Advances in Mathematics of Communications
Volume 5, No. 2, 2011, 407–416
Web site: http://www.aimSciences.org

THE NUMBER OF INVARIANT SUBSPACES UNDER A LINEAR OPERATOR ON FINITE VECTOR SPACES

This work is dedicated to Professor Adalbert Kerber
in deep gratitude and adoration.

Harald Fripertinger

Institut für Mathematik
Karl-Franzens Universität Graz
Heinrichstr. 36/4, A–8010 Graz, Austria

(Communicated by Marcus Greferath)

Abstract. Let V be an n-dimensional vector space over the finite field $\mathbb{F}_q$ and T a linear operator on V. For each $k \in \{1, \dots, n\}$ we determine the number of k-dimensional T-invariant subspaces of V. Finally, this method is applied for the enumeration of all monomially nonisometric linear (n, k)-codes over $\mathbb{F}_q$.

0. Introduction

Let q be a power of a prime p, $\mathbb{F}_q$ the finite field with q elements and n a positive integer. Consider V an n-dimensional vector space over $\mathbb{F}_q$, without loss of generality $V = \mathbb{F}_q^n$, and a linear operator T on V. A subspace U of V is called T-invariant if TU is contained in U. It is well known that the T-invariant subspaces of V form a lattice, the lattice $L(T)$ of T-invariant subspaces.

We show how to determine the polynomial $\sigma(T) = \sum_{k=0}^{n} \sigma_k(T) x^k \in \mathbb{Q}[x]$, where $\sigma_k(T)$ is the number of k-dimensional, T-invariant subspaces of V.

According to [2] the lattice $L(T)$ is self-dual, which means that the coefficients of $\sigma(T)$ satisfy $\sigma_k(T) = \sigma_{n-k}(T)$ for $0 \le k \le n$.

In the sequel we use basic facts about the decomposition of a vector space into primary components or the decomposition of a primary vector space as a direct sum of cyclic subspaces. The corresponding theory can be found in textbooks on algebra, e.g. in [8, mainly chapter III].

In the final section we apply our method to the enumeration of monomially nonisometric linear codes.

1. V as an $\mathbb{F}_q[x]$-module

The $\mathbb{F}_q$-vector space V is a left $\mathbb{F}_q[x]$-module when we define the product fv of $f = \sum_{i=0}^{r} a_i x^i \in \mathbb{F}_q[x]$ and $v \in V$ by $fv := \sum_{i=0}^{r} a_i T^i v$. The polynomial f annihilates v if $fv = 0$. The monic polynomial of least degree which annihilates v is called the minimal polynomial of v. There exists a monic polynomial $g \in \mathbb{F}_q[x]$ of least degree which annihilates all vectors in V. It is called the minimal polynomial of T.

2000 *Mathematics Subject Classification:* Primary: 05E18; Secondary: 47A46.
Key words and phrases: Invariant subspaces, enumeration, finite field, finite vector space, cyclic vector space, monomially nonisometric linear codes.

Let $g = \prod_{i=1}^{s} f_i^{c_i}$ be the factorization of g into its irreducible divisors f_i with $c_i \in \mathbb{N}_{\geq 1}$, $1 \leq i \leq s$. Furthermore, let $V_i := \{v \in V \mid f_i^{c_i} v = 0\}$, then V_i is a T-invariant subspace of V and

$$V = \bigoplus_{i=1}^{s} V_i.$$

This is the primary decomposition of V into its primary components V_i, $1 \leq i \leq s$. We call a vector space primary if its minimal polynomial is the power of an irreducible polynomial.

Denote by T_i the restriction of T to V_i, then T_i is a linear operator on V_i. According to [2] the lattice $L(T)$ is the direct product of the lattices $L(T_i)$, i.e.

$$L(T) = \prod_{i=1}^{s} L(T_i).$$

This means that for each $U \in L(T)$ there exists exactly one sequence $(U_1, \ldots, U_s) \in \prod_{i=1}^{s} L(T_i)$, so that $U = U_1 \oplus \cdots \oplus U_s$. Therefore, knowing the polynomials $\sigma(T_i) = \sum_{k=0}^{\dim V_i} \sigma_k(T_i) x^k$ we can compute $\sigma(T)$ as the product $\prod_{i=1}^{s} \sigma(T_i)$. Consequently, it is enough to study the lattices $L(T_i)$ of the primary components V_i, $1 \leq i \leq s$.

2. Cyclic vector spaces

For $v \in V$ let $[v] := \mathbb{F}_q[x]v = \{fv \mid f \in \mathbb{F}_q[x]\}$. Then $[v]$ is a T-invariant subspace. It is called the cyclic subspace generated by v. If d denotes the degree of the minimal polynomial of v, then $[v] = \langle v, Tv, \ldots, T^{d-1}v \rangle$ and its dimension is equal to d. In general, a vector space U is called cyclic if there exists some $v \in U$, so that $U = [v]$.

If U is a T-invariant vector space and if v belongs to U, then $[v]$ is a subspace of U, thus, $[v]$ is the smallest T-invariant subspace of V containing v.

3. Decomposition of a primary space into cyclic subspaces

Let V be primary, i.e. V is an n-dimensional vector space with minimal polynomial f^c where f is irreducible over $\mathbb{F}_q$ and $c \in \mathbb{N}_{\geq 1}$.

According to [2] the lattice $L(T)$ is either simple (which means that the only lattice homomorphisms of $L(T)$ are isomorphisms or constant mappings) or it is a chain. Moreover, $L(T)$ is a chain if and only if V is cyclic.

Let $I(h)$ denote the ideal generated by h in $\mathbb{F}_q[x]$. In the present situation V can be seen as an $\mathbb{F}_q[x]/I(f^c)$-module. It is well known that there exists a decomposition of V as a direct sum of cyclic subspaces, i.e.

$$V = \bigoplus_{i=1}^{r} U_i,$$

where $U_i = [v_i] \simeq \mathbb{F}_q[x]/I(f^{t_i})$ and $c = t_1 \geq \ldots \geq t_r \geq 1$.

For $v \in V$ define the height of both v and $[v]$ by

$$h([v]) := h(v) := \frac{\dim[v]}{\deg f}.$$

Then $f^{h(v)}$ is the minimal polynomial of v. Each $v \in V$ has a unique representation $v = u_1 + \cdots + u_r$ with $u_i \in [v_i]$, $1 \leq i \leq r$, and $h(v) = \max\{h(u_i) \mid 1 \leq i \leq r\}$.

We collect properties of a cyclic vector space in

Lemma 1. *Let T be a linear operator on V and let $U = [v] \simeq \mathbb{F}_q[x]/I(f^t)$, where f is irreducible, $t \in \mathbb{N}_{\geq 1}$, be a cyclic subspace of V.*

1. *$L(T|_U)$ is the chain*
$$U = [v] \supset [fv] \supset \ldots \supset [f^{t-1}v] \supset \{0\}.$$
2. *Consider some $\tau \in \{0, \ldots, t\}$, then $f^{t-\tau}$ is the minimal polynomial of $f^\tau v$ and of T restricted to $[f^\tau v]$.*
3. $\dim U = t \deg f$.
4. *Consider some $\tau \in \{1, \ldots, t\}$. The elements of height τ in U are the elements which belong to $[f^{t-\tau}v] \setminus [f^{t-\tau+1}v]$. If $Q := q^{\deg f}$, then there are $Q^\tau - Q^{\tau-1}$ vectors of height τ in U. Each vector of height τ in U generates the cyclic vector space $[f^{t-\tau}v]$.*
5. *Consider a polynomial $g \in \mathbb{F}_q[x]$ with $\gcd(g, f^t) = f^s$, and an integer $\tau \in \mathbb{N}$ with $s + \tau \le t$. Then $\{gv \mid v \in [f^\tau v]\} = [f^{s+\tau}v]$.*

The proof is left to the reader.

Consider the decomposition $V = \bigoplus_{i=1}^r [v_i]$ from above. Then (cf. [10]) the species of this decomposition is the vector $\lambda = (\lambda_1, \ldots, \lambda_c)$ of nonnegative integers, where λ_j is the number of summands $[v_i]$ of height j, i.e.
$$\lambda_j = |\{i \in \{1, \ldots, r\} \mid h(v_i) = j\}|.$$
Consequently, $\lambda_c \ge 1$, $\sum_{j=1}^c \lambda_j = r$, and $\sum_{j=1}^c j\lambda_j \deg f = \dim V = n$.

In general the decomposition of a primary vector space V as a direct sum of cyclic subspaces is not unique. However two different decompositions of V have the same species. Therefore, $\lambda = (\lambda_1, \ldots, \lambda_c)$ is the species of V and each decomposition of V as a direct sum of cyclic subspaces has the species λ.

Lemma 2. *Let V be a primary vector space of species $\lambda = (\lambda_1, \ldots, \lambda_c)$, $\lambda_c \ne 0$, and assume that there exists some $t \in \{1, \ldots, c\}$ so that $\lambda_j = 0$ for all $j < t$. Then for each $u \in V$ with $h(u) = s \le t$ and for each $g \in \mathbb{F}_q[x]$ with $\gcd(g, f^c) = f^{t-s}$ there exists some $v \in V$ with $h(v) = t$ and $gv = u$.*

Proof. Each $u \in V$ has the unique representation $u = u_1 + \cdots + u_r$ with $u_i \in [v_i]$. The height of u is equal to s if and only if $h(u_i) \le s$ for all $i \in \{1, \ldots, r\}$ and there exists some $i_0 \in \{1, \ldots, r\}$ so that $h(u_{i_0}) = s$. Hence, there exist polynomials $g_i \in \mathbb{F}_q[x]$ so that $u_i = g_i v_i$, $\gcd(g_i, f^c) = f^{a_i}$ where $a_i \ge t_i - s \ge t - s$ and $a_{i_0} = t_{i_0} - s$. Consequently, $g_i = \tilde{g}_i f^{t-s} f^{b_i}$ where $b_i = a_i - (t - s) \ge 0$ and $u_i = \tilde{g}_i f^{t-s}(f^{b_i} v_i) \in \tilde{g}_i f^{t-s}[f^{b_i} v_i]$.

Consider a polynomial g of the form $\tilde{g} f^{t-s}$ where $\tilde{g}$ and f are relatively prime. Then by Lemma 1.5 there exists $\tilde{u}_i \in [f^{b_i} v_i]$ so that $u_i = g\tilde{u}_i$ for $1 \le i \le r$. Thus $u = \sum_{i=1}^r u_i = g \sum_{i=1}^r \tilde{u}_i$. Moreover $h(\tilde{u}_i) = t_i - b_i = t_i - a_i + t - s \le t_i - (t_i - s) + t - s = t$ and $h(\tilde{u}_{i_0}) = t$. If we set $v = \sum_{i=1}^r \tilde{u}_i$, then $h(v) = t$ and $gv = u$. □

The next example shows how to generalize the formula for the enumeration of all k-dimensional subspaces to the enumeration of the k-dimensional T-invariant subspaces of V.

Example 1. Let $V = \mathbb{F}_q^n$, $T = \mathrm{id}_V$, then the minimal polynomial of T is $f = x - 1$, thus $c = 1$. Each 1-dimensional subspace is a cyclic one, hence $\langle v \rangle = [v]$ for all $v \in V$. The species of V is $\lambda = (n)$. Let $e^{(i)}$ be the i-th unit vector in $\mathbb{F}_q^n$, $1 \le i \le n$, then two decompositions of V as a direct sum of cyclic subspaces are

e.g.

$$V = \bigoplus_{i=1}^{n} [e^{(i)}] = \bigoplus_{i=1}^{n} [e^{(1)} + \cdots + e^{(i)}].$$

Each k-dimensional subspace of V is T-invariant and has the species $\mu = (k)$. Thus the number of k-dimensional T-invariant subspaces of V is

$$\prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}. \qquad (*)$$

The nominator determines the number of all k-tuples $(u_1, \ldots, u_k)$ in V^k so that the u_i, $1 \leq i \leq k$, are linearly independent. Hence, it is the number of all k-tuples $(u_1, \ldots, u_k)$ in V^k so that $h(u_i) = 1$, $1 \leq i \leq k$, and that the sum of the cyclic spaces $[u_i]$, $1 \leq i \leq k$, is direct. Therefore, the sum $\bigoplus_{i=1}^{k} [u_i]$ has the species μ.

Consider an arbitrary k-dimensional subspace U of V. Then its species is μ. The denominator in $(*)$ is the number of all k-tuples $(u_1, \ldots, u_k)$ in U^k so that the u_i, $1 \leq i \leq k$, are linearly independent. Hence, it is the number of all k-tuples $(u_1, \ldots, u_k)$ in U^k so that $h(u_i) = 1$, $1 \leq i \leq k$, and that the sum of the cyclic spaces $[u_i]$, $1 \leq i \leq k$, is direct. Therefore, the sum $\bigoplus_{i=1}^{k} [u_i]$ is equal to U and has the species μ. This method was generalized in [13] to the computation of the number of T-invariant subspaces of a primary space where the minimal polynomial of T is just irreducible, i.e. in our terminology $c = 1$.

Consider a primary vector space V of species λ. Each T-invariant subspace U of V has a decomposition as a direct sum of cyclic subspaces. Therefore, it has a species μ. In the sequel we describe how to construct for given μ all subspaces of V which have μ as their species, and which species μ occur as species of subspaces of V.

Lemma 3. *Let U be a T-invariant subspace of a primary space V. If there exists some $v \in V$ with $h(v) = t$ so that $U \cap [v] = \{0\}$, then $h(v - u) \geq t$ for all $u \in U$ (or equivalently, $v \neq u + w$ for all $u \in U$ and all $w \in V$ with $h(w) < t$).*

The proof is left to the reader.

Lemma 4. *Let V be a primary vector space of species $\lambda = (\lambda_1, \ldots, \lambda_c)$, $\lambda_c \neq 0$. Consider some $t \in \{1, \ldots, c\}$, and some $v \in V$ with $h(v) = t$. Let U be a T-invariant subspace of V of species $\nu = (\nu_1, \ldots, \nu_c)$ so that $\nu_i = 0$ for $i < t$. Then $U \cap [v] = \{0\}$ if and only if $h(v - u) \geq t$ for all $u \in U$ (or equivalently, $v \neq u + w$ for all $u \in U$ and all $w \in V$ with $h(w) < t$).*

Proof. The previous lemma proved that if $U \cap [v] = \{0\}$ then $h(v - u) \geq t$ for all $u \in U$. Conversely, assume that $U \cap [v] \neq \{0\}$, then there exists some $g \in \mathbb{F}_q[x]$ so that $0 \neq gv = u \in U$. Let $h(u) = s$, then $1 \leq s \leq t$ and $\gcd(g, f^t) = f^{t-s}$. By Lemma 2 there exists some $u' \in U$ so that $u = gv = gu'$, thus $g(v - u') = 0$. Therefore, the height $h(v - u') \leq t - s \leq t - 1$ is less than t which contradicts our assumption. □

Now we determine the number of vectors of height t in a primary vector space.

Lemma 5. *Let V be a primary vector space with minimal polynomial f^c and of species $\lambda = (\lambda_1, \ldots, \lambda_c)$. For $t \in \{1, \ldots, c\}$ the number of vectors of height t is equal*

to

$$\alpha_t(\lambda) = \frac{Q^t - Q^{t-1}}{Q-1} Q^{(t-1)(l_t-1)}(Q^{l_t}-1)\prod_{i=1}^{t-1} Q^{i\lambda_i}$$

where $l_t := \lambda_t + \cdots + \lambda_c$ *and* $Q = q^{\deg f}$.

Proof. In the decomposition $V = \bigoplus_{i=1}^{r}[v_i]$ the first $l := \lambda_t + \cdots + \lambda_c$ summands are spaces of height at least t, the remaining spaces are of height less than t. In order to determine all vectors $v \in V$ with $h(v) = t$ we determine all r-tuples $(u_1, \ldots, u_r)$ with $u_i \in [v_i]$, $1 \le i \le r$, so that $h(u_i) \le t$, and there exists at least one $i \in \{1, \ldots, l\}$ so that $h(u_i) = t$. Then the height of $v = u_1 + \cdots + u_r = t$. The set of these vectors can be partitioned into l disjoint subsets indexed by j so that for $1 \le j \le l$ the height $h(u_i) < t$ for $i < j$ and $h(u_j) = t$. For each $j \in \{1, \ldots, l\}$ the number of these r-tuples is equal to $Q^{(t-1)(j-1)}(Q^t - Q^{t-1})Q^{t(l-j)}\prod_{i=1}^{t-1} Q^{i\lambda_i}$. Summing these terms for $j \in \{1, \ldots, l\}$ gives the expression $\alpha_t(\lambda)$. □

Given a subspace U of V of species ν with $\nu_j = 0$ for $j < t$, Lemma 4 explains how to find a vector $v \in V$ so that the species of $U \oplus [v]$ is equal to μ where $\mu_t = \nu_t + 1$ and $\mu_j = \nu_j$ for $j \ne t$.

Lemma 6. *Let V be a primary vector space with minimal polynomial f^c and of species $\lambda = (\lambda_1, \ldots, \lambda_c)$. Consider some $t \in \{1, \ldots, c\}$. Let U be a T-invariant subspace of V of species $\nu = (\nu_1, \ldots, \nu_c)$ so that $\nu_i = 0$ for $i < t$. Let $Q := q^{\deg f}$. Then there exist*

$$\beta_t(\lambda, \nu) = \alpha_t(\lambda) - \alpha_t(\nu)\prod_{i=1}^{t-1} Q^{i\lambda_i} Q^{(t-1)\sum_{i=t}^{c}(\lambda_i - \nu_i)}$$

vectors $v \in V$ so that $h(v) = t$ and $U \cap [v] = \{0\}$.

Proof. The number of vectors $v \in V$ of the form $v = u + w$ where $u \in U$, $h(u) = t$ and $h(w) < t$ is equal to $\alpha_t(\nu)\prod_{i=1}^{t-1} Q^{i\lambda_i} Q^{(t-1)\sum_{i=t}^{c}(\lambda_i - \nu_i)}$. The assertion follows from Lemma 4. □

Consider a primary vector space V of species λ and μ the species of a subspace of V. Let $s = \sum_{i=1}^{c} \mu_i$. Now we describe an algorithm for determining all sequences $(u_1, \ldots, u_s) \in V^s$, so that $h(u_1) \ge \ldots \ge h(u_s)$, the sum $[u_1] + \cdots + [u_s]$ is direct and the species of $[u_1] \oplus \cdots \oplus [u_s]$ is μ.

Algorithm:

1): Let $k_1 := \max\{j \in \{1, \ldots, c\} \mid \mu_j \ne 0\}$.
2): Choose $u_1 \in V$ so that $h(u_1) = k_1$.
3): Let $U_1 := [u_1]$ and let $\nu^{(1)}$ be the species of U_1. Let $i := 1$.
4): If $\nu^{(i)} \ne \mu$ determine $k_{i+1} := \max\{j \in \{1, \ldots, c\} \mid \mu_j \ne \nu_j^{(i)}\}$, else goto 7).
5): Choose $u_{i+1} \in V$ so that $h(u_{i+1}) = k_{i+1}$ and $U_i \cap [u_{i+1}] = \{0\}$.
6): Let $U_{i+1} := U_i \oplus [u_{i+1}]$ and let $\nu^{(i+1)}$ be the species of U_{i+1}. Let $i := i + 1$. Goto 4).
7): Output $(u_1, \ldots, u_s)$ where $s = \sum_{i=1}^{c} \mu_i$.

The sequence $(\nu^{(1)}, \ldots, \nu^{(s)})$ of species is uniquely determined by μ. Also $(k_1, \ldots, k_s)$ is uniquely determined by μ. If U is of species μ, then $U = \bigoplus_{j=1}^{s} U_j$ where $U_j \simeq \mathbb{F}_q[x]/I(f^{k_j})$ for $1 \le j \le s$. By Lemma 5 the number of possible choices

for u_1 in 2) is equal to $\alpha_{k_1}(\lambda)$. By Lemma 6 the number of possible choices for u_{i+1} in 5) is $\beta_{k_{i+1}}(\lambda, \nu^{(i)})$. Consequently there exist

$$\gamma(\lambda, \mu) := \alpha_{k_1}(\lambda) \prod_{i=1}^{s-1} \beta_{k_{i+1}}(\lambda, \nu^{(i)})$$

sequences $(u_1, \ldots, u_s) \in V^s$, so that $h(u_1) \geq \ldots \geq h(u_s)$, the sum $[u_1] + \cdots + [u_s]$ is direct and the species of $[u_1] \oplus \cdots \oplus [u_s]$ is μ. This number corresponds to the nominator in $(*)$, whereas the denominator in $(*)$ corresponds to $\gamma(\mu, \mu)$.

Theorem 1. *Let V be a primary vector space of species $\lambda = (\lambda_1, \ldots, \lambda_c)$ and let μ be the species of a subspace of V.*

1. *The number of different subspaces of V of species μ is equal to*
$$\frac{\gamma(\lambda, \mu)}{\gamma(\mu, \mu)}.$$
2. *The number of different decompositions of V as a direct sum of cyclic subspaces is equal to*
$$\frac{\gamma(\lambda, \lambda)}{\prod_{i=1}^{c} \lambda_i! (Q^i - Q^{i-1})^{\lambda_i}}.$$
where $Q = q^{\deg f}$.

Proof. Let U be a subspace of V of species μ and let $s := \sum_{i=1}^{c} \mu_i$. Then $\gamma(\mu, \mu)$ is the number of sequences $(u_1, \ldots, u_s) \in U^s$ so that $h(u_i) \geq h(u_{i+1})$, $1 \leq i < s$, and $U = \bigoplus_{i=1}^{s} [u_i]$. This number does not depend on the particular choice of U, it only depends on the species μ. Therefore, $\gamma(\lambda, \mu)/\gamma(\mu, \mu)$ is the number of different subspaces of V of species μ.

For proving the second assertion let $r := \sum_{i=1}^{c} \lambda_i$. Two r-tuples $(u_1, \ldots, u_r)$ and $(u'_1, \ldots, u'_r)$ in V^r determine the same decomposition of V into cyclic subspaces $\bigoplus_{j=1}^{r} [u_j]$ or $\bigoplus_{j=1}^{r} [u'_j]$ if and only if there exists a permutation $\pi \in S_r$ which permutes the indices of summands of the same height, so that $[u'_j] = [u_{\pi(j)}]$ for all $j \in \{1, \ldots, r\}$. It is obvious that there exist $\prod_{i=1}^{c} \lambda_i!$ permutations which permute the indices of summands of the same height. According to Lemma 1 each cyclic subspace of height i has exactly $Q^i - Q^{i-1}$ generators. This finishes the proof. □

An immediate consequence is

Theorem 2. *Let V be a primary vector space of species λ. For $1 \leq k \leq n$ the number of k-dimensional T-invariant subspaces of V is*

$$\sigma_k(T) = \sum_{\mu} \frac{\gamma(\lambda, \mu)}{\gamma(\mu, \mu)}$$

where the sum is taken over all species μ which are species of k-dimensional subspaces of T.

Finally, we have to analyze which species μ occur as species of subspaces of a primary space of species λ.

Theorem 3. *Let V be a primary vector space of species $\lambda = (\lambda_1, \ldots, \lambda_c)$. The sequence $\mu = (\mu_1, \ldots, \mu_c)$ is the species of a subspace of V if and only if $\sum_{i=j}^{c} \mu_i \leq \sum_{i=j}^{c} \lambda_i$ for all $j \in \{1, \ldots, c\}$.*

Proof. Assume that $\sum_{i=j}^{c} \mu_i \leq \sum_{i=j}^{c} \lambda_i$ for all $j \in \{1, \ldots, c\}$. By definition $\sum_{i=j}^{c} \lambda_i$ is the number of summands in the decomposition of V as $\bigoplus_{i=1}^{r} [v_i]$ whose height is at least j. As always we assume that $h([v_i]) = t_i \geq t_{i+1} = h([v_{i+1}])$ for $1 \leq i < r$. We use the algorithm from above to determine a sequence $(u_1, \ldots, u_s)$ in V^s so that the species of $\bigoplus_{i=1}^{s} [u_i]$ is μ. If we have found such a sequence, then $h([u_i]) = k_i$, $1 \leq i \leq s$, where the k_i are constructed from μ. The assumption on λ and μ guarantees that $k_i \leq t_i$ for all $i \in \{1, \ldots, s\}$. Therefore, it is possible to choose $u_i = f^{t_i - k_i} v_i$, $1 \leq i \leq s$. Then it is obvious that $\bigoplus_{i=1}^{s} [u_i]$ is a subspace of V of species μ.

Let μ be the species of a subspace of V and let $s := \sum_{i=1}^{c} \mu_i$. Assume that there exists some $j \in \{1, \ldots, c\}$ such that $\sum_{i=j}^{c} \mu_i > \sum_{i=j}^{c} \lambda_i$ and let j_0 be the greatest j with this property. Using the algorithm above we try to determine a sequence $(u_1, \ldots, u_s)$ in V^s so that the species of $\bigoplus_{i=1}^{s} [u_i]$ is μ. Let $i_0 := \sum_{i=j_0}^{c} \lambda_i$ and assume that we have already chosen vectors $u_1, \ldots, u_{i_0}$ which form the space $U = \bigoplus_{i=1}^{i_0} [u_i]$. The species of U is $\nu^{(i_0)}$ and $\sum_{i=j_0}^{c} \nu_i^{(i_0)} = \sum_{i=j_0}^{c} \lambda_i = i_0$. According to the first part of this prove it is always possible to find these vectors. However, it is impossible to determine a vector u_{i_0+1} with $h(u_{i_0+1}) = j_0$ and $U \cap [u_{i_0+1}] = \{0\}$, since $\beta_{j_0}(\lambda, \nu^{(i_0)}) = \alpha_{j_0}(\lambda) - \alpha_{j_0}(\nu^{(i_0)}) \prod_{i=1}^{j_0-1} Q^{i\lambda_i} Q^{(j_0-1)\sum_{i=j_0}^{c}(\lambda_i - \nu_i)} = \alpha_{j_0}(\lambda) - \alpha_{j_0}(\nu^{(i_0)}) \prod_{i=1}^{j_0-1} Q^{i\lambda_i} = 0$. □

4. Monomial isometry classes of linear codes

For $1 \leq k \leq n$ a linear (n, k)-code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. Two linear (n, k)-codes are called monomially isometric if there exists a monomial matrix M, i.e. a regular $n \times n$-matrix which has in each row and in each column exactly one nonzero component, so that $C_2 = C_1 M^{-1} = \{c \cdot M^{-1} \mid c \in C_1\}$. (In coding theory its is common practice to write vectors as row vectors.)

The monomial matrices form the group $M_n(q)$, the full monomial group over the multiplicative group $\mathbb{F}_q^*$, which is isomorphic to the wreath product $\mathbb{F}_q^* \wr S_n$, where S_n is the symmetric group on $\{1, \ldots, n\}$. Then the multiplication of a code C with M^{-1} from the right describes an action of the group $M_n(q)$ on the set $\mathcal{U}_{nk}(q)$ of all (n, k)-codes over $\mathbb{F}_q$. The isometry class of the code C is then the orbit $\{CM \mid M \in M_n(q)\}$ of C. Therefore, using the Lemma of Cauchy-Frobenius, the number of monomially nonisometric linear (n, k)-codes over $\mathbb{F}_q$ is the average number of fixed points in $\mathcal{U}_{nk}(q)$ for all monomial matrices. (For group actions see [9, chapters 1 and 2.1] for monomial isometry see [1, section 1.4].)

Each monomial matrix M yields a linear operator T_M on $\mathbb{F}_q^n$ defined by $v \mapsto v \cdot M$. A linear code C is a fixed point of $M \in M_n(q)$ if and only if C is T_M-invariant. Thus the number of monomially nonisometric linear (n, k)-codes over $\mathbb{F}_q$ is the average number of T_M-invariant k-dimensional subspaces of $\mathbb{F}_q^n$ for all $M \in M_n(q)$.

Therefore, the method presented above allows the computation of the numbers of monomially nonisometric linear (n, k)-codes.

The actual computation using the method of Cauchy-Frobenius is possible since the conjugacy classes of full monomial groups are known (cf. [9, 1.3.3 and 2.2.7]). As was mentioned above, $M_n(q)$ is isomorphic to $\mathbb{F}_q^* \wr S_n$. As a matter of fact, it is more or less enough to know the cycle types of elements in S_n and the conjugacy classes of $\mathbb{F}_q^*$. The latter are of size one, since $\mathbb{F}_q^*$ is commutative.

The permutation $\pi \in S_n$ has the cycle type $(a_1, \ldots, a_n)$, if for $1 \leq j \leq n$ there are exactly a_j cycles of length j in the decomposition of π as a product

of pairwise disjoint cyclic permutations. Thus the cycle type $(a_1, \ldots, a_n)$ satisfies $\sum_{j=1}^{n} j a_j = n$.

The conjugacy classes of $M_n(q)$ are precisely described by all $(q-1) \times n$-matrices with nonnegative integer entries $a_{i,j}$, so that $\sum_{j=1}^{n} \sum_{i=1}^{q-1} j a_{i,j} = n$. Such a matrix determines a cycle type of a permutation by $(\sum_{i=1}^{q-1} a_{i,1}, \ldots, \sum_{i=1}^{q-1} a_{i,n})$ in S_n. Moreover, $a_{i,j}$ indicates how many cycles of length j are associated with the i-th element of $\mathbb{F}_q^*$.

Assume that the elements of $\mathbb{F}_q^*$ are labelled as $\mathbb{F}_q^* = \{\beta_1, \ldots, \beta_{q-1}\}$. Consider a monomial matrix M which belongs to the conjugacy class described by the matrix $(a_{i,j})$. If a cycle of length j is associated with the element β_i, then $x^j - \beta_i$ occurs as a factor of the minimal polynomial of T_M. Moreover, the characteristic polynomial of T_M can be determined from the matrix $(a_{i,j})$ as

$$\prod_{j=1}^{n} \prod_{i=1}^{q-i} (x^j - \beta_i)^{a_{i,j}}.$$

Instead of determining the minimal polynomial of T_M we immediately determine the species of all primary components. First we factor each of the $x^j - \beta_i$ where $a_{i,j} \neq 0$. Let p be the characteristics of $\mathbb{F}_q$. If p and j are relatively prime, then $x^j - \beta_i$ is the product of pairwise distinct prime factors f. The factor $(x^j - \beta_i)^{a_{i,j}}$ of the characteristic polynomial contributes $a_{i,j}$ summands of height 1 to the decompositions of the primary components determined by these f.

If $j = p^u j'$ and j' and p are relatively prime, then $x^j - \beta = (x^{j'} - \beta)^{p^u}$ and, consequently, each prime factor f occurs with the multiplicity p^u. In this situation the factor $(x^j - \beta_i)^{a_{i,j}}$ of the characteristic polynomial contributes $a_{i,j}$ summands of height p^u to the decompositions of the primary components determined by these f.

This way we determine the species of the primary components of V corresponding to the operator T_M where M is a representative of the conjugacy class in $M_n(q)$ determined by the matrix $A = (a_{i,j})$. Hence we know how to determine $\sigma_k(T_M)$, the number of k-dimensional T_M-invariant subspaces of $\mathbb{F}_q^n$. This number depends only on the conjugacy class described by A and not on the particular choice of M, so we indicate it by $\sigma_k(A)$. The size of this conjugacy class is (cf. [9, 2.2.7])

$$s(A) := \frac{n!(q-1)^n}{\prod_{j=1}^{n} \prod_{i=1}^{q-i} a_{i,j}! (j(q-1))^{a_{i,j}}}.$$

We summarize these results in

Theorem 4. *The number of linearly nonisometric linear (n,k)-codes over $\mathbb{F}_q$ is*

$$\frac{1}{n!(q-1)^n} \sum_{A} s(A)\sigma_k(A)$$

where we are summing over all possible types A of conjugacy classes in $M_n(q)$ and where $s(A)$ is the size of the conjugacy class given by A.

We were already determining numbers of isometry classes of linear codes using quite a different approach. (See e.g. [9, pages 40–43], [6], [4], [1, section 6.1].) Our method (cf. [3]) was implemented in SYMMETRICA [16]. In this approach a linear code C was represented by its generator matrices, actually by the orbit $\{A \cdot \Gamma \mid A \in \mathrm{GL}_k(q)\}$ of an arbitrary generator Γ matrix of C. For historical reasons

— we were following ideas of D. Slepian [14], [15] — isometry classes of linear codes were then considered as orbits of generator matrices, or more generally of $k \times n$-matrices over $\mathbb{F}_q$, under the operation of the direct product $\mathrm{GL}_k(q) \times M_n(q)$. In the case $q \neq 2$, using a result of Lehmann [11], [12], this action could be replaced by an action of $\mathrm{PGL}_k(q) \times S_n$ on the set of all functions from $\{1, \ldots, n\}$ to the projective geometry $\mathrm{PG}_{k-1}(q)$. Using some ideas of J. P. S. Kung's paper [10] it was possible to determine cycle index polynomials of linear and projective matrix groups over $\mathbb{F}_q$ (see [5] or [1, section 6.4]). Finally, the numbers of nonisometric linear codes could be computed by certain substitutions into these cycle index polynomials.

The new method is implemented in GAP and SYMMETRICA. GAP (cf. [7]) was used for factoring the polynomials $x^j - \beta_i$ over $\mathbb{F}_q$. The other computations were done in SYMMETRICA. Our results allow to confirm the previously computed data and to enlarge the sets of parameters (n, k, q) where we are able to determine the numbers of nonisometric codes explicitly. These enlarged tables containing numbers of nonisometric codes over different finite fields can be found on the author's web page http://www.uni-graz.at/~fripert/. Just from the description of the new method it is clear that this approach is the natural way for enumerating monomially nonisometric codes. Especially in situations where for given n we determine the number of monomially nonisometric (n, k)-codes for all k the new method is much faster than the previous one. On the other hand, the old method should be preferred when for given k (not too big) we determine numbers of monomially nonisometric (n, k)-codes for several $n > k$.

In several places it was important to consider vector spaces over fields and not modules over rings. Therefore, it rather seems to be impossible to give a direct generalization of this approach to the enumeration of codes over $\mathbb{Z}_4$.

References

[1] (MR2265727) A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert and A. Wassermann, "Error–Correcting Linear Codes — Classification by Isometry and Applications," Springer, Berlin, Heidelberg, New York, 2006.

[2] (MR0213378)[10.4153/CJM-1967-075-4] L. Brickman and P. A. Fillmore, *The invariant subspace lattice of a linear transformation*, Can. J. Math., **19** (1967), 810–822.

[3] (MR1319681) H. Fripertinger, *Enumeration of isometry classes of linear (n, k)-codes over $GF(q)$ in SYMMETRICA*, Bayreuth. Math. Schr., **49** (1995), 215–223.

[4] (MR1474009) H. Fripertinger, *Enumeration of linear codes by applying methods from algebraic combinatorics*, Grazer Math. Ber., **328** (1996), 31–42.

[5] (MR1453968)[10.1016/S0024-3795(96)00530-7] H. Fripertinger, *Cycle indices of linear, affine and projective groups*, Linear Algebra Appl., **263** (1997), 133–156.

[6] (MR1448165) H. Fripertinger and A. Kerber, *Isometry classes of indecomposable linear codes*, in "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes" (eds. G. Cohen, M. Giusti and T. Mora), Springer, 1995, 194–204.

[7] GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12, 2008.

[8] (MR0053905) N. Jacobson, "Lectures In Abstract Algebra, II," D. Van Nostrand Company Inc., New York, 1953.

[9] (MR1716962) A. Kerber, "Applied Finite Group Actions," Springer, Berlin, Heidelberg, New York, 1999.

[10] (MR0604337)[10.1016/0024-3795(81)90227-5] J. P. S. Kung, *The cycle structure of a linear transformation over a finite field*, Linear Algebra Appl., **36** (1981), 141–155.

[11] (MR0354393) W. Lehmann, *Das Abzähltheorem der Exponentialgruppe in gewichteter Form*, Mitteilungen aus dem Mathem. Seminar Giessen, **112** (1974), 19–33.

[12] W. Lehmann, "Ein vereinheitlichender Ansatz für die REDFIELD – PÓLYA – de BRUIJNSCHE Abzähltheorie," Ph.D thesis, Universität Giessen, 1976.

[13] (MR1484172) G. E. Séguin, *The algebraic structure of codes invariant under a permutation*, in "Information Theory and Applications, II," Springer, Berlin, (1996), 1–18.
[14] (MR0122628) D. Slepian, *Some further theory of group codes*, Bell Sys. Techn. J., **39** (1960), 1219–1252.
[15] (MR0373758) D. Slepian, *Some further theory of group codes*, in "Algebraic Coding Theory: History and Development" (ed. I.F. Blake), Stroudsbourg, Dowden, Hutchinson & Ross, Inc., (1973), 118–151.
[16] 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," available online at http://www.algorithm.uni-bayreuth.de/en/research/SYMMETRICA/

Received March 2010; revised April 2011.

E-mail address: fripert@uni-graz.at