Direct constructions of additive codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

September 2, 2000

1 Introduction

We start by defining a class of codes, which are sometimes known collectively as **additive codes.** A q^m- ary q-linear code $\mathcal{C}$ is defined over the alphabet $E = \mathbb{F}_q^m$. That means the alphabet is considered as a vector space over the ground field $\mathbb{F}_q$, not necessarily as a field. Code $\mathcal{C}$ has length n if every codeword is in E^n, and hence in $\mathbb{F}_q^{mn}$. The assumption of q-linearity means that linear combinations of codewords with coefficients in $\mathbb{F}_q$ are codewords again. This implies that the minimum distance d of our code will agree with the minimum weight among the nonzero codewords. We will write the basic parameters of our code as $[n, k, d]$, where k is the q^m-ary dimension. Observe that k is not necessarily an integer, but km, the dimension of $\mathcal{C}$ as a vector space over $\mathbb{F}_q$, is an integer.

The theory of **Twisted BCH-codes** was developed in [13]. The same concept was studied at about the same time under the name of **Reed-Solomon subspace codes** by Mc Eliece, Hattori and Solomon (see [16]). This concept represents a natural generalization of cyclic codes from the linear to the additive case. A different approach is in [2]. The special case of twisted codes, which are linear over their alphabet, is precisely the class of cyclic codes. As far as we know the following represent the main achievements obtained by use of additive codes:

1. The construction of a large class of **linear** 2-weight codes and strongly regular graphs, whose parameters are motivated by maximal arcs, [3].
2. The construction of a large number of optimal linear binary, ternary and quaternary codes by applying concatenation and other recursive constructions to twisted (additive) codes, see [13].
3. Use of twisted codes for the construction of quantum codes, see [14].
4. Use of additive codes for deep-space communication, see [16].
5. Use of additive codes in computer memory systems, see [10, 7, 9].

The first four of these applications rely on the general theory of twisted codes. Unfortunately the theory looks rather complicated, both in the form of [13] and in [16]. A different approach to the theory is in [2]. As a first consequence of the new approach we have been able to eliminate the use of the twisted theory completely in three instances:

- The codes proposed for deep-space communication in [16] can be derived from Reed-Solomon codes by applying an elementary construction due to Chen.
- The family of 2-weight codes can be constructed directly. All that is needed is some field arithmetic.
- A closely related family of 5.5-dimensional q^2-ary codes can be constructed directly. This family leads to most of the new optimal linear codes constructed in [13].

It is felt that the new explicit and efficient representation of the codes will facilitate applications and generalizations.

Our first application is a simplified proof for a slight generalization of the classical Bose-Bush construction of orthogonal arrays of strength 2 (see [4, 17]). The proof that this can be done within the theory of additive codes is due to Yves Edel. Only the simplest additive codes are used as ingredients.

2 Chen projection

Let $\mathcal{C}$ be a q^m-ary $q-$linear code $[n, k, d]$, where $m > 1$. Application of an arbitrary regular (m, m)-matrix in each coordinate yields a code, which is equivalent to $\mathcal{C}$ in the sense that the basic parameters are the same. We can therefore assume that $\mathcal{C}^{\perp}$ contains a word, which in each coordinate has as entry either $(0, \ldots, 0, 1)$ or $(0, \ldots, 0, 0)$. The q-ary dimension of $\mathcal{C}$ is km. Consider the subcode $\mathcal{D} \subset \mathcal{C}$ consisting of those words, which vanish in the last position of each coordinate. We observe that $dim_q(\mathcal{D}) \geq km - (n-1)$. This observation is also known as construction Y_1. Clearly we can omit this last position in each coordinate and obtain a q^{m-1}-ary $q-$linear code of q^{m-1}-ary dimension $\geq \frac{km-(n-1)}{m-1} = k - \frac{n-1-k}{m-1}$. We have proved the following result due to C.L.Chen [7]:

Theorem 1 (Chen projection). *If there is a q^m-ary $q-$linear code $[n, k, d]$ with $m > 1$, there is a q^{m-1}-ary $q-$linear code $[n, k - \dfrac{n-k-1}{m-1}, d]$.*

Application of Chen projection to hyperovals and ovoids yields additive codes with $d = 4$ and very high dimension. Some of these codes have found multiple applications in computer memory systems, see [7, 9].

We can apply Chen projection to (extended) Reed-Solomon codes. Let us start from the cyclic version of Reed-Solomon codes. These have parameters

$$[q^m - 1, k, q^m - k]_{q^m}.$$

Application of Theorem 1 yields $q^{m-1}-$ary $q-$linear codes with parameters

$$[q^m - 1, k - \frac{q^m - k - 2}{m-1}, q^m - k]$$

The special cases $q = 2, m = 9$ and $k = 512 - 30$ or $k = 512 - 42$ yield $256-$ary additive ($\mathbb{F}_2-$linear) codes

$$[511, 478.5, 30] \text{ and } [511, 465, 42].$$

These are the codes which have been proposed in [16] to replace the Reed-Solomon code $[255, 223, 33]_{256}$ of the old NASA standard as outer code in a concatenation scheme. This improvement appears to have been used for communication with Galileo. The original construction involves the theory of Reed-Solomon subspace codes.

2.1 Orthogonal arrays

Clearly the theory of additive codes may be equivalently described in the language of orthogonal arrays. The dual of a $q-$linear $[n,k,d]_{q^m}$ is a $q-$linear $OA_\lambda(d-1,n,q^m)$, where $\lambda = q^{m(n+1-k-d)}$, and vice versa. Chen projection states that a $q-$linear $OA_\lambda(t,n,q^m)$ implies a $q-$linear $OA_{\lambda q^{t-1}}(t,n,q^{m-1})$. As an example, the extended Reed-Solomon code $[q^n+1,q^n-1,3]$ yields as dual an $OA_1(2,q^n+1,q^n)$, which is q^n-linear and therefore $q-$linear. Repeated application of Chen projection yields $OA_{q^{n-m}}(2,q^n+1,q^m)$ for every $m\leq n$. If we start from the Reed-Solomon code of length q^n instead we obtain difference schemes $D(p^n,p^n,p^m)$ for every $m\leq n$ in the terminology of [17]. These difference schemes and the orthogonal arrays derived from them are important ingredients in many constructions.

3 The easiest case and the Bose-Bush construction

We start with the lowest-dimensional codes. Instead of applying the theory of twisted codes we give a direct treatment.

Theorem 2. *Let $n\geq m, F=\mathbb{F}_{q^n}$ and $\Phi: F\longrightarrow E=\mathbb{F}_q^m$ a surjective $\mathbb{F}_q-$linear mapping. Define a q^m-ary $q-$linear code $\mathcal{C}_q(n,m)$ of length q^n and $\mathbb{F}_q-$dimension $n+m$ as follows: The coordinates are indexed by $x\in F$, the code-words by pairs (a,b), where $a\in F, b\in\mathbb{F}_q^m$. The corresponding entry is*

$$v(a,b)_x=\Phi(ax)+b.$$

Then $\mathcal{C}_q(n,m)$ has strength $t=2$, and the $v(a,0)$ form a subcode of $\mathbb{F}_q-$dimension m and strength 1.

In the general terminology of additive codes we would say that the dual codes form a chain

$$[q^n,q^n-(1+\frac{n}{m}),3]_{q^m}\subset[q^n,q^n-1,2]_{q^m}$$

of q^m-ary $q-$linear codes, but in this case the language of Theorem 2 is more natural. We will also say that $\mathcal{C}_q(n,m)$ has parameters $[q^n,(n+m)/m]_{q^m}$ and strength 2, and its subcode, the **repetition code,** has parameters $[q^n,1]_{q^m}$ and strength 1.

Proof. Recall that each entry of a code-word is itself a $q-$ary tuple of length m. Also, strength t means that the projection onto any t coordinates is onto, equivalently that there is no nontrivial linear combination involving t columns. Clearly the repetition code has strength 1. We have to prove that $\mathcal{C}_q(n,m)$ has strength 2. Let x,y be two different columns and $e_1,e_2\in E=\mathbb{F}_q^m$ such that $\langle e_1,\Phi(ax)+b\rangle+\langle e_2,\Phi(ay)+b\rangle=0$ for all $a\in F, b\in E$. The choice $a=0$ shows because of the non-degeneracy of $\langle,\rangle$ that $e_2=-e_1$. The condition simplifies to $\langle e_1,\Phi(a(x-y))\rangle=0$, which because of the non-degeneracy of $\langle,\rangle$ and the surjectivity of Φ forces $e_1=0$. ∎

As a first application we derive the Bose-Bush construction for orthogonal arrays of strength 2. As a preparation we introduce a recursive construction:

Proposition 1. *Assume the following q^m-ary $q-$linear codes exist:*

- *A code $[n,K]$ of strength 2 containing a subcode $[n,k]$ of strength 1, and*
- *a code $[l,K-k]$ of strength 2 (the auxiliary code).*

Then we can construct such a code $[n+l,K]$ of strength 2.

Proof. It is easiest to work with $\mathbb{F}_q-$generator matrices. Choose such a generator matrix (with Km rows) for the code $[n,K]$ such that the first km rows form a generator matrix for the strength 1 subcode. Lengthen this generator matrix by a generator matrix of the auxiliary code in the last

$m(K-k)$ rows, by a 0-matrix in the first rows. The result is a generator matrix of a code with the right dimension, clearly of strength 2. ■

Let $n \geq m$. In the preceding section we constructed by different means a code $[q^n+1,(n+m)/m]_{q^m}$ of strength 2, which we denote by $\mathcal{C}'_q(n,m)$ here. This code is in fact obtainable by lengthening from the code $\mathcal{C}_q(n,m)$ as constructed in Theorem 2. The drawback of the longer code is that it does not contain a large subcode of strength 1. We start with code $\mathcal{C}_q(n,m)$. As it contains an $m-$dimensional strength 1 subcode ($\mathbb{F}_q-$dimensions), we can apply Proposition 1 with $\mathcal{C}_q(n-m,m)$ as auxiliary code (provided $n-m \geq m$). The resulting code has a $2m-$dimensional subcode of strength 1. We can apply Proposition 1 again, with $\mathcal{C}_q(n-2m,m)$ as auxiliary code. We can procede inductively in this fashion. The last inductive step occurs when $n-dm \geq m$, but $n-(d+1)m < m$. In this last step we can use $\mathcal{C}'_q(n-dm,m)$ as auxiliary code. Clearly $d = \lfloor n/m \rfloor - 1$. The length of the resulting code is $1+\sum_{i=0}^{d} q^{n-im}$.

Theorem 3 (Bose-Bush construction). *Let $n \geq m$. Recursive application of Proposition 1 to the codes of Theorem 2 and in the last step to a lengthened code produces a q^m-ary $q-$linear code $[l,(n+m)/m]_{q^m}$ of strength 2, with length*

$$l = 1 + \sum_{i=0}^{d} q^{n-im} = 1 + (q^{n+m} - q^{n-dm})/(q^m - 1),$$

where $d = \lfloor n/m \rfloor - 1$.

In the case when $q=p$ is prime these are the parameters of the classical Bose-Bush construction for orthogonal arrays of strength 2 (see [4, 17]). Theorem 3 is due to Yves Edel.

4 A family of additive codes

Consider field extensions

$$\mathbb{F}_q \subset F_0 = \mathbb{F}_{q^{r'}} \subset F = \mathbb{F}_{q^r},$$

where $r = 2r'$. Denote traces and norms by $T : F \longrightarrow F_0$, $N : F \longrightarrow F_0$, $Tr : F_0 \longrightarrow \mathbb{F}_q$. Choose $m \leq r'$ and a set $\{\eta_1, \ldots, \eta_m\} \subset F_0$, which is linearly independent over $\mathbb{F}_q$. We define an additive code $\mathcal{C}$ of length $q^r - 1$ with entries in $\mathbb{F}_q^m$, which is $\mathbb{F}_q-$linear. The coordinates are parametrized by $x \in F^*$. The code-words are parametrized by pairs (a, b), where $a \in F, b \in F_0$. The entry of the corresponding codeword $v(a, b)$ in coordinate x is defined as

$$v(a,b)_x = (Tr(\eta_j \cdot (T(ax) + bN(x)))_j \ , j = 1, 2, \ldots, m.$$

It is clear that the mapping $(a, b) \mapsto v(a, b)$ is $\mathbb{F}_q-$linear. There is no need for an explicit proof that the mapping has no kernel, as we will determine the weight of $v(a, b)$ in general. As this weight is never 0 unless $a = b = 0$ it will follow that that $dim_{\mathbb{F}_q}(\mathcal{C}) = 3r' = r + r'$. All that is needed for the determination of the weight is the following elementary lemma:

Lemma 1. *Let $\mathbb{F}_q \subset L = \mathbb{F}_{q^2}$ and denote by T, N the trace and norm, respectively. Let elements $a \in L, b \in \mathbb{F}_q^*, u \in \mathbb{F}_q$ be given. Denote by $\nu(a, b, u)$ the number of elements $x \in L^*$ satisfying*

$$T(ax) + bN(x) = u$$

Then

$$\nu(a,b,u) = \begin{cases} q & \text{if } u = 0 \\ 1 & \text{if } bu = -N(a) \\ q+1 & \text{otherwise} \end{cases}$$

Proof. The equation can be written equivalently as

$$N(x + \frac{a^q}{b}) = \frac{u}{b} + \frac{N(a)}{b^2}.$$

If $bu = -N(a)$ there is only one solution $x = -a^q/b$. In all other case the right side is nonzero. There are therefore $q + 1$ solutions $x \in L$. One of them is $x = 0$ if and only if $u = 0$. ■

It is easier to count zeroes than nonzeroes in $v(a,b)$. Let $\chi_0(v(a,b))$ be the number of coordinates x such that $v(a,b)_x = 0$ (here 0 represents the m-tuple $(0,0,\dots,0)$).

We use the fact that the **trace form,** defined by

$$(x,y) = Tr(xy)$$

defines a non-degenerate symmetric bilinear form on F_0, where we see this field as an r'−dimensional vector space over $\mathbb{F}_q$. Let $W_0 = \langle \eta_1,\dots,\eta_m\rangle^\perp \subset F_0$, in words: W_0 is the subspace consisting of those elements $c \in F_0$ satisfying $(\eta_j, c) = Tr(\eta_j c) = 0,\ j = 1,2\dots,m$. As the η_j generate a space of dimension m, we have $dim_{F_q}(W_0) = r' - m$. The definition shows that

$$v(a,b)_x = 0 \longleftrightarrow T(ax) + bN(x) \in W_0$$

In case $a = 0, b \neq 0$ the condition is $bN(x) \in W_0$. As every nonzero element of F_0 has precisely $q^{r'} + 1$ preimages under N we obtain

$$\chi_0(v(0,b)) = (q^{r'} + 1)(q^{r'-m} - 1).$$

In case $b = 0, a \neq 0$ the condition is $T(ax) \in W_0$. Each element of $c \in F_0$ has precisely $q^{r'}$ preimages under T. Letting c vary over W_0 and observing that we may not count $x = 0$ as a preimage we obtain

$$\chi_0 v((a,0)) = q^{r'-m}q^{r'} - 1 = q^{r-m} - 1.$$

Let now $ab \neq 0$. We can use Lemma 1. Assume at first $-\frac{N(a)}{b} \in W_0$. We obtain

$$\chi_0(v(a,b)) = q^{r'} + 1 + (q^{r'-m} - 2)(q^{r'} + 1) = q^{r-m} - q^{r'} + q^{r'-m} - 1.$$

The final case is $-\frac{N(a)}{b} \notin W_0$. The result is

$$\chi_0(v(a,b)) = q^{r'} + (q^{r'-m} - 1)(q^{r'} + 1) = q^{r-m} + q^{r'-m} - 1.$$

As $wt(v(a,b)) = q^r - 1 - \chi_0(v(a,b))$ the weights are as follows

Theorem 4. *We have constructed a q^m−ary $\mathbb{F}_q$−linear code of length $q^r - 1$ and dimension $\frac{3r'}{m}$, where $r = 2r'$, whose codewords have the following* *weights:*

$$wt(v(a,b)) = \begin{cases} 0 & \textit{if } a=b=0 \\ q^r - q^{r-m} & \textit{if } b=0, a\neq 0 \\ q^r - q^{r-m} + q^{r'} - q^{r'-m} & \textit{if } -\frac{N(a)}{b} \in W_0 \\ q^r - q^{r-m} - q^{r'-m} & \textit{if } -\frac{N(a)}{b} \notin W_0 \end{cases}$$

The special case of Theorem 4 of linear $p-$ary codes ($p = q^m$) makes its appearance in [11]. The binary linear case ($q^m = 2$) are the Kasami codes. In [18] the complete weight hierarchy of the Kasami codes is determined. The Kasami codes are of particular interest as they can be used to construct sequences with optimal autocorrelation.

The $v(a,0)$ form an $r-$dimensional subcode with constant weight $q^r - q^{r-m}$, and among the remaining codewords $v(a,b), b \neq 0$ only two different weights occur. Apply concatenation with the Simplex code $[\frac{q^m-1}{q-1}, m, q^{m-1}]_q$. The result is a linear $q-$ ary code. The length picks up a factor of $\frac{q^m-1}{q-1}$, the weights have to be multiplied by q^{m-1}.

Theorem 5. *Application of concatenation to $\mathcal{C}$ with the Simplex code $[\frac{q^m-1}{q-1}, m, q^{m-1}]_q$ yields a linear $3r'-$dimensional q-ary code $\tilde{\mathcal{C}}$ of length $(q^r-1)(q^m-1)/(q-1)$ whose codewords have the following weights:*

$$wt(v(\tilde{a},b)) = \begin{cases} 0 & \textit{if } a=b=0 \\ q^{r+m-1} - q^{r-1} & \textit{if } b=0, a\neq 0 \\ q^{r+m-1} - q^{r-1} + q^{r'+m-1} - q^{r'-1} & \textit{if } -\frac{N(a)}{b} \in W_0 \\ q^{r+m-1} - q^{r-1} - q^{r'-1} & \textit{if } -\frac{N(a)}{b} \notin W_0 \end{cases}$$

Finally, we apply construction X with the Simplex code $[\frac{q^{r'}-1}{q-1}, r', q^{r'-1}]_q$ as auxiliary code. The length increases by $\frac{q^{r'}-1}{q-1}$. The weights in the subcode consisting of the words with $b=0$ remain unchanged. The remaining weights increase by $q^{r'-1}$. We see that only two nonzero weights survive.

Theorem 6. *There is an explicit effective construction of a q-ary code of length $q^m(q^{r'}-1)(q^{r'}-q^{r'-m}+1)/(q-1)$ and dimension $3r'$ whose only nonzero weights are $d=q^{r+m-1}-q^{r-1}$ and $w_2=q^{r+m-1}-q^{r-1}+q^{r'+m-1}$, for all $1\le m\le r'$.*

4.1 The geometric connection

Assume $PG(2,q^{r'})$ contains a maximal q^m-arc. This situation is equivalently expressed as an (automatically projective) linear code

$$[q^{r'+m}-q^{r'}+q^m, 3, q^{r'+m}-q^{r'}]_{q^{r'}}$$

whose nonzero weights are $q^{r'+m}-q^{r'}$ and $q^{r'+m}-q^{r'}+q^m$. Concatenation with the Simplex code $[\frac{q^{r'}-1}{q-1}, r', q^{r'-1}]_q$ yields a linear $q-$ary code whose parameters are precisely those of Theorem 6. These maximal arcs do exist in characteristic 2 (see [12]), non-trivial such arcs do not exist in odd characteristic (see [1]). The smallest nontrivial member of the family constructed in Theorem 6 is a ternary code $[84,6,54]_3$ with nonzero weights 54 and 63. Such a code was first constructed by Gulliver [15]. In geometric language this represents a set of 84 points in $PG(5,3)$ such that every hyperplane meets the set either in 30 or in 21 points.

5 A closely related family of codes

The family of additive codes constructed in this section can be derived by lengthening from the family of the preceding section in the special case $r=6$. As before we give a direct and effective treatment.

We use the terminology of Section 4 in case $r=6, r'=3, m=2$. Our code $\mathcal{C}$ will therefore be q^2-ary. Its length is q^6, where the coordinates are parametrized by $x\in F=\mathbb{F}_{q^6}$. The codewords are parametrized by triples (a,b,c), where $a\in F, b\in F_0, c\in \mathbb{F}_{q^2}$. Let $\{\epsilon_1,\epsilon_2\}$ be a basis of $\mathbb{F}_{q^2}\mid \mathbb{F}_q$ and $\tau:\mathbb{F}_{q^2}\longrightarrow \mathbb{F}_q$ the trace. The entry of codeword $v(a,b,c)$ in coordinate x is defined as

$$v(a,b,c)_x=(Tr(\eta_j\cdot(T(ax)+bN(x))+\tau(\epsilon_j c))_{j=1,2}$$

As before our determination of the weights will yield as a by-product that the $\mathbb{F}_q-$linear mapping $(a,b,c) \mapsto v(a,b,c)$ is injective, and hence that $dim(\mathcal{C}) = 11/2 = 5.5$

Theorem 7. *We have constructed a family of q^2-ary $\mathbb{F}_q-$linear codes of length q^6 and dimension 5.5. The code-words are $v(a,b,c)$, where $a \in F, b \in F_0, c \in \mathbb{F}_{q^2}$ as described above. Let N be the additive coset of W_0 consisting of the elements y such that $Tr(\eta_j y) = -\tau(\epsilon_j c), j = 1,2$. Parametrize the coordinates by the elements $x \in F = \mathbb{F}_{q^6}$. The weights of the codewords are described as follows:*

$$wt((v(a,b,c)) = \begin{cases} 0 & \text{if } a=b=c=0, \\ q^6 & \text{if } a=b=0, c\neq 0. \\ q^6-q^4 & \text{if } b=0, a\neq 0 \\ q^6-q^4+q^3-q & \text{if } b\neq 0, -\frac{N(a)}{b} \in N \\ q^6-q^4-q & \text{if } b\neq 0, -\frac{N(a)}{b} \notin N \end{cases}$$

Proof. As $wt(v(a,b,0)) = wt(v(a,b))$ in the sense of Theorem 4, we can assume $c \neq 0$ in the sequel. Recall that $W_0 = \langle \eta_1, \eta_2 \rangle^\perp$, where the dual is with respect to the trace form. In our case $dim_{F_q}(W_0) = 1$. It is clear that for given c the elements y such that $Tr(\eta_j y) = -\tau(\epsilon_j c), j = 1,2$ describe a coset N of W_0 and hence a set of q elements. The statement of Lemma 1 simplifies as we do not have to exclude the case $x = 0$. We apply this information to the quadratic extension $F|F_0$ and obtain the statement of our theorem. ∎

Theorem 8. *Let $\mathcal{C}_1$ be the additive q^2-ary code constructed in Theorem 7. Then $\mathcal{C}_1 = \mathcal{C}_2 \bigoplus \mathcal{C}_2$ where $\mathcal{C}_2$ has parameters $[q^6, 4, q^6 - q^4]_{q^2}$ and $\mathcal{C}_3$ has parameters $[q^6, 1.5, q^6 - q^4 + q^3 - q]_{q^2}$. Moreover $\mathcal{C}_2$ contains a code $[q^6, 1, q^6]_{q^2}$.*

Proof. $\mathcal{C}_2$ consists of the codewords with $b = 0$, $\mathcal{C}_3$ contains the codewords with $a = c = 0$ and the repetition code (case $a = b = 0$) is contained in $\mathcal{C}_2$. ∎

Concatenation with the Reed-Solomon code $[q+1, 2, q]_q$ based on $\mathcal{C}_1$ yields a linear code $[q^6(q+1), 11, q^2(q^5 - q^3 - 1)]_q$ for every q. In the binary case this yields the length-optimal code $[192, 11, 92]_2$, which turned out to be the starting point for the construction of many good codes in [13].

6 A natural generalization

Let us generalize our earlier approach of the preceding section, using an extension $F \supset F_0$ of general degree. We are looking at a tower

$$\mathbb{F}_q \subset F_0 = \mathbb{F}_{q^{r'}} \subset F = \mathbb{F}_{q^r},$$

where $r = l \cdot r'$. Denote traces and norms by $T : F \longrightarrow F_0, N : F \longrightarrow F_0$, $Tr : F_0 \longrightarrow \mathbb{F}_q$. As before we have $m \leq r'$ and a set $\{\eta_1, \ldots, \eta_r\} \subset F_0$, which is linearly independent over $\mathbb{F}_q$. The definition of the codewords $v(a, b)$ is as before. The length is $q^r - 1$, the $\mathbb{F}_q-$dimension is $r + r' = (l+1)r'$. We still have $dim(W_0^{\perp}) = r' - m$. Every element $c \in F_0^*$ has $(q^r - 1)/(q^{r'} - 1)$ preimages under N. It follows

$$\chi_0(v(0, b)) = (q^r - 1)(q^{r'-m} - 1)/(q^{r'} - 1) \text{ for } b \neq 0.$$

Likewise

$$\chi_0(v(a, 0)) = q^{r'-m} q^{r-r'} - 1 = q^{r-m} - 1.$$

In case $ab \neq 0$ we use that $T(ax)+bN(x)$ is described by a nonzero polynomial of degree $1 + q^{r'} + \cdots + q^{(l-1)r'} = (q^r - 1)/(q^{r'} - 1)$. We obtain

$$\chi_0(v(a, b)) \leq q^{r'-m}(q^r - 1)/(q^{r'} - 1) - 1 = q^{r-m} + q^{(l-1)r'-m} + \cdots + q^{r'-m} - 1,$$

hence $d \geq q^r - q^{r-m} - \cdots - q^{r'-m}$.

Theorem 9. *$\mathcal{C}$ is a q^m-ary q-linear code of length $q^r - 1$, $\mathbb{F}_q-$dimension $r + r' = (l+1)r'$ and minimum distance d, where*

$$d \geq q^r - q^{r-m} - \cdots - q^{r'-m}.$$

Application of contatenation with the Simplex code $[\frac{q^m-1}{q-1}, m, q^{m-1}]_q$ yields a linear $(l+1)r'-$dimensional q-ary code $\tilde{\mathcal{C}}$ of length $(q^r-1)(q^m-1)/(q-1)$ with minimum distance

$$d \geq q^{r+m-1} - q^{r-1} - \cdots - q^{r'-1}.$$

References

[1] S.Ball, A.Blokhuis, F.Mazzocca: *Maximal arcs in desarguesian planes of odd order do not exist,* Combinatorica **56**(1996),39-47.

[2] J.Bierbrauer: *The theory of cyclic codes and a generalization to additive codes,* manuscript.

[3] J.Bierbrauer and Y.Edel: *A family of 2-weight codes related to BCH-codes,* Journal of Combinatorial Designs **5** (1997), 391-396.

[4] R.C.Bose and K.A.Bush: *Orthogonal arrays of strength two and three, A..Math.Statist.* **23** (1952),508-524.

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

[6] C.L.Chen: *Byte-oriented error-correcting codes for semiconductor memory systems,* IEEE Transactions on Computers **35**(1986),646-648.

[7] C.L.Chen: *Symbol error-correcting codes for computer memory systems,* IEEE Transactions on Computers **41**(1992),252-256.

[8] C.L.Chen and B.W.Curran: *Switching codes for delta-I noise reduction,* IEEE Transactions on Computers **45**(1996),1017-1021.

[9] C.L.Chen and L.E.Grosbach: *Fault-tolerant memory design in the IBM Application System/400,* Digest of Papers, The 21-th International Symposium on Fault-Tolerant Computing (1991),393-400.

[10] C.L.Chen and M.Y. Hsiao: *Error-correcting codes for semiconductor memory applications: a state-of-the-art review,* IBM Journal Res. Develop. **2**(1984),124-134.

[11] P.Delsarte and J.M.Goethals: *Tri-weight codes and generalized Hadamard matrices,* Information and Control **15**(1969),196-206.

[12] R.H.F.Denniston: *Some maximal arcs in finite projective planes,* Journal of Combinatorial Theory **6** (1969),317-319.

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

[14] Y.Edel and J.Bierbrauer:*Quantum twisted codes,* Journal of Combinatorial Designs **8**(2000),174-188.

[15] A.Gulliver: *Two New Optimal Ternary Two-Weight Codes and Strongly Regular Graphs,* Discrete Mathematics **149**(1996),83-92.

[16] M.Hattori, R.J.McEliece and G.Solomon: *Subspace subcodes of Reed-Solomon codes,* IEEE Transaction on Information Theory **44**(1998),1861-1880.

[17] A.S.Hedayat,N.J.A.Sloane and J.Stufken: *Orthogonal arrays - Theory and Applications,* Springer Series in Statistics, 1999.

[18] T.Helleseth and P.V.Kumar: *The weight hierarchy of the Kasami codes,* Discrete Mathematics **145**(1995),133-143.