Random Generation of Linear Codes

Harald Fripertinger*

Dedicated to Professor János Aczél on the occasion of his birthday.

Abstract

Isometry classes of linear codes can be expressed as orbits under the group action of a wreath product. Some combinatorial and algebraic methods are discussed which can be applied for generating linear codes distributed uniformly at random over all isometry classes.

1 Introduction

The methods and results presented in this paper are interesting in the framework of *classification of discrete structures* [10, 11]. Very often discrete structures can be described as equivalence classes of certain objects. In such cases when these equivalence classes can be expressed as orbits under a group G acting on a set X — i. e. there is a mapping $G \times X \to X$, $(g, x) \mapsto gx$ such that $g_1(g_2x) = (g_1g_2)x$ and $1x = x$ for all $g_1, g_2 \in G$, $x \in X$, where 1 is the unit element of G — then there exist some combinatorial and algebraic methods for the classification of these structures. We will apply these methods for the classification of linear codes.

Let n and $k \leq n$ be two positive integers. A *linear* (n, k)*-code* C over the *finite field* $GF(q)$, where q is the power of a prime p, is a k-dimensional subspace of $GF(q)^n$. The error correcting properties of C can be described by using the *minimum distance* $d(C)$ of C,

$$d(C) := \min \{d(c, c') \mid c, c' \in C,\ c \neq c'\},$$

where $d(c, c')$ is the *Hamming distance* of the two code words, which is the number of different coordinates of c and c';

$$d(c, c') = |\{1 \leq i \leq n \mid c_i \neq c'_i\}|.$$

Applying a *Maximum-Likelihood decoder*, which decodes a received message into one of the nearest code words in C with respect to the Hamming distance, it

*Supported by the Fonds zur Förderung der wissenschaftlichen Forschung P12642-MAT.
Keywords: linear codes, isometry classes, random generation, group actions.
AMS subject classification: 05E20, 94B05.

is possible to correct at most $\lfloor (d(C)-1)/2 \rfloor$ transmission errors and detect $d(C)-1$ errors.

If there is a vector space isomorphism $\iota : C \to C'$ which preserves the Hamming distance then C and C' are called isometric. The isomorphism ι is called an *isometry* between C and C' as well. Isometric codes have the same structure with respect to the Hamming metric, so they have the same error correcting properties, and we collect them all to one *isometry class*. For that reason we are interested rather in the classification of isometry classes of codes than in the classification of all codes. Each isometry can be described as a permutation of the coordinates together with a simultaneous multiplication in each coordinate with elements of $GF(q)^*$ (cf. [9]). To be more precise, the group of all isometries can be described as the *wreath product* $GF(q)^* \wr S_n$ of the multiplicative group $GF(q)^*$ and the symmetric group S_n. Its underlying set is

$$\{(\psi,\pi) \mid \psi \in {GF(q)^*}^n,\ \pi \in S_n\},$$

where ${GF(q)^*}^n$ is the set of all functions $\psi\colon n := \{1,\ldots,n\} \to GF(q)^*$, and the multiplication is defined by

$$(\psi,\pi)(\psi',\pi') := (\psi\psi'_\pi, \pi\pi'),$$

together with

$$\psi\psi'_\pi(i) := \psi(i)\psi'_\pi(i) := \psi(i)\psi'(\pi^{-1}i).$$

Each element of this group can also be described as an $n \times n$-matrix M over $GF(q)$ which has in each row and in each column exactly one entry different from zero. The action of this monomial group on $GF(q)^n$ is given by

$$GF(q)^* \wr S_n \times GF(q)^n \to GF(q)^n$$

$$((\psi,\pi), v := (\kappa_1,\ldots,\kappa_n)) \mapsto (\psi(1)\kappa_{\pi^{-1}(1)},\ldots,\psi(n)\kappa_{\pi^{-1}(n)}),$$

or

$$(M,v) \mapsto v \cdot M^{-1}.$$

It induces a group action on $\mathcal{U}(n,k,q)$, the set of all k-dimensional subspaces of $GF(q)^n$. Usually it is more convenient to represent an (n,k)-code C by a *generator matrix* Γ which is an $n \times k$-matrix over $GF(q)$, the rows of which form a basis of the code C. Obviously each code has many different generator matrices; the set of all generator matrices of C is the orbit[1] $GL_k(q)(\Gamma)$ under the following action of the *general linear group* $GL_k(q)$ on the set $GF(q)_k^{n\times k}$ of all $n \times k$-matrices over $GF(q)$ of rank k.

$$GL_k(q) \times GF(q)_k^{n\times k} \to GF(q)_k^{n\times k} :\ (A,\Gamma) \mapsto A \cdot \Gamma.$$

For technical reasons, we will drop the condition on the rank of these matrices Γ, and we will write them as functions from the set n to $GF(q)^k \setminus \{0\}$, since it

[1]The orbit $G(x)$ of $x \in X$ under the action of G is the set of all elements of X which can be described as gx for $g \in G$, i. e. $G(x) := \{gx \mid g \in G\}$.

is obvious that we can restrict our investigations to generator matrices having no 0-columns. (A 0-column in a generator matrix causes that the corresponding coordinate in all code words is 0, so this coordinate cannot carry any information.) Finally we end up with the following group action describing the isometry classes of linear (n, l)-codes for $l \leq k$ as orbits under the particular action:

$$(GL_k(q) \times GF(q)^* \wr S_n) \times (GF(q)^k \setminus \{0\})^n \to (GF(q)^k \setminus \{0\})^n$$

$$(A, \Gamma, M) \mapsto A \cdot \Gamma \cdot M^{-1}$$

This can be made more clear when applying *Lehmann's Lemma* [13, 14] which reduces the action of the wreath product $GF(q)^* \wr S_n$ on $GF(q)^k \setminus \{0\}$ to an action of S_n on the set of $GF(q)^*$-orbits on $GF(q)^k \setminus \{0\}$. Since each of these orbits collects all nonzero vectors of a one-dimensional vector space of $GF(q)$, each of these orbits can be identified with an element of the projective geometry $PG_{k-1}(q)$.

In our final description the isometry classes of linear (n, l)-codes for $l \leq k$ correspond to $GL_k(q) \times S_n$-orbits of functions $\Gamma : n \to PG_{k-1}(q)$, where S_n operates by permuting the coordinates, and $GL_k(q)$ acts by multiplication from the left. Since $GL_k(q)$ acts on elements of $PG_{k-1}(q)$ we can consider this action as an action of the *projective linear group* $PGL_k(q)$.

$$(PGL_k(q) \times S_n) \times (PG_{k-1}(q))^n \to (PG_{k-1}(q))^n \tag{1}$$

After having described the isometry classes in a suitable way as orbits under a group action, we were able to compute the number of these classes for many parameters n, k and q using methods from *Pólya theory* (cf. [8, 5, 4, 6]). The main point in all these calculations was the computation of the *cycle index* of the action of $PGL_k(q)$ acting on $PG_{k-1}(q)$ (cf. [7]).

Some further efforts were done, for computing complete lists of representatives of these isometry classes (cf. [1]). Even though we were applying a mixture of algebraic and combinatorial algorithms together with very skilled programming techniques this approach works only for small parameter values n, k and q. Soon the size of the operating group together with the number of representatives to be computed are getting too large. In such situations it is useful, helpful and makes sense to apply probabilistic methods which allow the construction of linear codes distributed over all isometry classes uniformly at random. This way we are able to produce huge sets of representatives, to check hypotheses on them and afterwards we can try to prove the valid ones.

2 Random generation of linear codes

In this section we want to demonstrate how the *Dixon-Wilf-algorithm* can be used in order to generate linear codes distributed over all isometry classes uniformly at random. Actually this algorithm was first developed for the random generation of unlabelled graphs (cf. [3]). Before describing it in all details for an arbitrary group action we need some more notions: The *stabilizer* of $x \in X$ under the action of a group G is the subgroup

$$G_x := \{g \in G \mid gx = x\}$$

of G, whereas the *set of fixed points* of $g \in G$ is the subset

$$X_g := \{x \in X \mid gx = x\}$$

of X. The *set of all G-orbits* in X will be denoted by

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

Theorem 1. The Dixon-Wilf-algorithm. *Let G be a finite group acting on a finite set X. Choose a conjugacy class $\mathcal{C}$ of G with the probability*

$$p(\mathcal{C}) := \frac{|\mathcal{C}| \cdot |X_g|}{|G| \cdot |G \backslash\backslash X|}, \text{ for an arbitrary } g \in \mathcal{C}.$$

Pick any $g \in \mathcal{C}$ and determine at random a fixed point x of g. Then the probability that x lies in a given orbit $\omega \in G \backslash\backslash X$ is equal to $1/|G \backslash\backslash X|$, i. e. it does not depend on the special choice of ω. So the output of this algorithm is distributed uniformly at random over all G-orbits on X.

Now we are in a position to apply this algorithm to the group action (1) describing the isometry classes of linear codes. The conjugacy classes of the operating group, which is a direct product of two groups, can be described as pairs of the conjugacy classes of the two factors. So each conjugacy class $\mathcal{C}$ is a direct product $\mathcal{C} = \mathcal{C}_P \times \mathcal{C}_S$ of a conjugacy class $\mathcal{C}_P$ in $PGL_k(q)$ and a conjugacy class $\mathcal{C}_S$ in S_n. Furthermore we will use T_{nkq} as an abbreviation for the cardinality $|PGL_k(q) \times S_n \backslash\backslash (PG_{k-1}(q))^n|$. In other words T_{nkq} is the number of all isometry classes of linear (n, l)-codes without 0-columns for $l \leq k$.

Corollary 2. *Let n and $k \leq n$ be positive integers. The following algorithm computes generator matrices Γ of linear (n, l)-codes over $GF(q)$ for $l \leq k$ uniformly at random:*

Choose a conjugacy class $\mathcal{C}$ of $PGL_k(q) \times S_n$ with the probability

$$p(\mathcal{C}) := \frac{|\mathcal{C}| \cdot \left|(PG_{k-1}(q))^n_{(A,\pi)}\right|}{|S_n| \cdot |PGL_k(q)| \cdot T_{nkq}}, \text{ for an arbitrary pair } (A, \pi) \in \mathcal{C},$$

where $(PG_{k-1}(q))^n_{(A,\pi)}$ is the set of all fixed points of (A, π) in $(PG_{k-1}(q))^n$, i. e. the set of all functions $\Gamma \in (PG_{k-1}(q))^n$ which fulfill $A \cdot \Gamma = \Gamma \circ \pi$. Then pick any $(A, \pi) \in \mathcal{C}$ and generate a fixed point Γ of (A, π) uniformly at random.

In order to apply this algorithm we want to take a closer look at it. The order of S_n is given by $n!$, the order of $PGL_k(q)$ equals $[q]_k/(q-1)$ where $[q]_k$ is the order of $GL_k(q)$ given by

$$[q]_k = (q^k - 1)(q^k - q) \cdots (q^k - q^{k-1}).$$

For the computation of T_{nkq} consult one of the articles [8, 5, 4, 6]. So we can compute the denominator in $p(\mathcal{C})$.

For computing the nominator we must know the conjugacy classes of S_n and of $PGL_k(q)$. Each conjugacy class of S_n can be described by a *cycle type* λ of length n. Such a cycle type λ is a sequence of nonnegative integers $(\lambda_1, \ldots, \lambda_n)$ such that

$$\sum_{i=1}^{n} i \cdot \lambda_i = n.$$

The conjugacy class of S_n corresponding to λ consists of all permutations of cycle type λ. These are

$$\frac{n!}{\prod_i i^{\lambda_i} \cdot \lambda_i!}$$

permutations.

In order to describe the conjugacy classes of $PGL_k(q)$ we first investigate the conjugacy classes of $GL_k(q)$. Two projectivities in $PGL_k(q)$ given in form of matrices A and B are conjugate in $PGL_k(q)$ if and only if there is a matrix $R \in GL_k(q)$ and $\alpha \in GF(q)^*$ such that $R \cdot B \cdot R^{-1} = \alpha \cdot A$. Whereas the two matrices A and B are conjugate in $GL_k(q)$ if and only if there is a matrix $R \in GL_k(q)$ such that $R \cdot B \cdot R^{-1} = A$. As a consequence each conjugacy class in $PGL_k(q)$ splits into (at most $q-1$) conjugacy classes in $GL_k(q)$. Let A be a regular $k \times k$-matrix over $GF(q)$. The conjugacy class $\mathcal{C}_P(A)$ of the projectivity induced by A consists of all the matrices in the union

$$\bigcup_{\alpha \in GF(q)^*} \mathcal{C}_G(\alpha \cdot A)$$

of conjugacy classes in $GL_k(q)$.

In [7] (but also in many text books on Algebra) the conjugacy classes in $GL_k(q)$ are described by the *Jacobi normal forms*, which are block diagonal matrices of blocks strongly related to monic polynomials.

Let $f = \sum_{i=0}^{d} \kappa_i x^i$, $\kappa_d = 1$ be a monic polynomial over $GF(q)$, then the *companion matrix* $C(f)$ of f is given by

$$C(f) := \begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -\kappa_0 \\ 1 & 0 & \ldots & 0 & 0 & -\kappa_1 \\ 0 & 1 & \ldots & 0 & 0 & -\kappa_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & -\kappa_{d-2} \\ 0 & 0 & \ldots & 0 & 1 & -\kappa_{d-1} \end{pmatrix}.$$

For an integer $r \geq 1$ the *hypercompanion matrix* $H(f^r)$ of f^r is an $rd \times rd$-matrix given as a block matrix

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

where

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

A complete list of all Jacobi normal forms, i. e. a complete set of representatives of the conjugacy classes in $GL_k(q)$ can be computed in the following way:

Theorem 3. *Let $\{f_1, \dots, f_{t_k}\}$ be the set of all monic irreducible polynomials over $GF(q)$ of degree $\deg(f_i) \leq k$ which are different from the polynomial $f = x$. Compute all solutions $\gamma = (\gamma_1, \dots, \gamma_{t_k})$ of*

$$\sum_{i=1}^{t_k} \gamma_i \cdot \deg(f_i) = k.$$

For each solution γ determine all possible combinations $\lambda = (\lambda^{(1)}, \dots, \lambda^{(t_k)})$ of cycle types $\lambda^{(i)}$ of length γ_i. From each choice of λ we compute a normal form

$$N_\lambda := \operatorname{diag}(D(f_1, \lambda^{(1)}), \dots, D(f_{t_k}, \lambda^{(t_k)})), \tag{2}$$

which is a block diagonal matrix of blocks of the form

$$D(f_i, \lambda^{(i)}) := \operatorname{diag}(\underbrace{C(f_i), \dots, C(f_i)}_{\lambda_1^{(i)}\text{-times}}, \underbrace{H(f_i^2), \dots, H(f_i^2)}_{\lambda_2^{(i)}\text{-times}}, \dots, \underbrace{H(f_i^{\gamma_i}), \dots, H(f_i^{\gamma_i})}_{\lambda_{\gamma_i}^{(i)}\text{-times}}).$$

For computing the size of a conjugacy class we can use the following method by Kung (cf. [12]):

Theorem 4. *Let f be a monic irreducible polynomial of degree d over $GF(q)$, and let λ be a cycle type of length γ. For $1 \leq i \leq \gamma$ determine numbers m_i by*

$$m_i := \sum_{j=1}^{i} j \cdot \lambda_j + \sum_{j=i+1}^{\gamma} i \cdot \lambda_j.$$

Then the size of the centralizer of $D(f, \lambda)$ in $GL_{d\cdot\gamma}(q)$ is given by

$$b(d, \lambda) := \prod_{i=1}^{\gamma} \prod_{j=1}^{\lambda_i} (q^{d \cdot m_i} - q^{d\cdot(m_i - j)}).$$

This formula proves that the size of the centralizer of $D(f,\lambda)$ depends only on the degree d and on the cycle type λ, but not on the special choice of the irreducible polynomial.

The number of matrices in the conjugacy class of the normal form in (2) is given by

$$|\mathcal{C}_G(N_\lambda)| = \frac{[q]_k}{\prod_{i=1}^{t_k} b(\deg(f_i), \lambda^{(i)})}.$$

In order to write down explicitly the Jacobi normal forms in $GL_k(q)$ it is necessary to know all the monic irreducible polynomials over $GF(q)$ of degree $d \leq k$. For certain parameters there are complete lists of these polynomials available. Moreover it is possible to compute irreducible polynomials from so called *Lyndon words* which will be described now. Any given total order of the elements in $GF(q)$ can be used for defining a lexicographic order on $GF(q)^d$. The cyclic group C_d of order d generated by $\pi := (1, 2, \ldots, d)$ acts on $GF(q)^d$ by a cyclic shift,

$$v := (\kappa_1, \ldots, \kappa_d) \stackrel{\pi}{\mapsto} \pi(v) := (\kappa_d, \kappa_1, \ldots, \kappa_{d-1}).$$

A vector $v \in GF(q)^d$ is called *acyclic* if its orbit $C_d(v)$ consists of d pairwise different vectors. An acyclic vector v is a Lyndon word if and only if it is the smallest vector in the orbit $C_d(v)$.

Let $\sigma : GF(q^d) \to GF(q^d)$ be the *Frobenius automorphism* $\tau \mapsto \sigma(\tau) := \tau^q$. There exist elements $\beta \in GF(q^d)$ such that the set

$$\left\{\beta, \sigma(\beta), \ldots, \sigma^{d-1}(\beta)\right\}$$

is a basis of $GF(q^d)$ over $GF(q)$, which is called a *normal basis* of $GF(q^d)$. Then each element τ of $GF(q^d)$ can uniquely be written as

$$\tau = \sum_{i=1}^{d} \kappa_i \cdot \beta_i, \quad \beta_i := \sigma^{i-1}(\beta),\ \kappa_i \in GF(q),$$

and we can identify τ with its coefficient vector $(\kappa_1, \ldots, \kappa_d)$. Applying the Frobenius automorphism to τ is the same as applying the cyclic shift π to its coefficient vector.

A monic irreducible polynomial f of degree d over $GF(q)$ has d different roots in $GF(q^d)$. It is the minimal polynomial of each of its roots over $GF(q)$. If $\tau \in GF(q^d)$ is a root of f then all the other roots, which are called *conjugates* of τ, are obtained by applying the Frobenius automorphism to τ, i. e. the set of roots is given by

$$\left\{\sigma^i(\tau) \mid 0 \leq i \leq d-1\right\}.$$

Then the minimal polynomial f of τ (and of each of its conjugates) over $GF(q)$ is given by

$$f = \prod_{i=0}^{d-1} (x - \sigma^i(\tau)).$$

Using a normal basis of $GF(q^d)$ the coefficient vector of τ (and so the coefficient vector of each root of f) must be an acyclic vector.

The other way round, if $\tau \in GF(q^d)$ has an acyclic coefficient vector with respect to a normal basis over $GF(q)$, then the minimal polynomial over $GF(q)$ of τ is a monic irreducible polynomial of degree d.

Since each monic irreducible polynomial of degree d over $GF(q)$ occurs as a minimal polynomial of certain elements of $GF(q^d)$, we only have to find all elements with an acyclic coefficient vector for determining all irreducible polynomials of degree d over $GF(q)$. The Frobenius automorphism collects d conjugate elements, which are the roots of the same irreducible polynomial over $GF(q)$, and which correspond to one C_d-orbit on the set of acyclic coefficient vectors. So we described a one to one correspondence between the set of all Lyndon words of length d over $GF(q)$ and the set of all monic irreducible polynomials of degree d over $GF(q)$.

In order to find the set of all conjugacy classes in $PGL_k(q)$ we have to determine which conjugacy classes in $GL_k(q)$ must be merged in order to get a conjugacy class in $PGL_k(q)$. So for each normal form N_λ (cf. (2)) and each $\alpha \in GF(q)^*$ we must determine the normal-form of $\alpha \cdot N_\lambda$. For doing this it is enough to determine the normal forms of $\alpha \cdot C(f)$ and $\alpha \cdot H(f^r)$ of monic irreducible polynomials $f = \sum_{i=0}^{d} \kappa_i x^i$. It is easy to deduce that these normal forms are given by the companion or hypercompanion matrices $C(f_\alpha)$ and $H(f_\alpha^r)$ of the polynomial

$$f_\alpha := \sum_{i=0}^{d} \alpha^{d-i} \kappa_i x^i,$$

which is again a monic and irreducible polynomial of degree d over $GF(q)$. It is irreducible since the roots of f_α are of the form $\alpha \cdot \tau$, where τ is a root of f, so the roots of f_α form a set of d conjugates in $GF(q^d)$.

From each conjugacy class in $PGL_k(q)$ we can choose a representative in form of a matrix, since we know the Jacobi normal-forms, from which we can compute a permutation representation on $PG_{k-1}(q)$.

Coming back to the description of the algorithm we finally have to investigate the set of all functions $f \in Y^X$ which fulfill $\rho \circ f \circ \pi^{-1} = f$ for given permutations π of X and ρ of Y. This set of fixed points $Y^X_{(\rho,\pi)}$ can be described in the following way: Choose from each cycle of length ℓ in the cycle decomposition of π one element x; this element must be mapped by f onto an element y which lies in a cycle of length dividing ℓ in the cycle decomposition of ρ. By $f \circ \pi^i(x) = \rho^i \circ f(x)$ the function f is defined on the whole cycle of x. When $\lambda = \lambda(\pi)$ denotes the cycle type of the permutation π, i. e. there are λ_i cycles of length i in the cycle decomposition of π, then

$$\left| Y^X_{(\rho,\pi)} \right| = \prod_{i=1}^{|X|} \left| Y_{\rho^i} \right|^{\lambda_i},$$

where Y_{ρ^i} is the set of all fixed points of ρ^i in Y.

This finishes the description of the algorithm for the random generation of linear codes. It was implemented in the computer algebra system SYMMETRICA [15] for the generation of linear codes over prime fields, i. e. for q is a prime. In order to minimize the amount of work before the algorithm actually starts to generate codes it is useful to start the generation at once after having computed the information on the first conjugacy class, and evaluate further conjugacy classes and their probabilities only if required. This means we have to compute $p(\mathcal{C}_i)$ only if the random number (lying in $[0, 1[$) determining which conjugacy class to choose exceeds $\sum_{j=1}^{i-1} p(\mathcal{C}_j)$.

n	k	S_{nk2}	d_2	1	2	3	4	5	6	7	8	9
15	5	62812	7	5.5	31.4	29.6	29.3	4.1	0.1	>0		
16	5	160106	8	3.9	24.1	26.8	34.7	9.8	0.7	>0	>0	
17	5	401824	8	2.8	18.2	22.8	36.6	16.9	2.7	0.01	>0	
18	5	992033	8	1.9	13.8	18.7	35.0	23.7	6.8	0.1	>0	
19	5	2.406329	8	1.3	10.0	15.0	31.6	27.9	13.1	1.0	0.02	
20	5	5.730955	9	1.0	7.4	11.7	27.2	29.4	19.9	3.4	1.1	.
15	6	350097	6	7.0	42.7	33.2	16.7	0.3	>0			
16	6	1.413251	6	4.4	32.1	33.4	27.9	2.1	0.01			
17	6	5.708158	7	2.7	23.1	29.7	36.7	7.5	0.2	>0		
18	6	22.903161	8	1.8	16.1	24.4	40.2	16.5	1.0	>0	.	
19	6	90.699398	8	1.0	11.0	18.6	38.7	26.2	4.4	0.02	.	
20	6	352.749035	8	0.7	7.4	13.7	33.6	33.2	11.1	0.3	>0	
15	7	901491	5	9.6	57.7	28.0	4.67	>0				
16	7	5.985278	6	5.9	44.8	36.0	13.2	0.07	.			
17	7	41.175203	6	3.4	31.9	36.9	26.7	1.1	>0			
18	7	287.813284	7	2.0	21.6	32.2	38.4	5.8	0.02	.		
19	7	2009.864185	8	1.1	13.9	25.2	43.6	15.7	0.4	.	.	
20	7	13848.061942	8	0.7	8.8	18.2	41.6	27.9	2.8	.		
15	8	957357	4	14.8	71.3	13.6	0.3					
16	8	10.174566	5	8.8	61.2	27.3	2.7	.				
17	8	119.235347	6	5.0	46.3	38.1	10.5	>0	.			
18	8	1482.297912	6	2.8	31.6	40.1	24.9	0.5	.			
19	8	18884.450721	7	1.5	20.3	34.6	39.3	4.2	>0	.		
20	8	240477.821389	8	0.8	12.6	26.1	46.5	13.9	0.1	.	.	
15	9	428260	4	23.9	73.4	2.6	>0					
16	9	6.592538	4	14.6	74.5	10.8	0.1					
17	9	123.424635	5	8.2	64.1	26.1	1.5	.				
18	9	2647.026212	6	4.5	47.8	39.5	8.2	>0	.			
19	9	61154.777955	6	2.4	32.1	42.7	22.5	0.2	.			
20	9	1.453217.697135	7	0.8	12.6	26.1	46.5	13.9	0.1	>0	.	
15	10	94177	4	36.5	63.4	0.1	.					
16	10	1.778699	4	24.0	74.5	1.5	>0					
17	10	46.354490	4	8.2	64.2	26.1	1.5					
18	10	1564.547344	4	8.0	66.8	24.4	0.8					
19	10	62319.506255	5	4.3	49.8	40.0	5.9	>0				
20	10	2.702716.939976	6	2.3	33.0	45.2	19.4	>0	.			

Table 1: Distribution (in %) of the minimum distance of binary linear (n, k)-codes.

Finally we want to present some results about the distribution of the minimum distance among binary linear codes of given parameters n and k which were generated uniformly at random using the algorithm above. For each pair of parameters (n, k) we were computing the minimum distance of 500000 codes of length n and dimension $\leq k$. The results are collected in table 1. S_{nk2}

indicates the number of isometry classes of linear (n,k)-codes over $GF(2)$ without 0-columns. Furthermore $d_2 = d_2(n,k)$ stands for the maximal value that occurs as the minimum distance of linear (n,k)-codes over $GF(2)$. Tables of $d_q(n,k)$ can be found in [2]. In the right half of table 1 for each $d \leq d_2(n,k)$ the percentage of codes with minimum distance d is indicated. We can deduce that in general the percentage of codes with maximal minimum distance is very small. In some cases indicated with "." in table 1 there was even no code with parameters (n,k,d) produced after having generated 500000 codes.

Acknowledgment: The author wants to thank both Prof. Adalbert Kerber and Prof. Jens Schwaiger for their guidance and support while preparing this article.

References

[1] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, and K.-H. Zimmermann. *Codierungstheorie — Konstruktion und Anwendung Linearer Codes.* Springer, Berlin, Heidelberg, New York, 1998. ISBN 3-540-64502-0.

[2] A.E. Brouwer. Bounds on the minimum distance of linear codes, `http://www.win.tue.nl/math/dw/voorlincod.html`.

[3] J.D. Dixon and H.S. Wilf. The random selection of unlabeled graphs. *J. Algorithms*, 4: 205 – 213, 1983.

[4] H. Fripertinger. Enumeration of isometry classes of linear (n,k)-codes over $GF(q)$ in SYMMETRICA. *Bayreuth. Math. Schr.*, 49: 215 – 223, 1995. ISSN 0172-1062.

[5] H. Fripertinger. Zyklenzeiger linearer Gruppen und Abzählung linearer Codes. *Sém. Lothar. Combin.*, Actes 33: 1 – 10, 1995. ISSN 0755-3390.

[6] H. Fripertinger. Enumeration of Linear Codes by Applying Methods from Algebraic Combinatorics. *Grazer Math. Ber.*, 328: 31 – 42, 1996.

[7] H. Fripertinger. Cycle Indices of Linear, Affine and Projective Groups. *Linear Algebra Appl.*, 263: 133 – 156, 1997.

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

[9] W. Heise and P. Quattrocchi. *Informations- und Codierungstheorie.* Springer Verlag, Berlin, Heidelberg, New York, Paris, Tokio, 1989. second edition.

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

[11] A. Kerber. Algebraic Combinatorics in Bayreuth. *Sém. Lothar. Combin.*, B34j, 1995. `http://cartan.u-strasbg.fr/~slc/`.

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

[13] H. Lehmann. Das Abzähltheorem der Exponentialgruppe in gewichteter Form. *Mitt. Math. Sem. Giessen*, 112: 19 – 33, 1974.

[14] H. Lehmann. *Ein vereinheitlichender Ansatz für die REDFIELD – PÓLYA – de BRUIJNSCHE Abzähltheorie.* PhD thesis, Universität Giessen, 1976.

[15] 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".
`http://www.mathe2.uni-bayreuth.de/axel/symneu_engl.html`.

Harald Fripertinger
Institut für Mathematik
Karl Franzens Universität Graz
Heinrichstr. 36/4
A–8010 Graz, AUSTRIA