Some codes related to BCH-codes of low dimension

Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany)
Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

December 2, 1998

Key Words

Optimal codes, BCH-codes, concatenation, residual codes, cyclotomic cosets.

Abstract

We construct a large number of record-breaking binary, ternary and quaternary codes. Our methods involve the study of BCH-codes over larger fields, concatenation, construction X and variants of the Griesmer construction (residual codes).

1 Review of the theory

Let $\mathbb{F}_q$ be the ground field, $F = \mathbb{F}_{q^2}$. Denote the interval $\{i, i+1, \ldots, j\} \subset \mathbb{Z}/(q^2-1)\mathbb{Z}$ by $[i, j]$. Let $A = [i, j] \subset \mathbb{Z}/(q^2-1)\mathbb{Z}$. Interval A determines a (primitive) BCH-code $\mathcal{C}(A)$ of length q^2-1 and minimum distance $\geq \mid A \mid +1$.

The dimension of $\mathcal{C}(A)$ is determined with the help of cyclotomic cosets. The cyclotomic coset containing $i \in \mathbb{Z}/(q^2-1)\mathbb{Z}$ is $Z(i) = \{i, qi\} \subset \mathbb{Z}/(q^2-1)\mathbb{Z}$. We have $\mid Z(i) \mid = 1$ if and only if $(q+1) \mid i$, $\mid Z(i) \mid = 2$ otherwise. $\mathbb{Z}/(q^2-1)\mathbb{Z}$ is the disjoint union of the different cyclotomic cosets. The dimension of $\mathcal{C}(A)$ is the sum of the cardinalities of the cyclotomic cosets, which intersect A trivially.

2 Tools

Aside of *concatenation* we also make use of construction X and of a variant of the Griesmer mechanism. We record construction X for linear codes (see [7]) in the following form:

Theorem 1 (construction X) *Let $\mathcal{C}_1 \supset \mathcal{C}_2$ be $q-$ary linear codes with parameters $[n, k+\kappa, d]$ and $[n, k, d+\delta]$, respectively. If there is a code $[e, \kappa, \delta]$, then a code $[n+e, k+\kappa, d+\delta]$ can be constructed as a lengthening of $\mathcal{C}_1$.*

We come to the Griesmer mechanism: Let $\mathcal{C}_1$ be a q-ary code $[n, k, d]$ with basis $\{v_1, \dots, v_k\}$, where $wt(v_1) = d$. Consider the code generated by $\{v_2, \dots, v_k\}$, project to the coordinates that do not belong to the support of v_1. This yields a code $[n-d, k-1, \lceil d/q \rceil]$. Let us call this process a *Griesmer step.* Repeated application yields to the celebrated *Griesmer bound:* $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$.
The following generalization has been used in [8] for binary codes.

Theorem 2 *Let $\mathcal{C}$ be a q-ary linear code with parameters $[n, k, d]$ and $v \in \mathcal{C}$ of weight w. Assume $d - w + \lceil w/q \rceil > 0$. Then there is a code $[n-w, k-1, d-w+\lceil w/q \rceil]$ (the* **residual code***) obtained by projecting a subcode of $\mathcal{C}$ to the coordinates which do not belong to the support of v.*

Proof: Proceed as in a Griesmer step, based on the word $v = v_1$ of weight w. Complete v_1 to a basis $\{v_1, \dots, v_k\}$, let $\mathcal{D}$ be the code obtained by projecting $< v_2, \dots, v_k >$ to the coordinates which do not belong to the support of v. Let x be a nonzero word of $\mathcal{D}$ having weight w' after projection to $\mathcal{D}$. We want a lower bound on w'. It can be assumed that the nonzero entries of v are 1. Denote by δ_i the number of coordinates in the support of v, where x has entry $i \in \mathbb{F}_q$. As $x - i \cdot v$ is a nonzero word of $\mathcal{C}$ we get

$wt(x - i \cdot v) = w' + w - \delta_i \geq d$, or $w' \geq d - w + \delta_i$. As the mean value of the δ_i is w/q, our claim concerning the minimum distance of the residual code is proved. The same considerations also show that the residual code does indeed have dimension $k-1$. ■

3 A family of low-dimensional BCH-codes

Let $A_1 = [1, q^2 - q - 3], A_2 = [1, q^2 - q - 2], A_3 = [1, q^2 - 1]$. The cyclotomic cosets $\{-1, -q\}$ and $\{-(q+1)\} = \{q^2 - q - 2\}$ show that the corresponding BCH-codes form a chain $\mathcal{C}(A_1) \supset \mathcal{C}(A_2) \supset \mathcal{C}(A_3)$ with parameters

$$[q^2 - 1, 3, q^2 - q - 2] \supset [q^2 - 1, 2, q^2 - q - 1] \supset 0.$$

Let $B_i = \{0\} \cup A_i, i = 1, 2, 3$. Then $\mathcal{C}(B_i)$ contains $\mathcal{C}(A_i)$ with codimension 1. Application of Theorem 1 to the chain $\mathcal{C}(A_1) \subset \mathcal{C}(B_1)$ with $[1, 1, 1]$ as auxiliary code produces a chain of codes as follows:

Lemma 1 *The extended BCH-codes* $\mathcal{C}_i = \tilde{\mathcal{C}}(A_i), i = 1, 2, 3$ *form a chain* $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$ *of linear* $q-$*ary codes with parameters*

$$[q^2, 4, q^2 - q - 1] \supset [q^2, 3, q^2 - q] \supset [q^2, 1, q^2].$$

We will use Lemma 1 to obtain new binary and ternary codes.

3.1 A geometrical description

As the coordinate functions of a linear code are linear functionals it is always possible to describe a k-dimensional linear q-ary code $\mathcal{C}$ in the following way (see [4]): the code words are parametrized by elements $x \in \mathbb{F}_q^k$, the coordinates by elements $\gamma \in \Gamma$, where Γ is an n-element subset of $\mathbb{F}_q^k$. The corresponding entry is $x \cdot \gamma$. Here we make use of the standard scalar product. It is clear that $\mathcal{C} = \mathcal{C}(\Gamma)$ has dimension k if and only if Γ generates the vector space $\mathbb{F}_q^k$. If $0 \notin \Gamma$, then $\mathcal{C}$ has no zero-column, equivalently $d'(\mathcal{C}) > 1$. Further $\mathcal{C}$ is projective ($d'(\mathcal{C}) \geq 3$) if and only if no two elements of Γ are multiples of each other. If $\mathcal{C}$ is projective we can consider Γ as a subset of the projective space $\mathcal{P}_{k-1}(q)$. Multiplying an element of Γ by a nonzero constant produces an equivalent code. The weight of x in $\mathcal{C}(\Gamma)$ is given by

$$wt(x) = n- \mid x^{\perp} \cap \Gamma \mid .$$

Consider the extended BCH-codes from Lemma 1. The 3-dimensional code $\mathcal{C}_2$ has the same weight-distribution as $\mathcal{C}(\Gamma)$, where Γ is the affine plane. As the dual distance is computable from the weight-distribution and $\mathcal{C}($ affine plane $)$ is projective, it follows that $\mathcal{C}_2$ and $\mathcal{C}_1$ are projective. Write $\mathcal{C}_1 = \mathcal{C}(\Gamma)$ and study the q^2-set Γ, which we consider as a subset of the 3-dimensional projective geometry. We want to show that no three points of Γ are collinear, equivalently $d'(\mathcal{C}_1) > 3$. As $d(\mathcal{C}_1) = q^2 - q - 1$, we have that every plane intersects Γ in at most $q+1$ points. Assume a line l meets Γ in $x \geq 2$ points. Counting points of Γ on the $q+1$ planes through l we g $q^2 \leq x + (q+1)(q+1-x)$. It follows $x \leq 2$. It is well-known that sets of points in $\mathcal{P}_3(q)$ with this property (no three on a line) have at most q^2+1 points. In the case of equality one speaks of **ovoids.** Examples of ovoids are elliptic quadrics. Choose coordinates such that $P_4 = (0,0,0,1)$ generates $\mathcal{C}_3$, together with P_2 and P_3 (using obvious notation) $\mathcal{C}_2$ is generated, and let finally $P_1 = (1,0,0,0)$ have weight $q^2 - q - 1$ in $\mathcal{C}_1$. As $wt(P_4) = q^2$ we have that $P_4^{\perp} =< P_1, P_2, P_3 >$ intersects Γ in the empty set. In particular $P_1 \notin \Gamma$. As $\mathcal{C}_2$ has minimum weight $q^2 - q$, it follows that planes through P_1 contain at most q points of Γ. The usual counting argument shows that P_1 is not collinear with any two points of Γ. It follows that $\mathcal{O} = \Gamma \cup \{P_1\}$ is an ovoid. If we add a $(q^2+1)-st$ column $(1,0,0,0)^t$ to the generator matrix of $\mathcal{C}_1$ we get an ovoid-code $\mathcal{C}(\mathcal{O})$. Our extended BCH-code $\mathcal{C}_1$ is a shortening of $\mathcal{C}(\mathcal{O})$. The weight-distribution of these codes is now easily determined: every plane E either is a tangent plane of $\mathcal{O}$ (meets $\mathcal{O}$ in one point) or it meets $\mathcal{O}$ in $q+1$ points. Furthermore every point of $\mathcal{O}$ is on precisely one tangent plane. This shows that the weight-distribution of $\mathcal{C}(\mathcal{O})$ is as follows:

$$A_0 = 1, A_{q^2-q} = q(q-1)(q^2+1), A_{q^2} = (q-1)(q^2+1).$$

The weight distribution of $\mathcal{C}_1$ is easily determined from this. We record this in the following Lemma:

Lemma 2 *The 4-dimensional extended q-ary BCH-code $\mathcal{C}_1 = \tilde{\mathcal{C}}(A_1)$ as described in Lemma 1 is obtained by shortening from an ovoid code. Its weight-*

distribution is

$$A_0 = 1, A_{q^2-q-1} = q^2(q-1)^2, A_{q^2-q} = q(q^2-1),$$
$$A_{q^2-1} = q^2(q-1), A_{q^2} = q-1.$$

Call a code $[n,k,d]$ d-optimal if it is known that no code $[n,k,d+1]$ exists.

3.2 Case $q = 8, n = 2$.

Consider the chain from Lemma 1 in case $q = 8$. We know that the parameters of these 8-ary codes are

$$[64,4,55]_8 \supset [64,3,56]_8 \supset [64,1,64]_8$$

and their weight distributions are given by

$$A_{64}(\mathcal{C}_3) = 7, A_{56}(\mathcal{C}_2) = 504, A_{55}(\mathcal{C}_1) = 3136, A_{63}(\mathcal{C}_1) = 448.$$

$\mathcal{C}_3$ is generated by the all-1 word, the words in $\mathcal{C}_2 \setminus \mathcal{C}_3$ are just the words of weight 56, whereas the words in $\mathcal{C}_1 \setminus \mathcal{C}_2$ have weights 55 or 63.
The binary code $[7,3,4]_2$, a subcode of the Hamming code $[8,4,4]_2$, has constant weight 4. Using concatenation of the 8-ary codes above with this binary code yields binary codes $\mathcal{B}_1 \supset \mathcal{B}_2 \supset \mathcal{B}_3$ of parameters

$$[448,12,220]_2 \supset [448,9,224]_2 \supset [448,3,256]_2.$$

The weight distributions are immediate:

$$A_{256}(\mathcal{B}_3) = 7, A_{224}(\mathcal{B}_2) = 504, A_{220}(\mathcal{B}_1) = 3136, A_{252}(\mathcal{B}_1) = 448.$$

$\mathcal{B}_2$ and $\mathcal{B}_3$ meet the Griesmer bound with equality, are therefore length-optimal. Apply Theorem 2 to $\mathcal{B}_1$. Case $w = 220$ leads to a code

$$[228,11,110]_2.$$

These parameters are new. They are known to be d-optimal (see [5]). It follows that $\mathcal{B}_1$ is d-optimal as well. Case $w = 224$ leads to parameters

$$[224,11,108]_2.$$

These are new and d-optimal as well (for the optimality see [5] again). The weight-distribution is $A_0 = 1, A_{108} = 1372, A_{112} = 248, A_{124} = 392, A_{128} = 7, A_{140} = 28$. Using Theorem 2 with $w = 108$ and $w = 112$ leads to the new d-optimal cases

$$[116, 10, 54] \text{ and } [112, 10, 52].$$

Applying Theorem 2 with $w = 252$ and $w = 256$ to $\mathcal{B}_1$ leads to d-optimal codes $[196, 11, 94]$ and $[192, 11, 92]$. Codes with these parameters have been constructed in [3] using twisted BCH-codes.
Apply construction X to the pair $\mathcal{B}_1 \supset \mathcal{B}_2$. We can use binary codes $[4, 3, 2]_2$ or $[7, 3, 4]_2$. This yields codes

$$[452, 12, 222]_2 \text{ and } [455, 12, 224]_2.$$

The Griesmer bound shows that both are d-optimal. Application of Theorem 2 yields some optimal codes with known parameters. A Griesmer step yields a new code, with the same parameters in both cases:

$$[231, 11, 112]_2.$$

The Griesmer bound shows that this is d-optimal. After another Griesmer step we get another new d-optimal code with parameters

$$[119, 10, 56]_2.$$

Let us apply construction X to the pair $[455, 12, 224]_2 \supset [455, 3, 256]_2$, which we just constructed by lengthening of the pair $\mathcal{B}_1 \supset \mathcal{B}_3$. We use as auxiliary codes the d-optimal binary codes $[10, 9, 2], [14, 9, 4], [18, 9, 6], [21, 9, 8], [27, 9, 10], [30, 9, 12], [35, 9, 14], [44, 9, 18], [52, 9, 22], [60, 9, 26], [67, 9, 30]$. This yields the following binary codes:

$$[465, 12, 226], [469, 12, 228], [473, 12, 230], [476, 12, 232], [482, 12, 234],$$

$$[485, 12, 236][490, 12, 238], [499, 12, 242], [507, 12, 246], [515, 12, 250], [522, 12, 254].$$

Griesmer steps yield new code parameters in a few cases:

$$[240, 11, 114]_2, [244, 11, 116]_2, [249, 11, 118]_2, [258, 11, 122]_2.$$

Apply construction X to the pair $\mathcal{U} \supset \mathcal{B}_2$, where $\mathcal{U}$ is a 10-dimensional subcode of $\mathcal{B}_1$, using $[4, 1, 4]$ as auxiliary code. This leads to a chain $[452, 10, 224]_2 \supset$

$[452, 3, 256]_2$. Applying construction X again in a second step, with $[8, 7, 2]$ as auxiliary code, yields a code $[460, 10, 226]_2$. An analogous procedure, based on an 11-dimensional subcode $\mathcal{U}$ of $\mathcal{B}_1$ and $[6, 2, 4]$ in the first step, and auxiliary codes $[9, 8, 2], [20, 8, 8], [51, 8, 24]$, respectively, in the second step, yields codes $[463, 11, 226]_2, [474, 11, 232]_2, [505, 11, 248]_2$. All these codes are rather good. One Griesmer step still yields the new parameters (eventually after addition of a parity check bit)

$$[235, 9, 114]_2, [238, 10, 114]_2, [242, 10, 116]_2, [257, 10, 124]_2.$$

Next we project the 8-ary codes $\mathcal{C}_j$ onto all but i coordinates. After concatenation with $[7, 3, 4]_2$ this yields a chain of binary codes

$$[448 - 7i, 12, 220 - 4i] \supset [448 - 7i, 9, 224 - 4i] \supset [448 - 7i, 3, 256 - 4i].$$

For small i these are good codes. Application of construction X to the first two members in the chain in case $i = 1$ with auxiliary code $[6, 2, 4]$ yields a chain $[447, 11, 220]_2 \supset [447, 3, 252]_2$. Another application of construction X with $[51, 8, 24]_2$ as auxiliary code produces the new code $[498, 11, 244]_2$. Even after a Griesmer step we get the new parameters $[254, 10, 122]_2$.
Observe that the largest code in the chain does contain words of weight $224 - 4i$. If we apply Theorem 2 in case $i = 1$ with this value of w we get the d-optimal code

$$[221, 11, 106].$$

Its weight distribution is $A_0 = 1, A_{106} = 993, A_{108} = 379, A_{110} = 186, A_{112} = 62, A_{122} = 324, A_{124} = 68, A_{126} = 6, A_{128} = 1$. Application of Theorem 2 with $w = 112$ yields the new parameters

$$[109, 10, 50].$$

As we know the weight distribution of the 8-ary codes it is possible to use Theorem 2 with different weights. Use case $i = 1$ with $w = 224$, case $i = 2$ with $w = 220$ and $w = 224$, and $i = 3$ with $w = 220$. This leads to the following codes:

$$[217, 11, 104]_2, [214, 11, 102]_2, [210, 11, 100]_2 \text{ and } [207, 11, 98]_2.$$

The first of these is d-optimal. Application of a Griesmer step to the second of these codes leads to new d-optimal parameters

$$[113, 10, 52]_2.$$

3.3 Case $q = 9, n = 2$.

We use Lemmas 1 and 2 in case $q = 9$. Concatenation with the code $[4, 2, 3]_3$ of constant weight 3 yields a chain $\mathcal{B}_1 \supset \mathcal{B}_2 \supset \mathcal{B}_3$

$$[324, 8, 213]_3 \supset [324, 6, 216]_3 \supset [324, 2, 243]_3.$$

The weight distributions are immediate:

$$A_{243}(\mathcal{B}_3) = 8, A_{216}(\mathcal{B}_2) = 720, A_{213}(\mathcal{B}_1) = 5184, A_{240}(\mathcal{B}_1) = 648.$$

Code $[324, 8, 213]_3$ is d-optimal. Application of Theorem 2 yields a new d-optimal ternary code

$$[108, 7, 69]_3$$

as well as the known parameters $[84, 7, 53]_3$ and $[81, 7, 51]_3$. Application of another Griesmer step yields some more known optimal codes. Application of construction X to the pair $\mathcal{B}_1 \supset \mathcal{B}_2$ using the auxiliary code $[4, 2, 3]_3$ yields $[328, 8, 216]_3$. After a Griesmer step we get a new length-optimal code

$$[112, 7, 72]_3.$$

In the same manner the pair $[328, 8, 216]_3 \supset [328, 2, 243]_3$, with auxiliary codes $[12, 6, 6], [15, 6, 7], [26, 6, 15]$ yields codes

$$[340, 8, 222]_3, [343, 8, 223]_3 \text{ and } [354, 8, 231]_3,$$

which after one Griesmer step produce the following new ternary parameters:

$$[118, 7, 74]_3, [120, 7, 75]_3 \text{ and } [123, 7, 77]_3.$$

Projecting the 9-ary codes $\mathcal{C}_j$ and concatenating with the ternary $[4, 2, 3]$ yields a chain of ternary codes $[324-4i, 8, 213-3i] \supset [324-4i, 3, 216-3i] \supset [324-4i, 2, 243-3i]$. Codes $[320, 8, 210]_3$ and $[316, 8, 207]_3$ are d-optimal. We apply Theorem 2 with $w = 216$ in cases $i = 1$ and $i = 2$, (it is in fact easy to see that words of weight w exist in these codes). This yields the following d-optimal parameters:

$$[104, 7, 66]_3, [100, 7, 63]_3.$$

3.4 Case $q = 16, n = 2$.

We consider the ovoid code. After concatenation with a quaternary code $[5, 2, 4]$ this yields a quaternary $[1285, 8, 960]_4$. Griesmer steps yield quaternary codes $[325, 7, 240]_4$ and $[85, 6, 60]_4$. The last of these codes achieves the largest known minimum distance, the upper bound being $d = 61$.

4 More quaternary and binary codes

In [2] we have developed a theory of general BCH-codes and constructed related codes which arise out of these codes by lengthening and extending. We consider here the primitive quaternary BCH-codes $\mathcal{C}(t)$ of length 63 with designed distance $t + 1$. Codes $\mathcal{C}(t)$ with $t \in \{41, 42, 46\}$ form a chain $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$ with parameters $[63, 8, 42]_4 \supset [63, 7, 43]_4 \supset [63, 4, 47]_4$. Moreover we consider the general (non narrow-sense) BCH-code $\mathcal{U}_1$ with defining interval $[0, 42]$. Then $\mathcal{U} \subset \mathcal{C}_1$. This code has parameters $[63, 7, 43]_4$ and it meets the $\mathcal{C}_i, i = 2, 3$ in BCH-codes with parameters $[63, 6, 44]_4$ and $[63, 3, 48]_4$. Apply concatenation with $[3, 2, 2]_2$. We get chains $\tilde{\mathcal{C}_i}$ and $\tilde{\mathcal{U}_i}$ of binary codes with parameters $[189, 16, 84]_2 \supset [189, 14, 86]_2 \supset [189, 8, 94]_2$ and $[189, 14, 86]_2 \supset [189, 12, 88]_2 \supset [189, 6, 96]_2$, respectively. Apply construction X to the pair $\tilde{\mathcal{C}_i} \supset \tilde{\mathcal{U}_i}$, with $[3, 2, 2]$ as auxiliary code. The images of the $\tilde{\mathcal{C}_i}$ after lengthening form a chain $[192, 16, 86]_2 \supset [192, 14, 88]_2 \supset [192, 8, 96]_2$. Apply construction X to the larger of these codes (where in fact we replace the largest code by a subcode of codimension one), with $[2, 1, 2]$ as auxiliary code. We get a pair of codes $[194, 15, 88]_2 \supset [194, 8, 96]_2$. Finally we apply construction X a last time. Choosing as auxiliary code binary codes with parameters $[8, 7, 2], [12, 7, 4], [16, 7, 6]$ and $[19, 7, 8]$ in turn we get as a final result four new binary codes:

$$[202, 15, 90]_2, [206, 15, 92]_2, [210, 15, 94]_2, [213, 15, 96]_3.$$

Consider the primitive quaternary BCH-codes of designed distances 43 and 47. They form a chain $[63, 7, 43]_4 \supset [63, 4, 47]_4$. After concatenation with the code $[3, 2, 2]_2$ we get binary codes $[189, 14, 86]_2 \supset [189, 8, 94]_2$. Using construction X with auxiliary code $[16, 5, 8]$ yields a new binary code $[205, 13, 94]_2$.

5 Parameters of new linear codes

For the convenience of the reader we collect the new parameters of linear codes constructed in this paper. More codes of interest may be obtained by standard constructions like shortening, puncturing and residues (Griesmer steps).

q	code parameters	section
2	[448,12,220]	3.2
2	[448,9,224]	3.2
2	[224,11,108]	3.2
2	[116,10,54]	3.2
2	[112,10,52]	3.2
2	[452,12,222]	3.2
2	[455,12,224]	3.2
2	[460,10,226]	3.2
2	[463,11,226]	3.2
2	[465,12,226]	3.2
2	[469,12,228]	3.2
2	[473,12,230]	3.2
2	[474,11,232]	3.2
2	[476,12,232]	3.2
2	[482,12,234]	3.2
2	[485,12,236]	3.2
2	[490,12,238]	3.2
2	[499,12,242]	3.2
2	[498,11,244]	3.2
2	[507,12,246]	3.2
2	[505,11,248]	3.2
2	[515,12,250]	3.2
2	[522,12,254]	3.2
2	[221,11,106]	3.2
2	[109,10,50]	3.2
2	[217,11,104]	3.2
2	[214,11,102]	3.2

q	code parameters	section
2	[210,11,100]	3.2
2	[207,11,98]	3.2
3	[324,8,213]	3.3
3	[324,6,216]	3.3
3	[108,7,69]	3.3
3	[328,8,216]	3.3
3	[340,8,222]	3.3
3	[343,8,223]	3.3
3	[354,8,231]	3.3
3	[320,8,210]	3.3
3	[316,8,207]	3.3
3	[104,7,66]	3.3
3	[100,7,63]	3.3
4	[1285,8,960]	3.4
2	[202,15,90]	4
2	[206,15,92]	4
2	[210,15,94]	4
2	[213,15,96]	4
2	[205,13,94]	4

References

[1] J.Bierbrauer, Y.Edel: *New code-parameters from Reed-Solomon subfield codes, IEEE Transactions on Information Theory* **43**(1997),953-968.

[2] J.Bierbrauer, Y.Edel: *Extending and lengthening BCH-codes, Finite Fields and Their Applications* **3**(1997),314-333.

[3] Y.Edel, J.Bierbrauer: *Twisted BCH-codes, Journal of Combinatorial Designs* **5** (1997), 377-389.

[4] R. Calderbank, W.M. Kantor: *The geometry of two weight-codes,* Bull.London Math.Soc (1986),97-122.

[5] S.M. Dodunekov, S.B. Encheva, A.I. Ivanov: *New bounds on the minimum length of binary linear block codes,* Report LiTH-ISY-I-1283, Linköping Univ., Sweden, 11 Nov. 1991.

[6] F.R.Kschischang, S.Pasupathy: *Some ternary and quaternary codes and associated sphere packings, IEEE Trans. Information Theory,* 38(1992), 227-246.

[7] F. J. MacWilliams, N. J. A. Sloane: *The Theory of Error-Correcting Codes,* North-Holland, 1977.

[8] B.Groneick, S.Grosse: *New binary codes,* IEEE Transactions on Information Theory 40(1994), 510-512.