Twisted BCH-codes

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)

Abstract

We develop the theory of a generalization of the notion of BCH-code to additive codes, which are not necessarily linear. The usefulness of this notion is demonstrated by constructing a large number of record-breaking linear codes via concatenation.

1 General Theory

We start out by generalizing our theory of BCH-codes as developed in [3, 4] to additive codes. Let $F = \mathbb{F}_{q^n}, m < n$, and E an m-dimensional $\mathbb{F}_q-$vectorspace. Let $\Phi : F \longrightarrow E$ be a surjective $\mathbb{F}_q-$linear mapping. We fix a divisor $w|(q^n - 1)$ and a natural number l. We construct an array $\mathcal{B} = \mathcal{B}(t, l, w, \Phi)$. The columns of $\mathcal{B}$ are indexed by the elements $u \in W$ of the subgroup of order w of F^*. Let $\mathcal{P}(l, t) = \{\sum_{i=l}^{l+t-2} a_i X^i | a_i \in F\}$. The rows of $\mathcal{B}$ are indexed by the polynomials $p(X) \in \mathcal{P}(l, t)$. The entry in row $p(X)$

and column $u \in W$ is defined as

$$\Phi(p(u)).$$

Proposition 1 *With notation as above the array $\mathcal{B}(t,l,w,\Phi)$ is an orthogonal array of strength $t-1$, with parameters $OA_{q^{(t-1)(n-m)}}(t-1,w,q^m)$.*

Proof: We can assume without restriction $w = q^n - 1$. Let columns $u_1, u_2, \ldots, u_{t-1}$ and entries $e_1, e_2, \ldots, e_{t-1} \in E$ be given. Count the rows $p(X)$ satisfying $\Phi(p(u_i)) = e_i, i = 1,2,\ldots,t-1$. We claim that this number is $\lambda = q^{(t-1)(n-m)}$. Fix a tuple $(y_1, y_2, \ldots, y_{t-1})$, where $\Phi(y_i) = e_i$. There are λ such tuples. We claim that there is precisely one $p(X) \in \mathcal{P}(l,t)$ such that $p(u_i) = y_i, i = 1,2,\ldots,t-1$. This is an elementary fact from polynomial interpolation.$\blacksquare$

Let

$$\mathcal{P}_0(t,l,w,\Phi) = \{p(X) \in \mathcal{P}(l,t), \Phi(p(W)) = 0\},$$

$$\rho_o(t,l,w,\Phi) = dim(\mathcal{P}_0(t,l,w,\Phi)).$$

All dimensions are dimensions of $\mathbb{F}_q-$ vectorspaces. The meaning of the parameter is that in $\mathcal{B}(t,l,w,\Phi)$ every row occurs with multiplicity q^{ρ_0}, where $\rho_0 = \rho_o(t,l,w,\Phi)$. It follows that the simplification $\mathcal{B}_0(t,l,w,\Phi)$ of $\mathcal{B}(t,l,w,\Phi)$, where each row is written only once, is an orthogonal array $OA_{q^{(t-1)(n-m)-\rho_0}}(t-1,w,q^m)$. We wish to define a dual (compare [6]).

Definition 1 *Identify E with $\mathbb{F}_q^m$. Then every row of $\mathcal{B}(t,l,w,\Phi)$ can be seen as an $mw-$tuple over $\mathbb{F}_q$. Define the dual $\mathcal{B}(t,l,w,\Phi)^\perp = \mathcal{B}_0(t,l,w,\Phi)^\perp$ as the dual with respect to the dot product in this space $\mathbb{F}_q^{mw}$. Then $\mathcal{B}(t,l,w,\Phi)^\perp$ clearly has dimension $mw - n(t-1) + \rho_o(t,\Phi)$.*

Observe that this definition is a generalization of the dual in the $\mathbb{F}_{q^m}-$linear case when $E = \mathbb{F}_{q^m}$ and Φ is an E-linear mapping.

Theorem 1 *Consider $\mathcal{B}(t,l,w,\Phi)^\perp$ as an $\mathbb{F}_q-$linear q^m-ary code of length w. Then the minimum distance d of $\mathcal{B}(t,l,w,\Phi)^\perp$ satisfies $d \geq t$.*

Proof: The $\mathbb{F}_q-$linearity of $\mathcal{C} = \mathcal{B}(t,l,w,\Phi)^\perp$ shows that d is the minimum weight of a nonzero vector.
Let $\chi = (\chi_i) \in \mathcal{C}, i = 1,2,\ldots,w$ and $\chi_i = 0 (i > t-1)$. We have to show $\chi = 0$. Observe that the entries χ_i are themselves $m-$tuples over $\mathbb{F}_q$. Fix $j, 1 \leq j \leq t-1$. As $\mathcal{B}(t,l,w,\Phi)$ is an orthogonal array of strength $t-1$ we find for every $e \in E$ a row $v = (v_i) \in \mathcal{B}(t,l,w,\Phi)$ such that $v_j = e$ and $v_k = 0$ for $k \leq t-1, k \neq j$. The orthogonality shows $\chi_j \cdot e = 0$. As this is true for all $e \in E$ we see that $\chi_j = 0$. ■

We propose the name **twisted** BCH**-codes** for these codes $\mathcal{B}(t,\Phi)^\perp$ when Φ is not $\mathbb{F}_{q^m}-$linear. These q^m-ary codes will be good if $\rho_o(t,l,w,\Phi)$ is large.

1.1 The function $\rho_o(t,\Phi)$

The above discussion shows that all we need to know about Φ is its kernel. It turns out to be advantageous to use the **trace form** defined by

$$(x,y) = tr(x \cdot y).$$

Here $tr = tr : F \longrightarrow \mathbb{F}_q$ is the trace. Let $U =< \gamma_1,\ldots,\gamma_m >$ such that its dual (with respect to the trace form) is the kernel of $\Phi : U^\perp = ker(\Phi)$.
Put $\Gamma = \{\gamma_1,\ldots,\gamma_m\}$. Then the condition $\Phi(p(u)) = 0$ is equivalent with $tr(\gamma p(u)) = 0$ for all $\gamma \in \Gamma$.
We wish to describe the growth of $\rho_0(t) = \rho_0(t,l,w,\Phi)$ as a function of t. It is clear that

$$0 \leq \Delta_\Phi(t) = \rho_0(t+1,l,w,\Phi) - \rho_0(t,l,w,\Phi) \leq n.$$

Definition 2 *Call a polynomial* $p(X) \in F[X]$ **cyclotomic** *if all the exponents of its nonzero monomials belong to the same* **cyclotomic coset***. Here a cyclotomic coset is an orbit of the Galois group* $Gal(F|\mathbb{F}_q)$ *in its operation on the integers mod* w*. We choose* $R = \{l, l+1, \ldots, l+w-1\}$ *as set of representatives.*

Let Z be a cyclotomic coset of length s. We determine its contribution to the growth of $\rho_0(t, \Phi)$.

Definition 3 *Let $Z = Z(i)$ be a cyclotomic coset of length s. The* **contribution** *$contr(Z, l, w, \Phi)$ of Z to $\rho_0(t, l, w, \Phi)$ is defined as the dimension of the space of coefficients $(a_j)_{j=0,\dots,s-1} \in F^s$ satisfying*

$$\sum_{j=0}^{s-1} a_j^{q^j} u^{iq^j} \in ker(\Phi) \text{ for all } u \in W.$$

Equivalently $contr(Z, l, w, \Phi) = \sum_{z \in Z} \Delta_\Phi(z)$.

Proposition 2

$$contr(Z, l, w, \Phi) = \mid Z \mid (n - m).$$

Proof: Let $Z = Z(i), s = \mid Z \mid$. Observe that the $\mathbb{F}_q-$ vector space generated by the x^i, where $x \in W$ is the subfield $\mathbb{F}_{q^s}$. Let $\alpha = (a_0, a_1, \dots, a_{s-1}) \in F^s$ and consider the polynomial $p_\alpha(X) = \sum_{j=0}^{s-1} a_j^{q^j} X^{q^j}$. The contribution $contr(Z, l, w, \Phi)$ is the dimension of the space of tuples α satisfying $p_\alpha(x^i) \in Ker(\Phi)$ for every $x \in W$. As the polynomial $p_\alpha(X)$ is linearized (it affords an $\mathbb{F}_q$-linear mapping) an equivalent condition is $p_\alpha(\mathbb{F}_{q^s}) \subseteq Ker(\Phi)$. Another equivalent condition is $tr(\gamma \cdot p_\alpha(u)) = 0$ for all $u \in \mathbb{F}_{q^s}$ and $\gamma \in \Gamma$. We have $\gamma \cdot p_\alpha(u) = \sum_{j=0}^{s-1} (\gamma^{q^{n-j}} a_j u)^{q^j}$. It follows $tr(\gamma \cdot p_\alpha(u)) = tr((\sum_{j=0}^{s-1} \gamma^{q^{n-j}} a_j) \cdot u) = 0$ for all $u \in \mathbb{F}_{q^s}$, equivalently $\sum_{j=0}^{s-1} \gamma^{q^{n-j}} a_j \in \mathbb{F}_{q^s}^\perp$, where the orthogonal complement is taken with respect to the trace-form.
As $\mathbb{F}_{q^s}^\perp$ has dimension $n - s$ we see that each such condition corresponding to an element $\gamma \in \Gamma$ defines a space of codimension precisely s. As Γ has m elements we see that our space of coefficients has codimension $\leq ms$. It follows $contr(Z, l, w, \Phi) \geq s(n - m)$.
Summing up this inequality over all cyclotomic cosets we get $\rho_0(w + 1) \geq w(n - m)$. The simplification $\mathcal{B}_0$ of $\mathcal{B}$ is an $OA_{q^{w(n-m)-\rho_0(w+1)}}(w, w, q^m)$. Certainly the parameter λ must be an integer. We conclude that we have equality all the way. We also see that $\mathcal{B}(w + 1)^\perp$ is the 0-code.■

In particular we conclude that it suffices to consider cyclotomic polynomials:

Proposition 3 *If there is a polynomial* $p(X)=\sum_{k=l}^{i} a_kX^k, a_i\neq 0$ *such that* $\Phi(p(W))=0$, *then there is a cyclotomic such polynomial with the same leading coefficient* a_i.

The values of $\rho_0(t,l,w,\Phi)$ remain unchanged if the elements of Γ are multiplied by a nonzero constant (from F). It follows in fact from the definition of our array that the effect of replacing Γ by $\gamma\cdot\Gamma$ for some $\gamma\neq 0$ is a permutation of the rows of $\mathcal{B}(t,l,w,\Phi)$. We can therefore assume $1\in\Gamma$. It follows that in case $m=1$ we may choose $\Phi=tr$. This reverts to linear BCH-codes in the ordinary sense.

Definition 4 *Let us call a family of* u *automorphisms of* $F|\mathbb{F}_q$ *an* **interval** *of length* u *if they have the form* $\phi^{j+a}, j=0,1,\dots,u-1$ *for fixed* a. *Here* ϕ *is the Frobenius automorphism.*

Theorem 2 *Any nontrivial linear combination of an interval of length* u *of automorphisms of* $F|\mathbb{F}_q$ *has a kernel of dimension* $<u$.

Proof: It is clear that we can assume without restriction $a=0$, so that our automorphisms are given by $\sigma_i(x)=x^{q^i}, i=0,\dots,u-1$. The kernel of the linear combination $\sum_{i=0}^{u-1}a_i\sigma_i$ consists of the roots of the linearized polynomial $\sum_{i=0}^{u-1}a_ix^{q^i}$. As this is a nonzero polynomial of degree $\leq q^{u-1}$, we conclude that the dimension of the kernel is $<u$.■

In our situation consider the square matrix M, with rows indexed by $\gamma\in\Gamma$ and columns indexed by ϕ^{j+l}, where ϕ is the Frobenius automorphism, and $j=1,2,\dots,m$. The preceding Theorem proves that M is a regular matrix (meaning that $det(M)\neq 0$). We will make use of this fact in the sequel.

Fix a cyclotomic coset $Z=Z(i)$ of length $|Z|=s$. Let $p(X)$ be a corresponding cyclotomic polynomial. Write $p(X)=\sum_{j=0}^{s-1}(a_jX^i)^{q^j}$. We want to simplify the condition $\Phi(p(W))=0$. Consider the polynomial $q(Y)=\sum_{j=0}^{s-1}(a_jY)^{q^j}$. We know from the proof of Proposition 3 that an equivalent condition is $\Phi(q(\mathbb{F}_{q^s}))=0$. For $\gamma\in\Gamma$ put $q_\gamma(Y)=\gamma\cdot q(Y)=\sum_{j=0}^{s-1}(\gamma^{q^{n-j}}a_jY)^{q^j}$. Another equivalent condition is $tr(q_\gamma(\mathbb{F}_{q^s}))=0$ for every $\gamma\in\Gamma$. Observe that $\mathbb{F}_{q^s}$ is an intermediate field between $\mathbb{F}_q$ and F. Therefore the trace tr factors:

$tr = tr_s \circ Tr$, where $Tr : F \longrightarrow I\!\!F_{q^s}, tr_s : I\!\!F_{q^s} \longrightarrow I\!\!F_q$. Our condition reads $tr_s(\sum_{j=0}^{s-1}(b_j u)^{q^j}) = 0$ for all $u \in I\!\!F_{q^s}$. Here $b_j = Tr(\gamma^{q^{n-j}} a_j)$. The condition simplifies: $tr_s((\sum_{j=0}^{s-1} b_j) \cdot u) = 0$ for all u, hence $\sum_{j=0}^{s-1} b_j = 0$. This is our final result:

Lemma 1 *The cyclotomic polynomial* $p(X) = \sum_{j=0}^{s-1}(a_j X^i)^{q^j}$ *satisfies* $\Phi(p(W)) = 0$ *if and only if for every* $\gamma \in \Gamma$ *we have* $\sum_{j=0}^{s-1} Tr(\gamma^{q^{n-j}} a_j) = 0$. *Here* $Tr : F \longrightarrow I\!\!F_{q^s}$ *is the trace.*

Observe that the choice of the set of representatives $R = \{l, l+1, \ldots, l+w-1\}$ implies an ordering of the degrees of our polynomials: $l < l+1 < \ldots < l+w-1$. We make use of the result above to compute $\Delta_\Phi(t)$. So let the cyclotomic coset $Z = Z(i)$ of length s be given. Use the ordering implied by R and write $Z = \{z_1, z_2, \ldots, z_s\}$. Write $z_j = z_1 q^{\pi(j)}$. Were π is a bijective mapping from $\{1, \ldots, s\}$ to $\{0, \ldots, s-1\}$.

We form a matrix $M = M(Z)$ with m rows and s columns. The rows are indexed by the elements $\gamma_k \in \Gamma, k = 1, 2, \ldots, m$. The entry of M in row k, column j is $m_{k,j} = \gamma_k^{q^{-\pi(j)}}$. Denote by K the kernel of the trace $Tr : F \longrightarrow I\!\!F_{q^s}$, put $\mathcal{D} = K^m$. Denote by $S_j \subset F^m$ the space generated by the first j columns of M. We introduce the $I\!\!F_q$−dimensions $d_j = dim(S_j \cap \mathcal{D})$. The main result of our discussion above reads as follows:

Lemma 2 *Put* $j = l + t - 1$. *With the terminology as introduced above we have* $\Delta(t) = \rho_0(t+1, l, w, \Phi) - \rho_0(t, l, w, \Phi) = n + (d_j - d_{j-1}) - (dim(S_j) - dim(S_{j-1}))$. *Here all dimensions are over* $I\!\!F_q$.

This can be considerably simplified. At first observe that $dim(S_j) - dim(S_{j-1})$ can only take on values 0 or n. Moreover we know from Theorem 2 that matrix M has maximal rank $r = min(m, s)$. Define H to be the set of indices h where $dim(S_h) - dim(S_{h-1}) = n$. We know that $H = \{h_1 < h_2 < \ldots, h_r\}$ has cardinality $r = min(m, s)$. Clearly $h_1 = 1$. If $j \notin H$, then $\Delta(t) = n$. If $j \in H$, then $\Delta(j) = d_j - d_{j-1}$. In the generic case $s = n$ of a cyclotomic coset of maximal length n we have $K = 0$, hence $\Delta(t) = 0$ if $j \in H$. Another extremal case is $s = 1$. Here we have $Tr = tr : F \longrightarrow I\!\!F_q$. Matrix M has only one column in that case. We see that $\Delta(t)$ is the dimension of the space $U^\perp$, which is $n-m$. Let us collect our result in the following main theorem:

Theorem 3 (Determination of $\Delta(t)$) *Put $i = l+t-1$, consider the cyclotomic coset $Z = Z(i)$ of length s. Write $Z = \{z_1 < z_2 < \ldots < z_s\}$ and $z_j = z_1 \cdot q^{\pi(j)}$. Here π is a bijective mapping from $\{1,\ldots,s\}$ to $\{0,\ldots,s-1\}$. In particular $\pi(1) = 0$.*
Form the matrix M with m rows and s columns, with entries

$$m_{k,j} = \gamma_k^{q^{-\pi(j)}}.$$

Let $K = ker(Tr)$, where $Tr : F \longrightarrow \mathbb{F}_{q^s}$ is the trace to the intermediate field. Let $S_j \in F^m$ be the space generated by the j first columns of M, put $\mathcal{D} = K^m$ and $d_j = dim(S_j \cap \mathcal{D})$ (as a vector space over $\mathbb{F}_q$). Let $H = \{h_1,\ldots,h_r\} \subset \{1,2,\ldots,s\}$ be the set of those indices h for which $S_h \supset S_{h-1}$. Here $r = min(m,s)$. If $i = z_j$, then the following holds:

$$\Delta(t) = \rho_0(t+1,l,w,\Phi) - \rho_0(t,l,w,\Phi) = \begin{cases} n & \text{if } j \notin H \\ d_j - d_{j-1} & \text{if } j \in H \end{cases}$$

Observe the special cases

$$\Delta(t) = \begin{cases} 0 & \text{if } j \in H, s = n \\ n-m & \text{if } j \in H, s = 1. \end{cases}$$

1.2 The linear case

The case of linear BCH-codes is $m = 1, \gamma_1 = 1$, hence $H = \{1\}$. It follows

$$\Delta(t) = \begin{cases} n & \text{if } l+t-1 \text{ is not minimal} \\ n-s & \text{if } l+t-1 \text{ is minimal.} \end{cases}$$

Here minimal means minimal in the cylcotomic coset, with respect to the ordering $l < l+1 < \ldots$.

1.3 Case $m = 2$

We know that we can choose $\Gamma = \{1, \gamma\}$. Denote by $\mathbb{F}_{q^k}$ the field generated by γ. Assume $s > 1$. Then $H = \{1, h_2\}$, where h_2 is the minimal j such that $\gamma \neq \gamma^{q^{\pi(j)}}$, equivalently such that k is not a divisor of $\pi(j)$. Consider $i = z_1$. We have to determine the dimension of the space of $u \in F$ such that $u \in K$ and $u\gamma \in K$. This is equivalent with $Tr(< 1, \gamma >) = 0$. Now the space $< 1, \gamma >$, seen as a vector space over $\mathbb{F}_{q^s}$, has dimension 1 or 2. Accordingly its dual with respect to Tr has dimension $\frac{n}{s} - 1$ or $\frac{n}{s} - 2$. It follows that $\Delta(t) = n - s$ and $= n - 2s$, respectively. As we know the contribution of the cyclotomic coset we do not have to consider the case then $i = z_{h_2}$ explicitly.

Theorem 4 *With notation as in Theorem 3 let* $m = 2, \Gamma = \{1, \gamma\}$. *Denote by* $\mathbb{F}_{q^k}$ *the field generated by* γ. *Assume* $s > 1$. *Then* $h_1 = 1, h_2$ *is the minimal* j *such that* k *does not divide* $\pi(j)$. *Put* $i = l + t - 1$, *write* $i = z_j$. *If* $j \notin h$, *then* $\Delta(t) = n$.

- *If* $k|s$, *then* $\Delta(t) = n - s$ *if* $j = 1$ *or* $j = h_2$.
- *If* k *does not divide* s, *then* $\Delta(t) = \begin{cases} n - 2s & \text{if } j = 1 \\ n & \text{if } j = h_2. \end{cases}$

2 Construction of good linear codes

We apply our theory of twisted BCH-codes as well as concatenation to construct a large number of good linear codes. We start with the primitive narrow-sense case $w = q^n - 1, l = 1$. Observe that $i = t$ in the notation of Theorem 3. We find it convenient in this case to consider the corresponding $\mathcal{A}$-array instead of $\mathcal{B}(t) = \mathcal{B}(t, 1, q^n - 1, \Phi)$. This array $\mathcal{A}(t)$ has an additional column corresponding to $0 \in F$, its rows are indexed by pairs $(p(X), z)$, where $p(X) \in \mathcal{P}(1, t), z \in E$. The entries are defined by $\Phi(p(u)) + z$. The same argument as in the case of the $\mathcal{B}$-array shows that $\mathcal{A}(t)$ is an orthogonal array of strength t (whereas the strength of $\mathcal{B}(t)$ is $t - 1$). It is clear that the multiplicity of each row in $\mathcal{A}(t)$ is the same as in $\mathcal{B}(t)$, hence $q^{\rho_0(t)}$. The parameters of $\mathcal{A}(t)$ are $OA_{q^{(t-1)(n-m)}}(t, q^n, q^m)$. We will refer to the $\mathcal{A}(t)^\perp$ as **extended**

twisted BCH-codes. We know from the proof of Proposition 3 that $\mathcal{A}(q^n)^\perp$ is the 0-code. As $Z(q^n-1)$ has length 1 we conclude from Theorem 4 that $\Delta(q^n-1)=n-m$. It follows that $\mathcal{A}(q^n-1)^\perp$ has dimension m (and distance q^n). It is clear that $\mathcal{A}(q^n-1)^\perp$ is the repetition code $\{(e,e,\dots,e)|e\in E\}$. In case $m=2$ we write $\Gamma=\{1,\gamma\}$.

2.1 Case $q=2, n=6, m=2, w=63, l=1$

For the convenience of the reader we list the nonzero cyclotomic cosets in this case:

cyclotomic cosets of $\mathbb{F}_{64}$ over $\mathbb{F}_2$
1,2,4,8,16,32
3,6,12,24,48,33
5,10,20,40,17,34
7,14,28,56,49,35
9,18,36
11,22,44,25,50,37
13,26,52,41,19,38
15,30,60,57,51,39
21,42
23,46,29,58,53,43
27,54,45
31,62,61,59,55,47

We know that $\Phi=tr_{F|F_4}$ corresponds to the choice $\gamma\in\mathbb{F}_4-\mathbb{F}_2$. Let us denote the function corresponding to $\gamma\in\mathbb{F}_8-\mathbb{F}_2$ simply by Φ. In the following table we give the values of $\rho_0(t,\Phi)$, and of $\rho_0(t,tr_{F|F_4})$ as well as the parameters of the linear quaternary codes and eventually of the corresponding (twisted) extended BCH-codes. We list the parameters of the twisted codes only if they are better than those of the BCH-codes. In order to facilitate comparison we have written in the place of the dimension k the quaternary dimension. Thus, if a code has 2^{11} elements, we write $k=5.5$. This convention will be used in this and the following subsection.

t	$\rho_0(t, tr_{F\|F_4})$	BCH-code	$\rho_0(t, \Phi)$	twisted code
4	0	$[64, 54, 5]$	0	
5	6	$[64, 54, 6]$	6	
6	6	$[64, 51, 7]$	6	
7	6	$[64, 48, 8]$	6	
8	6	$[64, 45, 9]$	6	
9	12	$[64, 45, 10]$	12	
10	12	$[64, 42, 11]$	15	$[64, 43.5, 11]$

t	$\rho_0(t, tr_{F\|F_4})$	BCH-code	$\rho_0(t,\Phi)$	twisted code
11	12	$[64,39,12]$	15	$[64,40.5,12]$
12	12	$[64,36,13]$	15	$[64,37.5,13]$
13	18	$[64,36,14]$	21	$[64,37.5,14]$
14	18	$[64,33,15]$	21	$[64,34.5,15]$
15	18	$[64,30,16]$	21	$[64,31.5,16]$
16	18	$[64,27,17]$	21	$[64,28.5,17]$
17	24	$[64,27,18]$	27	$[64,28.5,18]$
18	30	$[64,27,19]$	33	$[64,28.5,19]$
19	36	$[64,27,20]$	36	
20	42	$[64,27,21]$	36	
21	48	$[64,27,22]$	42	
22	52	$[64,26,23]$	44	
23	52	$[64,23,24]$	44	
24	52	$[64,20,25]$	44	
25	58	$[64,20,26]$	50	
26	64	$[64,20,27]$	56	
27	64	$[64,17,28]$	62	
28	64	$[64,14,29]$	65	$[64,14.5,29]$
29	70	$[64,14,30]$	71	$[64,14.5,30]$
30	76	$[64,14,31]$	71	
31	76	$[64,11,32]$	71	
32	76	$[64,8,33]$	71	
42	136	$[64,8,43]$	131	
43	140	$[64,7,44]$	137	
44	140	$[64,4,45]$	143	$[64,5.5,45]$
45	146	$[64,4,46]$	149	$[64,5.5,46]$
46	152	$[64,4,47]$	152	$[64,4,47]$
47	158	$[64,4,48]$	158	$[64,4,48]$
48	158	$[64,1,47]$	158	$[64,1,47]$

Some of the quaternary codes are rather good. In fact, quaternary linear codes of parameters $[64,43,11]$, $[64,40,12]$, $[64,37,14]$, $[64,34,15]$, $[64,28,19]$ or $[64,5,46]$ are not known to exist. Our code $[64,5.5,46]$ is in fact better than any linear quaternary code as a linear $[64,6,46]$ cannot exist. In the next subsection we will use just this $[64,5.5,46]$ and its subcodes $[64,4,48]$

and $[64, 1, 64]$ to construct new extremely good binary linear codes.

2.1.1 New binary codes

Let us use concatenation with a binary code $[3, 2, 2]$. When applied to our quaternary $[64, 5.5, 46]$ we obtain a binary linear code $\mathcal{C}_1$ with parameters

$$[192, 11, 92].$$

This code is optimal with respect to minimal distance and to dimension. By construction it contains subcodes $\mathcal{C}_2 \supset \mathcal{C}_3$ with parameters $[192, 8, 96]$ and $[192, 2, 128]$, respectively. Application of construction X (see [8], chapter 18 and [4]) to the pair $\mathcal{C}_1 \supset \mathcal{C}_2$ with auxiliary codes $[3, 3, 1]$ and $[6, 3, 3]$ yields, after addition of a parity check bit, new binary codes with parameters

$$[196, 11, 94] \text{ and } [199, 11, 96].$$

These codes are length-optimal. Observe that length-optimality implies optimality with respect to dimension and to minimum distance. Application of a Griesmer step yields codes

$$[100, 10, 46] \text{ and } [103, 10, 48].$$

Both are $d-$optimal, the latter code is length-optimal.
Code $[198, 11, 95]$ was obtained by lengthening of $\mathcal{C}_1$. It contains $\mathcal{C}_3$. Apply construction X to this pair, using auxiliary codes $[10, 9, 2], [14, 9, 4], [18, 9, 6]$ and $[21, 9, 8]$, add a final parity check bit in each case. This yields new code parameters

$$[209, 11, 98], [213, 11, 100], [217, 11, 102] \text{ and } [220, 11, 104].$$

Our $\mathbb{F}_2-$linear quaternary codes can be used in many respects like linear quaternary codes. It is clear that if truncation with respect to one coordinate is applied to such a quaternary code $[n, k, d]$, the result is an $\mathbb{F}_2-$linear quaternary $[n-1, k, d-1]$. In the same way shortening leads to a code $[n-1, k-1, d]$. Applying these mechanism recursively to our quaternary $[64, 5.5, 46]$ yields, after concatenation with $[3, 2, 2]$, the following new binary linear codes:

$$[189, 11, 90], [186, 11, 88], [183, 11, 86][180, 11, 84][177, 11, 82],$$

$$[174, 11, 80][171, 11, 78], [186, 9, 90].$$

The two first and the last of these codes are d-optimal. Codes $[196, 11, 94]$ and $[199, 11, 96]$ have dual distance three. Application of construction $Y1$ (see [8], chapter 18 and [4]) yields codes

$$[193, 9, 94] \text{ and } [196, 9, 96].$$

Both are optimal with respect to d and to k.
Groneick&Grosse ([7], see also [4]) observe that the Griesmer mechanism can be applied to any codeword of a binary linear code, not necessarily only those of minimal weight:

Lemma 3 (Groneick,Grosse) *If there is a binary linear code* $[n, k, d]$ *possessing a nonzero codeword of weight* w*, where* $d > \frac{w}{2}$*, then there is a code* $[n - w, k - 1, d - [\frac{w}{2}]]$.

The weight distribution of $\mathcal{C}_1$ is

$$A_0 = 1, A_{92} = 1344, A_{96} = 252, A_{108} = 448, A_{128} = 3.$$

We see that $\mathcal{C}_1$ is doubly-even. The words of weights 0,96 and 128 form the 8-dimensional subcode $\mathcal{C}_2$. Application of Lemma 3 in cases $w = 96$ and $w = 108$ yields codes

$$[96, 10, 44] \text{ and } [84, 10, 38].$$

Both are new and $d-$optimal. Case $w = 128$ yields $[64, 10, 28]$. This is a $d-$optimal code, but not new. The auxiliary code $[7, 3, 4]$ which was used to construct the code $[199, 11, 96]$ out of $\mathcal{C}_1$ has constant weight 4. In particular the lengthened code is doubly-even and has a code word of weight $w = 112$. Application of Lemma 3 yields a length-optimal code

$$[87, 10, 40].$$

Here are two more applications of Lemma 3: Our code $[186, 11, 88]$ has a word of weight 108, code $[189, 11, 90]$ has a word of weight 96. This leads to codes

$$[78, 10, 34] \text{ and } [93, 10, 42].$$

The latter code is optimal with respect to d. If a code $[186, 11, 88]$ could be constructed containing a word of weight 110, then a $d-$optimal code $[77, 10, 34]$ would exist. Finally we apply construction X to our chain
$[192, 11, 92] \supset [192, 8, 96] \supset [192, 2, 128]$ of binary linear codes. Start from a subcode of codimension 2 of the largest of these codes, apply X with the repetition code $[4, 1, 4]$. This produces a $[196, 9, 96]$, still containing $[196, 2, 128]$. Another application of X, with $[50, 7, 24]$ as auxiliary code, produces the new code $[246, 9, 120]$. In an analogous way we can start from a subcode of codimension one, use construction X with $[6, 2, 4]$ and in the last step with $[48, 8, 22]$ or $[51, 8, 24]$ to obtain new parameters $[246, 10, 118]$ and $[249, 10, 120]$.

2.2 Case $q = 2, n = 6, m = 2, w = 63$ and more new binary codes

We use the material collected in subsection 2.1, but we go back to the codes $\mathcal{B}(t, l, 63, \Phi)^{\perp}$, making use of the non-narrow sense case $l \neq 1$. The mapping Φ is the same as in subsection 2.1. Twisted BCH-codes may best be described by their defining intervals $I = \{l, l+1, \dots, l+t-2\}$. So we write $\mathcal{C}(I) = \mathcal{B}(t, l, 63, \Phi)^{\perp}$. Observe that if I_1 and I_2 are intersecting defining intervals, then $\mathcal{C}(I_1) \cap \mathcal{C}(I_2) = \mathcal{C}(I_1 \cup I_2)$. We consider the twisted BCH-codes corresponding to the defining intervals

$$[19, 63] \subset [19, 8], \ [17, 63].$$

Observe that we calculate mod 63. As an example the interval $[19, 8] = \{19, 20, \dots, 62, 63 = 0, 1, 2, \dots, 8\}$ has 53 elements. The corresponding additive quaternary codes have the following parameters, where the notational conventions of the preceding subsections are used:

$$\mathcal{D}_a = [63, 4.5, 46] \supset \mathcal{D}_b = [63, 1.5, 54], \mathcal{D}_c = [63, 3, 48].$$

We claim $\mathcal{D}_b \cap \mathcal{D}_c = 0$. As $\mathcal{D}_b \cap \mathcal{D}_c$ has defining interval $[17, 8]$ and the 0-code certainly has defining interval $[17, 16]$ it suffices in the light of Theorems 3 and 4 to show that for $i \in \{8, 9, \dots, 15\}$ we have that i is neither minimal nor second-to-minimal in its cyclotomic coset. Recall that the ordering is given by $17 < 18 < 19 < \dots < 16$. This is easily checked.

Apply concatenation with the binary code $[3,2,2]$. We obtain binary linear codes

$$\mathcal{C}_a = [189,9,92] \supset \mathcal{C}_b = [189,3,108], \mathcal{C}_c = [189,6,96].$$

Naturally the relations of inclusion and intersection carry over from the $\mathcal{D}_i$ to the $\mathcal{C}_i$.

An application of construction X to the pair $\mathcal{C}_a \supset \mathcal{C}_b$, with $[32,6,16]$ as auxiliary code, yields the new parameters $[221,9,108]$. Apply construction XX (see [1]) to the codes $\mathcal{C}_a \supset \mathcal{C}_b, \mathcal{C}_c$. In a first step apply construction X to the pair $\mathcal{C}_a \supset \mathcal{C}_c$, with $[7,3,4]$ as auxiliary code. We get lengthened codes $\tilde{\mathcal{C}}_a = [196,9,96] \supset \tilde{\mathcal{C}}_b = [196,3,112]$. Another application of construction X with auxiliary codes (in turn) $[7,6,2], [15,6,6], [18,6,8], [32,6,16]$ yields codes with new parameters:

$$[203,9,98], [211,9,102], [214,9,104], [228,9,112].$$

2.3 Case $m = 2, k = n$

With notation as in Theorem 4 this is the case when $\Gamma = \{1, \gamma\}$ and $\mathbb{F}_q(\gamma) = F$. Use the notation of Theorem 3. If the length of our cyclotomic coset is $s > 1$, then $H = \{1,2\}$. Let $t = z_j$. If $j > 2$, then of course $\Delta(t) = n$. Theorem 4 yields the following:

- If $s = n$, then $\Delta(t) = 0$ if $j = 1$ or $j = 2$.
- If $s < n$, then $\Delta(t) = \begin{cases} n - 2s & \text{if } j = 1 \\ n & \text{if } j = 2. \end{cases}$

Proposition 4 *In case $m = 2, k = n > 2$ the twisted BCH-code*

$\mathcal{A}(q^n - 1 - q^{n-2}, \Phi)^\perp$ is an $\mathbb{F}_{q^2}$-ary and $\mathbb{F}_q$−linear code with parameters

$$[q^n, n+2, q^{n-2}(q^2-1)].$$

It contains the repetition code $[q^n, 2, q^n]$. Here dimensions are over $\mathbb{F}_q$.

Proof: Let $t = q^n - 1 - j$, where $j < q^{n-2}$. As tq and tq^2 both are smaller than t it follows that $\Delta(t) = n$ in these cases. Let $t = q^n - 1 - q^{n-2}$. Then

$Z(t)$ has length n and consists of the $-q^j, j = 0, 1, \ldots, n-1$. It follows that t is second-smallest. We get $\Delta(t) = 0$.■

Observe that no linear $\mathbb{F}_{q^2}-$ary code can have such good parameters, because of the Griesmer bound. Concatenation with the $\mathbb{F}_q$-ary linear code $[q+1, 2, q]$ leads to a series of $\mathbb{F}_q$-ary linear codes with parameters $[q^n(q+1), n+2, q^{n-1}(q^2-1)]$, containing a subcode $[q^n(q+1), 2, q^{n+1}]$, This is a well-known family of two-weight codes, a special case of construction SU1 of [5]. They meet the Griesmer bound with equality. Let us consider a few special cases:

2.3.1 Case $q = 3, n = 5, m = 2, w = 242, l = 1$

We apply construction X to our pair of ternary linear codes

$$[972, 7, 648] \supset [972, 2, 729].$$

Using auxiliary codes $[11, 5, 6], [20, 5, 12], [34, 5, 21], [45, 5, 28], [61, 5, 39], [74, 5, 48], [87, 5, 57], [100, 5, 66]$ and $[113, 5, 75]$ yields the following ternary codes:

$$[983, 7, 654], [992, 7, 660], [1006, 7, 669], [1017, 7, 676], [1033, 7, 687],$$

$$[1046, 7, 696], [1059, 7, 705], [1072, 7, 714], [1085, 7, 723].$$

All but three of these codes meet the Griesmer bound with equality, the remaining three are one longer than the Griesmer bound. In two of these cases ($[1006, 7, 669]$ and $[1046, 7, 696]$) two Griesmer steps lead to optimal codes ($[114, 5, 75]$ and $[118, 5, 78]$, respectively). The Griesmer bound shows that even the last code $[1033, 7, 687]$ is $d-$optimal. Codes with parameters obtained by two Griesmer steps are already known. The best of them are $[112, 5, 74], [115, 5, 76], [121, 5, 81]$.

2.3.2 Case $q = 4, n = 3, m = 2, w = 63, l = 1$

We obtain quaternary codes

$$[320, 5, 240] \supset [320, 2, 256],$$

Construction X with auxiliary quaternary codes $[6,3,4],[9,3,6]$, $[16,3,12],[21,3,16]$ yields parameters

$$[326,5,244],[329,5,246],[336,5,252] \text{ and } [341,5,256].$$

Each of these codes meets the Griesmer bound with equality.

2.4 Case $m=2, n=6, k=3, w=q^6-1, l=1$

Let $t=q^6-1-j$, where $j<q^4$. Then $tq=q^6-1-jq, tq^2=q^6-1-jq^2$. Both these elements are smaller than t. We see that $t=z_j, j\notin H$. It follows $\Delta(t)=6$ in these cases.
Let $t=q^6-q^4-1$. The cyclotomic coset $Z(t)=-Z(1)$ has length 6, with minimal element $z_1=q^6-q^5-1$ and $t=z_2=z_1q$ It follows $2\in H$. By Theorem 4 we have $\Delta(q^6-q^4-1)=0$. It follows that $\mathcal{A}(q^6-q^4-1,\Phi)^\perp$ is a q^2-ary code with $\mathbb{F}_q$-dimension $2+6=8$.
Let $t=q^6-1-q^4-j$, where $j<q$. We have $tq=q^6-q^5-jq-1, tq^5=q^6-jq^5-q^3-1$. Again we see that both these elements are smaller than t. As $tq^5/tq=q^4$ and 3 does not divide 4 we see that $t=z_j, j\notin H$. Thus $\Delta(t)=6$.
Finally consider $t=q^6-1-q^4-q$. We have $s=3, z_1=q^6-1-q^5-q^2, z_2=t=z_1q^5$. As 3 does not divide 5 we have $2\in H$, hence $\Delta(t)=n-s=3$ (Theorem 4). We have shown the following:

Theorem 5 *Let $n=6, m=2, k=3, w=q^6-1, l=1$. Then the extended twisted BCH-codes $\mathcal{A}(q^6-q^4-q-1,\Phi)^\perp\supset\mathcal{A}(q^6-q^4-1,\Phi)^\perp\supset\mathcal{A}(q^6-1,\Phi)^\perp$ form a chain of q^2-ary $\mathbb{F}_q-$linear codes with parameters*

$$[q^6,11,q^6-q^4-q]\supset[q^6,8,q^6-q^4]\supset[q^6,2,q^6].$$

Here the dimensions are over $\mathbb{F}_q$. Concatenation with an $\mathbb{F}_q-$ary linear code $[q+1,2,q]$ leads to a chain of linear $\mathbb{F}_q-$ary codes

$$[q^6(q+1),11,q^2(q^5-q^3-1)]\supset[q^6(q+1),8,q^5(q^2-1)]\supset[q^6(q+1),2,q^7].$$

The middle code, of dimension 8, meets the Griesmer bound with equality. We have analized the special case $q = 2$ of this Theorem in subsection 2.1. In case $q = 3$ we obtain codes

$$[2916, 11, 1935] \supset [2916, 8, 1944] \supset [2916, 2, 2187].$$

Griesmer steps, when applied to the largest of these codes, produce ternary codes $[981, 10, 645]$, $[336, 9, 215]$ and $[121, 8, 72]$. Observe that no ternary code $[121, 8, 73]$ is known.

2.5 Parameters of new linear codes

For the convenience of the reader we collect the new parameters of linear codes constructed in this section. More parameters improving on the data base [2] may be obtained by standard constructions like shortening, puncturing and residues.

q	code parameters	section
2	[78,10,34]	2.1.1
2	[84,10,38]	2.1.1
2	[87,10,40]	2.1.1
2	[93,10,42]	2.1.1
2	[96,10,44]	2.1.1
2	[100,10,46]	2.1.1
2	[103,10,48]	2.1.1
2	[171,11,78]	2.1.1
2	[174,11,80]	2.1.1
2	[177,11,82]	2.1.1
2	[180,11,84]	2.1.1
2	[183,11,86]	2.1.1
2	[186,11,88]	2.1.1
2	[186,9,90]	2.1.1
2	[189,11,90]	2.1.1
2	[192,11,92]	2.1.1
2	[193,9,94]	2.1.1
2	[196,11,94]	2.1.1
2	[196,9,96]	2.1.1
2	[199,11,96]	2.1.1
2	[203,9,98]	2.2
2	[209,11,98]	2.1.1
2	[213,11,100]	2.1.1
2	[211,9,102]	2.2
2	[217,11,102]	2.1.1

q	code parameters	section
2	[214,9,104]	2.2
2	[220,11,104]	2.1.1
2	[221,9,108]	2.2
2	[228,9,112]	2.2
2	[246,10,118]	2.1.1
2	[249,10,120]	2.1.1
3	[983,7,654]	2.3.1
3	[992,7,660]	2.3.1
3	[1006,7,669]	2.3.1
3	[1017,7,676]	2.3.1
3	[1033,7,687]	2.3.1
3	[1046,7,696]	2.3.1
3	[1059,7,705]	2.3.1
3	[1072,7,714]	2.3.1
3	[1085,7,723]	2.3.1
3	[2916,11,1935]	2.4
3	[2916,8,1944]	2.4
4	[326,5,244]	2.3.2
4	[329,5,246]	2.3.2
4	[336,5,252]	2.3.2
4	[341,5,256]	2.3.2

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,* to appear in *IEEE Transactions on Information Theory.*

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

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

[6] P.Delsarte: *Bounds for unrestricted codes, by linear programming, Philips Research Reports* **27** (1972),272-289.

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

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