New code parameters from Reed-Solomon subfield 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 determine the dimensions of subfield codes of Reed-Solomon codes and construct certain extensions and lengthenings of these codes. We start from the duals, using the language of orthogonal arrays. As a first result this allows us to obtain a fair number of improvements in the list of binary, ternary and quaternary linear codes with largest known minimal distance.

1 Introduction

We determine the parameters of the Reed-Solomon subfield codes (RS-subfield codes for short) and construct several types of codes related to them. In section 2 we define a class of linear orthogonal arrays whose duals are the RS subfield codes. This description is used to show that in many parametric situations the RS subfield codes can be lengthened (Theorem 3 and Corollary 1). The parameters of the RS subfield codes are determined in section 3. Another method of lengthening is introduced in section 4 and used to obtain

some particularly good codes. In section 5 we collect the information obtained so far for the codes falling in the range of the data base [3]. Aside of the codes obtained by the methods of the preceding sections we also include here lengthenings of RS subfield codes obtained by computer search. The computer search was based on the orthogonal arrays described in section 2. Suitable extensions of these by additional columns lead to lengthenings of the RS subfield codes. The material collected in section 5 yields a large number of good codes, which form chains by inclusion. This is the setting for the application of construction X (Theorem 9, see [9], p.581/582). We do this systematically in section 6 and obtain a large number of new codes. In section 7 we use the fact (obtained by computer) that some of the RS subfield codes have large dual distance and obtain yet more good codes. Among others we make use of construction Y1 here (Theorem10, see [9],p.592). In the appendices we give check matrices or generator matrices of a few good codes and the proof of a technically difficult lengthening theorem.
Among our best codes we mention the optimal codes

$$[39, 12, 14]_2, [155, 132, 8]_2, [86, 77, 5]_3, [39, 29, 6]_3, [85, 74, 6]_3,$$

$$[30, 7, 16]_3, [85, 7, 54]_3, [65, 57, 5]_4, [70, 7, 48]_4$$

as well as the non-optimal codes

$$[39, 26, 7], [85, 70, 7]_3, [82, 66, 8]_3, [33, 8, 17]_3, [32, 23, 6]_4, [81, 70, 6]_4, [70, 8, 46]_4.$$

Here optimality means that the minimum distance is maximum. The subscript denotes the field over which the code is defined. Observe that a ternary code $[30, 7, 16]_3$ was obtained independently by Boukliev [4] with other means.

2 Basic Theory

An **orthogonal array** with parameters $OA_\lambda(t, k, v)$ is defined as a multiset $\mathcal{A}$ of mappings from a k-set C into a v-set E such that for every choice of t distinct elements $x_1, x_2, \dots x_t$ in C and t not necessarily distinct elements $y_1, y_2, \dots y_t$ in E there are exactly λ elements $f \in \mathcal{A}$ affording the operation $f(x_i) = y_i, i = 1, 2, \dots t$. We will often visualize an orthogonal array as an array with λv^t rows and k columns, where each mapping contributes a row.

Definition 1 *Let q be a prime-power, $n > 1$ a natural number, $tr : I\!\!F_{q^n} \longrightarrow I\!\!F_q$ the* **trace.** *Put $F = I\!\!F_{q^n}$, let $2 \leq t \leq q^n$. The array $\mathcal{A}(t) = \mathcal{A}(q,n,t)$ has q^n columns indexed by $u \in F$ and $q^{n(t-1)+1}$ rows indexed by pairs $(p(X), z)$, where $z \in I\!\!F_q$ and $p(X)$ is a polynomial of degree $< t, p(0) = 0$, with coefficients in F. The entry of $\mathcal{A}(t)$ in column u and row $(p(X), z)$ is*

$$tr(p(u)) + z.$$

From now on we fix the ground field $I\!\!F_q$ and the extension field $F = I\!\!F_{q^n}$. We showed in [1] that $\mathcal{A}$ is an orthogonal array of strength t, with parameters $OA_{q^{(t-1)(n-1)}}(t, q^n, q)$. This is a rather straightforward application of Lagrange interpolation. Our Theorem 2 will imply another proof of this fact.

We also studied the question of **simplicity** of these arrays.

Definition 2 *With the same notation as above let $\mathcal{P}_0(t) = \mathcal{P}_0(q,n,t)$ be the $I\!\!F_q-$vector space of polynomials $p(X) \in I\!\!F_{q^n}[X]$ satisfying $p(0) = 0, deg(p(X)) < t$ and $tr(p(u)) = 0$ for every $u \in F$. Denote by $\rho_0(t) = \rho_0(q,n,t)$ the dimension of the $I\!\!F_q-$vector space $\mathcal{P}_0(t)$.*

We showed in [1] that each row of $\mathcal{A}(t)$ occurs with multiplicity $q^{\rho_0(t)}$. This is the motivation behind the definition of $\mathcal{P}_0(t)$. It follows that the **simplification** of $\mathcal{A}(t)$, where each row is written only once, is an orthogonal array with parameters

$$OA_{q^{(t-1)(n-1)-\rho_0(t)}}(t, q^n, q).$$

Moreover these OA are $I\!\!F_q-$linear. It follows from Delsarte theory (and the reader can easily prove this claim) that the dual code has parameters

$$[q^n, q^n - (n(t-1)+1) + \rho_0(t), t+1].$$

Another basic Theorem (see [9], page 208) customarily attributed to Delsarte states that the trace-code of a code C is the subfield code of the dual $C^\perp$. We apply this buted to Delsarte states that the trace-code of a code C is the subfield code of the dual $C^\perp$. The dual of the array $\mathcal{A}(q,n,t)$ is the same as the dual of the trace-code of $RS(t, I\!\!F_{q^n})$. As the duals of Reed-Solomon codes are Reed-Solomon codes again we conclude that $\mathcal{A}^\perp$ is a subfield code of a Reed-Solomon code. We collect this information in the following Theorem:

Theorem 1 *$\mathcal{A}^\perp$ is the subfield code of the Reed-Solomon code of dimension $q^n - t$ over $I\!F_{q^n}$:*

$$\mathcal{A}^\perp = RS(q^n - t, I\!F_{q^n}) \mid_{F_q} .$$

It is well-known that $RS(q^n - t, I\!F_{q^n}) \mid_{F_q}$ has the affine group of order $q^n(q^n - 1)$ as a group of automorphisms (see [8], p.84). It is also clear that the Galois group of $F \mid I\!F_q$ operates as a group of automorphisms. The preceding Theorem shows that this is also true of our arrays $\mathcal{A}(t)$:

Proposition 1 *The group $A\Gamma L(1, q^n)$ of order $q^n(q^n - 1)n$ is contained in the group of automorphisms of $\mathcal{A}(t)$.*

We remark that in the generic case this is the full automorphism group of $\mathcal{A}(t)$. This follows from the fact, derived from the classification of finite simple groups, that the group $A\Gamma L(1, q^n)$ is almost always a maximal subgroup of the symmetric or of the alternate group.

We will show that $\mathcal{A}$ can be extended by n additional columns to an orthogonal array of the same strength. This will allow us to lengthen the Reed-Solomon subfield code $\mathcal{A}(t)^\perp$ in many cases.

Definition 3 *We define the array $\mathcal{A}^*(t)$ with q^n+n columns in the following way: In the first q^n columns $\mathcal{A}^*(t)$ coincides with $\mathcal{A}(t)$. Let $\phi_1, \phi_2, \ldots, \phi_n$ be a complete set of linear independent linear forms of $I\!F_{q^n}$, where $I\!F_{q^n}$ is seen as a vector space over $I\!F_q$. The n last columns of $\mathcal{A}^*(t)$ are indexed by the ϕ_i. The entry in row $(p(X), z)$ and column ϕ is defined as $\phi(a_{t-1})$, where a_{t-1} is the leading coefficient of $p(X)$.*

Theorem 2 *The array $\mathcal{A}^*(t)$ is an $I\!F_q-$linear orthogonal array of strength t, hence with parameters $OA_{q^{(t-1)(n-1)}}(t, q^n + n, q)$.*

Proof: Pick a set of t columns, indexed by $x_1, x_2, \ldots, x_a \in F = I\!F_{q^n}$ and by the linear forms $\phi_1, \phi_2, \ldots, \phi_{t-a}$. Further pick elements $\alpha_1, \ldots, \alpha_a, \beta_1, \ldots, \beta_{t-a} \in I\!F_q$. We have to count the number λ of rows $(p(X), z)$ satisfying

$$tr(p(x_i)) + z = \alpha_i, \ (i = 1, 2, \ldots, a)$$

$$\phi_j(a_{t-1}) = \beta_j, \ (j = 1, 2, \ldots, t - a).$$

By subtracting we see that we have to count the polynomials $p(X)$ of degree $\leq t-1$, satisfying $p(0)=0$ and

$$tr(p(x_1)-p(x_i))=\alpha_1-\alpha_i,\ (i=2,\ldots,a)$$

$$\phi_j(a_{t-1})=\beta_j,\ (j=1,2,\ldots,t-a).$$

Let $U_i=tr^{-1}(\alpha_1-\alpha_i), i=2,\ldots,a$ and fix a tuple $(u_2,\ldots,u_a)\in U_2\times\ldots\times U_a$. Consider the number of polynomials $p(X)$ as above satisfying instead of the above

$$p(x_1)-p(x_i)=u_i,\ (i=2,\ldots,a) \tag{1}$$

$$\phi_j(a_{t-1})=\beta_j,\ (j=1,2,\ldots,t-a). \tag{2}$$

Let μ be the number of solutions. We will see that μ does not depend on the choice of the u_i. It will then follow that $\lambda=q^{(a-1)(n-1)}\mu$: In fact, by Lagrange interpolation there is precisely one polynomial $p(X)$ of degree $\leq a-1$ satisfying $p(0)=0$ and equation 1. It follows that the number of such polynomials of degree $\leq t-1$ is $(q^n)^{(t-1)-(a-1)}=q^{n(t-a)}$. It is clear that each value of a_{t-1} is taken on the same number of times here. Condition 2 affects only a_{t-1}. It says that a_{t-1} is in a certain coset of a subspace of codimension $t-a$ of F. We get $\mu=q^{n(t-a-1)+n-(t-a)}$, and $\lambda=q^{(a-1)(n-1)}\mu=q^{(t-1)(n-1)}$, as predicted.■

We aim at extending the codes $\mathcal{A}(t)^\perp$. Let $\delta(t)=\rho_0(t)-\rho_0(t-1)$. The highest coefficient a_{t-1} of polynomials in our space $\mathcal{P}_0(t)$ of dimension $\rho_0(t)$ as in Definition 2 is in a subspace U of dimension $\delta(t)$. Choose the linear forms $\phi_1,\ldots,\phi_{n-\delta(t)}$ such that U is the intersection of their kernels and consider the extension of $\mathcal{A}(t)$ by the corresponding $n-\delta(t)$ columns. It follows right from the definition that the multiplicity of rows of this extension is still the same as in $\mathcal{A}(t)$, namely $q^{\rho_0(t)}$. In particular the dimension of the space of rows is unchanged. It follows that the dual code has the parameters of an $(n-\delta(t))$-fold lengthening of $\mathcal{A}(t)^\perp$. More precisely the following is obtained:

Theorem 3 *With $q,n,t,\rho_0(t)$ as before, and $\delta(t)=\rho_0(t)-\rho_0(t-1)$, there is a linear q-ary code with parameters*

$$[q^n+n-\delta(t), q^n-n(t-1)-1+\rho_0(t)+n-\delta(t), t+1] =$$
$$= [q^n+n-\delta(t), q^n-n(t-2)-1+\rho_0(t-1), t+1].$$

The proof of Theorem 3 shows that we do not really need the linear forms ϕ_i to be independent. It suffices when any t of them are linearly independent. This is equivalent to using a linear $OA_{q^{n-t}}(t,e,q)$ for some e. We can use this to append e columns to the array $\mathcal{A}(t)$. Observe that an orthogonal array as above will exist if and only if its dual, a q-ary linear code $[e, e-n, t+1]$, exists. We aim at lengthening $\mathcal{A}(t)^\perp$ again. Let us speak of an **e-step lengthening** if we construct a code with length and dimension increased by e and same minimum distance. In our situation it suffices to observe that an e-step lengthening certainly will exist whenever $t \leq n$ and $\rho_0(t) = \rho_0(t-1)$. We summarize this in the following Corollary:

Corollary 1 *If $t \leq n$ and $\rho_0(t) = \rho_0(t-1)$, and if there is a q-ary linear code $[e, e-n, t+1]$, then the Reed-Solomon subfield code $\mathcal{A}^\perp$ may be lengthened e times to yield a code with parameters*

$$[q^n+e, q^n-(n(t-1)+1-\rho_0(t))+e, t+1].$$

When applied in case $t=2$ Corollary 1 produces the Hamming codes. The determination of the dimension of the subfield subcodes of Reed-Solomon codes and of their extensions as described above is equivalent to the determination of $\rho_0(q,n,t)$. We will study this function in the next section.

3 The function $\rho_0(q,n,t)$.

Observe that all dimensions are dimensions of $\mathbb{F}_q-$vector spaces. Denote by $\mathcal{P}_0$ the space of all polynomials $p(X)$ with coefficients in F satisfying $p(0)=0$ and $tr(p(u)=0$ for all $u \in F$. First a basic fact:

Proposition 2

$$\rho_0(t) \leq \rho_0(t+1), \rho_0(t+1)-\rho_0(t) \leq n.$$

This is rather obvious. A first result is the following:

Theorem 4

$$\rho_0(q) = 0, \rho_0(q+1) = n.$$

Proof: It is clear that $\rho_0(q) = 0$ as a non-constant polynomial takes on each value at most as often as its degree. The polynomials $\alpha \cdot X - \alpha^q \cdot X^q$, where $\alpha \in F$ show $\rho_0(q+1) = n$. ■

Let us start from the other side and determine $\rho_0(q^n)$: Let $\tilde{\mathcal{P}_0}$ be the space of polynomials of degree $< q^n$, all of whose values have trace $= 0$. Put $U = \{u \mid u \in F, tr(u) = 0\}$. By Lagrange interpolation each polynomial in $\tilde{\mathcal{P}_0}$ is uniquely determined by the set of its values $v_u \in U, u \in F$. Thus $\mid \tilde{\mathcal{P}_0} \mid = (q^{n-1})^{q^n}$, or $dim(\tilde{\mathcal{P}_0}) = (n-1)q^n$. Now $\mathcal{P}_0(q^n)$ is exactly the set of polynomials without constant term in our space. As $\tilde{\mathcal{P}_0}$ is closed under addition of constants from U we get:

Lemma 1 $\rho_0(q^n) = (n-1)(q^n - 1)$.

It follows that the simplification of $\mathcal{A}(t)$ in case $t = q^n$ is $OA_1(q^n, q^n, q)$, the set of all such tuples.
Aart Blokhuis has pointed out to us the relevance of Rédei's book [10] to our problems. In fact, the introductory chapter of that book leads to a characterization of the function ρ_0 in terms of cyclotomic cosets. We need some preparation:

Definition 4 *Let $\rho_1(t)$ be the dimension of the $I\!\!F_q$-vector space of polynomials $p(X)$ with coefficients in $I\!\!F_{q^n}$, of degree $\leq t-1$, satisfying $p(0) = 0$ and*

$$p(\alpha) \in I\!\!F_q \textit{ for all } \alpha \in I\!\!F_{q^n}$$

We know that the dimension of $\mathcal{A}(t)^\perp$ is $q^n - (t-1)n - 1 + \rho_0(t)$. On the other hand we have a concrete description as a subfield subcode of a Reed Solomon code:

$$\mathcal{A}^\perp = \{p(X) \mid p(X) \in I\!\!F_{q^n}(X), deg(p(X)) < q^n - t, p(I\!\!F_{q^n}) \subseteq I\!\!F_q\}.$$

In fact, if two such polynomials would yield the same q^n-tuple of values, their difference would have degree $\geq q^n$. We observe that if $p(X) \in \mathcal{A}(t)^\perp$

and $z \in \mathbb{F}_q$, then $p(X) + z \in \mathcal{A}(t)^{\perp}$. If we add the condition $p(0) = 0$ to the above description, then we arrive at the definition of the space whose dimension is $\rho_1(t)$. This leads to the following relation, which may be seen as a relation of duality:

Theorem 5

$$q^n + \rho_0(t) = (t-1)n + 2 + \rho_1(q^n - t)$$

Rédei's theorem characterizes the function $\rho_1(t)$:

Theorem 6 (Rédei) *Write t in $q-$adic representation, with n digits. Consider the action of the cyclic group of order n on these digits. Call t* **maximal** *if none of these cyclic shifts represents a number $> t$. Denote by s the length of this orbit under the cyclic group (observe that s divides n). Then*

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

The duality between ρ_0 and ρ_1 shows that $\rho_0(t+1) - \rho_0(t)$ is determined by the cyclic shifts of the $q-$adic representations of the number $q^n - t - 1$. Let us fix notation:

Definition 5 *For every integer t, let $\lfloor t \rfloor$ denote the remainder mod $q^n - 1$, chosen among $\{1, 2, \ldots, q^n - 1\}$. Denote by $\pi(t) = \pi_n(t)$ the $q-$adic representation of $\lfloor t \rfloor$ with n digits. Thus, if $\lfloor t \rfloor = \sum_{i=0}^{n-1} a_i q^i$, then $\pi(t) = (a_{n-1}, \ldots, a_1, a_0)$.*

Lemma 2 *If $\pi(t) = (a_{n-1}, \ldots, a_1, a_0)$, then $\pi(tq) = (a_{n-2}, \ldots, a_1, a_0, a_{n-1})$.*

Proof: Let $\lfloor t \rfloor = \sum_{i=0}^{n-1} a_i q^i$. Then $\lfloor tq \rfloor = \sum_{i=0}^{n-2} a_i q^{i+1} + a_{n-1} q^n = \sum_{i=0}^{n-2} a_i q^{i+1} + a_{n-1}$.■

It follows that the $\pi(tq^i), i = 0, 1, \ldots, n-1$ are just the cyclic shifts of $\pi(t)$. So they form an orbit under the action of the cyclic group of order n (a cyclotomic coset). The relation between $\pi(t)$ and $\pi(q^n - 1 - t)$ is now obvious:

Lemma 3 *$\pi(q^n-1-t) = \overline{\pi(t)}$. This means that for $\pi(t) = (a_{n-1}, \dots, a_1, a_0)$ we have $\pi(q^n-1-t) = \overline{\pi(t)} = (q-1-a_{n-1}, \dots, q-1-a_1, q-1-a_0)$.*

In particular t is maximal in the sense of Rédei's theorem if and only if q^n-1-t is minimal. It is also clear that the length s of the orbit of $\pi(t)$ under Z_n equals the length of the orbit of $\pi(q^n-1-t) = \pi(-t)$. Thus Rédei's theorem, when applied to our function $\rho_0(t)$, looks as follows:

Corollary 2

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

Here s is the length of the orbit containing $\pi(t)$ under the action of the cyclic group of order n.

4 Another method of lengthening

We have obtained lengthenings of RS subfield codes $\mathcal{A}(t)^\perp$ in Theorem 3 and Corollary 3. In this section we introduce another method of obtaining such lengthened codes in suitable parametric situations. We start from a Definition, which may at first look strange.

Definition 6 *Let $F = \mathbb{F}_{q^n}, k$ a natural number.*
*(i) Let P be a 1-dimensional $\mathbb{F}_q-$subspace of F (equivalently a point in the $(n-1)-$dimensional projective geometry over $\mathbb{F}_q$). Call P k-**bad** if there exist k distinct elements $x_1, x_2, \dots, x_t \in F$ such that with $y_i = \prod_{j=1, j\neq i}^{k}(x_i - x_j)$ we have*

$$1/y_i \in P, i = 2, 3, \dots, k.$$

*In the contrary case P is k-**good**.*
*(ii) Let $tr : F \longrightarrow \mathbb{F}_q$ be the trace, $H = Ker(tr)$ the kernel of the trace. Further let $L \subset F$ be a hyperplane ($(n-1)-$dimensional $\mathbb{F}_q-$ subspace). Certainly $L = \alpha \cdot H$ for some $\alpha \in F$. L will be called k-**good** if $P = \alpha \cdot \mathbb{F}_q$ is.*
(iii) Let C be a linear q-ary code of dimension n and some length e. Write C as a collection of e linear functionals $\phi_i : F \longrightarrow \mathbb{F}_q, i = 1, 2, \dots, e$. Call ϕ_i k-good if its kernel is. The code C is k-good if all the ϕ_i are k-good.

Theorem 7 *Assume $\rho_0(t) = n + \rho_0(t-1)$ and $\rho_0(t-1) = m + \rho_0(t-2)$, where $m < n$. Let U be the m-dimensional $I\!\!F_q-$space of the coefficients at X^{t-2} of polynomials from $\mathcal{P}_0(t-1)$.*
If there is a $(t-1)$-good $I\!\!F_q-$ary code $\mathcal{C}$ of dimension n, length e and strength t such that $U \subseteq Ker(\phi)$ for every linear functional ϕ describing a column of $\mathcal{C}$, then there exists an e-step extension of the code $\mathcal{A}(t)^{\perp}$. This is then a code with parameters $[q^n + e, q^n - \{(t-1)n + 1\} + \rho_0(t) + e, t+1]$.

Proof: It is clear, by the results of the preceding sections, that the simplifications of $\mathcal{A}(t)$ and of $\mathcal{A}(t-1)$ are the same, and hence so are the duals. We will work with $\mathcal{A} = \mathcal{A}(t-1)$. Let $\phi_i : F \longrightarrow I\!\!F_q, i = 1, 2, \dots e$ be the linear functionals describing the columns of $\mathcal{C}$. Each ϕ_i yields an additional column, where the entry in row $(p(X), z)$ is defined as $\phi_i(a_{t-2})$. This defines an extension of $\mathcal{A}$ by e additional columns. The main point is to prove that this extension still is an orthogonal array of strength t.
So consider sets of t different columns. If they all belong to $\mathcal{A}$, then there is nothing to prove. Consider first the case that exactly one of the columns does not belong to $\mathcal{A}$. So let $t-1$ different elements $x_1, x_2, \dots, x_{t-1} \in F$ and $t-1$ elements $\alpha_1, \alpha_2, \dots, \alpha_{t-1} \in I\!\!F_q$ be given, and let ϕ be one of the ϕ_i. Proceeding as in the proof of Theorem 2 we see that we have to consider the polynomials $p(X)$ defined over F, of degree $\leq t-2$, satisfying $p(0) = 0$ and

$$tr(p(x_i) - p(x_1)) = \alpha_i - \alpha_1, (i = 2, \dots, t-1)$$

Fix u_i such that $tr(u_i) = \alpha_i - \alpha_1, i = 2, \dots, t-1$. Then this is equivalent with

$$p(x_i) - p(x_1) = u_i + h_i, i = 2, \dots, t-1.$$

Here the h_i vary through the hyperplane $H = Ker(tr)$. We see by Lagrange interpolation that the polynomial $p(X)$ affording the operation above is uniquely determined by the right side, the $u_i + h_i$. Its highest coefficient a_{t-2} is the same as that of the uniquely determined

polynomial $g(X)$ of degree $\leq t-2$ affording $g(x_1) = 0, g(x_i) = u_i + h_i, i = 2, \dots, t-1$. This highest coefficient is therefore

$$a_{t-2} = \sum_{i=2}^{t-1} \frac{u_i + h_i}{y_i}.$$

Here we have used the terminology of Definition 6. We will be done if we can show that $\phi(a_{t-2})$ attains each value $\in \mathbb{F}_q$ the same number of times. As the u_i and x_i are constants, we may replace a_{t-2} by $\sum_{i=2}^{t-1} \frac{h_i}{y_i}$. Observe that each $\frac{1}{y_i} \cdot H$ is a hyperplane. So our claim is equivalent with the statement that the $\frac{1}{y_i} \cdot H$ do not all coincide with the kernel of ϕ. This is guaranteed by the definition of $(t-1)-$goodness.
This was the hardest case. If we consider sets of t columns less than $t-1$ of which belong to $\mathcal{A}$, then proceeding along the same lines as above we see that Lagrange interpolation will guarantee that the coeffient a_{t-2} of $p(X)$ attains each value $\in F$ the same number of times. The properties of $\mathcal{C}$ guarantee then that the defining property of OA is satisfied.
So we have extended our orthogonal array $\mathcal{A}(t)$ by e columns. In order to prove that the dual code of this extension has the desired properties it remains to show that each row with all zero entries in $\mathcal{A}$ must be all zero in the extension, too. This is guaranteed by the assumption that $U \subseteq Ker(\phi)$.■

Natural candidates for applications of Theorem 7 are the cases $t = q+1$. We have $\rho_0(q+1) = n, \rho_0(q) = \rho_0(q-1) = 0$. In order to apply Theorem 7 in these cases we need information on the $q-$good 1-dimensional subspaces.

Lemma 4 *Let $F = \mathbb{F}_{q^n}$ as before.*

1. *If $q = 2$, then all 1-dimensional subspaces of F are 2-bad.*

2. *If $q = 3, n$ odd, then all 1-dimensional subspaces of F are 3-bad.*

3. *If $q = 3, n$ even, then $P = \alpha \cdot \mathbb{F}_3$ is 3-good if and only if $\alpha \in F$ is a nonsquare.*

Proof: The case $q = 2$ is an easy exercise. Let $q = 3$ and $x_1, x_2, x_3 \in F$ different elements. Assume $y_2^{-1}\mathbb{F}_q$ is bad. Additive constants don't change the y_i, so we may assume $x_0 = 0$. A multiplicative constant λ changes $P = \alpha\mathbb{F}_q$ into $\lambda^{-2}\mathbb{F}_q$. So $\alpha\mathbb{F}_q$ is $3 - bad$ if and only if $\lambda^2\alpha\mathbb{F}_q$ is for some $0 \neq \lambda \in F$, and we can therefore assume without restriction $x_2 = 1$. Then $y_2 = 1 - x_3, y_3 = x_3(x_3 - 1)$. We must have $y_2 = \pm y_3$. If $y_3 = -y_2$, then $x_3 = 1 = x_2$, contradiction. So $y_3 = y_2$. It follows $x_3 = -1$. We conclude that $P = \alpha\mathbb{F}_3 = \mathbb{F}_3$. Applying the remark above we see that $P = \alpha\mathbb{F}_3$ is 3-bad if and only if either α or $-\alpha$ is a square in F. If n is odd, this will always be the case. If n is even, then the 1-dimensional subspaces generated by nonsquares will be 3-good.■

4.1 The case $q = 3, t = 4$.

Theorem 7 and Lemma 4 show that in case $q = 3, n$ even, the corresponding RS subfield subcodes $[3^n, 3^n - 2n - 1, 5]$ can be lengthened. Let us consider small even values of n more closely:

Let at first $q = 3, n = 2$. As $t = 4 > n$, our method cannot yield more than $e = 2$. Consider $\mathbb{F}_9$ as extension over $\mathbb{F}_3$ with generator θ and defining equation $\theta^2 = -\theta + 1$. Then $H = Ker(tr) = \theta^2 \mathbb{F}_3$. Consider the linear functionals ϕ_1, ϕ_2, where $\phi_1(1) = 1, \phi_1(\theta) = 0, \phi_2(1) = 1, \phi_2(\theta) = -1$. Then $Ker(\phi_1) = \theta \mathbb{F}_3 = \frac{1}{\theta} H$ and $Ker(\phi_2) = (\theta + 1)\mathbb{F}_3 = \theta^3 \mathbb{F}_3 = \theta H$. As θ and $\frac{1}{\theta}$ are nonsquares, we can apply the foregoing theorem to the RS subfield subcode with parameters $[9, 4, 5]$ and obtain $[11, 6, 5]$. This is of course the truncation of the ternary Golay code.

Let now $q = 3, n = 4$. We use $p(X) = X^4 + X - 1$ as the irreducible polynomial generating $\mathbb{F}_{81} | \mathbb{F}_3$. The element $\Theta = X + (p(X))$ generates the multiplicative group of $F = \mathbb{F}_{81}$. We have $H = Ker(tr) =< \Theta, \Theta^2, \Theta^3 >$. Write the linear functionals $\phi : F \longrightarrow \mathbb{F}_3$ in the form $\phi = \phi_x$, where $\phi_x(y) = tr(x \cdot y)$. Then $tr = \phi_1$. In general $Ker(\phi_x) = \frac{1}{x} H$. Thus ϕ_x is 3-good if and only if x is a nonsquare. Consider the 3-good linear functionals ϕ_x, where $x \in \{\Theta, \Theta^3, \Theta^7, \Theta^9, \Theta^{19}\}$. Express these linear functionals as the columns of a matrix, with respect to the basis $1, \Theta, \Theta^2, \Theta^3$. The matrix is

$$\begin{array}{ccccc}
0 & 0 & -1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & -1 \\
1 & 0 & 1 & 1 & -1
\end{array}$$

The rows of this matrix generate the code $(1, -1, -1, -1, -1)^\perp$, which by Delsarte theory is therefore an orthogonal array of strength 4. It follows that we can apply the preceding theorem with $e = 5$. Higher values of e are clearly impossible. We conclude that we get a 5-step extension of the Reed-Solomon subfield code. This yields a ternary code with parameters

$$[86, 77, 5].$$

An exhaustive computer search shows that the ternary RS subfield codes $[9,4,5]$ and $[81,72,5]$ cannot be extended by more than 2 and 5 columns, respectively.

4.2 The case $q=3,t=5$.

Let $q=3,t=5,n>2$. We know $\rho_0(3)=0,\rho_0(4)=\rho_0(5)=n$. Consider the simple array $\mathcal{A}_0=\mathcal{A}_0(5)$, whose rows are indexed by pairs $(p(X),z)$, where $z\in \mathbb{F}_3, p(X)=aX^4+bX^2+cX, a,b,c\in F$. We want to extend $\mathcal{A}_0$ by columns, indexed by linear functionals $\phi : F\times F \longrightarrow \mathbb{F}_3$ such that the entry in row $(p(X),z)$ is $\phi(a,b)$. Each such linear functional can be written as a **trace-form** $\phi=\phi_{\alpha,\beta}$, where

$$\phi_{\alpha,\beta}(x,y)=tr(\alpha\cdot x+\beta\cdot y).$$

Theorem 8 *Let $q=3,t=5,n>2$. Extend the simple array $\mathcal{A}_0(5)$ by columns $\phi_i=\phi_{\alpha_i,\beta_i}$, where the entry in row (aX^4+bX^2+cX,z) and column ϕ is $\phi(a,b)$. Assume the ϕ_i form a linear orthogonal array of length e and strength 5.*
The extended array forms a (linear) orthogonal array of strength 5 if and only if the following conditions are satisfied:

1. *If $\phi_{\alpha,\beta}$ is a column, then (α,β) cannot be expressed in the form $(\alpha,\beta)=(-xy(x^2+y^2),xy)$ with $x,y\in F$.*
2. *For every pair $\phi_{\alpha,\beta},\phi_{\alpha',\beta'}$ of different columns neither $(\alpha+\alpha',\beta+\beta')$ nor $(\alpha-\alpha',\beta-\beta')$ can be written in the form (x^4,x^2) or $(-x^4,-x^2)$ for some $x\in F$.*

If this is satisfied, then the dual of the extended array is an $e-$step lengthening of $\mathcal{A}(5)^\perp$, and this is a ternary linear code with parameters

$$[3^n+e,3^n-\{3n+1\}+e,6].$$

As the proof of this Theorem is rather involved we chose to relegate it to an appendix. Let us consider applications of Theorem 8. We start from $n=2$, although this is not covered by the Theorem. In this case $\rho_0(5)=3<4=2n$. A computer program produced the ternary Golay code as an extension of our RS subfield code. In case $n = 3$ the computer found a representation of the ternary Golay code satisfying the conditions of Theorem 8, so that we could use it to construct a 12-step lengthening of the RS subfield code. This is a ternary code with parameters $[39, 29, 6]$. The check matrix is given in the appendix.

In the case $n = 4$ our RS subfield code has parameters $[81, 68, 6]$. We use the polynomial $X^4 + X - 1$ to generate the field $F = \mathbb{F}_{81}$. The image of X is mapped to a generator u of the multiplicative group of F. In the following table we give nineteen pairs (α, β) of field elements. Here entry i stands for u^i, symbol $*$ stands for 0. It can be checked that this set satisfies the conditions of Theorem 8 and therefore yields a ternary code $[100, 87, 6]$.

α	*	*	*	*	80	80	3	3	79	79	2	2	17	1	53	9	69	27	50
β	3	79	17	1	*	54	*	8	38	73	*	50	4	*	46	51	25	40	49

5 Small parameter values

We consider the cases $(q = 2, n = 7, 8)$, $(q = 3, n = 2, 3, 4)$ and $(q = 4, n = 3)$. The reason for this choice is that we get a large number of new code parameters and the codes we get fall in the range covered by the data base on minimum distances of linear codes. Generally we give the complete list of the values of $\rho_0(t)$. We also include the parameters of the codes obtained by lengthening $\mathcal{A}^{\perp}$, by application of Theorem 3, Corollary 1, Theorem 7 or by computer calculations. Entries marked **new** in the tables are record-breaking. A mark **opt** means that the maximal value of d had been known before and we reproduce it. **opt,new** means that our value of d is new and maximal. A mark **best known** means that we obtain the largest value of d which is hitherto known. Mark **comp** indicates that computer work was needed to find the extension of the Reed-Solomon subfield code. The computer searches leading to lengthenings of the RS subfield codes were based on extensions of the duals. Some generator matrices of computer-generated codes are given in the appendix. The complete information is to be found in the first author's home page [2]. The values of $\rho_0(t)$ are obtained by repeated use of Corollary 2. We do not give values for $t > q^n - q^{n-1}$ as they are easily calculated and the resulting codes are not interesting (they have dimension 1). We do not give complete information in case $q = 2, n < 8$. The codes we get in this range are described in the following subsection. Some of the less interesting values of t are omitted in the tables, but generally only when $\rho_0(t) - \rho_0(t-1) = n$ and when it is clear why this is the case. The values $t > 88$ in case $q = 2, n = 8$ have also been omitted.

5.1 Case $q = 2, n < 8$.

Consider first $n = 5, t = 12$. We have $\rho_0(12) = \rho_0(11) = 30$. This leads to a Reed Solomon subfield code $[32, 6, 13]$. Application of Corollary 1 leads to a code $[37, 11, 13]$. These parameters are known. A computer run yielded another extension step. This is a code $[38, 12, 13]$. An overall parity check finally yields a code

$$[39, 12, 14],$$

which is new and optimal. A generator matrix of the code $[38, 12, 13]$ will be given in the appendix.
A similar situation occurs in case $n = 6, t = 8$. Here $\rho_0(8) = \rho_0(7) = 18$. This gives us parameters $[64, 39, 9]$. Corollary 1 yields a 6-step lengthening. A computer-program produced a lengthening by 7. An overall parity check yields a code

$$[72, 46, 10].$$

Consider $n = 7, t = 6$. We have $\rho_0(6) = \rho_0(5) = 14$. Using Corollary 1 with a (trivial) code $[8, 1, 7]$ we get a binary code $[136, 114, 7]$. An overall parity-check yields a $[137, 114, 8]$, which is new and optimal. Again we can do better with the help of a computer- program. It produced a code $[154, 132, 7]$. As before we obtain a binary code with parameters

$$[155, 132, 8],$$

which is new and optimal.

5.2 Case $q = 2, n = 7$.

t	$\rho_0(t)$	codes	remarks
2	0	[255,247,3]	opt
3	7	[128,120,4]	opt
4	7	[139,124,5]	best known
5	14	[128,113,6]	opt
6	14	[154,132,7]	opt,new (comp)
7	21	[128,106,8]	opt
8	21	[135,106,9]	best known
9	28	[128,99,10]	best known
10	28	[135,99,11]	best known
11	35	[128,92,12]	best known
12	35	[135,92,13]	best known
13	42	[128,85,14]	best known
14	42	[135,85,15]	best known
15	49	[128,78,16]	best known
16	49	[135,78,17]	best known
17	56	[128,71,18]	
18	63	[128,71,19]	
19	70	[128,71,20]	best known
20	70	[135,71,21]	best known
21	77	[128,64,22]	best known
22	77	[135,64,23]	best known
23	84	[128,57,24]	best known
24	84	[135,57,25]	best known
25	91	[128,50,26]	
26	98	[128,50,27]	
27	105	[128,50,28]	best known
28	105	[135,50,29]	best known
29	112	[128,43,30]	
30	112	[135,43,31]	
31	119	[128,36,32]	
32	119	[135,36,33]	
33	126	[128,29,34]	
34	133		
35	140		

t	$\rho_0(t)$	codes	remarks
36	147		
43	196	[128,29,44]	best known
44	196	[135,29,45]	best known
45	203	[128,22,46]	
46	210		
47	217	[128,22,48]	best known
48	217	[135,22,49]	best known
49	224	[128,15,50]	
50	231		
51	238		
52	245		
53	252		
54	259		
55	266	[128,15,56]	opt
56	266	[135,15,57]	best known
57	273	[128,8,58]	
58	280		
59	287		
60	294		
61	301		
62	308		
63	315	[128,8,64]	opt
64	315	[135,8,65]	opt

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

t	$\rho_0(t)$	codes	remarks
2	0	[511,502,3]	opt
3	8	[256,247,4]	opt
4	8	[273,256,5]	
5	16	[256,239,6]	opt
6	16	[265,240,7]	new
7	24	[256,231,8]	opt
8	24	[265,232,9]	
9	32	[256,223,10]	opt
10	32	[264,223,11]	new
11	40	[256,215,12]	best known
12	40	[264,215,13]	
13	48	[256,207,14]	best known
14	48	[264,207,15]	new
15	56	[256,199,16]	best known
16	56	[264,199,17]	
17	64	[256,191,18]	best known
18	68	[260,191,19]	new
19	76	[256,187,20]	best known
20	76	[264,187,21]	new
21	84	[256,179,22]	best known
22	84	[264,179,23]	new
23	92	[256,171,24]	best known
24	92	[264,171,25]	new
25	100	[256,163,26]	best known
26	100	[264,163,27]	new
27	108	[256,155,28]	best known
28	108	[264,155,29]	new
29	116	[256,147,30]	best known
30	116	[264,147,31]	new
31	124	[256,139,32]	best known
32	124	[264,139,33]	
33	132	[256,131,34]	
34	140	[256,131,35]	
35	148	[256,131,36]	

t	$\rho_0(t)$	codes	remarks
36	156	[256,131,37]	
37	164	[256,131,38]	best known
38	164	[264,131,39]	new
39	172	[256,123,40]	best known
40	172	[264,123,41]	new
41	180	[256,115,42]	
42	188	[256,115,43]	
43	196	[256,115,44]	best known
44	196	[264,115,45]	new
45	204	[256,107,46]	best known
46	204	[264,107,47]	new
47	212	[256,99,48]	best known
48	212	[264,99,49]	new
49	220	[256,91,50]	
50	228	[256,91,51]	
51	236	[256,91,52]	best known
52	240	[260,91,53]	new
53	248	[256,87,54]	best known
54	248	[264,87,55]	new
55	256	[256,79,56]	best known
56	256	[264,79,57]	
57	264	[256,71,58]	
58	272	[256,71,59]	
59	280	[256,71,60]	best known
60	280	[264,71,61]	new
61	288	[256,63,62]	
62	288	[264,63,63]	
63	296	[256,55,64]	
64	296	[264,55,65]	
65	304	[256,47,66]	
66	312	[256,47,67]	
85	464	[256,47,86]	best known
86	470	[258,47,87]	new
87	478	[256,45,88]	best known
88	478	[264,45,89]	

5.4 Case $q = 3, n = 2$.

t	$\rho_0(t)$	codes	remarks
2	0	[13,10,3]	opt
3	0	[11,6,4]	
4	2	[11,6,5]	opt
5	3	[12,6,6]	Golay (comp)
6	3	[11,3,7]	opt

5.5 Case $q = 3, n = 3$.

t	$\rho_0(t)$	codes	remarks
2	0	[40,36,3]	opt
3	0	[31,24,4]	best known
4	3	[27,20,5]	opt
5	3	[39,29,6]	opt,new (comp)
6	3	[39,26,7]	new (comp)
7	6	[27,14,8]	best known
8	6	[30,14,9]	
9	6	[30,11,10]	
10	9	[27,8,11]	
13	18	[27,8,14]	opt
14	20	[28,8,15]	opt
15	20	[30,7,16]	opt,new
17	26	[27,4,18]	opt
18	26	[30,4,19]	opt

5.6 Case $q = 3, n = 4$.

t	$\rho_0(t)$	codes	remarks
2	0	[121,116,3]	opt
3	0	[85,76,4]	best known
4	4	[86,77,5]	opt,new
5	4	[100,87,6]	new (comp)
6	4	[101,84,7]	new (comp)
7	8	[83,66,8]	new(comp)
8	8	[85,64,9]	new
9	8	[85,60,10]	new
10	12	[81,56,11]	best known
11	14	[83,56,12]	new
12	14	[85,54,13]	new
13	18	[81,50,14]	best known
14	18	[85,50,15]	new
15	18	[85,46,16]	new
16	22	[81,42,17]	best known
17	22	[85,42,18]	best known
18	22	[85,38,19]	best known
19	26	[81,34,20]	
20	30	[81,34,21]	best known
21	32	[83,34,22]	new
22	36	[81,32,23]	best known
23	36	[85,32,24]	new
24	36	[85,28,25]	best known
25	40	[81,24,26]	best known
26	40	[85,24,27]	
27	40	[85,20,28]	
28	44	[81,16,29]	
29	48	[81,16,30]	
30	52	[81,16,31]	
31	56	[81,16,32]	
32	60	[81,16,33]	
33	64	[81,16,34]	
34	68	[81,16,35]	

t	$\rho_0(t)$	codes	remarks
35	72	[81,16,36]	
36	76	[81,16,37]	
37	80	[81,16,38]	
38	84	[81,16,39]	
39	88	[81,16,40]	
40	92	[81,16,41]	best known
41	95	[82,16,42]	best known
42	95	[85,15,43]	new
43	99	[81,11,44]	
44	103	[81,11,45]	best known
45	103	[85,11,46]	new
46	107	[81,7,47]	
47	111	[81,7,48]	
48	115	[81,7,49]	
49	119	[81,7,50]	
50	123	[81,7,51]	opt
51	125	[83,7,52]	opt,new
52	129	[81,5,53]	
53	133	[81,5,54]	opt
54	133	[85,5,55]	opt

5.7 Case $q = 4, n = 3$.

t	$\rho_0(t)$	codes	remarks
2	0	[85,81,3]	opt
3	0	[70,63,4]	opt
4	0	[126,116,5]	new (comp)
5	3	[64,54,6]	opt
6	3	[70,57,7]	new (comp)
7	3	[67,51,8]	best known
8	3	[67,48,9]	new
9	6	[64,45,10]	
10	6	[67,45,11]	new
11	6	[67,42,12]	new
12	6	[67,39,13]	new
13	9	[64,36,14]	best known
14	9	[67,36,15]	new
15	9	[67,33,16]	best known
16	9	[67,30,17]	best known
17	12	[64,27,18]	
18	15	[64,27,19]	
19	18	[64,27,20]	
20	21	[64,27,21]	
21	24	[64,27,22]	best known
22	26	[65,27,23]	new
23	26	[67,26,24]	new
24	26	[67,23,25]	new
25	29	[64,20,26]	
26	32	[64,20,27]	
27	32	[67,20,28]	new
28	32	[67,17,29]	best known
29	35	[64,14,30]	
30	38	[64,14,31]	best known
31	38	[67,14,32]	
32	38	[67,11,33]	
33	41	[64,8,34]	
34	44	[64,8,35]	

t	$\rho_0(t)$	codes	remarks
35	47	[64,8,36]	
36	50	[64,8,37]	
37	53	[64,8,38]	
38	56	[64,8,39]	
39	59	[64,8,40]	
40	62	[64,8,41]	
41	65	[64,8,42]	
42	68	[64,8,43]	opt
43	70	[65,8,44]	opt
44	70	[67,7,45]	new
45	73	[64,4,46]	
46	76	[64,4,47]	
47	79	[64,4,48]	opt
48	79	[67,4,49]	opt

In [7] a quaternary code $[65, 8, 44]$ was constructed from scratch and used to obtain good binary codes via concatenation and other constructions. Here we see that a quaternary $[65, 8, 44]$ can be obtained by applying Theorem 3 to the RS subfield code $[64, 7, 43]$.

6 Codes obtained by extension

The projection of an $[n + 1, k, d]$-code onto all but one of its coordinates (custumarily called **truncation** in coding theory) obvious yields $[n, k, d-1]$. The inverse process, if possible, goes under the name of **extension.** We use a basic fact on extension known as construction X ([9], p.581/582, which we use in the following form

Theorem 9 (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 $\mathcal{C}$.*

It is clear that the projection (truncation) onto the n first coordinates leads back to $\mathcal{C}$ from $\tilde{\mathcal{C}}$. The easiest application of this occurs in the binary case when d is odd. We have $e = 1$ then. This operation is known as adding a parity check. Let us apply the procedure to our RS subfield codes. If we use the codes $\mathcal{A}(t)^\perp$ and their subcodes $\mathcal{A}(t+1)^\perp$ we obtain another explanation for most of our lengthening results: the lengthenings of $\mathcal{A}(t+1)^\perp$ can be seen as extensions of $\mathcal{A}(t)^\perp$. The details are left to the reader.

The tables in section 5 provide us with a large number of codes contained in each other. In each such case we can use Theorem 9 and obtain an extension. The **auxiliary codes** $[e, \kappa, \delta]$ needed to apply Theorem 9 are taken from the data base [3]. In the following tables we list examples of this construction, which led to new code parameters.

6.1 The binary case

pair of codes	auxiliary code	result
$[67,18,24]\supset[64,7,32]$	$[23,11,8]$	$[90,18,32]$
$[129,79,15]\supset[128,71,20]$	$[13,8,4]$	$[142,79,19]$
$[130,80,15]\supset[128,71,20]$	$[14,9,4]$	$[144,80,19]$
$[131,81,15]\supset[128,71,20]$	$[15,10,4]$	$[146,81,19]$
$[129,58,23]\supset[128,50,28]$	$[13,8,4]$	$[142,58,27]$
$[130,59,23]\supset[128,50,28]$	$[14,9,4]$	$[144,59,27]$
$[131,60,23]\supset[128,50,28]$	$[15,10,4]$	$[146,60,27]$
$[128,36,32]\supset[128,29,44]$	$[19,7,8]$	$[147,36,40]$
$[128,36,32]\supset[128,29,44]$	$[24,7,10]$	$[152,36,42]$
$[128,36,32]\supset[128,29,44]$	$[27,7,12]$	$[155,36,44]$
$[130,31,33]\supset[128,29,44]$	$[12,2,8]$	$[142,31,41]$
$[129,30,33]\supset[128,29,44]$	$[11,1,11]$	$[140,30,44]$
$[130,31,33]\supset[128,29,44]$	$[15,2,10]$	$[145,31,43]$
$[129,23,45]\supset[128,22,48]$	$[3,1,3]$	$[132,23,48]$
$[130,24,45]\supset[128,22,48]$	$[4,2,3]$	$[134,24,48]$
$[132,23,48]\supset[128,15,49]$	$[8,8,1]$	$[140,23,49]$
$[134,24,48]\supset[128,15,49]$	$[9,9,1]$	$[143,24,49]$
$[130,17,49]\supset[128,15,53]$	$[6,2,4]$	$[136,17,53]$
$[130,17,49]\supset[128,15,55]$	$[9,2,6]$	$[139,17,55]$
$[128,29,44]\supset[128,15,56]$	$[34,14,10]$	$[162,29,54]$
$[130,24,45]\supset[128,15,56]$	$[21,9,8]$	$[151,24,53]$
$[131,25,45]\supset[128,15,56]$	$[22,10,8]$	$[153,25,53]$
$[132,26,45]\supset[128,15,56]$	$[23,11,8]$	$[155,26,53]$
$[133,27,45]\supset[128,15,56]$	$[24,12,8]$	$[157,27,53]$
$[128,8,64]\supset[128,1,127]$	$[27,7,12]$	$[155,8,76]$
$[128,8,64]\supset[128,1,127]$	$[40,7,18]$	$[168,8,82]$
$[128,8,64]\supset[128,1,127]$	$[43,7,20]$	$[171,8,84]$
$[128,8,64]\supset[128,1,127]$	$[47,7,22]$	$[175,8,86]$
$[128,8,64]\supset[128,1,127]$	$[50,7,24]$	$[178,8,88]$

The first code needs explanation: we are in case $q=2, n=6$. The code $\mathcal{A}(22)^\perp$ has parameters $[64,16,23]$ and possesses a 2-step lengthening. A parity check yields a code $\mathcal{C}$ with parameters $[67,18,24]$. As $\mathcal{A}(31)^\perp$ has parameters $[64,7,32]$ we see that $\mathcal{C}$ has a subcode of codimension 11 and

minimum distance ≥ 32. The binary Golay code shows that there is a binary code $[23, 11, 8]$. Application of Theorem 9 yields a code with the new parameters $[90, 18, 32]$.
Also, in the construction of the code $[140, 23, 49]$ we use the code $[132, 23, 48]$ construct two rows earlier, which by construction contains the code $[128, 22, 48]$. This latter code contains $[128, 15, 49]$. We are now in a position to apply Theorem 9. Apparently the 8-dimensional codes are known (see [6]). We obtain here an effortless conceptual construction.

6.2 The ternary case

pair of codes	auxiliary code	result
$[28,8,15] \supset [27,4,18]$	$[5,4,2]$	$[33,8,17]$
$[81,68,6] \supset [81,64,8]$	$[5,4,2]$	$[86,68,8]$
$[81,64,8] \supset [81,56,11]$	$[11,8,3]$	$[92,64,11]$
$[81,60,9] \supset [81,56,11]$	$[5,4,2]$	$[86,60,11]$
$[83,57,11] \supset [81,54,12]$	$[3,3,1]$	$[86,57,12]$
$[81,60,9] \supset [81,54,12]$	$[9,6,3]$	$[90,60,12]$
$[82,61,9] \supset [81,54,12]$	$[10,7,3]$	$[92,61,12]$
$[81,56,11] \supset [81,50,14]$	$[7,6,2]$	$[88,56,13]$
$[81,56,11] \supset [81,50,14]$	$[9,6,3]$	$[90,56,14]$
$[81,54,12] \supset [81,50,14]$	$[5,4,2]$	$[86,54,14]$
$[82,55,12] \supset [81,50,14]$	$[6,5,2]$	$[88,55,14]$
$[81,50,14] \supset [81,46,15]$	$[4,4,1]$	$[85,50,15]$
$[82,51,13] \supset [81,46,15]$	$[6,5,2]$	$[88,51,15]$
$[81,50,14] \supset [81,42,17]$	$[9,8,2]$	$[90,50,16]$
$[81,50,14] \supset [81,42,17]$	$[11,8,3]$	$[92,50,17]$
$[81,46,15] \supset [81,42,17]$	$[5,4,2]$	$[86,46,17]$
$[82,35,19] \supset [81,34,21]$	$[2,1,2]$	$[84,35,21]$
$[81,38,18] \supset [81,32,23]$	$[11,6,5]$	$[92,38,23]$
$[81,34,21] \supset [81,32,23]$	$[3,2,2]$	$[84,34,23]$
$[81,24,26] \supset [81,16,41]$	$[28,8,15]$	$[109,24,41]$
$[82,21,27] \supset [81,16,41]$	$[20,5,12]$	$[102,21,39]$
$[82,12,43] \supset [81,11,45]$	$[2,1,2]$	$[84,12,45]$
$[83,13,43] \supset [81,11,45]$	$[3,2,2]$	$[86,13,45]$
$[84,12,45] \supset [81,7,51]$	$[6,5,2]$	$[90,12,47]$
$[84,12,45] \supset [81,7,51]$	$[11,5,6]$	$[95,12,51]$
$[86,13,45] \supset [81,7,51]$	$[12,6,6]$	$[98,13,51]$
$[81,16,41] \supset [81,11,45]$	$[9,5,4]$	$[90,16,45]$
$[81,15,42] \supset [81,11,45]$	$[5,4,2]$	$[86,15,44]$
$[81,15,42] \supset [81,11,45]$	$[7,4,3]$	$[88,15,45]$
$[81,15,42] \supset [81,7,51]$	$[20,8,9]$	$[101,15,51]$

pair of codes	auxiliary code	result
$[81, 15, 42] \supset [81, 5, 54]$	$[28, 10, 12]$	$[109, 15, 54]$
$[82, 16, 42] \supset [81, 11, 45]$	$[6, 5, 2]$	$[88, 16, 44]$
$[82, 16, 42] \supset [81, 7, 51]$	$[17, 9, 6]$	$[99, 16, 48]$
$[82, 16, 42] \supset [81, 7, 51]$	$[21, 9, 9]$	$[103, 16, 51]$
$[82, 16, 42] \supset [81, 5, 54]$	$[29, 11, 12]$	$[111, 16, 54]$
$[82, 12, 43] \supset [81, 7, 51]$	$[11, 5, 6]$	$[93, 12, 49]$
$[83, 13, 43] \supset [81, 7, 51]$	$[12, 6, 6]$	$[95, 13, 49]$
$[81, 11, 45] \supset [81, 7, 51]$	$[5, 4, 2]$	$[86, 11, 47]$
$[81, 11, 45] \supset [81, 7, 51]$	$[10, 4, 6]$	$[91, 11, 51]$
$[81, 11, 45] \supset [81, 5, 54]$	$[15, 6, 7]$	$[96, 11, 52]$
$[81, 11, 45] \supset [81, 5, 54]$	$[18, 6, 9]$	$[99, 11, 54]$
$[81, 7, 51] \supset [81, 5, 54]$	$[4, 2, 3]$	$[85, 7, 54]$
$[81, 7, 51] \supset [81, 1, 80]$	$[26, 6, 15]$	$[107, 7, 66]$
$[81, 7, 51] \supset [81, 1, 80]$	$[40, 6, 24]$	$[121, 7, 75]$
$[81, 7, 51] \supset [81, 1, 80]$	$[44, 6, 27]$	$[125, 7, 78]$

Observe that code $[86, 13, 45]$ is not of independent interest here as its parameters are implied by the $[88, 15, 45]$, but we use the code three rows below to construct $[98, 13, 51]$. The parameters $[85, 7, 54]$ improve on those of our code $[83, 7, 52]$ constructed in subsection 5.6.

6.3 The quaternary case

pair of codes	auxiliary code	result
$[64, 48, 8] \supset [64, 45, 10]$	$[4, 3, 2]$	$[68, 48, 10]$
$[64, 42, 11] \supset [64, 36, 14]$	$[9, 6, 3]$	$[73, 42, 14]$
$[64, 39, 12] \supset [64, 36, 14]$	$[4, 3, 2]$	$[68, 39, 14]$
$[64, 36, 14] \supset [64, 27, 22]$	$[18, 9, 8]$	$[82, 36, 22]$
$[64, 33, 15] \supset [64, 27, 22]$	$[12, 6, 6]$	$[76, 33, 21]$
$[65, 31, 16] \supset [64, 27, 22]$	$[10, 4, 6]$	$[75, 31, 22]$
$[65, 28, 17] \supset [64, 27, 22]$	$[5, 1, 5]$	$[70, 28, 22]$
$[64, 33, 15] \supset [64, 27, 22]$	$[14, 6, 7]$	$[78, 33, 22]$
$[64, 33, 15] \supset [64, 26, 23]$	$[16, 7, 8]$	$[80, 33, 23]$
$[64, 30, 16] \supset [64, 27, 22]$	$[9, 3, 6]$	$[73, 30, 22]$
$[64, 30, 16] \supset [64, 26, 23]$	$[12, 4, 7]$	$[76, 30, 23]$
$[65, 31, 16] \supset [64, 27, 22]$	$[10, 4, 6]$	$[75, 31, 22]$
$[64, 27, 22] \supset [64, 23, 24]$	$[5, 4, 2]$	$[69, 27, 24]$
$[64, 26, 23] \supset [64, 20, 27]$	$[10, 6, 4]$	$[74, 26, 27]$
$[65, 27, 23] \supset [64, 20, 27]$	$[11, 7, 4]$	$[76, 27, 27]$
$[64, 23, 24] \supset [64, 20, 27]$	$[5, 3, 3]$	$[69, 23, 27]$
$[65, 24, 24] \supset [64, 20, 27]$	$[5, 4, 2]$	$[70, 24, 26]$
$[64, 20, 27] \supset [64, 14, 31]$	$[7, 6, 2]$	$[71, 20, 29]$
$[64, 20, 27] \supset [64, 14, 31]$	$[10, 6, 4]$	$[74, 20, 31]$
$[64, 17, 28] \supset [64, 14, 31]$	$[5, 3, 3]$	$[69, 17, 31]$
$[65, 18, 28] \supset [64, 14, 31]$	$[5, 4, 2]$	$[70, 18, 30]$
$[64, 8, 43] \supset [64, 4, 48]$	$[9, 4, 5]$	$[73, 8, 48]$
$[64, 7, 44] \supset [64, 4, 48]$	$[6, 3, 4]$	$[70, 7, 48]$
$[65, 8, 44] \supset [64, 4, 48]$	$[5, 4, 2]$	$[70, 8, 46]$
$[65, 8, 44] \supset [64, 1, 63]$	$[32, 7, 19]$	$[97, 8, 63]$

7 The dual codes

In a number of cases the duals of the RS subfield codes and their extensions have large minimum distances and therefore yield good codes. Most of the results presented in this section rely on computer calculations.

7.1 The ternary case

The RS subfield code $[81, 72, 5]$ has dual distance 48. The ternary parameters $[81, 9, 48]$ are new. Truncation of this code (projection onto the first 72 coordinates produces an $[72, 9, 40]$. The code $[86, 77, 5]$ obtained by lengthening in subsection 4.1 has dual distance 50. This leads to the new parameters $[86, 9, 50]$. The code $[82, 16, 42]$ obtained by lengthening in section 5 has dual distance 8 and therefore yields the new parameters $[82, 66, 8]$. Another new parameter is obtained by applying construction Y1 ([9],p.592), which we use in the following form:

Theorem 10 (construction Y1) *A linear code $[n, k, d]$ with dual distance d' contains a subcode $[n - d', k - d' + 1, \geq d]$.*

If we apply this to our code $[82, 16, 42]$ the new parameters $[74, 9, 42]$ are obtained.
The duals of the chain $[81, 11, 45] \subset [81, 15, 42] \subset [81, 16, 41]$ form a chain of codes $[81, 65, 8] \subset [81, 66, 7] \subset [81, 70, 6]$. All these parameters are new, the last one is optimal. Application of Theorem 9 with the obvious auxiliary codes gives us the following codes: $[85, 70, 7], [87, 70, 8], [82, 66, 8]$. The last of these parameters has been constructed above, the others are new. We also constructed a lengthening of the code $[81, 70, 6]$ by computer. This code has parameters $[85, 74, 6]$ and is optimal. It has dual distance 46. Application of Theorem 10 yields another construction of a code $[39, 29, 6]$. These parameters had been obtained in section 5 by other means.

7.2 The quaternary case

The RS subfield code $[64, 54, 6]$ has dual distance 32. Application of Theorem 10 yields $[32, 23, 6]$. The code $[67, 11, 33]$ from section 5 has dual distance 6. Its dual therefore has parameters $[67, 56, 6]$. We used a computer program to lengthen this code 14 times, thus obtaining a new code $[81, 70, 6]$. The dual of the chain $[64, 7, 44] \subset [64, 8, 43]$ is a chain $[64, 56, 5] \subset [64, 57, 4]$. Application of Theorem 9 with $[1, 1, 1]$ as auxiliary code yields the new and optimal parameters $[65, 57, 5]$.

8 Conclusion

We have studied Reed-Solomon subfield codes. While the parameters of these codes are at least partly implicit in the existing literature, our method is rather streamlined and paves the way to the construction of extensions and lengthenings of these codes. These are new. Our main interest here is in the construction of codes improving upon the data base of parameters of binary, ternary and quaternary codes ([3], for the binary case see also Brouwer-Verhoeff [5]). It turns out that we are able to improve on the entries of the data base as of november 26, 1994 in well above two percent of the cases.

A Some good codes

A.1 Generator matrix of binary code $[38, 12, 13]$

```
11110010100001111101101001100000000000
00011011100110110011011101010000000000
11010111110110001100000111001000000000
01011001111101001011101010000100000000
00101100111100011101110101000010000000
10110100001111101011010011000001000000
10001001010110000111001110000000100000
00101111011011001011110110000000010000
01111101000100001000110011000000001000
10010001111111011101011001000000000100
01101000100011100110001101000000000010
10101010010110111001111011000000000001
```

A.2 Check matrix of ternary code $[39, 29, 6]$

```
111111111111111111111111111000000000000
000222111111000222222111000000000000000
021210102102021210210102021000000000000
000222111000222111000222111000000000000
000120102021222012012021222100012100101
022112121121100001112010100010001100221
000012021222201210222201210001001120102
000012021210222201201210222000101010212
022100100010121121001112112000011001122
000210201102120222120222102000000111111
```

A.3 Check matrix of ternary code $[39, 26, 7]$

```
100000000000020022220211000122121210100
010000000000002212121220011210200022001
001000000000001011200010221212112011122
000100000000010111122101201102212212122
000010000000002110102121111111112210002
000001000000012112111122221012120122012
000000100000020210001021011101020020022
000000010000000000011111111011001012212
000000001000011000021021210000110101221
000000000100020200112022002000001101010
000000000010000011021102102000000011120
000000000001011221121001011000000000112
000000000000101220010110201000000000001
```

B Proof of Theorem 8

We have to show that our extended array is an orthogonal array of strength 5. Consider a set of 5 columns of our extended array. If they all belong to $\mathcal{A}_0$, then there is nothing to prove. The hardest case is when all but one of the columns belong to $\mathcal{A}_0$. So let x_1, x_2, x_3, x_4 be different elements of F, let $\epsilon_i \in \mathbb{F}_3, i = 1, 2, 3, 4$ and let $\phi = \phi_{\alpha,\beta}$ be one of the ϕ_i. Consider the rows of $\mathcal{A}_0$ having entry ϵ_i in column $x_i, i = 1, 2, 3, 4$. As before this is equivalent with $tr(p(x_i)-p(x_1)) = \epsilon_i-\epsilon_1 (i = 2, 3, 4)$, the corresponding value of z being uniquely determined when this condition is met. Fix elements $u_i \in F, i = 1, 2, 3$ such that $tr(u_i) = \epsilon_i - \epsilon_1$. Write $p(X) = aX^4 + g(X)$, let $h_i \in H = Ker(tr), i = 1, 2, 3$. If $a \in F$ and $h_2, h_3, h_4 \in H$ are given, then the polynomial $g(X)$ of degree ≤ 3 is uniquely determined by Lagrange interpolation. As the constant term is irrelevant in our situation, we may consider the polynomial $g(X)$ of degree ≤ 3 satisfying

$$g(x_1) = -ax_1^4, g(x_i) = u_i + h_i - ax_i^4, i = 2, 3, 4.$$

We have therefore

$$g(X) = -ax_1^4\frac{(X - x_2)(X - x_3)(X - x_4)}{(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)} + \sum_{i=2}^{4}(u_i + h_i - ax_i^4)\frac{\prod_{j\neq i}(X - x_j)}{\prod_{j\neq i}(x_i - x_j)}.$$

The first condition to be met is that the highest coefficient of $g(X)$ has to vanish, hence

$$a \cdot S_1 = \sum_{i=2}^{4}\frac{u_i + h_i}{y_i}.$$

Here $y_i = \prod_{j\neq i}(x_i - x_j), S_1 = \sum_{i=1}^4 x_i^4/y_i$. It is an easy exercise to show that indeed $S_1 = x_1+x_2+x_3+x_4$, thus justifying the notation. The coefficient of $g(X)$ (and of $p(X)$) at X^2 is then

$$b = aS_2 - \sum_{i=2}^{4}(u_i + h_i)\frac{\sum_{j\neq i} x_j}{y_i}.$$

We see that $S_2 = \sum_{i=1}^4 \frac{x_i^4}{y_i} \sum_{j\neq i} x_j = \sum_{i>j} x_i x_j$ is indeed the second elementary symmetric function of the x_i. Consider first the case $S_1 \neq 0$. We see that the rows in question are parametrized precisely by the triples of the $h_i \in H, i = 2, 3, 4$. Our values a and b are then uniquely determined. We have to check that the values $\phi(a, b)$ are uniformly distributed in $\mathbb{F}_3$ when the h_i vary in H. As additive constants do not influence this property we may as well consider the expression

$$tr(\frac{\alpha}{S_1}\sum_{i=2}^{4}\frac{h_i}{y_i} + \beta(\frac{S_2}{S_1}\sum_{i=2}^{4}\frac{h_i}{y_i} - \sum_i(S_1 - x_i)\frac{h_i}{y_i}).$$

As this is linear in the h_i, we only have to check that the expression is not identically zero. We may therefore fix i, put $h_j = 0, j \neq i$. We have to show that the three corresponding linear functions : $H \longrightarrow \mathbb{F}_3$ are not all identically zero. Put

$$z_i = \frac{1}{S_1 y_i}\{\alpha + \beta(S_2 - S_1(S_1 - x_i)\},\ i = 2, 3, 4.$$

The linear function corresponding to i above will be identically zero if and only $z_i \cdot H \subseteq H$. This is equivalent to $z_i \in \mathbb{F}_3$. We therefore have to show that it is impossible that $z_i \in \mathbb{F}_3$ for all $i = 2, 3, 4$.

We assume first that none of the z_i vanishes: consider the case that the z_i are equal and nonzero. Taking differences and using $S_1 \neq 0$ this leads to $\beta = (x_j - x_1)(x_j - x_l) + (x_k - x_1)(x_k - x_l)$ whenever $\{j, k, l\} = \{2, 3, 4\}$. Taking differences again yields $0 = (x_2 - x_1)(x_3 - x_4) + (x_3 - x_4)(x_1 + x_3 + x_4) = (x_3 - x_4)(x_2 + x_3 + x_4)$, hence $x_2 + x_3 + x_4 = 0$. Putting this back into one of the expressions above yields $\beta = -(x_j - x_k)^2 = S_2$ when $j, k \in \{2, 3, 4\}, j \neq k$. If all the $z_i = 1$, then substituting this into z_2 leads to $\alpha = -\beta^2$, contradicting our assumption (with $y = -x$). Let all the $z_i = -1$. Then $\alpha = -\beta^2\{x_1(x_i - x_1) - S_2\}$ for every $i \in \{2, 3, 4\}$. This forces $x_1 = 0$, hence $S_1 = 0$, contradiction.

Let $z_2 = z_3 = 1, z_4 = -1$. Consider the definition of the z_i, take differences. This yields $\beta = (y_2 - y_3)/(x_2 - x_3) = (y_2 + y_4)/(x_2 - x_4)$. Comparing these expressions yields $x_1 + x_4 = x_2 + x_3$, hence $\beta = (x_1 - x_2)(x_1 - x_3), S_1 = -(x_2 + x_3), \alpha = \beta^2 - \beta(x_2 - x_3)^2$. In particular an additive translation of the x_i will not change the values of α or β nor will it change our assumptions. We may therefore assume $x_1 = 0, x_2 = x, x_3 = y, x_4 = x + y$. This leads to a contradiction to our first condition, where x, y are linearly independent over $\mathbb{F}_3$. Case $z_2 = 1, z_3 = z_4 = -1$ leads to the same situation.

So assume without restriction $z_2 = 0$, consequently $\alpha = -\beta S_2 + \beta S_1(S_1 - x_2))$. Clearly then $\beta \neq 0$. This shows that $z_3 z_4 \neq 0$ as otherwise $x_2 = x_3$ or $x_2 = x_4$. Then $z_3 = \pm 1$ is equivalent to $\pm\beta = (x_3 - x_1)(x_3 - x_4)$, analogously for z_4. If $z_3 \neq z_4$, then this yields the contradiction $x_3 = x_4$. Assume $z_3 = z_4 = 1$. Then $\beta = (x_3 - x_1)(x_3 - x_4)$ and $\beta = (x_4 - x_1)(x_4 - x_3)$. Considering the difference of these expressions yields $x_1 + x_3 + x_4 = 0$. Then $\beta = -(x_3 - x_1)^2, S_1 = x_2, S_2 = \beta$. Substituting into the first equation yields $\alpha = -\beta^2$.

Case $z_2 = 0, z_3 = z_4 = -1$ leads in an analogous fashion to $\beta = (x_3 - x_1)^2, \alpha = \beta^2$. We get contradictions to our first condition (cases $y = x$ and $y = -x$, respectively).

So we can assume $S_1 = 0$. It follows that (h_2, h_3, h_4) has to be chosen such that $\sum_{i=2}^{4} \frac{u_i+h_i}{y_i} = 0$. Then $a \in F$ is arbitrary. Let $L = \{(h_2, h_3) \mid (\frac{h_2}{y_2}+\frac{h_3}{y_3})y_4 \in H$. Then (h_2, h_3) varies over a coset of L. As ϕ is linear and additive constants therefore don't influence the property in question, we can instead consider the expression

$$tr(\alpha \cdot a + \beta\{aS_2 + \frac{1}{(x_2 - x_1)(x_2 - x_3)}h_2 + \frac{1}{(x_3 - x_1)(x_3 - x_2)}h_3\}).$$

We have to show that it varies uniformly over $I\!F_3$ when $a \in F$ and $(h_2, h_3) \in L$. Choosing $h_2 = h_3 = 0$ we see that we can assume without restriction $\alpha = -\beta S_2$. Remains to show that $tr(\frac{\beta}{x_3-x_2}\{\frac{h_2}{x_1-x_2} + \frac{h_3}{x_3-x_1}\})$ is not identically zero when $(h_2, h_3) \in L$.

We shall use repeatedly the nondegenerate scalar product $<,>$ given by the trace:

$$< x, y >= tr(x \cdot y)$$

Consider first the case when no partial sum of the $x_i, i = 1, 2, 3, 4$ vanishes. We shall prove that $\frac{h_2}{x_1-x_2}+\frac{h_3}{x_3-x_1}$ takes on every value in F when $(h_2, h_3) \in L$. This forces then the contradiction $\beta = \alpha = 0$. Consider the linear mapping $\Phi : H \times H \longrightarrow F$ given by $\Phi(h_2, h_3) = \frac{h_2}{x_1-x_2} + \frac{h_3}{x_3-x_1}$. Clearly Φ is surjective. We claim that the restriction of Φ to L is still surjective. If not, then we would have $Ker(\Phi) \subset L$. We have to show that this is not the case. So assume the equation $\frac{h_2}{x_1-x_2} + \frac{h_3}{x_3-x_1} = 0$ forces $(\frac{h_2}{y_2} + \frac{h_3}{y_3})y_4 \in H$. By substituting h_3 from the first equation this yields $y_4 h_2(\frac{1}{y_2} - \frac{x_3-x_1}{(x_1-x_2)y_3}) \in H$, equivalently $tr(h_2\frac{x_3}{x_2-x_1}) = 0$. Put $H_0 = H \cap \frac{x_3-x_1}{x_1-x_2}H$. This has codimension 1 in H. Our assumption is equivalent to $\{\frac{x_3-x_1}{x_1-x_2}, \frac{x_3}{x_1-x_2}\} \subset H_0^{\perp}$ (with respect to the scalar product $<,>$), equivalently $\{\frac{x_1}{x_1-x_2}, \frac{x_3}{x_1-x_2}\} \subset H_0^{\perp}$. It is obvious that both elements are nonzero and linearly independent over $I\!F_3$. As $H_0 \subset H$ and $H^{\perp} = I\!F_3$, it follows that the element 1 must be a linear combination of these elements. Each of the corresponding eight cases leads to either one of the x_i or a sum of two of the x_i to vanish, contradiction.

So we can assume without restriction that either $x_1 = x_2 + x_3 + x_4 = 0$ or $x_1 + x_2 = x_3 + x_4 = 0$. Consider first the former case. We have
$y_2 = -x_2(x_2 - x_3)^2, y_3 = -x_3(x_2 - x_3)^2, y_4 = -(y_2 + y_3), S_2 = -(x_2 - x_3)^2$.
Moreover $L = \{(h_2, h_3) \mid h_i \in H, \frac{x_3}{x_2}h_2 + \frac{x_2}{x_3}h_3 \in H\}$.

Put $H_0 = H \cap \frac{x_2}{x_3}H$. Then $h_2 \in H_0$ if and only if $(h_2, 0) \in L$. Our assumption yields then $tr(\frac{\beta}{x_2(x_3-x_2)}h_2) = 0$, or $\{\frac{x_3}{x_2}, \frac{\beta}{x_2(x_3-x_2)}\} \subset H_0^{\perp}$. None of these elements is zero. It follows that either they are linearly dependent or 1 is a linear combination of the two. Each of the corresponding cases leads to a contradiction. As an example, consider the case of equality. This is equivalent to $\beta = x_3(x_3 - x_2)$. Going back to the original assumption we see that this means: if $tr(\frac{x_3}{x_2}h_2 + \frac{x_2}{x_3}h_3) = 0$, then $tr(\frac{x_3}{x_2}h_2) = 0 = tr(\frac{x_2}{x_3}h_3)$. This is impossible for dimensional reasons. As another example consider the case $1 = \frac{x_3}{x_2} + \frac{\beta}{x_2(x_3-x_2)}$. It follows $\beta = -(x_2 - x_3)^2, \alpha = -(x_3 - x_2)^4$. This contradicts our first condition. All the contradictions arise in one of these two ways.

The final case is $x_1 + x_2 = x_3 + x_4 = 0$. Put $x = x_1, y = x_3$. Then $y_2 = x(x+y)(x-y), y_3 = y(x+y)(x-y) = -y_4$ and $S_2 = -(x^2 + y^2)$. We have $L = H_0 \times H$, where $H_0 = H \cap \frac{x}{y}H$. The assumption says that for $h_2 \in H_0, h_3 \in H$ we have $tr(\frac{\beta}{x+y}\{\frac{h_2}{x} + \frac{h_3}{x-y}\}) = 0$. As h_3 varies through H we must have $\frac{\beta}{x^2-y^2} \in I\!F_3$. As certainly $\beta \neq 0$, it follows $\beta = \pm(x^2 - y^2), \alpha = \pm(x^4 - y^4)$. This is excluded by our first condition, with $x + y$ and $x - y$ in the roles of x and y, respectively.

Consider the case that three of our five columns, indexed x_1, x_2, x_3, belong to $\mathcal{A}_0$. Proceeding like in the former case and with analogous notation we see that the highest coefficient a of F is arbitrary and that

$$b = -a\sum_{i=1}^{3}\frac{x_i^4}{y_i} + \sum_{i=2}^{3}(u_i + h_i)/y_i.$$

It is easy to see that $\sum_{i=1}^{3}\frac{x_i^4}{y_i} = S_1^2 - S_2$. Let the remaining two of the set of five columns under consideration be indexed by $\phi_{\alpha,\beta}$ and $\phi_{\alpha',\beta'}$.

Let us first make sure that $\phi_{\alpha,\beta}(a, b)$ is uniformly distributed in $I\!F_3$ when a, h_2, h_3 vary through F, H and H, respectively. As before it suffices to consider the expression

$$tr(a(\alpha - \beta S_1^2 + \beta S_2)) + tr(\beta h_2/y_2) + tr(\beta h_3/y_3).$$

Assume this expression is identically zero. Putting $h_2 = h_3 = 0$ it follows $\alpha = \beta S_1^2 - \beta S_2$. Moreover $\frac{\beta}{y_2}H = \frac{\beta}{y_3}H = H$. This forces $S_1 = x_1 + x_2 + x_3 = 0, S_2 = -(x_1 - x_2)^2 = y_2$ and $\beta = \pm y_2$. We get the usual contradiction.

Assume finally $(\phi_{\alpha,\beta}(a, b), \phi_{\alpha',\beta'}(a, b))$ is not surjective when a varies through

F, and h_2, h_3 through H. It follows that either $\phi_{\alpha,\beta}(a,b) = \phi_{\alpha',\beta'}(a,b)$ for every (a, h_2, h_3) or $\phi_{\alpha,\beta}(a,b) = -\phi_{\alpha',\beta'}(a,b)$ for every (a, h_2, h_3). This is excluded by our second condition.
If finally less than three of our five columns belong to $\mathcal{A}$, then it is clear that (a,b) varies uniformly over $F \times F$. The proof is complete.

References

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

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

[3] 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.

[4] Boukliev, *A method for construction of good linear codes,* manuscript.

[5] A.E. Brouwer,T. Verhoeff: *An updated table of minimum-distance bounds for binary linear codes,* IEEE Trans. Inform. Th. 39 (1993) 662-677.

[6] S.M.Dodunekov, T.Helleseth, N.Manev and O.Ytrehus, *New bounds on binary linear codes of dimension eight,* IEEE Trans. Inform. Th. 33 (1987) 917-919.

[7] B.Groneick and S. Grosse, *New binary codes,* IEEE Trans. Inform. Th. 40 (1994) 510-512.

[8] J.H. van Lint: *Introduction to Coding Theory,* Springer 1982.

[9] F. J. MacWilliams, N. J. A. Sloane: *The Theory of Error-Correcting Codes,* North-Holland, 1977, ^{7}1992.

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