunterstützte Abzählung von Codes. Master's thesis, Universität Bayreuth, 1994.

[14] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications.* Addison-Wesley Publishing Company, London, Amsterdam, Don Mills – Ontario, Sydney, Tokyo, 1983. ISBN 0-201-13519-1.

[15] G. Pólya. Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen. *Acta Mathematica*, **68** (1937) 145 – 254.

[16] D. Slepian. Some Further Theory of Group Codes. *The Bell System Technical Journal*, **39** (1960) 1219 – 1252.

[17] SYMMETRICA. A program system devoted to representation theory, invariant theory and combinatorics of finite symmetric groups and related classes of groups. Copyright by "Lehrstuhl II für Mathematik, Universität Bayreuth, 95440 Bayreuth". Distributed via anonymous ftp 132.180.16.20 in dist/SYM.tar.Z.

[18] M. Wild. Enumeration of binary and ternary matroids and other applications of the Brylawski–Lucas–Theorem. Preprint 1693, Technische Hochschule Darmstadt, November 1994.

[19] M. Wild. Consequences of the Brylawski–Lucas–Theorem for Binary Matroids. *Europ. J. Combinatorics*, **17** (1996) 309–316.