Mathematica
Balkanica

New Series Vol. 18, 2004, Fasc. 1-2

On the $[10,5,6]_9$ Reed-Solomon and Glynn Codes[1]

Tsonka Baicheva[2], *Iliya Bouyukliev*[2], *Stefan Dodunekov*[3], *Wolfgang Willems*[4]

MDS codes with the same parameters $[n,k,d]_q$ look very similiar. In particular they have the same weight distribution. So we may ask for invariants they might differ. In this note we compare in detail the $[10,5,6]_9$ Reed-Solomon and the $[10,5,6]_9$ Glynn code which are the only two inequivalent $[10,5,6]_9$ codes. It turns out that both codes differ in the geometry but have the same weight distribution on coset leaders as computer computations show. In particular they perform equally good with respect to error detection and error correction.

AMS Subj. Classification: 94B60.

Key Words: Reed-Solomon codes, MDS codes, Glynn code, arc, self-dual code, code equivalence.

1. Introduction

Let $I\!F_q^n$ denote the vector space of n-tuples over the field $I\!F_q$ with q elements. A q-ary linear code $\mathcal{C}$ of length n and dimension k, or an $[n,k]_q$ code, is a k-dimensional subspace of $I\!F_q^n$. The Euclidean inner product of two vectors $\mathbf{u} = (u_1, u_2, \ldots u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ in $I\!F_q^n$ is defined by

$$\mathbf{uv} = u_1v_1 + u_2v_2 + \ldots + u_nv_n.$$

Two vectors are said to be orthogonal if their inner product is 0. The set of all vectors of $I\!F_q^n$ orthogonal to all codewords in $\mathcal{C}$ is called the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$, i.e.,

$$\mathcal{C}^\perp = \{\mathbf{x} \in I\!F_q^n | \mathbf{xy} = 0 \text{ for any } \mathbf{y} \in \mathcal{C}\}.$$

By a well-known fact from linear algebra, the code $\mathcal{C}^\perp$ is a linear $[n, n-k]_q$ code.

[1] Partially supported by the Bulgarian National Science Fund under Contracts MM901/1999 and MM1304/2003.

A k-by-n matrix $\mathbf{G}_{\mathcal{C}}$ having as rows the vectors of a basis of $\mathcal{C}$ is called a generator matrix of $\mathcal{C}$. A generator matrix $\mathbf{H}_{\mathcal{C}}$ of the dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$ is a parity check matrix of minimal rank for $\mathcal{C}$.

The number of nonzero positions in a vector $\mathbf{x} \in \mathbb{F}_q^n$ is called the Hamming weight $\mathrm{wt}(\mathbf{x})$ of $\mathbf{x}$. The Hamming distance $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is defined by

$$d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$$

and the minimum distance of a linear code $\mathcal{C}$ by

$$d(\mathcal{C}) = \min\left\{d(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\right\} = \min\left\{\mathrm{wt}(\mathbf{c}) | \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\right\}.$$

A q-ary linear code of length n, dimension k and minimum distance d is referred to an $[n, k, d]_q$ code.

A *coset* of the code $\mathcal{C}$, determined by the vector $x \in \mathbb{F}_q^n$, is the set $x + \mathcal{C} = \{x + c \mid c \in \mathcal{C}\}$. A *coset leader* is a vector of smallest weight in its coset. We will denote by α_i for $i = 0, 1, \ldots, n$ the number of coset leaders of weight i.

The *covering radius* R of a code may be defined as the largest weight in a set of weights of coset leaders, or equivalently, as the smallest integer, such that the spheres of radius R around the codewords cover $\mathbb{F}_q^n$.

Cosets in which a minimum weight vector is unique are of special interest. The *Newton radius* ν of a code is the largest weight in the set of weights of unique coset leaders. This parameter determines the largest weight of a uniquely correctable error (see [1]).

In this note we investigate the Reed-Solomon code RS(10;9) and the Glynn code Gl(10;9) (see [2]) which are defined over the field $\mathbb{F}_9$. Note that these codes are inequivalent $[10, 5, 6]$ MDS codes. The Reed-Solomon is defined by a rational curve (i.e. a classical arc), the Glynn code by the so-called Glynn arc, the only example of a non-classical arc the authors are aware (see [2]). More precisely (see [3]), the Glynn arc is the only known $(q+1)$-arc in $PG(N, q)$, q odd, $2 \leq N \leq q - 2$, which is not a normal rational curve. In section 2 we collect some preliminary results and define the RS(10;9) and Gl(10;9) codes. In section 3 the geometry of both codes is studied. The last three sections are based on computer computations. In section 4 we compute the projections of the two codes over $GF(3)$ which depend on the generation of $\mathbb{F}_9$ over $\mathbb{F}_3$. Both codes have extensions to $[12, 6, 6]_9$ codes and we compute the inequivalent classes in section 5. Conclusions about the error detecting and error correcting performance of both codes are given in section 6.

2. Preliminaries

Definition 1 Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two linear $[n,k]_q$ codes. They are said to be equivalent if the codewords of $\mathcal{C}_2$ can be obtained from the codewords of $\mathcal{C}_1$ via a sequence of transformations of the following types:

(2.1) permutation on the set of coordinate positions;

(2.2) multiplication of all elements in a given position by a fixed non-zero element of $I\!\!F_q$;

(2.3) application of a field automorphism to all elements in all coordinate positions.

An automorphism of a linear code $\mathcal{C}$ is a sequence of transformations of type (2.1)–(2.3), which map each codeword of $\mathcal{C}$ onto another. The set of all automorphisms of a code $\mathcal{C}$ form a group, which is called the automorphism group $Aut(\mathcal{C})$ of the code.

Definition 2 A linear $[n,k,d]_q$ code with $d = n-k+1$ (i.e. meeting the Singleton bound) is called a maximum distance separable code, or an MDS code.

For detailed information on properties of MDS codes the reader is referred to [4,Chapter 11].

Taking the columns of a generator matrix of an $[n,k]_q$ code C we may associate to C a set of points of the projective geometry of dimension $k-1$ which we denote by $PG(k-1,q)$.

Definition 3 A κ-arc in $PG(N,q)$ is a set K of $\kappa \geq N+1 \geq 3$ points in $PG(N,q)$ such that no $N+1$ points of K lie in a hyperplane. Or in other words, any $N+1$ points of K form a basis of $PG(N,q)$.

Note that κ-arcs as columns of a generator matrix define MDS codes and vice versa. A normal rational curve is a set of points in the projective space $PG(N,q)$ $(1 \leq N \leq q-2)$ which is projectively equivalent to

$$\{(1:t:\ldots:t^N) \mid t \in I\!\!F_q\} \cup \{(0:0:\ldots:1)\}.$$

It is readily checked that every normal rational curve is a $(q+1)$-arc in $PG(N,q)$.

We consider MDS codes with parameters $[10,5,6]$ over $I\!\!F_9$. They correspond to 10-arcs in $PG(4,9)$. Glynn proved in [2] that there are exactly two non-equivalent 10-arcs in $PG(4,9)$. One of them is a rational curve and the other one is defined as the set of points

$$\{(1:x:x^2+bx^6:x^3:x^4)|x \in I\!\!F_9\} \bigcup \{(0:0:0:0:1)\}$$

where b is a non-square in $\mathbb{F}_9$.

The corresponding codes have the following generator matrices:

$$\mathbf{G}_{RS(10;9)} = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_9 & 0 \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_9^2 & 0 \\ \alpha_1^3 & \alpha_2^3 & \dots & \alpha_9^3 & 0 \\ \alpha_1^4 & \alpha_2^4 & \dots & \alpha_9^4 & 1 \end{pmatrix}$$

$$\mathbf{G}_{Gl(10;9)} = \begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_9 & 0 \\ \alpha_1^2 + b\alpha_1^6 & \alpha_2^2 + b\alpha_2^6 & \dots & \alpha_9^2 + b\alpha_9^6 & 0 \\ \alpha_1^3 & \alpha_2^3 & \dots & \alpha_9^3 & 0 \\ \alpha_1^4 & \alpha_2^4 & \dots & \alpha_9^4 & 1 \end{pmatrix},$$

where $\alpha_1, \alpha_2, \dots, \alpha_9$ are the elements of $\mathbb{F}_9$. Note that RS(10;9) and Gl(10;9) are not equivalent as codes (see [5], section 5.1). According to Proposition 1 from [6], it follows from the result of Glynn that these are the only non-equivalent $[10, 5, 6]_9$ codes. Since both codes are MDS codes with the same parameters they have the same weight distribution which is

$$1 + 1680z^6 + 2880z^7 + 14040z^8 + 22160z^9 + 18288z^{10}$$

(see [4, Chapter 11]). The automorphism groups of RS(10;9) and Gl(10;9), computed by Q-EXTENSION [7], have order 11520 resp. 5760 which also shows that the codes are non-equivalent. Note that by [8] the automorphism group of RS(10:9) is isomorphic to the group ($\mathbb{F}_9^*\times$ PGL(2,9))Gal($\mathbb{F}_9/\mathbb{F}_3$) which has order 11520. We would like to mention that the Frobenius map

$$(c_1, \dots, c_{10}) \to (c_1^3, \dots, c_{10}^3)$$

is not an automorphism of RS(10:9) (see Proposition 3). By [2] the automorphism group of the Gynn arc is PGL(2,9). Since |GL(10:9)| = 5760 the Gynn code has $\mathbb{F}_9^*\times$ PGL(2,9) as automorphism group.

3. Geometries

For codes over $\mathbb{F}_q$ where q is an even power of an arbitrary prime p one can consider two different types of inner products, namely the Euclidean and the Hermitean. The Euclidean (natural) was already defined in the first section. The Hermitean product of two vectors $\mathbf{u} = (u_1, u_2, \dots u_n)$ and $\mathbf{v} = (v_1, v_2, \dots, v_n)$ in $\mathbb{F}_q^n$ is defined by

$$(\mathbf{u}, \mathbf{v}) = u_1\bar{v}_1 + u_2\bar{v}_2 + \dots + u_n\bar{v}_n,$$

where $\bar{v}_i = v_i^{\sqrt{q}}$ for $v_i \in I\!F_q$. For $q = 9$ we have

$$(\mathbf{u}, \mathbf{v}) = u_1 v_1^3 + u_2 v_2^3 + \ldots + u_n v_n^3.$$

Proposition 1 *Let C be a $[q+1, \frac{q+1}{2}, \frac{q+3}{2}]_q$ code defined by a normal rational curve over $I\!F_q$ with q odd.*

a) C is Euclidean self-dual.

b) If q is a square then C is not Hermitean self-dual.

Proof. Let $d = \frac{q-1}{2}$. A generator matrix of C is given by

$$\mathbf{G}_C = \begin{pmatrix} 1 & 1 & \ldots & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_q & 0 \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_q^2 & 0 \\ \vdots & \vdots & & & \vdots \\ \alpha_1^{d-1} & \alpha_2^{d-1} & \ldots & \alpha_q^{d-1} & 0 \\ \alpha_1^d & \alpha_2^d & \ldots & \alpha_q^d & 1 \end{pmatrix}$$

a) If $\mathbf{z}$ denotes the last row of the generator matrix then

$$(\mathbf{z}, \mathbf{z}) = (\sum_{j=1}^{q} \alpha_j^{2d}) + 1 = 0.$$

Next we forget the last column in $\mathbf{G}_C$. The new matrix then defines a generalized Reed-Solomon code $GRS_{d+2}(\mathbf{a}, \mathbf{v})$ with $\mathbf{a} = (\alpha_1, \ldots, \alpha_q)$ and $\mathbf{v} = (1, \ldots, 1)$ (see [5], 1.2.10). By 3.1.3 of [5], we have

$$GRS_{d+2}(\mathbf{a}, \mathbf{v})^{\perp} = GRS_{d+1}(\mathbf{a}, \mathbf{v}')$$

where $\mathbf{v}' = (v_1', \ldots, v_q')$ with

$$v_k' = \prod_{i \neq k} \frac{1}{\alpha_k - \alpha_i}.$$

For $\alpha_k \neq 0$ this forces

$$1 = v_k' \prod_{i \neq k} (\alpha_k - \alpha_i) = v_k' \alpha_k^8 \prod_{i \neq k} (1 - \alpha_i \alpha_k^{-1}).$$

As $\alpha_k^8 = 1$ and

$$\prod_{i \neq k} (1 - \alpha_i \alpha_k^{-1}) = \prod_{b \in I\!F_q^*} b = -1$$

we get $v'_k = -1$ for $\alpha_k \neq 0$. This holds obviously also true for $\alpha_k = 0$. Thus

$$GRS_{d+2}(\mathbf{a},\mathbf{v})^{\perp} = GRS_{d+1}(\mathbf{a},\mathbf{v}') = GRS_{d+1}(\mathbf{a},-\mathbf{v}) = GRS_{d+1}(\mathbf{a},\mathbf{v})$$

which proves part a) of the proposition.

b) Let $\mathbf{u} = (\alpha_1^i, \ldots, \alpha_q^i, 0)$ and $\mathbf{v} = (\alpha_1^j, \ldots, \alpha_q^j, 0)$. We choose $i = \frac{q^2-q-2}{2}$ and $j = \frac{q+1}{2}$. The Hermitean inner product of these two vectors is

$$(\mathbf{u},\mathbf{v}) = \sum_{k=1}^{q^2} \alpha_k^i \alpha_k^{jq} = \sum_{k=1}^{q^2} \alpha_k^{i+jq} = \sum_{k=1}^{q^2} \alpha_k^{q^2-1} = -1.$$

■

Corollary 1 *The RS(10;9) code is self-dual with respect to the Euclidean but not with respect to the Hermitean inner product.*

Proposition 2 *The code Gl(10;9) is self-dual with respect to the Hermitean but not with respect to the Euclidean inner product.*

Proof. As a generator matrix for Gl(10;9) we may choose

$$\begin{pmatrix} 1 & 1 & \ldots & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_9 & 0 \\ \alpha_1^2 + b\alpha_1^6 & \alpha_2^2 + b\alpha_2^6 & \ldots & \alpha_9^2 + b\alpha_9^6 & 0 \\ \alpha_1^3 & \alpha_2^3 & \ldots & \alpha_9^3 & 0 \\ \alpha_1^4 & \alpha_2^4 & \ldots & \alpha_9^4 & 1 \end{pmatrix}.$$

a) The Euclidean inner product of the third row of the generator matrix with itself yields

$$\sum_{i=1}^{9} (\alpha_i^2 + b\alpha^6)^2 = (1+b^2)\sum_{i=1}^{9} \alpha_i^4 + 2b\sum_{i=1}^{9} \alpha_i^8 = 0 + b \neq 0.$$

Thus the Glynn code is not Euclidean self-dual.

b) Let $(\cdot\,,\cdot)$ denote the Hermitean inner product on $I\!\!F_9^{10}$. In order to prove that the Glynn code is Hermitean self-dual we have to show that

$$(\mathbf{u},\mathbf{v}) = 0$$

for the rows of a generator matrix. Since

$$(\mathbf{u},\mathbf{v})^3 = (\mathbf{v},\mathbf{u})$$

exactly 15 equations must be checked. The only critical equation is the inner product of the third row with itself which also turns out to be 0 since

$$\begin{array}{rcl} \sum_{i=1}^{9}(\alpha_i^2+b\alpha_i^6)(\alpha_i^6+b^3\alpha_i^2) & = & \sum_{i=1}^{9}\alpha_i^8+(b^3+b)\sum_{i=1}^{9}\alpha_i^4+b^4\sum_{i=1}^{9}\alpha_i^8 \\ & = & -1+0+(-1)(-1)=0. \end{array}$$

■

Since the (Euclidean) dual of a Reed-Solomon code is again a Reed-Solomon code, it follows from Proposition 2 that the dual of the Glynn code Gl(10;9) is equivalent to itself. The code Gl(10;9) is an interesting representative of the family q^H of Hermitean self-dual codes over F_{q^2} (see [9]).

Proposition 3 *Let C be an $[n,k,d=n-k+1]$ MDS code defined over the field $I\!F_{q^t}$ and $k \geq 2$. If $C^q = C$, i.e. C is invariant under the Frobenius map, then $d \leq q$.*

Proof. Let $0 \neq c \in C$ be a codeword of minimal weight. Changing c by a scalar in $I\!F_{q^t}$ we may assume that at least one entry of c is equal to 1. Since $c^q - c \in C$ and $\mathrm{wt}(c^q-c) < \mathrm{wt}(c)$ we get that c is a vector with entries in $I\!F_q$. Furthermore C has a generator matrix of the form

$$G = \begin{pmatrix} 1 & & & \\ & \ddots & & * \\ & & 1 & \end{pmatrix}.$$

Thus each row vector is a codeword of minimal weight. Therefore, by the above we may assume that G is a matrix over $I\!F_q$. Moreover G defines an MDS code over $I\!F_q$. Thus, by Lemma 4.4.3 of [5], we obtain $d \leq q$. ■

Now suppose that C is an $[q^2+1, \frac{q^2+1}{2}, \frac{q^2+3}{2}]$ MDS code defined over $I\!F_{q^2}$. If C is self-dual with respect to both the Euclidean and the Hermitean inner product than $C^q \subseteq C^\perp = C$ where $C^\perp$ is the dual with respect to the Euclidean form. Hence $C^q = C$ and an application of Proposition 3 yields a contradiction. This explains parts of Corollary 1 and Proposition 2.

By computer search we discovered

Proposition 4 *Let $f(x)$ be a polynomial of x over $I\!F_q$. The code with the following generator matrix*

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 0 \\ \alpha_1 & \alpha_2 & \dots & \alpha_9 & 0 \\ \alpha_1^2+f(\alpha_1) & \alpha_2^2+f(\alpha_2) & \dots & \alpha_9^2+f(\alpha_9) & 0 \\ \alpha_1^3 & \alpha_2^3 & \dots & \alpha_9^3 & 0 \\ \alpha_1^4 & \alpha_2^4 & \dots & \alpha_9^4 & 1 \end{pmatrix}$$

is Hermitean self-dual iff $f(x) = bx^6$, where b is a non-square in $\mathbb{F}_9$.

4. Projections to $\mathbb{F}_3$

Since $\mathbb{F}_9$ is a 2-dimensional vector space over $\mathbb{F}_3$ we may consider both the RS(10;9) and the Gl(10;9) code as ternary $[20, 10]$ codes which we call the projection to $\mathbb{F}_3$. These projections obviously have minimum distance $d \geq 6$. Furthermore they depend on the normed irreducible polynomial of degree two over $\mathbb{F}_3$ which defines the extension $\mathbb{F}_9$. There are three such polynomials and according to this there arise three projections, say C_1, C_2 and C_3. In the following table we present the correspondence between the generator polynomials and the projections.

Generator polynomials	x^2+1	x^2+x+2	x^2+2x+2
RS(10;9)	C_1	C_2	C_2
Gl(10;9)	C_2	C_3	C_3

The orders of the automorphism groups and the weight enumerators are as follows:

C_1 :

$|Aut(C_1)| = 2073600$

$1+120z^6+900z^8+40z^9+5184z^{10}+7200z^{11}+3600z^{12}+12960z^{13}+15120z^{14}+2400z^{15}+8100z^{16}+2880z^{17}+400z^{18}+144z^{20}$

C_2 :

$|Aut(C_2)| = 2073600$

$1+120z^6+4360z^9+26280z^{12}+25728z^{15}+2560z^{18}$

C_3 :

$|Aut(C_3)| = 518400$

$1+120z^6+450z^8+2200z^9+2592z^{10}+3600z^{11}+14940z^{12}+6480z^{13}+7560z^{14}+14064z^{15}+4050z^{16}+1440z^{17}+1480z^{18}+72z^{20}$

Since all weights of the codewords in C_2 are divisible by 3 the ternary code C_2 is Euclidean self-dual. The classification of ternary self-dual $[20, 10, 6]$ codes can be found in [10]. According to the list in that paper C_2 is equivalent to the code labelled by 24. This was checked by the computer package Q-EXTENSION.

5. Extensions

Usually codes which are optimal in some sense have a rigid structure and more often can not be extended. In our case using the computer package Q-EXTENSION we extended both codes to $[12, 6, 6]_9$ codes. From RS(10;9) code we have obtained 8 inequivalent codes and from Gl(10;9) code 7 inequivalent codes. The orders of the automorphism groups and the weight enumerators are as follows:

Codes obtained from RS(10;9)

$|Aut| = 32$

$1 + 1824z^6 + 4032z^7 + 21240z^8 + 56720z^9 + 120168z^{10} + 182016z^{11} + 145440z^{12}$

$|Aut| = 64$

$1 + 1856z^6 + 3840z^7 + 21720z^8 + 56080z^9 + 120648z^{10} + 181824z^{11} + 145472z^{12}$

$|Aut| = 16$

$1 + 1832z^6 + 3984z^7 + 21360z^8 + 56560z^9 + 120288z^{10} + 181968z^{11} + 145448z^{12}$

$|Aut| = 16$

$1 + 1848z^6 + 3888z^7 + 21600z^8 + 56240z^9 + 120528z^{10} + 181872z^{11} + 145464z^{12}$

$|Aut| = 32$

$1 + 1832z^6 + 3984z^7 + 21360z^8 + 56560z^9 + 120288z^{10} + 181968z^{11} + 145448z^{12}$

$|Aut| = 32$

$1 + 1832z^6 + 3984z^7 + 21360z^8 + 56560z^9 + 120288z^{10} + 181968z^{11} + 145448z^{12}$

$|Aut| = 144$

$1 + 1848z^6 + 3888z^7 + 21600z^8 + 56240z^9 + 120528z^{10} + 181872z^{11} + 145464z^{12}$

$|Aut| = 11520$

$1 + 1920z^6 + 3456z^7 + 22680z^8 + 54800z^9 + 121608z^{10} + 181440z^{11} + 145536z^{12}$

Codes obtained from Gl(10;9)

$|Aut| = 16$

$1 + 1832z^6 + 3984z^7 + 21360z^8 + 56560z^9 + 120288z^{10} + 181968z^{11} + 145448z^{12}$

$|Aut| = 64$

$1 + 1856z^6 + 3840z^7 + 21720z^8 + 56080z^9 + 120648z^{10} + 181824z^{11} + 145472z^{12}$

$|Aut| = 64$

$1 + 1816z^6 + 4080z^7 + 21120z^8 + 56880z^9 + 120048z^{10} + 182064z^{11} + 145432z^{12}$

$|Aut| = 128$

$1 + 1792z^6 + 4224z^7 + 20760z^8 + 57360z^9 + 119688z^{10} + 182208z^{11} + 145408z^{12}$

$|Aut| = 64$

$1 + 1840z^6 + 3936z^7 + 21480z^8 + 56400z^9 + 120408z^{10} + 181920z^{11} + 145456z^{12}$

$|Aut| = 288$

$1 + 1848z^6 + 3888z^7 + 21600z^8 + 56240z^9 + 120528z^{10} + 181872z^{11} + 145464z^{12}$

$|Aut| = 46080$

$1 + 1920z^6 + 3456z^7 + 22680z^8 + 54800z^9 + 121608z^{10} + 181440z^{11} + 145536z^{12}$

A code with $d = n - k$ is called an Almost MDS code (see [11]). An almost MDS code for which the dual code is also almost MDS is called a Near

MDS code [12]. In our case all the codes are almost MDS, but not near MDS because the minimum distances of the corresponding dual codes are equal to 2.

Let Gol(12) denote the ternary extended $[12,6,6]$ Golay code. If we extend scalars to $\mathbb{F}_9$ we get a $[12,6,6]_9$ code, say C, as the following lemma shows.

Lemma *Let F/K denote a finite extension of fields where K is an arbitrary finite field. We denote by $C \otimes F$ the F-code obtained by extending scalars of the code C which is defined over K. Then the minimum distance of $C \otimes F$ is equal to the minimum distance of C.*

Proof. Let $\Gamma = \mathrm{Gal}(F/K)$ be the Galois group of F over K and let $0 \neq w \in C \otimes F$ be of minimum weight. As w is an F-linear combination of words in C we have $w^\sigma \in C \otimes F$ for any $\sigma \in \Gamma$. By multiplying w with a scalar if necessary we may assume that $0 \neq v = \sum_{\sigma \in \Gamma} w^\sigma$. Thus we have $v \in C$ and $\mathrm{wt}(v) \leq \mathrm{d}(C \otimes F)$. Therefore $\mathrm{d}(C) \leq \mathrm{d}(C \otimes F)$. The opposite inequality is obvious.

A natural question which arises is the following: "Is the $[12,6,6]_9$ code C among the codes in the two lists above?". By a computer check we found that the dual of C has minimum distance 6, hence is a Near MDS code which gives a negative answer to the question.

6. Error detecting and error correcting performance

The coset weight distributions of both RS(10;9) and Gl(10;9) codes were determined by computer calculations and it turned out that they coincide. The two codes have the following weight distribution of coset leaders

$$\alpha_1 = 80, \ \alpha_2 = 2880, \ \alpha_3 = 44960, \ \alpha_4 = 11128.$$

This implies that they have equal covering and Newton radii. The same holds true for the average error probability, since this probability is uniquely determined by the weight distribution of coset leaders. More precisely the covering radius is 4 and the Newton radius is 3. Both codes have 28800 unique coset leaders which are of weight 3. In particular the probabilities of an undetected error after t-error-correction are also the same (see [13]).

Acknowledgement

This work was started during a visit of the third author at the Institute for Algebra and Geometry at the Otto-von-Gruericke-University Magdeburg. He would like to thank his hosts for the nice working conditions and hospitality.

References

[1] T. Helleseth, T. Kløve and V. Levenshtein, The Newton radius of equidistant codes, *Proc. IEEE Intern. Symp. on Inform. Theory and its Applications*, Victoria, B.C., Canada, Sept. 17-30, 1996, 721-722.

[2] D. G. Glynn. The non-classical 10-arc of $PG(4,9)$, *Discrete Math.*, **59** (1986), 43-51.

[3] J. W. P. Hirschfeld, L. Storme. The packing problem in statistics, coding theory and finite projective spaces: update 2001. *Developments in Mathematics*, vol. 3, Kluwer Academic Publishers. Finite Geometries, *Proceedings of the Fourth Isle of Thorns Conference*, Chelwood Gate, July 16-21, 2000 (Eds. A. Blokhuis, J.W.P. Hirschfeld, D.Jungnickel and J.A. Thas), 201-246.

[4] F.J. MacWilliams, N.J.A. Sloane. *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[5] W. Willems. Codierungstheorie. *DeGruyter*, Berlin 1999.

[6] S. M. Dodunekov, J. Simonis. Codes and Projective Multisets, *Electronic Journal of Combinatorics*, **5**, 1998, R37, 23.

[7] I. Bouyukliev. 'Q-EXTENSION' - strategy in algorithms, *Proc. of the International Workshop on Algebraic and Combinatorial Coding Theory*, Bansko, 2000, 84-88.

[8] A. Dür. The automorphism groups of Reed -Solomon codes, *J. Combinatorial Theory*, Series A, **4** (1987), 69-82.

[9] E. M. Rains, N. J. A. Sloane, Self-dual codes, Chapter 3 in: V. S. Pless, W. C. Huffman, Eds. *Handbook of Coding Theory*, Elsevier, Amsterdam, New York, Oxford, 1998.

[10] V. S. Pless, N. J. A. Sloane, H. N. Ward. Ternary codes of minimum weight 6 and the classification of the self-dual codes of length 20, *IEEE Trans. Inform. Theory*, May, 1980, 305-316.

[11] M. A. de Boer. Almost MDS codes, *Designs, Codes and Cryptography*, 1996, 143-155.

[12] S. Dodunekov, I. Landgev. On near-MDS codes, *J. of Geometry*, **54** (1995), 30-34.

[13] T. Kasami, S. Lin. On the probability of undetected error for the Maximum Distance Separable codes, *IEEE Trans. Communications*, **32** (1984), 998-1006.

[2] *Institute of Mathematics and Informatics*
Bulgarian Academy of Sciences
P.O. Box 323, Veliko Tarnovo 5000, BULGARIA
e-mails: tsonka@moi.math.bas.bg, iliya@moi.math.bas.bg

Received 30.09.2003

[3] *Institute of Mathematics and Informatics*
Bulgarian Academy of Sciences
8 G.Bonchev st., 1113 Sofia, Bulgaria
e-mail: stedo@moi.math.bas.bg

[4] *Department of Mathematics*
University of Magdeburg
31016 Mageburg, Germany
e-mail: wolfgang.willems@mathematik.uni-magdeburg.de