Bayreuther Mathematische Schriften **49** (1999), 215-223

Enumeration of isometry-classes of linear (n, k)-codes over $GF(q)$ in SYMMETRICA

Fripertinger Harald

December 20, 1999

Abstract

Isometry classes of linear codes can be described as orbits of generator matrices, as it was shown by Slepian. The author demonstrates how they can be enumerated using cycle index polynomials and the tools already incorporated in SYMMETRICA, a computer algebra package devoted to representation theory and combinatorics of symmetric groups and of related classes of groups.

1 Isometry classes of linear codes

A *linear* (n, k)*-code* over the Galois field $GF(q)$ is a k-dimensional subspace of the vector space $Y^X := GF(q)^n$, where n denotes the set $\{0, 1, \ldots, n-1\}$. As usual codewords will be written as rows $x = (x_0, \ldots, x_{n-1})$. A $k \times n$-matrix Γ over $GF(q)$ is called *a generator matrix* of the linear (n, k)-code C, if and only if the rows of Γ form a basis of C, so that $C = \{x \cdot \Gamma \mid x \in GF(q)^k\}$. Two linear (n, k)-codes C_1, C_2 are called *equivalent*, if and only if there is an isometry (with respect to the Hamming metric) which maps C_1 onto C_2. Using the notion of finite group actions (see [8]) one can easily express equivalence of codes in terms of the wreath product action: C_1 and C_2 are equivalent, if and only if there exist $(\psi, \pi) \in GF(q)^* \wr S_n = \big\{(\psi, \pi) \mid \psi \in (GF(q)^*)^n, \pi \in S_n\big\}$ (where $GF(q)^*$ denotes the multiplicative group of the Galois field) such that $(\psi, \pi)(C_1) = C_2$.
The *complete monomial group* $GF(q)^* \wr S_n$ of degree n over $GF(q)^*$ acts on $GF(q)^n$ by the following definition:

$$GF(q)^* \wr S_n \times GF(q)^n \to GF(q)^n \qquad (\psi, \pi)\left((x_i)_{i \in n}\right) = \left(\psi(i) x_{\pi^{-1}(i)}\right)_{i \in n}.$$

In order to apply the results of the theory of finite group actions, this equivalence relation for linear (n,k)-codes is translated into an equivalence relation for generator matrices of linear codes, and these generator matrices are considered to be functions $\Gamma\colon n \to GF(q)^k \setminus \{0\}$ where $\Gamma(i)$ is the i-th column of the generator matrix Γ. (We exclude 0-columns for obvious reasons.)

1.1 Theorem *The matrices corresponding to the two functions Γ_1 and Γ_2 from n to $GF(q)^k \setminus \{0\}$ are generator matrices of two equivalent codes, if and only if Γ_1 and Γ_2 lie in the same orbit of the following action of $GL_k(q) \times GF(q)^* \wr S_n$ as permutation group on $(GF(q)^k \setminus \{0\})^n$:*

$$(A,(\psi,\pi))(\Gamma) = A\psi(\cdot)\Gamma(\pi^{-1}\cdot),$$

or, more explicitly,

$$(A,(\psi,\pi))(\Gamma)(i) := A\psi(i)\Gamma(\pi^{-1}(i)).$$

As a generalization of SLEPIAN's article [11] we show in [5] that, by using LEHMANN's Lemma about actions of the wreath product, the generating function for the numbers

$$T_{nkq} := \left|(GL_k(q) \times GF(q)^* \wr S_n) \backslash\backslash (GF(q)^k \setminus \{0\})^n\right|$$

can be computed by the following substitution into the cycle index of the *projective group* $PGL_k(q)$ acting on the $k-1$-dimensional *projective space* $PG_{k-1}(q)$:

$$\sum_{n=0}^{\infty} T_{nkq} x^n = Z(PGL_k(q))\big|_{x_i = \sum_{j=0}^{\infty} x^{ij}} = Z(PGL_k(q))\big|_{x_i = \frac{1}{1-x^i}}. \tag{1}$$

Since the T_{nkq} can be interpreted as numbers of classes of $k \times n$-matrices of rank $\leq k$ the numbers S_{nkq}, which are the numbers of isometry classes of linear (n,k)-codes with no columns of zeros, satisfy

$$S_{nkq} = T_{nkq} - T_{n,k-1,q}. \tag{2}$$

Restricting our attention to codes with generator matrices Γ, such that $\bar{\Gamma} : n \to PG_{k-1}(q)$, $\bar{\Gamma}(i) := GF(q)^*(\Gamma(i))$ is injective, we can derive the numbers of isometry classes of "injective" linear codes, obtaining

$$\bar{S}_{nkq} = \bar{T}_{nkq} - \bar{T}_{n,k-1,q}, \tag{3}$$

where the $\bar{T}_{nkq}$ are computed by:

$$\sum_{n=0}^{\infty} \bar{T}_{nkq} x^n = Z(PGL_k(q))\big|_{x_i=1+x^i}. \tag{4}$$

In [3] it is shown how the cycle index of $PGL_k(q)$ acting on $PG_{k-1}(q)$ can be computed. This paper is a generalization of [11] and of Harrison [7, 6], where the cycle indices of $GL_k(2)$ are computed. The idea for computing these cycle indices is the following: First determine the conjugacy classes in $GL_k(q)$, which can be done by using the theory of normal forms of matrices. Then determine the number of elements in these conjugacy classes, for instance by applying a very nice formula of Kung [9]. Finally compute the cycle type of one representative of each class. (It is well known that all elements in one conjugacy class are of the same cycle type.) These formulae have been implemented into SYMMETRICA, so a C-program for computing S_{ikq} for $i = k, \dots, n$ can be written in the following way:

```
INT S_nkq_maxgrad(n,k,q,f)
OP n,k,q,f;
{
OP c,d;
INT erg=OK;
c=callocobject();
d=callocobject();
erg+=T_nkq_maxgrad(n,k,q,c);
if (gt(k,cons_eins))
{
  erg+=dec(k);
  erg+=T_nkq_maxgrad(n,k,q,d);
  erg+=inc(k);
  erg+=sub(c,d,f);
}
else erg+=copy(c,f);
erg+=freeall(c);
erg+=freeall(d);
if (erg!=OK) return error(" in computation of S_nkq_maxgrad");
return erg;
}
```

The program for the computation of the T_{ikq} for $i \leq n$ is the following:

```
INT T_nkq_maxgrad(n,k,q,f)
OP k,q,n,f;
{
OP c,d;
INT erg=OK;
c=callocobject();
d=callocobject();
erg+=zykelind_pglkq(k,q,c);
erg+=numberofvariables(c,d);
erg+=co_polya3_sub(c,d,n,f);
erg+=freeall(c);
erg+=freeall(d);
if (erg!=OK) return error(" in computation of T_nkq_maxgrad");
return erg;
}
```

With the routine `zykelind_pglkq(k,q,c)` one can compute the cycle index of $PGL_{k-1}(q)$ acting on the projective space $PG_{k-1}(q)$, and the routine `co_polya3_sub(c,d,n,f)` computes the first part of degree $\leq n$ of the substitution $x_i \mapsto \sum_{j=0}^{\infty} x^{ij}$ in the polynomial `c`. Both these routines can be found in the source file `zykelind.c`.

2 Indecomposable codes

In order to minimize the number of orbits that must be enumerated or represented, and following SLEPIAN again, we can restrict attention to *indecomposable* linear (n,k)-codes. Let C_1 be a linear (n_1,k_1)-code over $GF(q)$ with generator matrix Γ_1 and let C_2 be a linear (n_2,k_2)-code over $GF(q)$ with generator matrix Γ_2, then the code C with generator matrix

$$\Gamma := \left(\begin{array}{c|c} \Gamma_1 & 0 \\ \hline 0 & \Gamma_2 \end{array}\right)$$

is called the *direct sum* of the codes C_1 and C_2, and it will be denoted by $C = C_1 \oplus C_2$. A code C is called *decomposable*, if and only if it is equivalent to a code which is the direct sum of two or more linear codes. Otherwise it is called *indecomposable*.

Since there are some errors in Slepian's table of the numbers of isometry classes of indecomposable (n, k)-codes, denoted by R_{nkq} or $\bar{R}_{nkq}$, the following theorem is proved in [5]:

2.1 Theorem *The number R_{nkq} is equal to*

$$S_{nkq} - \sum_a \sum_b \prod_{\substack{j=1 \\ a_j \neq 0}}^{n-1} \left(\sum_{\substack{c=(c_1,\ldots,c_{a_j}) \in \mathbb{N}^{a_j} \\ j \geq c_1 \geq \ldots \geq c_{a_j} \geq 1,\ \sum c_i = b_j}} U(j,a,c) \right), \tag{5}$$

where

$$U(j,a,c) = \prod_{i=1}^{j} Z(S_{\nu(i,a_j,c)})\big|_{x_\ell = R_{jiq}}, \quad \nu(i,a_j,c) = \left|\left\{1 \leq l \leq a_j \;\middle|\; c_l = i\right\}\right|,$$

and where the first sum is taken over the cycle types $a = (a_1, \ldots, a_{n-1})$ of n, (which means that $a_i \in \mathbb{N}_0$ and $\sum ia_i = n$) such that $\sum a_i \leq k$, while the second sum is over the $(n-1)$-tuples $b = (b_1, \ldots, b_{n-1}) \in \mathbb{N}_0^{n-1}$, for which $a_i \leq b_i \leq ia_i$, and $\sum b_i = k$. In the same way the $\bar{R}_{nkq}$ can be computed from the $\bar{S}_{nkq}$. The numerical results show that for fixed q and n the sequence of R_{nkq} is unimodal and symmetric. (It is easy to prove that this sequence must be symmetric, but the proof of the unimodality is still open.)

This formula is implemented in SYMMETRICA as well. For instance for computing the tables of S_{nkq} and R_{nkq} one can use the next program:

```
INT co_all_codes()
{
OP n,k,q,R,S;
INT i,j;
INT erg=OK;
n=callocobject();
k=callocobject();
q=callocobject();
S=callocobject();
R=callocobject();
erg+=printeingabe("maximum value of n=? ");
erg+=scan(INTEGER,n);
erg+=printeingabe("maximum value of k=? ");
erg+=scan(INTEGER,k);
erg+=printeingabe("q=? ");
erg+=scan(INTEGER,q);
erg+=all_codes(n,k,q,S,R);
erg+=println(S);
erg+=println(R);
erg+=freeall(n); erg+=freeall(k); erg+=freeall(q);
erg+=freeall(S); erg+=freeall(R);
if (erg!=OK) return error(" in computation of co_all_codes");
return erg;
}
```

The routine `all_codes(n,k,q,S,R)` first computes the numbers T_{ijq} for $1 \leq i \leq n$ and $1 \leq j \leq k$ by (1), then the S_{ijq} by (2) and finally the R_{ijq} by (5). For computing the numbers of classes of injective linear (n,k)-codes by (3), (4) and (5) there is the routine `all_inj_codes(n,k,q,S,R)`. The following tables for $q = 8$, $n \leq 15$ and $k \leq 4$ were computed using these two routines:

Table 1: Number of isometry classes of linear (n,k)-codes over $GF(8)$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	1	1	0	0
3	1	2	1	0
4	1	4	3	1
5	1	6	9	4
6	1	13	43	21
7	1	20	252	282
8	1	38	1995	11897
9	1	63	16604	697905
10	1	108	132128	40.614006
11	1	172	986280	2187.942319
12	1	285	6.875894	108580.294923
13	1	438	44.880497	4.985498.095659
14	1	685	275.497100	212.944334.871779
15	1	1027	1597.384440	8503.509808.998891

Table 2: Number of isometry classes of indecomposable linear (n, k)-codes over $GF(8)$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	1	0	0	0
3	1	1	0	0
4	1	2	1	0
5	1	4	4	1
6	1	10	33	10
7	1	17	231	231
8	1	34	1956	11596
9	1	59	16529	695614
10	1	103	131993	40.595108
11	1	167	986040	2187.791284
12	1	279	6.875485	108579.157553
13	1	432	44.879807	4.985490.082276
14	1	678	275.495976	212.944281.977581
15	1	1020	1597.382635	8503.509480.606942

Table 3: Number of isometry classes of injective linear (n, k)-codes over $GF(8)$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	0	1	0	0
3	0	1	1	0
4	0	1	2	1
5	0	1	4	3
6	0	1	24	14
7	0	1	131	232
8	0	1	900	10507
9	0	1	6154	613247
10	0	0	38344	34.772483
11	0	0	217432	1812.280847
12	0	0	1119290	86639.601001
13	0	0	5.242484	3.818387.464701
14	0	0	22.449375	156.004956.091612
15	0	0	88.267837	5938.561168.433472

Table 4: Number of isometry classes of injective indecomposable linear (n,k)-codes over $GF(8)$

$n\backslash k$	1	2	3	4
1	1	0	0	0
2	0	0	0	0
3	0	1	0	0
4	0	1	1	0
5	0	1	3	1
6	0	1	23	9
7	0	1	130	207
8	0	1	899	10374
9	0	1	6153	612345
10	0	0	38343	34.766326
11	0	0	217432	1812.242500
12	0	0	1119290	86639.383565
13	0	0	5.242484	3.818386.345408
14	0	0	22.449375	156.004950.849125
15	0	0	88.267837	5938.561145.984095

In [5] there are tables of R_{nkq} and $\bar{R}_{nkq}$ for $q = 2, 3, 4, 5, 7$. Tables of S_{nkq} can be found in [3, 4] and in the article of Wild [12], when interpreting matroids as linear codes. Extensions of the tables given in [11] for the binary case were evaluated by Lattermann in [10].
In her thesis [1], Arnold evaluated transversals of isometry classes of linear codes. Another implementation, due to Betten allowed to evaluate representatives of all the isometry classes of indecomposable binary (n,k)-codes for $n \leq 12$ except for the case of $n = 12$ and $k = 6$. Use was made of orderly generation in connection with isomorphism checking [2]. Details will be given elsewhere.

References

[1] E. Arnold. Äquivalenzklassen linearer Codes. Master's thesis, Universität Bayreuth, 1993.

[2] A. Betten. Gruppenaktionen auf Verbänden und die Konstruktion kombinatorischer Objekte. Master's thesis, Universität Bayreuth. To appear.

[3] H. Fripertinger. Cycle indices of linear, affine and projective groups. To be published.

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

[5] H. Fripertinger and A. Kerber. Isometry classes of indecomposable codes. Submitted paper.

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

[7] 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.

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

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

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

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

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

Address of the author:
Harald Fripertinger
Institut für Mathematik
Karl-Franzens-Universität Graz
Heinrichstr. 36/4
A–8010 Graz
harald.fripertinger@balu.kfunigraz.ac.at