New codes via the lengthening of BCH codes with UEP codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA),
Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany),
Ludo Tolhuizen
Philips Research Laboratories
Prof. Holstlaan 4
5656 AA Eindhoven (The Netherlands)

Abstract

We describe a code lengthening technique that uses Unequal Error Protection codes as suffix codes and combine it with iteration of the conventional Construction X. By applying this technique to BCH codes, we obtain 5 new binary codes, 13 new ternary codes and 13 new quaternary codes. An improvement of Construction XX yields 2 new ternary codes.

1 Introduction

The first two authors applied several lengthening techniques to BCH-codes in [3, 4] and obtained linear codes with new parameters. A different rather sophisticated lengthening method was introduced in [10]. The suffix codes used in this technique are known in literature as unequal error protection (UEP) codes (see [5, 9]). The third author used this method for the construction of linear codes with new parameters [8, Ch. 6].

In this paper we combine lengthening of UEP codes and the "iteration of Construction X" from [4]. Starting from BCH codes, we obtain 5 new binary codes, 13 new ternary codes and 13 new quaternary codes. (In fact, three of the quaternary codes already appeared in [8, Ch. 6]). The paper is organized as follows.

In Section 2, we define two-level UEP codes and give two constructions for such codes. In Section 3, we describe the basic lengthening technique and show the usefulness of UEP codes in this construction. We also briefly recall the "iteration of Construction X" from [4]. In Section 4, we apply the results of Sections 2 and 3 to the lengthening of BCH codes. In the final section, we improve Construction XX from [1] and obtain two new ternary codes.

2 Unequal Error Protection Codes

The intention of unequal error protection codes (or briefly UEP codes) is to offer a larger error protection to more important message symbols than to less important ones [5, 9]. As shown in [10] and in the next section, UEP codes can advantageously be applied in code lengthening techniques. In this paper we restrict ourselves to two-level UEP codes. For our purposes, the following definition is most suited.

Definition 1 *Let $D > d$. An $[n, k]$ code $\mathcal{C}$ is an $[n, k, (D^m, d^{k-m})]$ code if it has minimum distance at least d and it contains an $(k-m)$-dimensional subcode $\mathcal{D}$ such that any word of $\mathcal{C} \setminus \mathcal{D}$ has weight at least D.*

We continue with two constructions of two-level UEP codes.

Definition 2 *Let the q-ary codes $\mathcal{C}_1$ and $\mathcal{C}_2$ have lengths n_1 and n_2, respectively, and let $i < min(n_1, n_2)$. The code $\mathcal{C}_1 \vee_i \mathcal{C}_2$ of length $n_1 + n_2 - i$ is defined as*

$$\mathcal{C}_1 \vee_i \mathcal{C}_2 = \{(u_1, \ldots, u_{n_1-i}, u_{n_1-i+1}+v_1, \ldots, u_{n_1}+v_i, v_{i+1}, \ldots, v_{n_2}) \mid \mathbf{u} \in \mathcal{C}_1, \mathbf{v} \in \mathcal{C}_2\}.$$

Note that $\mathcal{C}_1 \vee_0 \mathcal{C}_2$ is simply the direct sum of $\mathcal{C}_1$ and $\mathcal{C}_2$.

Lemma 1 *Let $\mathcal{C}_j$ be a q-ary $[n_j, k_j, d_j]$ code, $j = 1, 2$. Assume that $d_2 < d_1$ and $2i \leq d_1$. Then $\mathcal{C} = \mathcal{C}_1 \vee_i \mathcal{C}_2$ is an $[n, k_1 + k_2, (D^{k_1}, d_2^{k_2})]$ code, where $n = n_1 + n_2 - i$ and $D = min(d_1, d_1 + d_2 - 2i)$.*

Proof: Let $\mathbf{u} \in \mathcal{C}_1$, $\mathbf{v} \in \mathcal{C}_2$, and consider

$$\mathbf{x} = (u_1, \ldots, u_{n_1-i}, u_{n_1-i+1} + v_1, \ldots, u_{n_1} + v_i, v_{i+1}, \ldots, v_n).$$

If $\mathbf{u}=\mathbf{0}$ and $\mathbf{v} \neq \mathbf{0}$, then wt$(\mathbf{x}) \geq d_2$. If $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{v}=\mathbf{0}$, then wt$(\mathbf{x}) \geq d_1$. If $\mathbf{u}$ and $\mathbf{v}$ both are non-zero, then wt$(\mathbf{x}) \geq (d_1 - i) + (d_2 - i)$.
Hence, if $(\mathbf{u},\mathbf{v}) \neq (\mathbf{0},\mathbf{0})$, then wt$(\mathbf{x}) \geq \min(d_2, d_1, d_1 + d_2 - 2i) = d_2$. Moreover, take $\mathcal{D} = \{(0, \ldots, 0, v_1, \ldots, v_n) \mid \mathbf{v} \in \mathcal{C}_2\}$. If $\mathbf{x} \notin \mathcal{D}$, then $\mathbf{u} \neq 0$ and as shown above, wt$(\mathbf{x}) \geq \min(d_1, d_1 + d_2 - 2i)$. ∎

In particular, the quaternary $[8, 6, (3^3, 2^3)]$ code that was used in [8, Ch. 6] can be obtained as $[5, 3, 3] \vee_1 [4, 3, 2]$. To give another example, we can construct a quaternary $[9, 6, (4^3, 2^3)]$ code as $[6, 3, 4] \vee_1 [4, 3, 2]$.

Here is a second construction of a two-level UEP code.

Theorem 1 *Let $q = 2^f \geq 4$. Let $\omega_1, \omega_2, \ldots, \omega_{q-2}$ denote the elements of $\mathbf{F_q}$ different from 0 and 1. Let I denote the unit matrix of size $k-1$, and let J denote the $k-1 \times q-2$ matrix with all entries equal to one. The matrix*

$$G = \begin{pmatrix} 1 \ldots 1 & 0 \ldots 0 & \omega_1 \ldots \omega_{q-2} \\ I & I & J \end{pmatrix}$$

generates an $[2k + q - 4, k, ((k + q - 3)^1, 4^{k-1})]$ code.

Proof We take for $\mathcal{D}$ the code generated by the $(k-1)$ bottom rows of G. Let $\mathbf{m}=(m_1, \ldots, m_{k-1}) \in (\mathbf{F_q})^{\mathbf{k-1}}$ and let $m_0 \in \mathbf{F_q}$. Consider the codeword $\mathbf{c}$ defined by

$$\mathbf{c} = (m_0, \mathbf{m})G = (m_0\mathbf{1} + \mathbf{m}, \mathbf{m}, m_0(\omega_1, \ldots, \omega_{q-2}) + (\sum_{j=1}^{k-1} m_j)\mathbf{1}).$$

If $m_0 = 0$ and wt$(\mathbf{m}) \geq 2$, then wt$(\mathbf{c}) \geq 2$wt$(\mathbf{m}) \geq 4$. If $m_0 = 0$ and wt$(\mathbf{m})=1$, then $\sum_{j=1}^{k-1} m_j \neq 0$, and so wt$(\mathbf{c}) \geq 1 + 1 + (q-2) = q \geq 4$.
Now assume that $m_0 \neq 0$, so $\mathbf{c} \in \mathcal{C} \setminus \mathcal{D}$. Clearly, wt$(m_0\mathbf{1} + \mathbf{m})$ + wt$(\mathbf{m})$ $\geq k - 1$. Equality only holds if for $1 \leq i \leq k-1$, $m_i = 0$ or $m_i = m_0$. As

$\omega_1, \ldots, \omega_{q-2}$ are all distinct, $\mathbf{c}$ ends in $q-2$ distinct symbols, and so $\mathbf{c}$ ends in at least $q-3$ non-zero symbols. We conclude that wt$(\mathbf{c}) \geq (k-1)+(q-3)$. If equality would hold, then m_i would be in $\{0, m_0\}$ for all i, $1 \leq i \leq k-1$. This then would imply that $\sum_{i=1}^{k-1} m_i$ is either 0 or m_0, and in either case $\mathbf{c}$ ends in $q-2$ non-zero symbols. We conclude that wt$(\mathbf{c}) \geq k+q-3$ whenever $m_0 \neq 0$. ■

As an example, Theorem 1 yields a quaternary $[8, 4, (5, 4^3)]$ code.
Finally we construct two-level UEP codes by a variant of the familiar $(u, u+v)$-construction.

Theorem 2 *If q-ary codes $\mathcal{C}_i$ with parameters $[n_i, k_i, d_i], i = 1, 2$ exist, then a q-ary $[n_1 + max(n_1, n_2), k_1 + k_2, (d_2^{k_2}, (2d_1)^{k_1})]$ code exists.*

Proof: Let $u \in \mathcal{C}_1, v \in \mathcal{C}_2$. The linear mapping ϕ is defined on the direct sum of $\mathcal{C}_1$ and $\mathcal{C}_2$ by $\phi(u, v) = (u, u+v)$. Here the second component $u+v$ has length $\max(n_1, n_2)$. If $n_1 \neq n_2$, then the shorter of the vectors u, v is filled with zeroes at the end. Code $\mathcal{C}$ is defined as the image of ϕ. As ϕ obviously has trivial kernel, $\mathcal{C}$ has dimension $k_1 + k_2$. If $v = 0$, then $wt(u, u+v) = 2wt(u)$. If $v \neq 0$, then $wt(u, u+v) \geq wt(v)$.■

Choosing for $\mathcal{C}_1$ in Theorem 2 an $[i, i, 1]$ code or an $[i+1, i, 2]$ code leads to the following:

Corollary 1 *Let $\mathcal{C}$ be a q-ary $[n, k, d]$ code. There is a q-ary $[n+i, k+i, (d^k, 2^i)]$ code for all $i \leq n$. If $d \geq 4$ and $i+1 \leq n$, there is a q-ary $[n+i+1, k+i, (d^k, 4^i)]$ code.*

It may be noted that Theorem 2 can be generalized to allow the use of UEP codes as ingredients. We will not pursue this in the present paper. In Section 4 we will make use of the binary two-level UEP-code $[16, 8, (8, 4^7)]$ and of the ternary two-level UEP codes $[12, 8, (4^6, 2^2)]$ and $[8, 6, (3^2, 2^4)]$. These can be obtained from Corollary 1.

3 Code lengthening

In this section we describe the basic code lengthening technique known as Construction X ([7, Ch. 17, Sec. 7]). We point out the "iteration of Construction X" from [4] and show how *UEP* codes can advantageously be used in

Construction X. Throughout, $d(\mathcal{A})$ denotes the minimum Hamming distance of the code $\mathcal{A}$.

Let $\mathcal{C}$ be an $[n,k,d]$ code and let the suffix code $\mathcal{S}$ be an $[e,\kappa,\delta]$ code defined over the same field. To each word $x \in \mathcal{C}$, we append a suffix $s(x) \in \mathcal{S}$, and the extended code $E(\mathcal{C})$ is defined as

$$E(\mathcal{C}) = \{(x, s(x)) \mid x \in C\}.$$

If s induces a linear mapping (what we assume in the sequel), $E(\mathcal{C})$ is an $[n+e,k]$ code. We wish of course that $E(\mathcal{C})$ has large minimum weight. The most simple situation is the following. Suppose that $\mathcal{C}$ contains an $(k-\kappa)$-dimensional subcode $\mathcal{U}$ such that $d(\mathcal{U}) > d$. We choose s such that it has kernel U. If $x \notin \mathcal{U}$, then $\mathrm{wt}(x, s(x)) = \mathrm{wt}(x) + \mathrm{wt}(s(x)) \geq d + \delta$. If x is a non-zero word of $\mathcal{U}$, then $\mathrm{wt}(x, s(x)) = \mathrm{wt}(x) \geq d(\mathcal{U})$, and so

$$d(E(\mathcal{C})) \geq \min\{d+\delta, d(\mathcal{U})\}.$$

More generally, we define for any linear subcode $\mathcal{D}$ of $\mathcal{C}$ the extension $E(\mathcal{D})$ by

$$E(\mathcal{D}) = \{(x, s(x)) \mid x \in \mathcal{D}\}.$$

Obviously, $E(\mathcal{D})$ is linear whenever $\mathcal{D}$ is linear, and $E(\mathcal{A}) \subset E(\mathcal{B})$ whenever $\mathcal{A} \subset \mathcal{B}$. Reasoning similarly as above, we find that

$$d(E(\mathcal{D})) \geq \min\{d(\mathcal{D}) + \delta, d(\mathcal{U} \cap \mathcal{D})\}. \tag{1}$$

This is the result of "iteration of Construction X" [4].

The usefulness of UEP codes in code lengthening [10] is shown in the following theorem. We lengthen the code $\mathcal{C}_1$ with a suffix code $\mathcal{S}$.

Theorem 3 *Let $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$ be a chain of linear q-ary codes with parameters $[n,k_1,d_1] \supset [n,k_2,d_2] \supset [n,k_3,d_3]$, where $k_1 > k_2 > k_3, d_1 < d_2 < d_3$. Suppose that $\mathcal{S}$ is an $[e, k_1-k_3, ((d_3-d_1)^{k_1-k_2}, (d_3-d_2)^{k_2-k_3})]$ code. With an appropriate choice of $s, E(\mathcal{C}_1)$ is an $[n+e,k_1,d_3]$ code.*

Proof: Let $\mathcal{S}'$ be a subcode of $\mathcal{S}$ of dimension k_2-k_3 such that any word of $\mathcal{S} \setminus \mathcal{S}'$ has weight at least d_3-d_1. Choose the linear mapping s with kernel $\mathcal{C}_3$ such that $s(C_2) = \mathcal{S}'$. If x is a non-zero word of $\mathcal{C}_3$, then $\mathrm{wt}(x,s(x)) = \mathrm{wt}(x) \geq d_3$. If $x \in \mathcal{C}_2 \setminus \mathcal{C}_3$, then $s(x)$ is a non-zero word in $\mathcal{D}$ and so $\mathrm{wt}(x,s(x)) = \mathrm{wt}(x) + \mathrm{wt}(s(x)) \geq d_2 + (d_3-d_2) = d_3$. Finally, if $x \in \mathcal{C}_1 \setminus \mathcal{C}_2$, then $s(x) \notin \mathcal{D}'$, whence $\mathrm{wt}(s(x)) \geq d_3 - d_1$, and so $\mathrm{wt}(x,s(x)) \geq d_1 + (d_3-d_1) = d_3$. Consequently, $E(C_1)$ has minimum distance at least d_3. ■

4 Using BCH-codes

We aim at extending binary, ternary and quaternary BCH-codes of moderate lengths. It turns out that two-level UEP codes combined with the iteration of Construction X produce good codes in certain situations.

The following notation for q-ary BCH-codes will be used. The length n divides $q^r - 1$ for some integer r. We put $[i,j] = \{i, i+1, \ldots, j\} \subset \mathbb{Z}/n\mathbb{Z}$. Then $\mathcal{C}([i,j],n)$ denotes the q-ary BCH-code of length n with zeroes $\alpha^i, \alpha^{i+1}, \ldots, \alpha^j$, where α is a primitive n-th root of unity in $\mathbb{F}_{q^r}$. We will call $[i,j]$ the defining interval. By the BCH bound, the minimum distance of $\mathcal{C}([i,j],n)$ is at least $j-i+2$. Moreover, the dimension of $\mathcal{C}([i,j],n)$ is $n-\kappa$, where κ is the cardinality of the union of the cyclotomic cosets, which intersect $[i,j]$ non-trivially.

The tables are organized as follows. Choose $\mathcal{C}_i = \mathcal{C}([l,r_i],n)$ where $r_1 < r_2 < r_3$. Let k_i be the dimension of $\mathcal{C}_i$. Choose $\mathcal{U}$ to be the BCH-code with defining interval $[l', r_1]$ for some $l' < l$. It will suffice to give l' in the tables. The members of the second chain of codes are then the BCH-codes with defining intervals $[l', r_i]$. We also give the dimension k of $\mathcal{U}$. Finally we list the parameters of the suffix codes being used. These suffix codes have been constructed in Section 2.

We illustrate the procedure with the first binary example. The first chain of BCH-codes, with defining intervals $[0,6],[0,8]$ and $[0,10]$, respectively, has parameters $[63,44,8] \supset [63,38,10] \supset [63,35,12]$. The second chain corresponds to defining intervals $[61,6],[61,8]$ and $[61,10]$. The minimum distances of these codes are two larger than those of the corresponding members of the first chain. Now we first apply Construction X with the $[7,6,2]$ code as suffix code to the codes $\mathcal{C}_1$ with defining interval $[0,6]$ and $\mathcal{U}$ with defining interval $[61,6]$. According to (1), we obtain a chain $[70,44,10] \supset [70,38,12] \supset [70,35,14]$. Finally we use Theorem 3 with $[8,4,4] \vee_1 [4,3,2] = [11,(4^4,2^3)]$ as suffix code $\mathcal{S}$. The dimension of $\mathcal{S}$ indicates that we apply the method to a 42-dimensional subcode of our 44-dimensional code. The result is a binary $[81,42,14]$ code.

4.1 $q = 2, n = 63$

l	r_1, r_2, r_3	k_1, k_2, k_3	l'	k	suffix codes	result
0	6, 8, 10	44, 38, 35	61	38	$[7,6,2], [8,4,4] \vee_1 [4,3,2]$	$[81,42,14]$
1	6, 8, 10	45, 39, 36	0	44	$[1,1,1], [8,4,4] \vee_1 [4,3,2]$	$[75,43,12]$

4.2 $q = 2, n = 127$

l	r_1, r_2, r_3	k_1, k_2, k_3	l'	k	suffix codes	result
0	18, 20, 22	70, 63, 56	125	63	$[8,7,2], [12,7,4] \vee_1 [8,7,2]$	$[154,70,26]$
1	22, 26, 28	57, 50, 43	0	56	$[1,1,1], [16,8,(8,4^7)]$	$[144,51,32]$
1	42, 46, 54	29, 22, 15	0	28	$[1,1,1], [16,8,(8,4^7)]$	$[144,23,52]$

For the second example in this subsection it is vital that the primitive BCH-code with designed distance 29 has true minimal distance 31. This was observed in [6]. The construction results in a code $[143, 51, 31]$. This improves upon a result in the last section of [4].

4.3 $q = 3, n = 80$

l	r_1, r_2, r_3	k_1, k_2, k_3	l'	k	suffix codes	result
0	3, 4, 6	71, 67, 63	79	67	$[4,4,1], [4,2,3] \vee_1 [5,4,2]$	$[92,69,9]$
0	7, 9, 10	59, 55, 53	79	55	$[4,4,1], [4,2,3] \vee_1 [3,2,2]$	$[90,57,13]$
0	7, 10, 12	59, 53, 49	79	55	$[4,4,1], [11,6,5] \vee_1 [5,4,2]$	$[99,59,15]$
0	9, 10, 12	55, 53, 49	79	51	$[4,4,1], [4,2,3] \vee_1 [5,4,2]$	$[92,55,15]$
1	7, 9, 10	60, 56, 54	0	59	$[1,1,1], [4,2,3] \vee_1 [3,2,2]$	$[87,58,12]$
1	7, 10, 12	60, 54, 50	0	59	$[1,1,1], [11,6,5] \vee_1 [5,4,2]$	$[96,60,14]$
1	9, 10, 12	56, 54, 50	0	55	$[1,1,1], [4,2,3] \vee_1 [5,4,2]$	$[89,56,14]$
1	9, 10, 12	56, 54, 50	79	51	$[6,5,2], [4,2,3] \vee_1 [5,4,2]$	$[94,56,15]$
30	40, 41, 43	53, 49, 45	28	49	$[5,4,2], [4,2,3] \vee_1 [5,4,2]$	$[93,51,17]$
31	49, 50, 52	35, 33, 29	30	33	$[2,2,1], [4,2,3] \vee_1 [5,4,2]$	$[90,35,24]$
0	6, 9, 10	63, 55, 53	79	59	$[4,4,1], [12,8,(4^6,2^2)]$	$[96,61,13]$
0	9, 10, 12	55, 53, 49	77	47	$[11,8,3], [8,6,(3^2,2^4)]$	$[99,55,17]$
1	6, 9, 10	64, 56, 54	0	63	$[1,1,1], [12,8,(4^6,2^2)]$	$[93,62,12]$

4.4 $q = 4, n = 63$

l	r_1, r_2, r_3	k_1, k_2, k_3	l'	k	suffix codes	result
0	5, 6, 8	50, 47, 44	62	47	$[3,3,1], [5,3,3] \vee_1 [4,3,2]$	$[74,50,11]$
0	9, 10, 12	41, 38, 35	62	38	$[3,3,1], [5,3,3] \vee_1 [4,3,2]$	$[74,41,15]$
1	21, 22, 25	26, 23, 20	0	25	$[1,1,1], [5,3,3] \vee_1 [4,3,2]$	$[72,26,26]$
1	5, 6, 8	51, 48, 45	0	50	$[1,1,1], [5,3,3] \vee_1 [4,3,2]$	$[72,51,10]$
1	9, 10, 12	42, 39, 36	0	41	$[1,1,1], [5,3,3] \vee_1 [4,3,2]$	$[72,42,14]$
1	22, 25, 26	23, 20, 17	62	19	$[5,4,2], [6,3,4] \vee_1 [4,3,2]$	$[77,23,29]$
1	25, 26, 29	20, 17, 14	0	19	$[1,1,1], [5,3,3] \vee_1 [4,3,2]$	$[72,20,30]$
15	22, 23, 25	44, 41, 38	13	41	$[4,3,2], [5,3,3] \vee_1 [4,3,2]$	$[75,44,14]$
20	42, 43, 46	22, 19, 16	17	19	$[5,3,3], [5,3,3] \vee_1 [4,3,2]$	$[76,22,30]$
1	21,22,25	26,23,20	0	25	$[1,1,1], [7,4,(4,3^3)]$	$[71,24,27]$
1	25,26,29	20,17,14	0	19	$[1,1,1], [7,4,(4,3^3)]$	$[71,18,31]$
1	41,42,46	8,7,4	0	7	$[1,1,1], [8,4,(5,4^3)]$	$[72,8,48]$
0	41,42,46	7,6,3	59	4	$[6,3,4], [8,4,(5,4^3)]$	$[77,7,52]$

5 An improvement on Construction XX

In this section, we improve on Construction XX from [1] and use this improvement to construct two new ternary codes.

Theorem 4 *Let $\mathcal{C}_1, \mathcal{C}_2$ be q-ary codes of length n, put $\mathcal{C} = \mathcal{C}_1 + \mathcal{C}_2, \mathcal{C}_0 = \mathcal{C}_1 \cap \mathcal{C}_2$, $dim(\mathcal{C}) = k, dim(\mathcal{C}/\mathcal{C}_j) = dim(\mathcal{C}_j/\mathcal{C}_0) = \kappa_j, j = 1,2$. Let the minimum distances of the codes be $dist(\mathcal{C}) = d, dist(\mathcal{C}_i) = d_i, i = 0,1,2$. Put $\gamma_1 = d_0 - d_1, \gamma_2 = d_0 - d_2, \gamma = d_0 - d$.*
Assume $\gamma \leq \gamma_1 + \gamma_2 - 2$, put $i = \lfloor \frac{\gamma_1 + \gamma_2 - \gamma}{2} \rfloor$.
If there exist $[e_j, \kappa_j, \gamma_j]$ codes $\mathcal{S}_j, j = 1,2$, then an $[n + e_1 + e_2 - i, k, d_0]$ code exists.

Proof As suffix code $\mathcal{S}$, we choose the $[e_1 + e_2 - i, \kappa_1 + \kappa_2]$ code $S_1 \vee_i S_2$. Clearly, $\mathcal{S}$ enjoys the following properties.

- $\mathcal{S} = \mathcal{S}_1 \oplus \mathcal{S}_2$, where $\mathcal{S}_j$ has dimension κ_j and minimum distance at least $\gamma_j, j = 1,2$.
- The minimum weight of $\mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2)$ is at least γ.

We choose s such that it has kernel C_0, $s(\mathcal{C}_1) = \mathcal{S}_1$ and $s(\mathcal{C}_2) = \mathcal{S}_2$. We now show that $d(E(\mathcal{C})) \geq d_0$. If x is a non-zero word of $\mathcal{C}$ and $s(x) = 0$, then $x \in C_0$ and so $\mathrm{wt}(x) \geq d_0$. If $s(x) \neq 0$ and $x \in C_j$, then $\mathrm{wt}(x, s(x)) = \mathrm{wt}(x) + \mathrm{wt}(s(x)) \geq d_j + \gamma_j = d_0$ $(j = 1, 2)$. Finally, if $x \notin C_1$ and $x \notin C_2$, then $s(x) \notin \mathcal{S}_1 \cup \mathcal{S}_2$, and so $\mathrm{wt}(x, s(x)) \geq d + \gamma = d_0$.■

We note that with the same assumptions as in Theorem 4, Construction XX would produce an $[n + e_1 + e_2, k, d_0]$ code.

We give two applications: In [4] we considered among others ternary primitive BCH-codes of length 80. If we consider those codes with defining intervals $[37, 0], [37, 3], [31, 0], [31, 3]$ we obtain ternary codes $\mathcal{C}, \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_0$ with parameters $[80, 10, 45], [80, 6, 48], [80, 6, 51], [80, 2, 60]$, which satisfy our conditions. Put $d_0 = 56$. We have $\gamma = 11, \gamma_1 = 8, \gamma_2 = 5$. As ternary $[9, 4, 5]$ and $[14, 4, 8]$ codes exist, we can use the suffix code $\mathcal{S} = [14, 4, 8] \vee_1 [9, 4, 5]$ and obtain a code with parameters

$$[102, 10, 56]_3.$$

The defining intervals $[37, 79], [37, 3], [31, 79], [31, 3]$ yield ternary codes $\mathcal{C}, \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_0$ with parameters $[80, 11, 44], [80, 6, 48], [80, 7, 50], [80, 2, 60]$. Put $d_0 = 56$ again. We have $\gamma = 12, \gamma_1 = 8, \gamma_2 = 6$. The suffix code $\mathcal{S} = [14, 4, 8] \vee_1 [11, 5, 6]$ yields an extended code with parameters

$$[104, 11, 56]_3.$$

References

[1] W.O.Alltop: *A method for extending binary linear codes, IEEE Transactions on Information Theory* **30** (1984), 871-872.

[2] A.E. Brouwer: Data base of bounds for the minimum distance for binary, ternary and quaternary codes,
URL http://www.win.tue.nl/win/math/dw/voorlincod.html or
URL http://www.cwi.nl/htbin/aeb/lincodbd/2/136/114 or
URL ftp://ftp.win.tue.nl/pub/math/codes/table[234].gz.

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

[4] J.Bierbrauer and Y.Edel: *Extending and lengthening BCH-codes,* to appear in *Finite Fields and Their Applications*.

[5] L.A.Dunning and W.E.Robbins: *Optimal encoding of linear block codes for unequal error protection, Information and Control* **37** (1978),150-177.

[6] T.Kasami and N.Tokura: *Some remarks on BCH bounds and minimum weights of binary primitive BCH codes, IEEE Transactions on Information Theory* **15** (1969), 408-413.

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

[8] L.M.G.M. Tolhuizen: *Cooperating error-correcting codes and their decoding,* Ph.D. dissertation, Eindhoven University of Technology, Eindhoven, The Netherlands, June 1996.

[9] W.J. van Gils: *Two topics on linear unequal error protection codes:bounds on their length and cyclic code classes, IEEE Transactions on Information Theory* **29** (1983),866-876.

[10] V.A.Zinov'ev, S.N.Litsyn: *Methods of code lengthening, Problems in Information Transmission* **18**(1982),244-254.