Extending and lengthening BCH-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)

Abstract

We give a simplified and self-contained treatment of the theory of $BCH-$codes. This allows us to make use of various recursive construction techniques and obtain a large number of linear codes with new parameters.

Index Terms

BCH codes, extension, lengthening, construction X, construction XX, cyclotomic cosets.

1 Introduction

We have studied the structure of Reed-Solomon subfield codes in an earlier paper [5]. This enabled us to construct new codes by making use of various recursive techniques, most prominently Construction X (see [11],p.581f and Theorem 8). As the one-point truncations of Reed-Solomon subfield codes are precisely the primitive BCH codes it is natural to extend our study to

BCH codes in general. The use of general (not necessarily narrow-sense) BCH codes makes the application of Construction XX (see [1],Theorem 9) particularly profitable. The structure of this paper may be summarized as follows: firstly, in Section 2 we develop the basic theory of BCH codes. This enables us to determine the parameters of these codes and to construct certain related codes by the method of lengthening (see Theorem 7). In Subsection 2.3 we construct some new codes of moderate length with these techniques. The bulk of the paper is in Section 3. We apply Construction X, Construction XX and some related methods and obtain a large number of new binary, ternary and quaternary codes. Among the best codes constructed in this paper we mention the following:

- $[76, 39, 14]_2, [154, 14, 66]_2, [170, 25, 60]_2, [273, 246, 8]_2,$
- $[33, 21, 7]_3, [40, 27, 7]_3, [51, 37, 7]_3, [44, 29, 8]_3, [90, 71, 8]_3, [89, 67, 9]_3,$ $[25, 10, 10]_3, [58, 10, 30]_3, [95, 10, 53]_3, [92, 7, 57]_3, [96, 7, 60]_3,$
- $[82, 73, 5]_4, [93, 81, 6]_4, [69, 50, 9]_4, [43, 12, 19]_4, [53, 6, 36]_4, [75, 7, 50]_4,$ $[77, 8, 50]_4, [95, 6, 66]_4.$

Here the subscript denotes the field over which the code is defined. Codes $[76, 39, 14]_2, [92, 7, 57]_3, [43, 12, 19]_4$ are constructed in Subsections 3.3, 3.2 and 2.3, respectively. The other codes are to be found in Tables 1, 2, 6, 8, 9, 10, 14, 16, and 17. In Section 5 a few of these codes are given concretely in terms of either a generator matrix or a check matrix.

2 Basic theory

The following notation will be used throughout the paper.

Notation 1 *Let q be a prime-power, $n > 1$ a natural number, $tr : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ the* **trace.** *Put $F = \mathbb{F}_{q^n}$, let W be the subgroup of the multiplicative group of F of order w (so w is a divisor of $q^n - 1$) and $2 \leq t \leq w$.*

We will define a family of linear orthogonal arrays, whose duals will turn out to be the BCH codes.

Definition 1 *Let $\mathcal{P}(l,t)$ be the space of polynomials in one variable with coefficients in F, whose monomials have degrees between l and $l+t-2$ (here $t \geq 2$). We define an array $\mathcal{B}(l,t,w)$ with w columns indexed by $u \in W$ and $q^{n(t-1)}$ rows indexed by the polynomials $p(X) \in \mathcal{P}(l,t)$. The entry in column u and row $p(X)$ is*

$$tr(p(u)).$$

Definition 2 *An* **orthogonal array** *$OA_\lambda(t,k,v)$ is a $(v^t\lambda, k)$-array of symbols from a set of cardinality v having the property that in the projection onto any set of t columns each t-tuple of entries occurs precisely λ times. t is the* **strength** *of the array.*

Lemma 1 *The array $\mathcal{B}(l,t,w)$ of Definition 1 is an orthogonal array of strength $t-1$ over $\mathbb{F}_q$.*

Proof: Given $t-1$ pairwise different elements $u_j \in F$ and $t-1$ arbitrary elements $\alpha_j \in \mathbb{F}_q, j = 1,2,\ldots,t-1$, we have to show that the number of rows of our array with entries α_j in columns u_j for all j is independent of the choice of the u_j and α_j. Pick $\beta_j \in F$ such that $tr(\beta_j) = \alpha_j, j = 1,2,\ldots,t-1$. It suffices to show that there is precisely one polynomial $p(X) \in \mathcal{P}(l,t)$ satisfying $p(u_j) = \beta_j$ for all j. This is an elementary fact in polynomial interpolation.■

Our arrays $\mathcal{B}(l,t,w)$ are in fact linear over $\mathbb{F}_q$ in the sense that its rows form a vector space over $\mathbb{F}_q$. It is obvious that the dual of a linear orthogonal array of strength $t-1$ (dual with respect to the usual dot product) is a linear code of minimum distance $\geq t$. Moreover we can identify the dual codes $\mathcal{B}(l,t,w)^\perp$ with the BCH codes (for an Introduction into these Bose-Chaudhuri-Hocquenghem codes see [11], Chapter 9). Case $l = 1$ leads to the BCH codes in the **narrow sense,** case $w = q^n - 1$ to the **primitive** BCH codes. As a preparation we introduce cyclotomic cosets. The set $I = \{l, l+1, \ldots, l+t-2\} = [l, l+t-2]$ will be called the **defining interval** of the code $\mathcal{B}(l,t,w)^\perp$.

Definition 3 *Let $G = G(F|\mathbb{F}_q)$ be the Galois group, generated by the Frobenius automorphism ϕ. Consider the permutation representation of G on $\mathbb{Z}/w\mathbb{Z}$ defined by*

$$\phi : i \longrightarrow j \text{ if and only if } iq \equiv j (mod\ w).$$

The orbits of this action are the **cyclotomic cosets.** *The orbit containing i is $Z_w(i)$. In the case of the codes $\mathcal{B}(l,t,w)$ we use $[l, l+w-1]$ as the set of representatives for the action and use the ordering $l < l+1 < \ldots < l+w-1$. Denote the smallest member of the cyclotomic coset containing i (with respect to this ordering, for given l) by $\bar{i}$.*

Theorem 1 *$\mathcal{B}(l,t,w)^\perp$ is a general BCH-code of designed distance t.*

Proof: Let $p(X) = \sum_{j=l}^{l+t-2} a_j X^j \in \mathcal{P}(l,t)$. Choose a primitive w-th root of unity $\beta \in F$. Let coordinate i of the code correspond to the field element $\beta^i, i = 1, 2, \ldots, w$. The entry c_i of $\mathcal{B}(l,t,w)$ indexed by $p(X)$ is $c_i = tr(p(\beta^i))$. As is common usage in the theory of cyclic codes we consider a polynomial which has the c_i as coefficients: $\tilde{p}(X) = \sum_{i=1}^{w} c_i X^{w-i}$. Then $\tilde{p}(\beta^k) = \sum_{i=1}^{w} \sum_{r=0}^{n-1} \sum_{j=l}^{l+t-2} a_j^{q^r} \beta^{i(jq^r-k)} = \sum_{r=0}^{n-1} \sum_{j=l}^{l+t-2} a_j^{q^r} \sum_{i=1}^{w} \beta^{i(jq^r-k)}$. The last sum vanishes if $jq^r \neq k$. It follows that $\tilde{p}(\beta^k) = 0$ if the cyclotomic coset containing k is disjoint from the defining interval I.
Assume now $Z_w(k)$ does contain an element $j \in I$. Consider $p(X) = ax^j, a \in F$. Then $\tilde{p}(\beta^k) = w \cdot \sum_{r:jq^r=k} a^{q^r}$. As $w|(q^n-1)$ we have $w \neq 0$. A suitable choice of $a \in F$ leads to $\tilde{p}(\beta^k) \neq 0$ as otherwise the polynomial $\sum_{r=0}^{n-1} X^{q^r}$, of degree q^{n-1}, would have q^n roots, which is impossible. We have shown that β^k is a common root of all the polynomials $\tilde{p}(X)$, where $p(X) \in \mathcal{P}(l,t)$, if and only if $Z_w(k) \cap I = \emptyset$. This is the standard description in the theory of cyclic codes for the dual of the BCH code with designed distance t.■

It may be noted that is not quite appropriate to call t in Theorem 1 the designed distance of $\mathcal{B}(l,t,w)^\perp$. If for instance $\mathcal{B}(l,t,w)^\perp = \mathcal{B}(l,t+1,w)^\perp$ or $\mathcal{B}(l,t,w)^\perp = \mathcal{B}(l-1,t+1,w)^\perp$, then we know that the minimum distance is $> t$. We shall nonetheless hold on to the terminology of Theorem 1.

Notation 2 *Denote by $\mathcal{P}_0(l,t,w)$ the set of those polynomials $p(X) \in \mathcal{P}(l,t)$ satisfying $tr(p(W)) = 0$. It is clear that $\mathcal{P}_0(l,t,w)$ is a vector-space over $\mathbb{F}_q$. Denote its dimension by $\rho_0(l,t,w)$.*

Definition 1 shows that each row of the array $\mathcal{B}(l,t,w)$ occurs with frequency $q^{\rho_0(l,t,w)}$. We conclude that the row space of $\mathcal{B}(l,t,w)$ has dimension $n(t-1)-\rho_0(l,t,w)$. This shows that the dual code's dimension is determined by $\rho_0(l,t,w)$:

Theorem 2 *The q-ary BCH code $\mathcal{B}(l,t,w)^\perp$ of length w and designed distance t has dimension $w - n(t-1) + \rho_0(l,t,w)$.*

2.1 The function $\rho_0(l,t,w)$

Definition 4 *Denote by $C_{l,i}$ the q^n-ary code of dimension i and length w with generator matrix whose columns are indexed by $u \in W$ and whose rows are indexed by $k \in [l, l+i-1]$, with entry u^k in row k, column u. Here $1 \leq i \leq w$.*

Lemma 2 $C_{l,i}^{\perp} = C_{w-l+1,w-i}$ *if $l \leq w$.*

Proof: As $dim(C_{l,i}) = i$ and $dim(C_{w-l+1,w-i}) = w - i$, the dimensions are right (these dimensions are over F). It remains to show that the rows of the generator matrices are orthogonal to each other. This follows from the fact that $\sum_{u \in W} u^k = 0$ if k is not a multiple of w. ■

Definition 5 *Let $\rho_1(l,t,w)$ denote the dimension of the $\mathbb{F}_q$-vector space of polynomials $p(X) \in \mathcal{P}(l,t)$ satisfying*

$$p(W) \subseteq \mathbb{F}_q.$$

We can now express the dimension of $\mathcal{B}(l,t,w)^{\perp}$ with the help of the function ρ_1 now. A basic theorem of Delsarte's ([8], Theorem 2) states that the trace-code of a code C is the subfield code of the dual $C^{\perp}$. It follows that $\mathcal{B}(l,t,w)^{\perp}$, being the subfield code of $C_{w-l+1,w-t+1}$ by Lemma 2, has dimension $\rho_1(w-l+1, w+2-t, w)$. Comparison with Theorem 2 yields a relation of duality between the functions ρ_0 and ρ_1 :

Theorem 3

$$w + \rho_0(l,t,w) = (t-1)n + \rho_1(w-l+1, w+2-t, w)$$

We will now use cyclotomic cosets to describe the growth of $\rho_1(l,t,w)$ as a function of t. Let $p(X) = \sum_{j=l}^{l+t-2} a_j X^j \in \mathcal{P}(l,t)$ be a polynomial satisfying $p(W) \subseteq \mathbb{F}_q$. We are only interested in the cases where $t < w$. The condition $p(W) \subseteq \mathbb{F}_q$ is obviously equivalent with $X^w - 1 \mid p(X)^q - p(X)$. Consider $p(X)^q = \sum_j a_j^q X^{jq}$. This polynomial affords the same mapping as $\sum_j a_j^q X^{\lfloor jq \rfloor}$, where $\lfloor i \rfloor$ is the remainder of i modulo w, chosen in the defining set I. So this last polynomial is congruent to $p(X)$ modulo $X^w - 1$. As the degrees of these polynomials are less than w, they must coincide. We conclude: $a_j^q = a_{\lfloor jq \rfloor}$. Observe that the mapping $j \longrightarrow \lfloor jq \rfloor$ is the action of the Frobenius automorphism introduced in Definition 3. We conclude that the coefficient a_j uniquely determines the coefficients of X^k for each member k of the cyclotomic coset $Z_w(j)$. The following is an easy consequence:

Theorem 4 *Let $t < w$. Call t* **maximal** *if it is the maximal element of its cyclotomic coset $Z_w(t)$, with respect to the ordering of $[l, l+w-1]$ as introduced in Definition 3. Put $s = \mid Z_w(t) \mid$. Then*

$$\rho_1(l, t+1, w) - \rho_1(l, t, w) = \begin{cases} 0 & \textit{if } l+t-1 \textit{ is not maximal} \\ s & \textit{if } l+t-1 \textit{ is maximal.} \end{cases}$$

Using the duality Theorem 3 we get the desired expression for the growth of function ρ_0, as follows.

Theorem 5

$$\rho_0(l, t+1, w) - \rho_0(l, t, w) = \begin{cases} n & \textit{if } l+t-1 \textit{ is not minimal} \\ n-s & \textit{if } l+t-1 \textit{ is minimal} \end{cases}$$

Here s is the length of the cyclotomic coset $Z_w(t)$, and we are still using the ordering $l < l+1 < \ldots < l+w-1$.

These results facilitate the determination of the dimension of BCH codes.

2.2 Lengthening BCH-codes

Definition 6 *Let U be the $\mathbb{F}_q$-vector space of highest coefficients a_{l+t-2} of the polynomials in $\mathcal{P}_0(l, t, w)$ and $\Phi = \{\phi_i | i = 1, 2, \ldots, n - dim(U)\}$ a complete set of linearly independent linear functionals $\phi_i : F \longrightarrow \mathbb{F}_q$ having U in their kernels. Define an extension $(\mathcal{B}(l, t, w), \Phi)$ of the orthogonal array $\mathcal{B}(l, t, w)$ (see Definition 1) by $n - dim(U)$ additional columns indexed by the $\phi_i \in \Phi$. The entry in row $p(X)$ of the column indexed by ϕ_i is $\phi_i(a_{l+t-2})$, where $p(X) = \sum_{j=l}^{l+t-2} a_j X^j$.*

Theorem 6 *Let $\delta(l, t, w) = \rho_0(l, t, w) - \rho_0(l, t-1, w)$. Choose U and Φ as in Definition 6. Then $dim(U) = \delta(l, t, w)$.*
The code $(\mathcal{B}(l, t, w), \Phi)^\perp$ has parameters

$$[w + n - \delta(l, t, w), w - n(t-2) + \rho_0(l, t-1, w), t]$$

It may be described as an $(n - \delta(l, t, w))$-fold lengthening of $\mathcal{B}(l, t, w)^\perp$.

Proof: This proof is largely analogous to that of Theorem 3 in [5], so we can be short here. As there is a natural isomorphism between U and the factor space $\mathcal{P}_0(l,t,w)/\mathcal{P}_0(l,t-1,w)$ we have $dim(U)=\delta(l,t,w)$. It follows from polynomial interpolation that $(\mathcal{B}(l,t,w),\Phi)$ still has strength $t-1$. The dual code $\mathcal{B}(l,t,w)^{\perp}$, of length $w+n-\delta(l,t,w)$, therefore has minimum distance $\geq t$. As each $\phi_i \in \Phi$ has U in its kernel the row space of $(\mathcal{B}(l,t,w),\Phi)$ has the same dimension as that of $\mathcal{B}(l,t,w)$. It follows that the dimension of the dual code increases by $n-\delta(l,t,w)$.■

Corollary 1 *Assume* $\rho_0(l,t,w)=\rho_0(l,t-1,w)$.
If $t \leq n+1$ *and there is a* q*-ary linear code* $[e,e-n,t]$, *then* $\mathcal{B}(l,t,w)^{\perp}$ *may be lengthened* e *times to yield a code with parameters*

$$[w+e,w-n(t-1)+\rho_0(l,t,w)+e,t].$$

This is a slight generalization of Theorem 6 for small values of t. Observe that the linear functionals defining the extension of $\mathcal{B}(l,t,w)$ do not need to be independent. It suffices that any $t-1$ of them are independent. The existence of e linear functionals any $t-1$ of which are independent is equivalent with that of a linear q-ary code with parameters $[e,e-n,t]$. This proves Corollary 1.
We can generalize Theorem 6 in a different direction: Symmetrize the approach and consider linear functionals operating on the lowest coefficient a_l of $p(X)$, too. In this way we can extend our orthogonal array $\mathcal{B}(l,t,w)$ by $2n$ columns. In order to get a corresponding lengthening of the code $\mathcal{B}(l,t,w)^{\perp}$ we have to take care to use only linear functionals which vanish on the subspaces covered by the highest and lowest coefficients of $\mathcal{P}_0(l,t,w)$. This leads to the following theorem:

Theorem 7 *Let* $\delta(l,t,w)=\rho_0(l,t,w)-\rho_0(l,t-1,w), \delta'(l,t,w)=\rho_0(l,t,w)-\rho_0(l+1,t-1,w)$. *The code* $\mathcal{B}(l,t,w)^{\perp}$ *can be lengthened* $2n-\delta(l,t,w)-\delta'(l,t,w)$ *times.*

A particular case is $l=0$. By definition $\delta'(0,t,w)$ is the dimension of the space of $u \in F$ satisfying $tr(u)=0$, and hence $n-\delta'(0,t,w)=1$. It follows from Theorem 7 that $\mathcal{B}(0,t,w)^{\perp}$ can always be lengthened once. Let us denote the corresponding extended array by $\mathcal{A}(0,t,w)$. We have seen that

the lengthened BCH-code $\mathcal{A}(0,t,w)^{\perp}$ has parameters $[w+1, w+1-n(t-1)+\rho_0(0,t,w), t]$. In case $w=q^n-1$ the code $\mathcal{A}(0,t,w)^{\perp}$ is a Reed-Solomon subfield code. These are the codes we studied in [5].
In Section 3 we shall introduce and apply Constructions X and XX. It is easy to see that Theorem 6 and Corollary 1 are special cases of Construction X and Theorem 7 is a special case of Construction XX (see Theorems 8 and 9).

2.3 New codes via lengthening

We now give some applications of Theorem 7. In Table 1 we give the values of q, n, w, l and the parameters of the code obtained. The value of t coincides with the distance of the code, and the difference between the length and w equals $2n-(\delta(l,t,w)+\delta'(l,t,w))$. The most interesting of these codes is the quaternary $[53,6,36]_4$. It is optimal. Concatenation with the binary code $[3,2,2]_2$ yields a code with the new binary parameters $[159,12,72]_2$. Let us explain the mechanism in more detail for this example: we have $q=4, n=4, w=51, t=36$. Repeated use of Theorem 5 shows that $\rho_0(0,35,51)=90, \rho_0(0,36,51)=93$. By Theorem 2 the code $\mathcal{B}(0,36,51)^{\perp}$ has parameters $[51,4,36]$. We apply Theorem 7. As explained after the statement of that theorem we have $n-\delta'(0,t,w)=1$. The values above show that $n-\delta(0,t,w)=1$. Theorem 7 guarantees that our BCH-code $[51,4,36]$ can be lengthened twice.
Next we list, in Table 2, a few lengthenings generated by computer. In each case we list q, n, w, the parameters of the BCH code $\mathcal{B}(0,t,w)^{\perp}$, and the parameters of the code obtained via computer by repeated lengthening. Here is an example: in case $q=3, n=4, w=20$ repeated use of Theorem 5 shows $\rho_0(0,10,20)=21$. Theorem 2 shows that $\mathcal{B}(0,10,20)^{\perp}$ has parameters $[20,5,10]$. A computer search produced a 5-step lengthening, hence a code $[25,10,10]_3$. This explains the third entry in Table 2. Full information on these codes is available in the first author's homepage [4]. Consider the check matrix of $[93,81,6]_4$ as given there. The first 43 columns of this matrix generate a code with the new parameters $[43,12,19]_4$.

3 Extending BCH codes

3.1 Using Construction X

We use a basic result on lengthening codes known as Construction X ([11], p.581/582) in the following form

Theorem 8 (construction X) *Let $\mathcal{C}$ be a q-ary code with parameters $[n, k, d]$ and $\mathcal{D}$ a subcode of $\mathcal{C}$ of codimension κ and minimum distance $\geq d + \delta$ for some $\delta > 0$. If there is a code with parameters $[e, \kappa, \delta]$ then there is a code $\tilde{\mathcal{C}}$ with parameters $[n + e, k, d + \delta]$, which projects onto $\mathcal{C}$.*

Let I_1, I_2 be the defining intervals of BCH codes $\mathcal{C}$ and $\mathcal{D}$, respectively. If $I_1 \subset I_2$, then $\mathcal{C} \supset \mathcal{D}$. Theorem 8 can then be applied to this chain of codes. The auxiliary codes $[e, \kappa, \delta]$ are usually taken from the data base [6]. Sometimes we use one of our own new codes as an auxiliary code. In Tables 3,4,5, 6 we give the parameters of the pairs $\mathcal{C} \supset \mathcal{D}$ of BCH codes, the boundaries $(l, l + t - 2)$ of the defining interval for $\mathcal{C}$ and for $\mathcal{D}$, the parameters of the auxiliary code, and finally the parameters of the code obtained from Theorem 8. We also take the liberty to eventually apply Construction X not to the pair $\mathcal{C} \supset \mathcal{D}$, but to a pair $\mathcal{C}' \supset \mathcal{D}$, where $\mathcal{C}'$ is a code between $\mathcal{D}$ and $\mathcal{C}$. The dimension of the auxiliary code shows when this happens. Here is an instance where we can use one of the computer-generated lengthenings of Table 2: we saw in [5] that there is a pair of ternary Reed-Solomon subfield codes $[81, 15, 42] \supset [81, 5, 54]$. Application of Theorem 8 with the computer-generated $[25, 10, 10]$ from Table 2 as auxiliary code yields a new code $[106, 15, 52]_3$.
The values of w used correspond to the factorizations $3^3 - 1 = 26, 3^4 - 1 = 80, 3^8 - 1 = 80 \cdot 82, 3^5 - 1 = 2 \cdot 121$ and $4^6 - 1 = 63 \cdot 65, 4^4 - 1 = 3 \cdot 85$. A quaternary code $[65, 27, 23]$ had been constructed in [5] by different means. Here we see that there is in fact a BCH code with these parameters and we use it in Table 6 to construct longer codes with new parameters. In the same vein, a quaternary $[65, 8, 44]$ has been constructed by Groneick and Grosse in [9]. These authors used the code for the construction of several new binary codes. In [5] we constructed a code with these parameters as an extension of a primitive BCH code. It turns out that there is a BCH code with these parameters. We use it for the construction of a $[77, 8, 50]$ in Table 6. Likewise, it had not been observed that there is a BCH code with

parameters $[85, 6, 60]$. In the data base [6] a manuscript of de Boer is given as source for these parameters.

3.2 Iterating construction X

When we have a chain of codes $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$ we apply Construction X to the pair $\mathcal{C}_1 \supset \mathcal{C}_2$ first, producing a chain of codes $\tilde{\mathcal{C}_i}$. Then we apply Construction X to the pair $\tilde{\mathcal{C}_1} \supset \tilde{\mathcal{C}_3}$. Let us illustrate with a ternary example in case $w = 80, l = 31$. We obtain a chain of codes $[80, 7, 50] \supset [80, 6, 51] \supset [80, 2, 60]$. Using the trivial auxiliary code $[1, 1, 1]$ produces a $[81, 7, 51] \supset [81, 2, 60]$. Finally we use the auxiliary code $[11, 5, 6]$ (a subcode of the ternary Golay code) and obtain a code $[92, 7, 57]_3$. Apart from this example, our applications of this method that yield new code parameters are all in the case $q = 2, w = 127, l = 1$ (see Table 7) and correspond to primitive BCH codes. It suffices therefore to give the parameters of our codes and of the auxiliary codes. As before we give the chain of BCH codes, but eventually we apply the procedure to subcodes. Observe how the binary Golay code furnishes auxiliary codes in these constructions.
The following is a slight generalization of Alltop's Construction XX (see [1]).

3.3 Applying construction XX

Theorem 9 (Construction XX) *Let $\mathcal{C}, \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_0$ be q-ary codes of length n such that $\mathcal{C} \supset \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_0 = \mathcal{C}_1 \cap \mathcal{C}_2$. Put $dim(\mathcal{C}) = k, dim(\mathcal{C}/\mathcal{C}_j) = \kappa_j, j = 1, 2$. Let the minimum distances of the codes be $dist(\mathcal{C}) = d, dist(\mathcal{C}_i) = d_i, i = 0, 1, 2$. If there exist codes $[e_1, \kappa_1, x_1]$ and $[e_1, \kappa_2, x_2]$, then a code with parameters $[n + e_1 + e_2, k, min\{d_0, d_1 + x_2, d_2 + x_1, d + x_1 + x_2\}]$ can be constructed by lengthening $\mathcal{C}$.*

Proof: Apply Construction X (Theorem 8) to the pair $\mathcal{C} \supset \mathcal{C}_1$. This yields a code $\tilde{\mathcal{C}}$ with parameters $[n + e_1, k, min(d_1, d + x_1)]$, containing the subcode $\tilde{\mathcal{C}_2}$. As $\mathcal{C}_0 = \mathcal{C}_1 \cap \mathcal{C}_2$ we see that each vector in $\mathcal{C}_2 - \mathcal{C}_0$ will have weight $\geq d_2 + x_1$ in $\tilde{\mathcal{C}}$. It follows that the minimum weight of $\tilde{\mathcal{C}_2}$ is $\geq min\{d_0, d_2 + x_1\}$. An application of Construction X to the pair $\tilde{\mathcal{C}} \supset \tilde{\mathcal{C}_2}$ yields the final result. ■

Let us apply this theorem in the situation of BCH codes. More precisely put $\mathcal{C}_0 = \mathcal{B}(l, t, w)^\perp, \mathcal{C}_1 = \mathcal{B}(l + i, t - i, w)^\perp, \mathcal{C}_2 = \mathcal{B}(l, t - j, w)^\perp, \mathcal{C} = \mathcal{B}(l +$

$i, t-i-j, w)^\perp$. It is clear that the conditions of Theorem 9 are satisfied, in particular $\mathcal{C}_1 \cap \mathcal{C}_2 = \mathcal{C}_0$. In the following tables we list applications of this construction method. As before our BCH codes $\mathcal{B}(l,t,w)^\perp$ may be easiest described by their defining intervals $I = [l, l+1, \dots, l+t-2]$. We know that the minimum distance of the code is lower-bounded by 1 plus the cardinality of the defining interval. It is therefore unnecessary to include the distance in the tables. If $I_0 = [a, a+1, \dots, b]$ is the interval of $\mathcal{C}_0$, then the intervals of $\mathcal{C}_1$ and $\mathcal{C}_2$ will be $I_1 = [a+i, \dots, b]$ and $I_2 = [a, \dots, b-j]$, respectively. The fact that $\mathcal{C}_0 = \mathcal{C}_1 \cap \mathcal{C}_2$ follows from $I_0 = I_1 \cup I_2$. The interval I of $\mathcal{C}$ will be contained in $[a+i, \dots, b-j]$. Naturally we only consider situations where $a+i < b-j$.

In Tables 8-13 we give the pair (a,b) (and thus the code $\mathcal{C}_0$), the best estimate for the minimum distance of $\mathcal{C}_0$ (recall that if the same code $\mathcal{C}_0$ is defined by an interval which is is larger than I_0, then by our theory the minimum distance of $\mathcal{C}_0$ will be larger than $b-a+1$), the values i,j defining $\mathcal{C}_1, \mathcal{C}_2$, the pair (x,y) giving the defining interval I of $\mathcal{C}$, the dimensions of the four codes involved, the parameters of the auxiliary codes and finally the parameters of the resulting code. Let us illustrate with an example in case $q=2, w=63$. We have $I_0 = \{53, \dots, 65\}$, hence $a=53, b=65$. This code has parameters $[63,29,14]$. We use $i=3, j=2$, leading to codes $\mathcal{C}_1, \mathcal{C}_2$ of parameters $[63,36,11]$ and $[63,32,12]$, respectively (note that the distances of $\mathcal{C}_1$ and $\mathcal{C}_2$ are, respectively, i and j less than that of $\mathcal{C}_0$). The interval defining $\mathcal{C}$ is $I = [55, \dots, 62]$, hence $x=55, y=62$. This code has parameters $[63,39,9]$. Application of Construction XX with auxiliary codes $[4,3,2]$ and $[8,7,2]$ yields a code $[75,39,13]_2$.

3.4 Iterating Construction XX

Let $\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3$ be a chain of q-ary codes of length n, and let $\mathcal{U} \subset \mathcal{C}_1$ be another subcode of $\mathcal{C}_1$, of codimension κ. Apply Construction X to the pair $\mathcal{C}_1 \supset \mathcal{U}$, with an auxiliary code $[e, \kappa, \delta]$. We obtain a chain of lengthened codes $\tilde{\mathcal{C}_1} \supset \tilde{\mathcal{C}_2} \supset \tilde{\mathcal{C}_3}$, (lengths $n+e$). The minimum distances of these codes are bounded as follows: $d(\tilde{\mathcal{C}_1}) \geq min\{d(\mathcal{C}_1)+\delta, d(\mathcal{U})\}, d(\tilde{\mathcal{C}_1}) \geq min\{d(\mathcal{C}_2)+\delta, d(\mathcal{U} \cap \mathcal{C}_2)\}, d(\tilde{\mathcal{C}_3}) \geq min\{d(\mathcal{C}_3)+\delta, d(\mathcal{U} \cap \mathcal{C}_3)\}$. We then apply the iteration of Construction X to this chain.

Choose $\mathcal{C}_i = \mathcal{B}(l, t_i, w)^\perp$, where $t_1 < t_2 < t_3$. As before we will give in Tables 14-17 the values of l, of the largest member $r_i = l + t_i - 2$ of the defining interval of $\mathcal{C}_i$ and the dimension k_i of $\mathcal{C}_i$. Choose $\mathcal{U}$ to be the BCH code with defining interval $[l', l+t_1-2]$ 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 $[l', l+t_i-2]$. We also give the dimension k of U. Finally we need to know which auxiliary codes are being used. As before we apply this mechanism not only to the BCH codes themselves but also to intermediate codes. The dimensions of the auxiliary codes show when this happens. We illustrate the procedure with an example from Table 15. The first chain of BCH codes, with defining intervals $[1, 14], [1, 16]$ and $[1, 18]$, respectively, has parameters $[255, 199, 15] \supset [255, 191, 17] \supset [255, 187, 19]$. The second chain corresponds to defining intervals $[0, 14], [0, 16]$ and $[0, 18]$. Their minimum distances are clearly one larger than those of the members of the first chain. First apply Construction X (i.e. Theorem 8) with the auxiliary code $[1, 1, 1]$. This indicates that the larger of the two codes to which we apply the construction is not $\mathcal{C}_1$, but a subcode $[252, 192, 15]$. After lengthening we have a chain of codes with parameters $[256, 199, 16] \supset [256, 191, 18] \supset [255, 187, 20]$. We are now in a position to apply the iterated X-construction. The result is a code $[264, 192, 20]_2$.

3.5 When the distance is larger

In some cases the minimal distance is larger than designed. It was shown in [10] that the binary primitive BCH code of length 127, dimension 43 and designed distance 29 has true minimal distance 31, and hence has parameters $[127, 43, 31]$. Moreover it was shown in [2] that in 2 cases binary primitive BCH codes of length 255 have true minimum distance two larger than designed. This accounts for binary codes $[255, 63, 63]$ (designed distance 61) and $[255, 71, 61]$ (designed distance 59). Using these values in Construction X leads to some new codes. Tables 18 and 19 are organized as in Subsection 3.1 dedicated to the application of Construction X. The iterated construction X yields two more new codes in case $q = 2, w = 127, l = 1$, see Table 20.

4 Tables

Table 1: Standard lengthenings

q	n	w	l	parameters
3	4	80	31	[84,35,22]
3	4	80	34	[88,63,10]
3	4	80	31	[86,55,13]
3	4	80	28	[88,49,16]
3	4	80	25	[88,41,19]
3	4	80	19	[88,31,25]
3	4	80	31	[82,35,21]
3	5	121	59	[126,101,9]
3	5	121	59	[126,91,12]
3	5	121	0	[127,76,18]
3	5	121	53	[126,91,12]
3	5	121	52	[131,91,13]
3	6	56	0	[58,10,30]
4	3	63	62	[69,50,9]
4	3	63	62	[69,44,12]
4	3	63	62	[69,41,13]
4	3	63	62	[69,25,25]
4	3	63	62	[69,19,29]
4	4	85	50	[89,63,11]
4	4	51	0	[53,6,36]

Table 2: Computer-generated lengthenings

q	n	w	$\mathcal{B}(0,t,w)^{\perp}$	result
3	3	26	[26,14,7]	[33,21,7]
3	4	16	[16,3,7]	[40,27,7]
3	4	20	[20,5,10]	[25,10,10]
3	4	40	[40,26,7]	[51,37,7]
3	4	40	[40,25,8]	[44,29,8]
3	4	80	[80,64,7]	[88,72,7]
4	3	63	[63,54,5]	[82,73,5]
4	3	63	[63,51,6]	[93,81,6]

Table 3: Construction X: case $q = 2, w = 127$

pair of codes	$\mathcal{C}$	$\mathcal{D}$	aux. code	result
$[127,36,31] \supset [127,29,43]$	$(1,30)$	$(1,42)$	$[16,5,8]$	$[143,34,39]$
			$[21,5,10]$	$[148,34,41]$
			$[24,5,12]$	$[151,34,43]$
$[127,29,43] \supset [127,22,47]$	$(1,42)$	$(1,46)$	$[8,4,4]$	$[135,26,47]$
$[127,22,47] \supset [127,15,55]$	$(1,46)$	$(1,54)$	$[12,4,6]$	$[139,19,53]$
$[127,29,43] \supset [127,15,55]$	$(1,42)$	$(1,54)$	$[34,12,12]$	$[161,27,55]$
			$[32,13,10]$	$[159,28,53]$
			$[37,14,12]$	$[164,29,55]$

Table 4: Construction X: case $q = 2, w = 255$

pair of codes	$\mathcal{C}$	$\mathcal{D}$	aux. code	result
$[255, 231, 7] \supset [255, 223, 9]$	$(1, 6)$	$(1, 8)$	$[9, 8, 2]$	$[264, 231, 9]$
$[255, 215, 11] \supset [255, 207, 13]$	$(1, 10)$	$(1, 12)$	$[9, 8, 2]$	$[264, 215, 13]$
$[255, 199, 15] \supset [255, 191, 17]$	$(1, 14)$	$(1, 16)$	$[9, 8, 2]$	$[264, 199, 17]$
$[255, 45, 87] \supset [255, 37, 91]$	$(1, 86)$	$(1, 90)$	$[9, 8, 2]$	$[264, 45, 89]$
$[255, 10, 122] \supset [255, 8, 128]$	$(171, 36)$	$(165, 36)$	$[3, 2, 2]$	$[258, 10, 124]$
			$[6, 2, 4]$	$[261, 10, 126]$
$[255, 38, 90] \supset [255, 36, 92]$	$(171, 4)$	$(169, 4)$	$[3, 2, 2]$	$[258, 38, 92]$
$[255, 30, 94] \supset [255, 28, 96]$	$(171, 8)$	$(169, 8)$	$[3, 2, 2]$	$[258, 30, 96]$
$[255, 22, 102] \supset [255, 20, 104]$	$(171, 16)$	$(169, 16)$	$[3, 2, 2]$	$[258, 22, 104]$
$[255, 134, 34] \supset [255, 130, 36]$	$(239, 16)$	$(237, 16)$	$[5, 4, 2]$	$[260, 134, 36]$
$[255, 142, 30] \supset [255, 134, 34]$	$(239, 12)$	$(239, 16)$	$[4, 1, 4]$	$[259, 135, 34]$

Table 5: Construction X: case $q = 3$

pair of codes	$\mathcal{C}$	$\mathcal{D}$	aux. code	result
$[80,39,17] \supset [80,35,20]$	$(31,46)$	$(31,49)$	$[5,4,2]$	$[85,39,19]$
$[82,65,8] \supset [82,57,10]$	$(38,44)$	$(37,45)$	$[9,8,2]$	$[91,65,10]$
$[121,71,18] \supset [121,66,21]$	$(44,60)$	$(41,60)$	$[4,2,3]$	$[125,68,21]$
			$[6,5,2]$	$[127,71,20]$
			$[8,5,3]$	$[129,71,21]$
$[121,76,16] \supset [121,66,21]$	$(46,60)$	$(41,60)$	$[11,6,5]$	$[132,72,21]$
$[121,66,21] \supset [121,61,23]$	$(41,60)$	$(41,62)$	$[6,5,2]$	$[127,66,23]$
$[121,36,36] \supset [121,31,41]$	$(41,75)$	$(41,80)$	$[10,5,5]$	$[131,36,41]$
$[121,11,67] \supset [121,10,69]$	$(55,120)$	$(55,1)$	$[2,1,2]$	$[123,11,69]$
$[121,15,63] \supset [121,10,69]$	$(61,1)$	$(55,1)$	$[6,5,2]$	$[127,15,65]$
			$[11,5,6]$	$[132,15,69]$
$[121,16,61] \supset [121,15,63]$	$(61,120)$	$(61,1)$	$[2,1,2]$	$[123,16,63]$
$[121,75,17] \supset [121,65,21]$	$(106,0)$	$(106,4)$	$[15,10,4]$	$[136,75,21]$

Table 6: Construction X: case $q = 4$

pair of codes	$\mathcal{C}$	$\mathcal{D}$	aux. code	result
$[65, 27, 23] \supset [65, 15, 31]$	$(22, 43)$	$(18, 47)$	$[19, 12, 6]$	$[84, 27, 29]$
$[65, 27, 23] \supset [65, 21, 25]$	$(22, 43)$	$(21, 44)$	$[7, 6, 2]$	$[72, 27, 25]$
$[65, 8, 44] \supset [65, 2, 52]$	$(44, 21)$	$(40, 25)$	$[12, 6, 6]$	$[77, 8, 50]$
$[65, 46, 10] \supset [65, 40, 12]$	$(61, 4)$	$(60, 5)$	$[7, 6, 2]$	$[72, 46, 12]$
$[85, 67, 8] \supset [85, 63, 10]$	$(29, 35)$	$(27, 35)$	$[5, 4, 2]$	$[90, 67, 10]$
$[85, 6, 60] \supset [85, 2, 68]$	$(56, 29)$	$(52, 33)$	$[10, 4, 6]$	$[95, 6, 66]$
$[85, 27, 29] \supset [85, 26, 31]$	$(57, 84)$	$(57, 1)$	$[2, 1, 2]$	$[87, 27, 31]$

Table 7: Construction X iterated: $q = 2, w = 127$

chain of codes	auxiliary codes	result
$[127, 29, 43] \supset [127, 22, 47] \supset [127, 15, 55]$	$[4, 1, 4], [17, 8, 6]$	$[148, 23, 53]$
	$[4, 1, 4], [20, 8, 8]$	$[151, 23, 55]$
	$[6, 2, 4], [21, 9, 8]$	$[154, 24, 55]$
	$[7, 3, 4], [22, 10, 8]$	$[156, 25, 55]$
	$[8, 4, 4], [23, 11, 8]$	$[158, 26, 55]$
$[127, 22, 47] \supset [127, 15, 55] \supset [127, 8, 63]$	$[8, 1, 8], [17, 8, 6]$	$[152, 16, 61]$
	$[8, 1, 8], [20, 8, 8]$	$[155, 16, 63]$
	$[14, 3, 8], [22, 10, 8]$	$[163, 18, 63]$
	$[11, 3, 6], [22, 10, 8]$	$[160, 18, 61]$
	$[12, 4, 6], [23, 11, 8]$	$[162, 19, 61]$

Table 8: Construction XX: $q = 2, w = 127$

(a, b)	$d(\mathcal{C}_0)$	i, j	(x, y)	k, k_1, k_2, k_0	aux. codes	result
$(65, 8)$	127	$8, 8$	$(73, 0)$	$14, 7, 7, 0$	$[8, 7, 2], [19, 7, 8]$	$[154, 14, 66]$
					$[11, 7, 3], [19, 7, 8]$	$[158, 14, 68]$
					$[15, 7, 5], [19, 7, 8]$	$[162, 14, 70]$
					$[18, 7, 7], [19, 7, 8]$	$[165, 14, 72]$
$(65, 8)$	127	$9, 8$	$(73, 126)$	$15, 8, 7, 0$	$[12, 7, 4], [20, 8, 8]$	$[160, 15, 68]$
					$[16, 7, 6], [20, 8, 8]$	$[164, 15, 70]$
					$[19, 7, 8], [20, 8, 8]$	$[167, 15, 72]$
					$[19, 7, 8], [9, 8, 2]$	$[156, 15, 66]$
$(73, 4)$	64	$4, 8$	$(81, 0)$	$21, 14, 14, 7$	$[18, 7, 7], [12, 7, 4]$	$[158, 21, 60]$
					$[19, 7, 8], [8, 7, 2]$	$[154, 21, 58]$
		$7, 8$			$[23, 7, 9], [15, 7, 5]$	$[166, 21, 62]$
$(73, 4)$	64	$4, 12$	$(85, 0)$	$28, 14, 21, 7$	$[37, 14, 12], [8, 7, 2]$	$[172, 28, 58]$
$(73, 4)$	64	$5, 8$	$(81, 126)$	$22, 15, 14, 7$	$[19, 7, 8], [9, 8, 2]$	$[156, 22, 58]$
					$[19, 7, 8], [13, 8, 4]$	$[160, 22, 60]$
					$[23, 7, 9], [17, 8, 6]$	$[168, 22, 62]$
$(73, 4)$	64	$5, 12$	$(85, 126)$	$29, 15, 21, 7$	$[37, 14, 12], [9, 8, 2]$	$[174, 29, 58]$
					$[37, 14, 12], [13, 8, 4]$	$[178, 29, 60]$
$(73, 4)$	64	$4, 8$	$(81, 0)$	$21, 14, 14, 7$	$[16, 5, 8], [7, 7, 1]$	$[151, 19, 58]$
					$[16, 5, 8], [11, 7, 3]$	$[155, 19, 60]$
$(81, 4)$	52	$4, 4$	$(85, 0)$	$28, 21, 21, 14$	$[8, 7, 2], [12, 7, 4]$	$[147, 28, 50]$
					$[12, 7, 4], [12, 7, 4]$	$[151, 28, 52]$
$(81, 4)$	52	$5, 4$	$(85, 126)$	$29, 22, 21, 14$	$[12, 7, 4], [9, 8, 2]$	$[149, 29, 50]$
					$[12, 7, 4], [13, 8, 4]$	$[153, 29, 52]$
$(81, 4)$	52	$4, 4$	$(85, 0)$	$28, 21, 21, 14$	$[8, 7, 2], [7, 4, 3]$	$[143, 25, 50]$
					$[12, 7, 4], [7, 4, 3]$	$[147, 25, 52]$
$(85, 2)$	48	$2, 12$	$(97, 0)$	$35, 28, 28, 21$	$[27, 7, 12], [8, 7, 2]$	$[162, 35, 46]$
					$[24, 5, 12], [7, 7, 1]$	$[159, 33, 46]$
$(125, 18)$	22	$2, 1$	$(1, 14)$	$78, 70, 71, 63$	$[9, 8, 2], [12, 7, 4]$	$[149, 78, 22]$
$(125, 20)$	24	$2, 3$	$(1, 18)$	$71, 63, 64, 56$	$[9, 8, 2], [8, 7, 2]$	$[145, 71, 24]$
$(125, 26)$	30	$4, 3$	$(1, 22)$	$57, 49, 50, 42$	$[9, 8, 2], [12, 7, 4]$	$[149, 57, 30]$

Table 9: Construction XX: $q = 2, w = 255$

(a, b)	$d(\mathcal{C}_0)$	i, j	(x, y)	k, k_1, k_2, k_0	aux. codes	result
(203, 2)	56	2, 2	(205, 0)	90, 86, 82, 78	[5, 4, 2], [9, 8, 2]	[269, 90, 56]
(211, 2)	48	2, 2	(213, 0)	114, 106, 106, 98	[9, 8, 2], [9, 8, 2]	[273, 114, 48]
(213, 2)	46	2, 2	(217, 0)	122, 114, 114, 106	[8, 4, 4], [9, 8, 2]	[272, 118, 46]
(213, 2)	46	2, 4	(217, 0)	122, 114, 114, 106	[13, 8, 4], [9, 8, 2]	[277, 122, 46]
(227, 2)	32	2, 2	(229, 0)	154, 146, 146, 138	[9, 8, 2], [9, 8, 2]	[273, 154, 32]
(229, 2)	30	2, 2	(231, 0)	162, 154, 154, 146	[9, 8, 2], [9, 8, 2]	[273, 162, 30]
(229, 2)	30	2, 4	(233, 0)	170, 154, 162, 146	[16, 11, 4], [9, 8, 2]	[280, 165, 30]
(231, 2)	28	2, 2	(233, 0)	170, 162, 162, 154	[9, 8, 2], [9, 8, 2]	[273, 170, 28]
(231, 2)	28	2, 2	(235, 0)	178, 162, 170, 154	[16, 11, 4], [9, 8, 2]	[280, 173, 28]
(233, 2)	26	2, 2	(235, 0)	178, 170, 170, 162	[9, 8, 2], [9, 8, 2]	[273, 178, 26]
(233, 2)	26	2, 4	(237, 0)	186, 170, 178, 162	[16, 11, 4], [9, 8, 2]	[280, 181, 26]
(235, 2)	24	2, 2	(237, 0)	186, 178, 178, 170	[9, 8, 2], [9, 8, 2]	[273, 186, 24]
(235, 2)	24	2, 4	(239, 0)	190, 178, 182, 170	[16, 11, 4], [9, 8, 2]	[280, 189, 24]
(237, 2)	22	2, 2	(239, 0)	190, 186, 182, 178	[5, 4, 2], [9, 8, 2]	[269, 190, 22]
(237, 2)	22	2, 4	(241, 0)	198, 186, 190, 178	[16, 11, 4], [9, 8, 2]	[280, 197, 22]
(243, 2)	16	2, 2	(245, 0)	214, 206, 206, 198	[9, 8, 2], [9, 8, 2]	[273, 214, 16]
(243, 2)	16	2, 4	(247, 0)	222, 206, 214, 198	[16, 11, 4], [9, 8, 2]	[280, 217, 16]
(243, 2)	16	2, 4	(247, 0)	222, 206, 214, 198	[22, 16, 4], [9, 8, 2]	[286, 222, 16]
(247, 2)	12	2, 2	(249, 0)	230, 222, 222, 214	[9, 8, 2], [9, 8, 2]	[273, 230, 12]
(247, 2)	12	2, 4	(251, 0)	238, 222, 230, 214	[16, 11, 4], [9, 8, 2]	[280, 233, 12]
					[22, 16, 4], [9, 8, 2]	[286, 238, 12]
(251, 2)	8	2, 2	(253, 0)	246, 238, 238, 230	[9, 8, 2], [9, 8, 2]	[273, 246, 8]
(251, 8)	8	2, 4	(0, 0)	254, 238, 246, 230	[16, 11, 4], [9, 8, 2]	[280, 249, 8]
(251, 2)	8	2, 4	(0, 0)	254, 238, 246, 230	[22, 16, 4], [9, 8, 2]	[286, 254, 8]
(251, 2)	8	3, 2	(253, 254)	247, 239, 238, 230	[9, 8, 2], [13, 9, 3]	[277, 247, 8]

Table 10: Construction XX: $q = 3, w = 80$

(a,b)	$d(\mathcal{C}_0)$	i,j	(x,y)	k,k_1,k_2,k_0	aux. codes	result
$(19,41)$	24	$1,2$	$(21,40)$	$33,31,29,27$	$[3,2,2],[4,4,1]$	$[87,33,24]$
$(19,41)$	24	$2,2$	$(21,39)$	$34,32,29,27$	$[3,2,2],[6,5,2]$	$[89,34,24]$
$(25,41)$	18	$1,2$	$(27,40)$	$45,41,41,37$	$[5,4,2],[4,4,1]$	$[89,45,18]$
$(28,41)$	15	$1,2$	$(30,40)$	$53,49,49,45$	$[5,4,2],[4,4,1]$	$[89,53,15]$
$(28,41)$	15	$1,3$	$(31,40)$	$55,49,51,45$	$[9,6,3],[4,4,1]$	$[93,55,15]$
$(28,41)$	15	$2,2$	$(30,39)$	$55,50,49,45$	$[5,4,2],[6,5,2]$	$[91,54,15]$
$(28,41)$	15	$2,3$	$(31,39)$	$56,50,51,45$	$[9,6,3],[6,5,2]$	$[95,56,15]$
$(28,43)$	17	$2,2$	$(30,41)$	$49,45,45,41$	$[5,4,2],[5,4,2]$	$[90,49,17]$
$(28,43)$	17	$3,2$	$(30,40)$	$53,49,45,41$	$[5,4,2],[9,8,2]$	$[94,53,16]$
					$[5,4,2],[11,8,3]$	$[96,53,17]$
$(28,43)$	17	$3,3$	$(31,40)$	$55,49,47,41$	$[9,6,3],[11,8,3]$	$[100,55,17]$
$(30,41)$	13	$1,3$	$(33,50)$	$59,53,55,49$	$[9,6,3],[4,4,1]$	$[93,59,13]$
$(30,41)$	13	$2,3$	$(33,49)$	$60,54,55,49$	$[9,6,3],[6,5,2]$	$[95,60,13]$
$(30,49)$	21	$3,1$	$(31,46)$	$39,37,35,33$	$[2,2,1],[7,4,3]$	$[89,39,21]$
$(31,3)$	60	$6,3$	$(37,0)$	$10,6,6,2$	$[10,4,6],[5,4,2]$	$[95,10,53]$
					$[10,4,6],[7,4,3]$	$[97,10,54]$
					$[13,4,7],[8,4,4]$	$[101,10,55]$
$(31,3)$	60	$9,3$	$(40,0)$	$14,10,6,2$	$[20,8,9],[5,4,2]$	$[105,14,53]$
					$[20,8,9],[7,4,3]$	$[107,14,54]$
$(31,3)$	60	$6,4$	$(37,79)$	$11,6,7,2$	$[13,4,7],[10,5,5]$	$[103,11,55]$
					$[14,4,8],[11,5,6]$	$[105,11,56]$
$(34,41)$	9	$1,2$	$(36,40)$	$67,63,63,59$	$[5,4,2],[4,4,1]$	$[89,67,9]$
$(34,41)$	9	$2,2$	$(36,39)$	$68,64,63,59$	$[5,4,2],[6,5,2]$	$[91,68,9]$
$(34,43)$	11	$2,2$	$(36,41)$	$63,59,59,55$	$[5,4,2],[5,4,2]$	$[90,63,11]$
$(34,43)$	11	$2,3$	$(37,41)$	$67,59,63,55$	$[11,8,3],[5,4,2]$	$[96,67,11]$
$(37,43)$	8	$2,2$	$(39,41)$	$71,67,67,63$	$[5,4,2],[5,4,2]$	$[90,71,8]$
$(37,3)$	48	$3,3$	$(40,0)$	$14,10,10,6$	$[5,4,2],[5,4,2]$	$[90,14,46]$
					$[5,4,2],[7,4,3]$	$[92,14,47]$
					$[7,4,3],[7,4,3]$	$[94,14,48]$
$(37,3)$	48	$3,4$	$(41,0)$	$15,10,11,6$	$[9,5,4],[5,4,2]$	$[94,15,47]$
					$[9,5,4],[7,4,3]$	$[96,15,48]$
$(37,3)$	48	$4,4$	$(41,79)$	$16,11,11,6$	$[6,5,2],[9,5,4]$	$[95,16,46]$
					$[9,5,4],[9,5,4]$	$[98,16,48]$
$(30,49)$	21	$3,1$	$(31,46)$	$39,37,35,33$	$[2,2,1],[4,2,3]$	$[86,37,21]$
$(37,3)$	48	$3,3$	$(40,0)$	$14,10,10,6$	$[5,4,2],[4,2,3]$	$[89,12,47]$
$(37,0)$	48	$3,3$	$(40,0)$	$14,10,10,6$	$[7,4,3],[4,2,3]$	$[91,12,48]$

Table 11: Construction XX: $q = 3, w = 121$

(a, b)	$d(\mathcal{C}_0)$	i, j	(x, y)	k, k_1, k_2, k_0	aux. codes	result
$(52, 62)$	12	3,2	$(55, 60)$	$101, 96, 91, 86$	$[13, 10, 3], [6, 5, 2]$	$[140, 101, 12]$
$(0, 15)$	17	1,3	$(1, 12)$	$81, 76, 80, 75$	$[6, 5, 2], [1, 1, 1]$	$[128, 81, 16]$
					$[4, 2, 3], [1, 1, 1]$	$[126, 78, 17]$
					$[8, 5, 3], [1, 1, 1]$	$[130, 81, 17]$
$(0, 15)$	17	1,5	$(1, 10)$	$86, 76, 85, 75$	$[1, 1, 1], [11, 6, 5]$	$[133, 82, 17]$
					$[1, 1, 1], [14, 8, 5]$	$[136, 84, 17]$
$(46, 62)$	18	3,2	$(49, 60)$	$81, 76, 76, 71$	$[6, 5, 2], [4, 2, 3]$	$[131, 78, 18]$
					$[6, 5, 2], [8, 5, 3]$	$[135, 81, 18]$
$(41, 62)$	23	3,2	$(44, 60)$	$71, 66, 66, 61$	$[6, 5, 2], [6, 5, 2]$	$[133, 71, 22]$
					$[6, 5, 2], [4, 2, 3]$	$[131, 68, 23]$
					$[6, 5, 2], [8, 5, 3]$	$[135, 71, 23]$
$(55, 1)$	69	6,2	$(61, 120)$	$16, 15, 11, 10$	$[2, 1, 2], [6, 5, 2]$	$[129, 16, 65]$
$(55, 1)$	69	6,2	$(61, 120)$	$16, 15, 11, 10$	$[2, 1, 2], [11, 5, 6]$	$[134, 16, 69]$
$(46, 1)$	78	9,2	$(55, 120)$	$11, 10, 6, 5$	$[6, 5, 2], [2, 1, 2]$	$[129, 11, 71]$
					$[2, 1, 2], [11, 5, 6]$	$[134, 11, 75]$

Table 12: Construction XX: $q = 4, w = 63$

(a, b)	$d(\mathcal{C}_0)$	i, j	(x, y)	k, k_1, k_2, k_0	aux. codes	result
$(9, 22)$	15	$1, 2$	$(11, 21)$	$38, 35, 35, 32$	$[4, 3, 2], [3, 3, 1]$	$[70, 38, 15]$
$(11, 22)$	13	$1, 2$	$(13, 21)$	$44, 38, 41, 35$	$[7, 6, 2], [3, 3, 1]$	$[73, 44, 13]$
$(13, 22)$	11	$1, 2$	$(15, 21)$	$47, 44, 44, 41$	$[4, 3, 2], [3, 3, 1]$	$[70, 47, 11]$
$(13, 22)$	11	$1, 3$	$(16, 21)$	$50, 44, 47, 41$	$[9, 6, 3], [3, 3, 1]$	$[75, 50, 11]$
$(13, 25)$	14	$2, 2$	$(15, 23)$	$41, 38, 38, 35$	$[4, 3, 2], [4, 3, 2]$	$[71, 41, 14]$
$(15, 22)$	9	$1, 2$	$(17, 21)$	$53, 47, 50, 44$	$[7, 6, 2], [3, 3, 1]$	$[73, 53, 9]$
$(17, 25)$	10	$2, 2$	$(19, 23)$	$50, 47, 47, 44$	$[4, 3, 2], [4, 3, 2]$	$[71, 50, 10]$
$(17, 43)$	28	$1, 3$	$(20, 42)$	$22, 19, 19, 16$	$[5, 3, 3], [3, 3, 1]$	$[71, 22, 28]$
$(17, 43)$	28	$1, 4$	$(21, 42)$	$25, 19, 22, 16$	$[10, 6, 4], [3, 3, 1]$	$[76, 25, 28]$
$(17, 43)$	28	$2, 3$	$(20, 41)$	$23, 20, 19, 16$	$[5, 3, 3], [5, 4, 2]$	$[73, 23, 28]$
$(17, 43)$	28	$2, 4$	$(21, 41)$	$26, 20, 22, 16$	$[10, 6, 4], [5, 4, 2]$	$[78, 26, 28]$
$(17, 46)$	31	$3, 4$	$(21, 43)$	$22, 16, 19, 13$	$[7, 6, 2], [5, 3, 3]$	$[75, 22, 29]$
					$[10, 6, 4], [5, 3, 3]$	$[78, 22, 31]$
$(17, 46)$	31	$3, 5$	$(22, 43)$	$23, 16, 20, 13$	$[11, 7, 4], [5, 3, 3]$	$[79, 23, 30]$
$(17, 46)$	31	$4, 4$	$(21, 42)$	$25, 19, 19, 13$	$[7, 6, 2], [10, 6, 4]$	$[80, 25, 29]$
					$[10, 6, 4], [10, 6, 4]$	$[83, 25, 31]$

Table 13: Construction XX: $q = 4, w = 85$

(a, b)	$d(\mathcal{C}_0)$	i, j	(x, y)	k, k_1, k_2, k_0	aux. codes	result
$(27, 35)$	10	$2, 2$	$(29, 33)$	$69, 65, 67, 63$	$[5, 4, 2], [3, 2, 2]$	$[93, 69, 10]$
$(27, 36)$	11	$1, 2$	$(29, 35)$	$67, 63, 63, 59$	$[5, 4, 2], [4, 4, 1]$	$[94, 67, 11]$

Table 14: Construction XX iterated: $q = 2, w = 127$

l	r_1, r_2, r_3	k_1, k_2, k_3	l'	k	aux. codes	result
0	12,14,18	84,77,70	125	77	$[8, 7, 2], [3, 2, 2], [14, 9, 4]$	$[152, 79, 22]$
					$[8, 7, 2], [4, 3, 2], [15, 10, 4]$	$[154, 80, 22]$
1	42,46,54	29,22,15	123	21	$[9, 8, 2], [8, 4, 4], [23, 11, 8]$	$[167, 26, 57]$
					$[9, 8, 2], [4, 1, 4], [20, 8, 8]$	$[160, 23, 57]$
					$[13, 8, 4], [8, 4, 4], [23, 11, 8]$	$[171, 26, 59]$
					$[13, 8, 4], [4, 1, 4], [20, 8, 8]$	$[164, 23, 59]$
0	42,46,54	28,21,14	123	21	$[8, 7, 2], [8, 4, 4], [23, 11, 8]$	$[166, 25, 58]$
0	42,46,54	28,21,14	123	21	$[8, 7, 2], [7, 3, 4], [22, 10, 8]$	$[164, 24, 58]$
					$[12, 7, 4], [8, 4, 4], [23, 11, 8]$	$[170, 25, 60]$

Table 15: Construction XX iterated: $q = 2, w = 255$

l	r_1, r_2, r_3	k_1, k_2, k_3	l'	k	aux. codes	result
249	254,255,2	231,230,222	247	223	$[9, 8, 2], [1, 1, 1], [10, 9, 2]$	$[275, 231, 12]$
245	254,255,2	215,214,206	243	207	$[9, 8, 2], [1, 1, 1], [10, 9, 2]$	$[275, 215, 16]$
0	8,10,12	222,214,206	253	214	$[9, 8, 2], [3, 2, 2], [11, 10, 2]$	$[278, 216, 16]$
1	14,16,18	199,191,187	0	198	$[1, 1, 1], [2, 1, 2], [6, 5, 2]$	$[264, 192, 20]$
					$[1, 1, 1], [3, 2, 2], [7, 6, 2]$	$[266, 193, 20]$
239	254,255,2	191,190,182	237	187	$[5, 4, 2], [1, 1, 1], [10, 9, 2]$	$[271, 191, 22]$
0	14,16,18	198,190,186	253	190	$[9, 8, 2], [3, 2, 2], [7, 6, 2]$	$[274, 192, 22]$
237	254,255,2	187,186,178	235	179	$[9, 8, 2], [1, 1, 1], [10, 9, 2]$	$[275, 187, 24]$
0	16,18,20	190,186,178	253	182	$[9, 8, 2], [3, 2, 2], [11, 10, 2]$	$[278, 188, 24]$
235	254,255,2	179,178,170	233	171	$[9, 8, 2], [1, 1, 1], [10, 9, 2]$	$[275, 179, 26]$
0	18,20,22	186,178,170	253	178	$[9, 8, 2], [3, 2, 2], [11, 10, 2]$	$[278, 180, 26]$
233	254,255,2	171,170,162	231	163	$[9, 8, 2], [1, 1, 1], [10, 9, 2]$	$[275, 171, 28]$
0	20,22,24	178,170,162	253	170	$[9, 8, 2], [3, 2, 2], [11, 10, 2]$	$[278, 172, 28]$
231	254,255,2	163,162,154	229	155	$[9, 8, 2], [1, 1, 1], [10, 9, 2]$	$[275, 163, 30]$
0	22,24,26	170,162,154	253	162	$[9, 8, 2], [3, 2, 2], [11, 10, 2]$	$[278, 164, 30]$
229	254,255,2	155,154,146	227	147	$[9, 8, 2], [1, 1, 1], [10, 9, 2]$	$[275, 155, 32]$
0	24,26,28	162,154,146	253	154	$[9, 8, 2], [3, 2, 2], [11, 10, 2]$	$[278, 156, 32]$
213	254,255,2	115,114,106	211	107	$[9, 8, 2], [1, 1, 1], [10, 9, 2]$	$[275, 115, 48]$
1	46,50,52	99,91,87	0	98	$[1, 1, 1], [4, 1, 4], [6, 5, 2]$	$[266, 92, 54]$
205	254,255,2	91,90,82	203	87	$[5, 4, 2], [1, 1, 1], [10, 9, 2]$	$[271, 91, 56]$

Table 16: Construction XX iterated: $q = 3, w = 80$

l	r_1, r_2, r_3	k_1, k_2, k_3	l'	k	aux. codes	result
1	7,9,12	60,56,50	0	59	$[1,1,1], [2,1,2], [10,7,3]$	$[93,57,14]$
1	16,19,21	38,34,32	0	37	$[1,1,1], [3,1,3], [4,3,2]$	$[88,35,23]$
1	40,43,49	15,11,7	0	14	$[1,1,1], [4,2,3], [12,6,6]$	$[97,13,51]$
1	40,43,52	15,11,5	0	14	$[1,1,1], [3,1,3], [19,7,9]$	$[103,12,54]$
					$[1,1,1], [4,2,3], [20,8,9]$	$[105,13,54]$
31	79,0,9	7,6,2	28	5	$[4,2,3], [1,1,1], [11,5,6]$	$[96,7,60]$
1	49,52,79	7,5,1	0	6	$[1,1,1], [4,2,3], [44,6,27]$	$[129,7,81]$
40	49,50,52	55,54,49	37	47	$[11,8,3], [1,1,1], [6,5,2]$	$[98,54,17]$
40	80,83,89	14,10,6	39	10	$[4,4,1], [4,2,3], [12,6,6]$	$[100,12,52]$
41	80,83,89	15,11,7	39	10	$[6,5,2], [4,2,3], [12,6,6]$	$[102,13,52]$
41	79,80,89	16,15,7	39	11	$[6,5,2], [1,1,1], [21,9,9]$	$[108,16,52]$
0	39,40,43	15,14,10	77	11	$[5,4,2], [1,1,1], [6,5,2]$	$[92,15,46]$
1	39,40,43	16,15,11	77	11	$[9,5,4], [1,1,1], [6,5,2]$	$[96,16,47]$
37	79,80,3	11,10,6	31	7	$[10,4,6], [1,1,1], [6,5,2]$	$[97,11,53]$
0	40,43,49	14,10,6	77	10	$[5,4,2], [4,2,3], [12,6,6]$	$[101,12,53]$
0	39,40,49	15,14,6	77	11	$[5,4,2], [1,1,1], [21,9,9]$	$[107,15,53]$

Table 17: Construction XX iterated: $q = 4, w = 63$

l	r_1, r_2, r_3	k_1, k_2, k_3	l'	k	aux. codes	result
21	41,42,46	26,25,19	19	20	$[7,6,2], [1,1,1], [11,7,4]$	$[82,26,29]$
22	41,42,46	27,26,20	20	23	$[5,4,2], [1,1,1], [11,7,4]$	$[80,27,28]$
0	41,42,46	7,6,3	59	4	$[6,3,4], [1,1,1], [5,4,2]$	$[75,7,50]$
41	62,63,4	25,22,16	38	20	$[5,3,3], [1,1,1], [8,7,2]$	$[77,23,29]$
					$[5,3,3], [1,1,1], [11,7,4]$	$[80,23,31]$

Table 18: Construction X plus: $q = 2, w = 127$

pair of codes	$\mathcal{C}$	$\mathcal{D}$	aux. code	result
$[127, 50, 27] \supset [127, 43, 31]$	$(1, 26)$	$(1, 28)$	$[4, 1, 4]$	$[132, 44, 32]$
			$[8, 4, 4]$	$[136, 47, 32]$
			$[12, 7, 4]$	$[140, 50, 32]$
$[127, 57, 23] \supset [127, 43, 31]$	$(1, 22)$	$(1, 28)$	$[24, 12, 8]$	$[152, 55, 32]$
$[127, 43, 31] \supset [127, 29, 43]$	$(1, 28)$	$(1, 42)$	$[18, 9, 6]$	$[146, 38, 38]$
			$[28, 10, 10]$	$[156, 39, 42]$
			$[16, 11, 4]$	$[144, 40, 36]$
			$[32, 11, 12]$	$[160, 40, 44]$
			$[24, 12, 8]$	$[152, 41, 40]$
			$[34, 12, 12]$	$[162, 41, 44]$
			$[32, 13, 10]$	$[160, 42, 42]$
			$[15, 14, 2]$	$[143, 43, 34]$
			$[20, 14, 4]$	$[148, 43, 36]$
			$[24, 14, 6]$	$[152, 43, 38]$
			$[28, 14, 8]$	$[156, 43, 40]$
			$[34, 14, 10]$	$[162, 43, 42]$
			$[37, 14, 12]$	$[165, 43, 44]$

Table 19: Construction X plus: $q = 2, w = 255$

pair of codes	$\mathcal{C}$	$\mathcal{D}$	aux. code	result
$[255, 79, 55] \supset [255, 71, 61]$	$(1, 54)$	$(1, 58)$	$[6, 1, 6]$	$[262, 72, 62]$
			$[9, 2, 6]$	$[265, 73, 62]$
			$[12, 4, 6]$	$[268, 75, 62]$
$[255, 71, 61] \supset [255, 63, 63]$	$(1, 58)$	$(1, 60)$	$[9, 8, 2]$	$[264, 71, 63]$

Table 20: Construction X iterated plus: $q = 2, w = 127$

chain of codes	auxiliary codes	result
$[127, 57, 23] \supset [127, 50, 27] \supset [127, 43, 31]$	$[4, 1, 4], [13, 8, 4]$	$[144, 51, 31]$
	$[6, 2, 4], [14, 9, 4]$	$[147, 52, 31]$

5 Some good codes

5.1 Check matrix of $[33, 21, 7]_3$

```
010000000000212121102002211201221
100000000000112121011201011111121
001000000000102121002121220000001
000100000000222000202211000010021
000010000000002220002022111011120
000001000000022200020221102100220
000000100000001211012012000201210
000000010000012110120120002020201
000000001000121101201200000122101
000000000100000121101201202200012
000000000010000012110120120021000
000000000001212122010011220011110
```

5.2 Generator matrix of $[25, 10, 10]_3$

```
1112101001200221000000000
2120001111210110100000000
1200212010111020010000000
2102102222001020001000000
0122021120020220000100000
1121010010202210000010000
2001221012020020000001000
0022212211111200000000100
0221200102221000000000010
2102222001002100000000001
```

5.3 Generator matrix of $[53,6,36]_4$

```
10000032303321033010333122002333103213001320322001132
01000021113031032331333011123213202221223110120321010
00100010220203122232331032132223102332211303302221302
00010001032303321030313033122002333123003103123120232
00001010323033210331030331220023331002331012330022133
00000103230332103303103312200233310330210133202112031
```

References

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

[2] D.Augot, P.Charpin, N.Sendrier: *Studying the locator polynomials of minimum weight codewords of BCH codes, IEEE Transactions on Information Theory* 38 (1992), 960-973.

[3] J.Bierbrauer: *Construction of orthogonal arrays,* to appear in *Journal of Statistical Planning and Inference.*

[4] Jürgen Bierbrauer's home page:
http://www.math.mtu.edu/home/math/jbierbra/Home.html

[5] J.Bierbrauer and Y.Edel: *New code-parameters from Reed-Solomon subfield codes,* to appear in *IEEE Transactions on Information Theory*

[6] 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.

[7] A.E. Brouwer and T. Verhoeff: *An updated table of minimum-distance bounds for binary linear codes, IEEE Transactions on Information Theory* **39** (1993) 662-677.

[8] P.Delsarte, *On subfield subcodes of modified Reed-Solomon codes,* IEEE Trans. Inform. Th. 21 (1975) 575-576.

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

[10] 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.

[11] F. J. MacWilliams and N. J. A. Sloane: *The Theory of Error-Correcting Codes,* North-Holland, ^{7}1992.

[12] L.Rédei: *Lückenhafte Polynome,* Birkhäuser Verlag, Basel, Stuttgart 1970.