Construction of digital nets from BCH-codes

Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany)
Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

Abstract. We construct four infinite families of digital (t, m, s)-nets based on BCH-codes.

1 Introduction

The needs of quasi-Monte Carlo methods of numerical integration have led Niederreiter [3] to the definition of (t, m, s)-nets. These are finite point sets in the s-dimensional Euclidean unit cube satisfying certain uniformity conditions. It has emerged from the work of Schmid and Lawrence [2, 1] that (t, m, s)-nets are equivalent with certain finite combinatorial structures, which are closely related to **orthogonal arrays**, short OA. We will term these structures **ordered orthogonal arrays** or OOA. In this paper we consider linear OOA. These are OOA, which are vector spaces over an underlying finite field. The corresponding nets are special cases of what has been termed **digital nets.** We will describe a close relationship between linear OOA and linear codes, and formulate the important problem to decide if a given code possesses a **net-embedding.** We then prove some systematic positive results in this direction by constructing certain infinite families of $(t, t + 4, s)$-nets, which are based on binary and ternary BCH-codes.

2 Basic definitions and statement of results

Definition 1 *An* **ordered orthogonal array** *of* **depth** l *with parameters*

$$OOA_\lambda(k, s, l, v)$$

is an array with $v^k\lambda$ rows, sl columns and entries from a v-set, where the columns occur in s ordered **blocks** *$B_j, j=1,2,\ldots,s$ of l each, subject to the following condition:*
Whenever $k=\sum_{j=1}^{s}k_j$, where $k_j\leq l$ for each j, then the set of k columns consisting of the first k_j columns from each block B_j is independent.

Here we call a set of columns **independent** if in the projection onto these columns each tuple of entries occurs the same number of times. This can be interpreted probabilistically as follows: identify the rows of the array with the points of a probability space, with uniform distribution. Interpret each column as a random variable with values in the v-set of entries. Assume each entry occurs with the same frequency in each column. Then a family of columns is independent if and only if the corresponding random variables are statistically independent. An OOA is **linear** if $v=q$ is a prime-power, the set of entries is the field $\mathbb{F}_q$ and the rows form a linear subspace. It is then natural to consider generator matrices of linear OOA. These are matrices whose rows form a basis of the OOA. It is clear that in the linear case independence of columns is equivalent with linear independence of the corresponding columns in the generator matrix. We are led to the following Definition:

Definition 2 *Let q be a prime-power. An $M_q(s,l,m,k)$ is an (m,sl)-matrix with entries in $\mathbb{F}_q$, where the columns are divided into s* **blocks** *$B_j, j=1,2,\ldots,s$ of l columns each, such that the following conditions are satisfied:*
whenever $k=\sum_{j=1}^{s}k_j$, where $k_j\leq l$ for all j, then the set of k columns consisting of the first k_j columns from each B_j is linear independent.

Observe that the columns of each block are linear ordered: there is a first column, a second column, ... This is the reason why the name of ordered OA has been chosen. Denote the sets of columns as considered in this Definition as **qualifying collections.** We call s the **length**, l the **depth**, m the **dimension** and k the **strength**. Denote be $(k_1,k_2,\ldots,k_s)$ the **type** of the qualifying collection in question (terms $k_j=0$ are omitted, the order is immaterial). Values $l>k$ are not interesting as the $(k+1)$-st, $(k+2)-$nd ... columns of each block do not have to satisfy any condition. We will therefore restrict to $l\leq k$. It is clear that the row space of an $M_q(s,l,m,k)$ is a linear $OOA_{q^{m-k}}(k,s,l,q)$. If $l=k$ then a digital $(m-k,m,s)$-net in base q can be constructed. For details we refer to Schmid.
Let $l'<l$. If we use only the l' first rows per block we see that we get an $M_q(s,l',m,k)$ out of an $M_q(s,l,m,k)$. It has been observed by Schmid in a slightly more general context that an $M_q(s,k-1,m,k)$ yields an $M_q(s,k,m,k)$ in various ways: as k-th column of block B_j we may choose the first column of some block $B_{j'}, j'\neq j$.
It is natural to start from depth 1. By definition an $M_q(s,1,m,k)$ is an

$(m, s)-$matrix each k columns of which are linearly independent. Its rowspace is known as a **linear** OA of strength k. Assume $s > m$. Its dual with respect to the usual dot-product is then an $(s-m)$-dimensional code C of length s and minimum distance $> k$. The parameters of such codes are often written in the form $[s, s-m, > k]_q$. Matrix $M_q(s, 1, m, k)$ is known as a **check matrix** of C (an s-tuple belongs to C if and only if its scalar product with each row of the matrix vanishes). We collect this information in the following Lemma:

Lemma 1 *Let $s > m$. If an $M_q(s, l, m, k)$ exists for some $l \geq 1$ then the family of first columns per block is a check matrix of a code $[s, s-m, > k]_q$.*

In particular the bounds on codes imply bounds on $M_q(s, l, m, k)$. We raise the question when this relationship between codes and digital nets can be inverted:

Definition 3 *A q-ary linear code C with parameters $[s, s-m, > k]$ possesses an $(m-k, m, s)$-**net embedding** if there is an $M_q(s, k, m, k)$ whose first columns per block form a check matrix of C.*

In the final section we will describe certain BCH-codes and construct net-embeddings. The results are as follows:

Theorem 1 *The following digital nets exist and can be effectively constructed:*

- $M_2(2^{2r}+1, 4, 4r, 4)$, *thus digital binary* $(4r-4, 4r, 2^{2r}+1)-$*nets* $(r \geq 2)$.
- $M_2(2^r+1, 4, 2r+1, 4)$, *thus digital binary* $(2r-3, 2r+1, 2^r+1)-$*nets* $(r \geq 3)$.
- $M_2(2^r-2, 4, 2r, 4)$, *thus digital binary* $(2r-4, 2r, 2^r-2)$-*nets* (r *odd*, $r \geq 3$).
- $M_3(3^r-1, 4, 2r+1, 4)$, *thus digital ternary* $(2r-3, 2r+1, 3^r-1)-$*nets* $(r \geq 2)$.

3 Constructions from BCH-codes

3.1 The first binary family

We consider the tower of finite fields

$$\mathbb{F}_2 \subset \mathbb{F}_{2^r} \subset \mathbb{F}_{2^{2r}} \subset \mathbb{F}_{2^{4r}} = F, \text{ where } r \geq 2.$$

Put $s = 2^{2r}+1$ and let $W \subset F$ be the multiplicative subgroup of order s. Choose a basis of $F \mid \mathbb{F}_2$, define the binary $(4r, s)-$matrix M whose columns are indexed by the $a \in W$, column a being the $4r$-tuple of coefficients obtained when when a is developed with respect to the basis. We will have opportunity repeatedly to use the fact that $W \cap \mathbb{F}_{2^{2r}} = \{1\}$. This follows simply from $gcd(2^{2r}+1, 2^{2r}-1) = 1$.

Our first observation is that M has rank $4r$. This is equivalent with the statement that the $\mathbb{F}_q$-vector space $< W >$ generated by W is $< W >= F$. In fact, it is obvious that $< W >$ is closed under multiplication, so is a subfield. As $2^{2r}+1$ divides the order of its multiplicative group, we obtain $< W >= F$.

Next we show that any four columns of M are linearly independent. First of all, there is no 0-column and no two columns are identical. Assume three columns have vanishing sum. This amounts to $a = b + c$, where a, b, c are pairwise different elements of W. Raising this equation to the s-th power we get

$$1 = a^s = (b+c)(b+c)^{2^{2r}} = (b+c)(b^{2^{2r}} + c^{2^{2r}}) = (b+c)(\frac{1}{b} + \frac{1}{c}).$$

Here we have used that the mapping $x \longrightarrow x^{2^{2r}}$ is a field-automorphism and that $b^s = c^s = 1$. Multiplying out we get $1 = x + \frac{1}{x}$, where $1 \neq x = b/c \in W$. Equivalently $x^2 + x + 1 = 0$. It follows that $x \in \mathbb{F}_4 \subset \mathbb{F}_2^{2r}$. We obtain the contradiction $1 \neq x \in W \cap \mathbb{F}_{2^{2r}}$.

Assume $a + b + c + d = 0$, where $a, b, c, d \in W$ are pairwise different. Write this in the form $a + b = c + d$, raise to power s as before. We obtain $x + \frac{1}{x} = y + \frac{1}{y}$, where $x = a/b, y = c/d$. Removing the denominator and simplifying we obtain $0 = (x + y)(1 + xy)$. As a field has no divisors of zero we conclude that either $x = y$ or $x = 1/y$. This means in clear that either $ad = bc$ or $ac = bd$. This is our result when we use the partition $\{a, b, c, d\} = \{a, b\} \cup \{c, d\}$. We see that we can assume without restriction $ac = bd$. Use the partition $\{a, b, c, d\} = \{a, c\} \cup \{b, d\}$. Then either $ab = cd$ or $ad = bc$. None of these equations is compatible with the former equation (in the first case we obtain by division $b/c = c/b$, hence $b = c$. In the second case a similar contradiction is obtained).

We have shown that matrix M is an $M_2(s, 1, 4r, 4)$, equivalently the check matrix of a code C with parameters $[s, s-4r, \geq 5]$. In fact, C is a BCH-code and the parameters can also be obtained by invoking results from the theory of cyclic codes (cyclotomic cosets for the dimension, the Roos bound for the minimum distance), but we preferred to give a direct treatment. We proceed to the construction of an $M_2(s, 3, 4r, 4)$ (remember that this is equivalent with an $M_2(s, 4, 4r, 4)$). The blocks are indexed by the $a \in W$. Choose $\alpha \in \mathbb{F}_{2^r} - \mathbb{F}_2, \beta \in \mathbb{F}_{2^{2r}} - \mathbb{F}_{2^r}$. Define block B_a as $B_a = (a, \alpha a, \beta a)$. We have to check that each qualifying collection of 4 columns is linearly independent. Type (1,1,1,1) has been checked already.

- type (2,1,1)

Assume $a, \alpha a, b, c$ are linearly dependent ($a, b, c \in W$, different). Clearly αa must be involved in the relation. It is impossible that $\rho a = b$ for some $\rho \in \mathbb{F}_{2^r}$ as otherwise $\rho = b/a \in \mathbb{F}_{2^r} \cap W = \{1\}$, contradiction. This shows that we must have $\rho a = b + c$, where $\rho = \alpha$ or $\rho = \alpha + 1$. Raising this to power s we obtain $\rho = x + 1/x$, where $1 \neq x = b/c \in W$. Equivalently $x^2 + \rho x + 1 = 0$. This shows that x must be in the quadratic extension $\mathbb{F}_{2^{2r}}$ of $\mathbb{F}_{2^r}$. This leads to our standard contradiction again.

- type (2,2)

Assume $a, \alpha a, b, \alpha b$ are linearly dependent ($a, b \in W, a \neq b$). Because of type (2,1,1) we know that αa and αb must be involved. $\alpha(a + b) = a + b$ is clearly impossible. We can assume $\alpha(a + b) = a$, hence $1/\alpha = 1 + x$, where $x = b/a$. We obtain the usual contradiction.

- type (3,1)

Assume $a, \alpha a, \beta a, b$ are linearly dependent ($a, b \in W, a \neq b$). We get $b = \rho a$ for some $\rho \in \mathbb{F}_{2^{2r}}$, leading to the usual contradiction.

3.2 The second binary family

Consider the finite fields

$$\mathbb{F}_2 \subset \mathbb{F}_{2^r} \subset \mathbb{F}_{2^{2r}} = F, \text{ where } r \geq 2.$$

Put $s = 2^r + 1$ and let $W \subset F$ be the multiplicative subgroup of order s. Choose a basis of $F \mid \mathbb{F}_2$, define the binary $(2r+1, s)-$matrix M such that the column corresponding to $a \in W$ is $(1, a)^t$, where the superscript ^{t} denotes transposition. As in the previous subsection it is clear that $W \cap \mathbb{F}_{2^r} = \{1\}$ and that $< W >= F$, where $< W >$ denotes the linear span. These facts will be freely used in the sequel. We begin by showing that the rows of M are linearly independent, so that M has full rank $2r + 1$. We have seen in the preceding subsection that the last $2r$ rows of M are independent. Remains to show that the first row of M, which is constant $= 1$, is not contained in the linear span of the remaining rows. In order to see this it is handy to interpret the entries of M in a different way: until now the choice of the basis of $F \mid \mathbb{F}_2$ had been irrelevant. Now we choose this basis as $z_i, i = 1, 2, \ldots, 2r$ such that $tr(z_i z_j) = \delta_{ij}$. Here we use the fact that every linear functional : $F \longrightarrow \mathbb{F}_2$ can be written as $x \longrightarrow tr(\alpha x)$ for some $\alpha \in F$. With this choice we can interpret the space generated by columns $2, 3, \ldots, 2r + 1$ as follows: the rows are indexed by $u \in F$, the columns by $a \in W$, with corresponding entry $tr(ua)$. We have to show that there is no $u \in F$ satisfying $tr(ua) = 1$ for all $a \in W$. Assume there is such an element u. It follows $tr(u^2 a^2) = 1$ for all $a \in W$. As W has odd order a^2 varies over all elements of W, consequently $tr((u + u^2)W) = 0$. As W generates F as a vector space and the trace-form is a non-degenerate bilinear form it follows $u + u^2 = 0$, hence $u \in \mathbb{F}_2$. Certainly $u \neq 0$. It follows $u = 1$, thus $tr(a) = 1$ for every $a \in W$. Choosing $a = 1$ we obtain a contradiction.

Next we show that no five columns of M are linearly dependent. As before, there is no 0-column, and no two columns are identical. The presence of the first row shows that the sum of an odd number of columns can never vanish. The remaining case of four columns of M with vanishing sum is led to a contradiction exactly as in the previous subsection. We have shown that matrix M is an $M_2(s, 1, 4r + 1, 5)$, equivalently the check matrix of a code C with parameters $[s, s-4r-1, \geq 6]$. Again C is a BCH-code, but we chose not to invoke the pertinent theory. We proceed to the construction of an $M_2(s, 3, 4r+1, 4)$. Choose some $\alpha \in \mathbb{F}_{2^r} - \mathbb{F}_2$. The choice of α will have to be restricted later. Define block B_a as $B_a = ((1, a)^t, (1, \alpha a)^t, (0, a)^t)$. As before we have to check three types of quadruples of columns:

- type (2,1,1)

Assume $(1, a)^t, (1, \alpha a)^t, (1, b)^t, (1, c)^t$ are linearly dependent ($a, b, c \in W$, different). Certainly $(1, \alpha a)^t$ has to be involved in the linear relation, and the number of summands is 2 or 4. If the number of summands is 2 our standard contradiction is obtained. Assume the sum of all four columns vanishes: $a+\alpha a = b+c$. Raising this to power s we obtain $(1+\alpha)^s = x+\frac{1}{x}$, where $1 \neq x = b/c \in W$. As $(1 + \alpha)^s = (1 + \alpha)(1 + \alpha^{2^r}) = (1 + \alpha)(1 + \alpha) = 1 + \alpha^2$ this simplifies to

$$x^2 + (1 + \alpha^2)x + 1 = 0.$$

This is where we have to restrict the choice of α. In fact, choose $\alpha \in \mathbb{F}_{2^r} - \mathbb{F}_2$ such that $1 + \alpha^2 = \gamma + \frac{1}{\gamma}$ for some $\gamma \in \mathbb{F}_{2^r} - \mathbb{F}_2$. Then the quadratic expression splits and we obtain $(x+\gamma)(x + \frac{1}{\gamma}) = 0$. It follows that $x \in \mathbb{F}_{2^r}$, and the usual contradiction is obtained. Remains to make sure that γ can be chosen as required. The condition that $\alpha \notin \mathbb{F}_2$ is equivalent with $1 + \alpha^2 \notin \mathbb{F}_2$, hence with $\gamma + \frac{1}{\gamma} \notin \mathbb{F}_2$. This expression is certainly nonzero, and $\gamma + \frac{1}{\gamma} = 1$ is equivalent with $\gamma \in \mathbb{F}_4$. It follows that we need to assume $r > 2$.

Type $(2, 2)$ presents no problems whatsoever.

- type (3,1)

Assume that $(1, a)^t$, $(1, \alpha a)^t$, $(0, a)^t$, and $(1, b)^t$ are linearly dependent with $a, b \in W, a \neq b$. As before $(0, a)^t$ has to be involved, and exactly two of the remaining three columns. The only critical case is $a + \alpha a = b$. This leads to $b/a = 1 + \alpha \in W \cap \mathbb{F}_{2^r}$, the usual contradiction.

3.3 The third binary family

Let $r \geq 3$ be an odd integer. Consider the fields

$$\mathbb{F}_2 \subset \mathbb{F}_{2^r} \subset \mathbb{F}_{2^{2r}} = F.$$

Put $w = 2^r + 1$. Observe that F contains $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$. Let $W \subset F$ be the multiplicative subgroup of order w, just as in the preceding subsection. M is the binary $(2r+1, w)$–matrix whose column corresponding to $a \in W$ is $(1, a)^t$, as before. We have shown that M has maximal rank $2r+1$ and that no 5 columns of M are linearly dependent. This means that the BCH-code B which has M as a check matrix has minimum distance ≥ 6. Let us consider the code C which is obtained by truncating this BCH-code in the sense that the coordinate corresponding to $1 \in W$ is omitted. Then C has length $w - 1 = 2^r$, minimum distance ≥ 5 and a check matrix for C is the $(2r, 2^r)$-matrix M' with columns $(a+1)^t$ corresponding to $a \in W - \{1\}$. In fact, let $(\chi_a) \in C$, where $\chi_a \in \mathbb{F}_2, a \in W - \{1\}$. Define $\chi_1 = \sum_{a \neq 1} \chi_a$. Then $(\chi_a)_{a \in W} \in B$ if and only if $0 = \sum_{a \in W} \chi_a a = \sum_{a \neq 1} \chi_a (a+1)$.
So far we have not been able to construct systematically an $M_2(2^r, 4, 2r, 4)$ whose set of first columns per block are the columns of M'. We are convinced that this ought to be possible as computer experiments led to positive results in the first cases $r \in \{3, 5, 7\}$. We proceed by considering matrix M'' obtained by restricting M' to the columns $(a+1)^t$, where $a \in W' = W - \{1, \omega, \omega^2\}$. The block corresponding to $a \in W'$ is defined as $B_a = ((a+1)^t, (\omega(a+1))^t, 1^t)$. We claim that this defines an $M_2(2^r - 2, 4, 2r, 4)$. As before type (1,1,1,1) is all right by definition.

- type (2,1)

Assume $(a+1), \omega(a+1), (b+1)$ are linearly dependent $(a, b \in W', a \neq b)$. As the relation must involve $\omega(a+1)$ and $1 + \omega = \omega^2$ we can assume without restriction $\omega(a+1) = b+1$. Raise this to power w and observe that $w = 2^r + 1$ is a multiple of 3 as r is odd. We obtain $a + 1/a = b + 1/b$, after simplification $(a+b)(a+1/b) = 0$. As $a \neq b$ we obtain $a = 1/b$. The original equation now reads $\omega(a+1) = 1/a + 1 = (a+1)/a$. As $a \neq 1$ we obtain $a = 1/\omega \in \mathbb{F}_4$, a contradiction.

- type (2,2)

Assume $a+1, \omega(a+1), b+1, \omega(b+1)$ are linearly dependent. Case (2,1) shows that $\omega(a+1)$ and $\omega(b+1)$ must be involved in the relation. If the sum of all four terms vanishes, then clearly $a = b$, a contradiction. The only remaining case is without restriction $\omega(a+1) = \omega^2(b+1)$. After division by ω we are back to the case of type (2,1).

- type (2,1,1)

Assume $a+1, \omega(a+1), b+1, c+1$ are linearly dependent. We know that $b+1$ and $c+1$ must be involved in the relation. If $\omega(a+1)$ was not involved this would contradict the fact that M' has strength 4. We have without restriction $\omega(a+1) = b + c$. Raising this to power w we obtain $a + 1/a = b/c + c/b$. As all four summand are elements of W we conclude that we have without restriction $a = b/c$. The original relation now reads $\omega(a+1) = b + c = c(a+1)$, leading to the contradiction $c = \omega$.

- type (3,1)

Assume $a+1, \omega(a+1), 1, b+1$ are linearly dependent. We know that 1 is involved in the relation. If $b+1$ was not involved we would obtain the contradiction $a \in \mathbb{F}_4$. Assume $b = a+1$. Raising to power w be obtain $1 = a + 1/a$, whence the contradiction $a \in \mathbb{F}_4$. It follows that the relation is without restriction $b = \omega(a+1)$. Raising to power w again we get the same contradiction $a \in \mathbb{F}_4$.

3.4 The ternary family

Let $F = \mathbb{F}_{3^r}, s = 3^r - 1$. Define a ternary $(2r+1, 3^r-1)$-matrix M, whose columns are indexed by the nonzero elements $a \in F$. Define this column as $u_a = (1, a, a^2)^t$. In this case we do not find it rewarding to circumvent the theory of BCH-codes. Matrix M is in fact a check matrix of a ternary primitive BCH-code with dimension $s-(2r+1)$ and minimum distance ≥ 5. In particular the rows of M are independent and any four columns of M are independent. We proceed to the construction of an $M_3(s, 3, 2r+1, 4)$: choose u_a as first column in block B_a. The second column is $v_a = (0, \nu a, (\nu a)^2)^t$, the third column is $w_a = (0, 0, (\nu a)^2)^t$. We know that it suffices to check types $(2,1,1), (2,2)$ and $(3,1)$ to prove our claim. The crucial point is the choice of the element $\nu \in F$. We will assume that ν satisfies the following conditions:

$$\nu \in F - \mathbb{F}_9, \nu \text{ nonsquare}, \nu - 1 \text{ square}.$$

Lemma 2 *Columns u_a, u_b, where a, b are different nonzero elements of F, are always independent of any column $c = (0, \gamma, \gamma^2)$, where $\gamma \neq 0$.*

Proof: Assume there is a nontrivial linear combination of these columns. Observe that all our linear combinations are over $\mathbb{F}_3$. We can assume that the coefficient of c is $= 1$. By changing the roles of a, b, if necessary, we get the equations $\gamma = a - b, \gamma^2 = a^2 - b^2$. As $\gamma^2 = a^2 + b^2 + ab$, we get $ab = b^2$, from which the contradiction $a = b$ is derived. ∎

- type $(2,1,1)$

Assume $v_a = xu_a + yu_b + zu_c$ with coefficients $x, y, z \in \mathbb{F}_3$. The Lemma shows that no coefficient vanishes. The first coordinate shows that $x + y + z = 0$. It follows that they must be equal, either $= 1$ or $= -1$. In the first case the remaining coordinates yield the equations $(\nu - 1)a = b + c, (\nu^2 - 1)a^2 = b^2 + c^2$. Adding the square of the first equation to the second yields after simplification $\nu(\nu-1)a^2 = (b+c)^2$. This contradicts our assumption that $\nu(\nu - 1)$ is a nonsquare.
So assume $x = y = z = -1$. We get the equations $(\nu + 1)a = -b - c, (\nu^2 + 1)a^2 = -b^2 - c^2$. An analogous procedure yields after subtraction

Table 1: An $M_3(8,3,5,4)$

100	022	011	021	011	122	211	011
021	100	001	001	011	121	111	221
011	021	100	010	020	110	010	200
010	010	020	100	010	010	110	110
000	000	010	010	100	110	100	100

and simplification $\nu a^2 = (b-c)^2$. This contradicts the assumption that ν is a nonsquare.

- type $(2,2)$

Assume we have a nontrivial linear combination $wu_a + xv_a = yu_b + zv_b$ for some $a \neq b$. Observe at first that v_a and v_b are not linearly dependent. In fact, they are not equal as otherwise $a = b$, nor are they negatives of each other, or $(\nu a)^2 = -(\nu a)^2$, contradiction. It follows that w, y cannot both vanish. The first coordinate shows $w = y$. We can assume $w = y = 1$. The Lemma shows that $xz \neq 0$. If $x = z = 1$, then the second coordinate shows $(\nu+1)a = (\nu+1)b$, hence $a = b$. The same contradiction is derived when $x = z = -1$. It follows that we can assume $x = 1, z = -1$. We obtain the equations $(\nu+1)a = (1-\nu)b$ and $(\nu^2+1)a^2 = (1-\nu^2)b^2$. Subtracting the square of the first equation from the second we get after simplification $\nu - 1 = a^2/b^2$. Use this in the first equation, substituting for $(1-\nu)$. We get $\nu + 1 = -a/b$. It follows $(\nu+1)^2 = \nu - 1$. This yields $\nu^2 + \nu - 1 = 0$. We see that $\nu \in \mathbb{F}_9$, contradiction.■

- Type $(3,1)$

Assume $wu_b = xu_a + yv_a + zw_a$. As the columns belonging to one block are independent, we may assume $w = 1$. The first coordinate shows $x = 1$. The second coordinate shows $y \neq 0$ as otherwise $a = b$. The Lemma shows $z \neq 0$. Assume $y + z = 0$. The last coordinate shows $b^2 = a^2$, hence $b = -a$. The second coordinate yields the contradiction $\nu \in \mathbb{F}_3$. Two cases are left: if $y = z = -1$, then $b = a(1-\nu), b^2 = a^2(1+\nu^2) = a^2(\nu^2+\nu+1)$. It follows $\nu = 0$. If finally $y = z = 1$, then the same procedure yields $\nu \in \mathbb{F}_3$ again.■

In case $r = 2$ we constructed a ternary net $(1,5,8)$ by computer. An $M_3(8,3,5,4)$ is given in Table 1.

If $r > 2$ we have to prove that F contains an element satisfying our requirements. The Theorem will be proved once the following Lemma is established:

Lemma 3 *For every $r > 2$ the field $F = \mathbb{F}_{3^r}$ contains an element ν such that ν generates the field F over $\mathbb{F}_3, \nu$ is a nonsquare and $\nu - 1$ is a square.*

Proof: Let ϵ be a generator of the multiplicative group of F. In particular ϵ is a nonsquare. If $\epsilon - 1$ is a square we can use $\nu = \epsilon$ and are done. So assume $\epsilon - 1$ is a nonsquare. It follows that the quotient $1 - 1/\epsilon$ is a square. We distinguish the case when r is even (-1 is a square) and when r is odd (equivalently -1 is a nonsquare). When r is even we have that $1/\epsilon - 1$ is a square. Put $\nu = 1/\epsilon$. Assume now r is odd. As $\epsilon - 1$ is a nonsquare we can repeat the argument above and assume that $\epsilon + 1$ is a nonsquare. It follows that $1 - 1/\epsilon$ and $1 + 1/\epsilon$ are squares, so that $1/\epsilon - 1$ is a nonsquare. Put $\nu = 1/\epsilon - 1$. ∎

References

[1] K.M.Lawrence, *A combinatorial characterization of (t, m, s)-nets in base b,* J. Comb. Designs **4** (1996),275-293.

[2] G.L.Mullen and W.C.Schmid, *An equivalence between (t, m, s)-nets and strongly orthogonal hypercubes,* Journal of Combinatorial Theory A **76** (1996), 164-174.

[3] H.Niederreiter, *Point sets and sequences with small discrepancy,* Monatshefte Mathematik **104** (1987),273-337.