Families of ternary (t, m, s)-nets related to 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

A link between the theory of error-correcting codes and (t, m, s)-nets leads to the efficient construction of two families of very good ternary nets. These have parameters $(4r-4, 4r, (3^{2r}+1)/2$ (for all $r \geq 2$) and $(2r-4, 2r, (3^r-1)/2)$ (for all odd $r \geq 3$). The underlying codes are cyclic codes.

1 Introduction

$(t, m, s)-$nets were defined by Niederreiter [5] in the context of quasi-Monte Carlo methods of numerical integration. Niederreiter pointed out close connections to certain combinatorial and algebraic structures. In the work of Lawrence, Mullen and Schmid [2, 4, 7] an equivalence is established between $(t, m, s)-$nets and a class of finite combinatorial structures, which contain orthogonal arrays as a subclass. For a recent survey see [6].

A systematic relationship with the theory of error-correcting codes was exhibited in [1], where we used the theory of $BCH-$codes to construct three infinite binary families and one ternary family of $(t, m, s)-$nets. In the present paper two more ternary families are constructed. For basic definitions concerning (digital) $(t, m, s)-$nets, orthogonal arrays and ordered orthogonal arrays we refer to [1] and its bibliography. A standard reference on coding theory is [3]. Our main result is the following:

Theorem 1 *Ternary digital nets with the following parameters exist and can be effectively constructed:*

1. $(4r - 4, 4r, (3^{2r} + 1)/2)-$*nets* $(r \geq 2)$.
2. $(2r - 4, 2r, (3^r - 1)/2)-$*nets* $(r$ *odd,* $r \geq 3)$.

The first family uses ternary BCH-codes with parameters $[(3^{2r}+1)/2, (3^{2r}+1)/2-4r, 5]$ for $r \geq 2$. The second family uses BCH-codes $[(3^r - 1)/2, (3^r - 1)/2 - 2r, 5]$, for odd r, which are not only non-primitive but also non-narrow sense. The smallest net parameters we obtain are

$$(2, 6, 13)_3, (4, 8, 41)_3, (6, 10, 121)_3, (8, 12, 365)_3.$$

In the next section we list basic facts and definitions. The constructions are in the final section.

2 Basic definitions

Definition 1 *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 $l \leq k$ columns each, such that the following hold:*
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 linearly independent.

Observe that the columns of each block are linearly ordered: there is a first column, a second column, ... Denote the sets of columns as considered in Definition 1 as **qualifying collections.** We call s the **length**, l the **depth**, m the **dimension** and k the **strength**. Denote by $(k_1, k_2, \ldots, k_s)$ the **type** of the qualifying collection in question (terms $k_j = 0$ are omitted, the order of the k_j is immaterial). Let an $M_q(s,l,m,k)$ be given. The collection of first columns per block forms an $M_q(s,1,m,k)$, and an $M_q(s,1,m,k)$ is an $(m,s)-$matrix each k columns of which are linearly independent. If $s>m$, then an $M_q(s,1,m,k)$ is a check-matrix of a linear code $[s,s-m,k+1]_q$. Finally we record the basic equivalence between nets and ordered orthogonal arrays in the linear case as follows:

Theorem 2 *The following are equivalent:*

- $M_q(s,k-1,m,k)$
- *A digital net, defined over* $\mathbb{F}_q$*, with parameters* $(m-k,m,s)_q$.

3 The constructions

3.1 The first family

Let $r\geq 2$. We have to construct $M_3((3^{2r}+1)/2,3,4r,4)$. The first columns per block form a linear orthogonal array. We start by constructing this orthogonal array, which is then a check matrix of a ternary code
$[(3^{2r}+1)/2,(3^{2r}+1)/2-4r,5]$: Consider the tower of finite fields

$$\mathbb{F}_3\subset\mathbb{F}_{3^r}\subset\mathbb{F}_{3^{2r}}\subset\mathbb{F}_{3^{4r}}=F.$$

Let $s=(3^{2r}+1)/2$ and $W\subset F$ the multiplicative subgroup of order s. Choose a basis of $F\mid\mathbb{F}_3$, define the ternary $(4r,s)-$matrix M whose columns are indexed by the $a\in W$, column a being the $4r$-tuple of coefficients obtained when a is expanded with respect to the basis. In our notation we will make no distinction between $a\in W$ and the column indexed by a.

Lemma 1 *We have* $W\cap\mathbb{F}_{3^{2r}}=\{1\}$.

Lemma 1 follows from the fact that $gcd(s,3^{2r}-1)=1$. We will make repeated use of it. Our first observation is that M has rank $4r$. This is equivalent with the statement that the $\mathbb{F}_3$-vector space generated by W is $\langle W\rangle=F$. In fact, it is obvious that $\langle W\rangle$ is closed under multiplication, so is a subfield. As $(3^{2r}+1)/2$ divides the order of its multiplicative group, we obtain $\langle W\rangle=F$. In order to see that any four columns of M are linearly

independent we may invoke the theory of cyclic codes. In fact M is a check matrix of a narrow-sense BCH-code. The cyclotomic coset of 1 contains $\{-3,-1,1,3\}$. This follows from the fact that $1\cdot 3^{2r}\equiv -1 \pmod{s}$. As this is an arithmetic progression of four numbers and the step length 2 is coprime to s, we conclude from the BCH-bound that M has indeed strength 4.
We proceed to the construction of the $M_3((3^{2r}+1)/2,3,4r,4)$. The blocks are indexed by the $a\in W$. Choose $\alpha\in \mathbb{F}_{3^r}\setminus \mathbb{F}_3, \beta\in \mathbb{F}_{3^{2r}}\setminus \mathbb{F}_{3^r}$. 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 $\rho\in \mathbb{F}_{3^r}\setminus \mathbb{F}_3$ as otherwise $\rho=b/a\in \mathbb{F}_{3^r}\cap W=\{1\}$, contradicting Lemma 1. This shows that we must have

$$\rho a=\gamma b+\delta c,$$

where $\rho\in \mathbb{F}_{3^r}\setminus \mathbb{F}_3$ and γ,δ are nonzero elements in $\mathbb{F}_3$. Raise this equation to the power $2s=3^{2r}+1$. Observe that raising to power 3^{2r} is a field automorphism. We obtain

$$\rho^2=(\gamma/b+\delta/c)(\gamma b+\delta c)=\gamma^2+\delta^2+\gamma\delta(x+1/x),$$

where $1\neq x=b/c\in W$. This shows that x must be in the quadratic extension $\mathbb{F}_{3^{2r}}$ of $\mathbb{F}_{3^r}$. We obtain our standard contradiction to Lemma 1.

- 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. It follows that the linear relation can be written as follows: $\alpha(a+\lambda b)=\gamma a+\delta b$, where $\lambda=\pm 1$. Raising this to power $2s$ again we obtain $\alpha^2(1/a+\lambda/b)(a+\lambda b)=(\gamma/a+\delta/b)(\gamma a+\delta b)$. After simplification and using $x=a/b$ this yields

$$\alpha^2(1+\lambda^2+\lambda x+\lambda/x)=\gamma^2+\delta^2+\gamma\delta(x+1/x).$$

This yields a quadratic equation for x with leading coefficient $\alpha^2\lambda-\gamma\delta$. If this coefficient does not vanish, we obtain that $x\in \mathbb{F}_{3^{2r}}$. As $1\neq x\in W$

the usual contradiction results. Assume the leading coefficient vanishes. We must have $\alpha^2 = -1, \lambda = -\gamma\delta$. In particular $\lambda^2 = \delta^2 = \gamma^2 = 1$. The basic equation simplifies to $1 = -1$, 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 $\rho \in \mathbb{F}_{3^{2r}}$, leading to the same contradiction as before.

3.2 The second family

Let $r > 1$ be odd. We have to construct $M_3((3^r - 1)/2, 3, 2r, 4)$. Consider the field $F = \mathbb{F}_{3^r}$ and its subgroup W of order $s = (3^r - 1)/2$. Observe that s is odd. Put $u = (s-1)/2 = (3^r - 3)/4$. Consider the cyclotomic coset $Z(u)$ containing u. We have $3u = (3s-3)/2 \equiv (s-3)/2 \equiv u - 1 \pmod{s}$. By induction we obtain

$$Z(u) = \{u\} \cup \{u - \frac{3^i - 1}{2} | i = 1, \ldots, r-1\}.$$

In particular $|Z(u)| = r$ and $-u \notin Z(u)$. As $-u = u + 1$ we see that $Z(u) \cup Z(-u)$ contains $\{u-1, u, u+1, u+2\}$. It follows that the dual of the BCH-code defined by these exponents has dimension $4r$ and strength 4. A check matrix of this BCH-code may therefore be described as a ternary $(2r, s)$-matrix, where the column indexed by a is (a^u, a^{-u}). We have $a^{2u} = 1/a$. The column indexed by a^2 is therefore $(1/a, a)$. As s is odd the mapping $a \mapsto a^2$ is an automorphism of the cyclic group W. This shows that we can change the indexing and arrive at a check matrix as follows: Define the ternary $(2r, s)-$matrix M whose columns are indexed by the $a \in W$, and where column a is $(a, 1/a)$ (the first r entries form the representation of a when expressed with respect to the basis, the second r entries represent $1/a$). Then M is a check matrix of a ternary code of dimension $s - 2r$ and minimum distance 5. We proceed to the construction of an $M_3((3^r - 1)/2, 3, 2r, 4)$. Choose an element $\rho \in F \setminus \mathbb{F}_3$. Then block B_a is defined as $B_a = \{(a, 1/a), (-a, 1/a), (0, \rho/a)\}$. We have to check that each qualifying collection of 4 columns is linearly independent. Type (1,1,1,1) has been dealt with already.

- type (2,1,1)

Assume $\alpha(a,1/a)+\beta(-a,1/a)+\gamma(b,1/b)+\delta(c,1/c)=0$, where $\alpha,\beta,\gamma,\delta\in\mathbb{F}_3$ and a,b,c are different elements in W. We can assume $\beta=1$. If $\alpha=1$, then the first component shows $\gamma=\delta=0$, the second component yields a contradiction. If $\alpha=-1$, then an analogous process yields a contradiction. We have $\alpha=0$, hence

$$\begin{aligned} a &= \gamma b+\delta c \\ -1/a &= \gamma/b+\delta/c \end{aligned}$$

We observe that $\gamma\delta\neq 0$ as otherwise the first equation contradicts the fact that $W\cap\mathbb{F}_3=\{1\}$. Simplify the second equation, take the reciprocal. This yields $a=-bc/(\gamma c+\delta b)$. Comparison with the first equation yields $(\gamma c+\delta b)(\gamma b+\delta c)=-bc$. The left-hand side is $(\gamma^2+\delta^2)bc+\gamma\delta(b^2+c^2)$. As $\gamma^2=\delta^2=1$ this simplifies the equation to $\gamma\delta(b^2+c^2)=0$. It follows $b^2=-c^2$, which shows $-1\in W$, contradiction.

- type (2,2)

Assume $\alpha(a,1/a)+\beta(-a,1/a)+\gamma(b,1/b)+\delta(-b,1/b)=0$, where $\alpha,\beta,\gamma,\delta\in\mathbb{F}_3$ and a,b are different elements of W. The first coordinate shows $\alpha=\beta,\gamma=\delta$. The second coordinate yields a contradiction.

- type (3,1)

Assume $\alpha(a,1/a)+\beta(-a,1/a)+\gamma(0,\rho/a)+\delta(b,1/b)=0$, with notation as before. The first coordinate shows $\alpha=\beta,\delta=0$. The second coordinate yields $-\alpha/a+\gamma\rho/a=0$, equivalently $\gamma\rho=\alpha$. If $\gamma=0$, then all coefficients vanish, contradiction. If $\gamma\neq 0$, then $\rho\in\mathbb{F}_3$, a final contradiction.

References

[1] Y.Edel and J.Bierbrauer: *Construction of digital nets from BCH-codes, Monte Carlo and Quasi-Monte Carlo Methods 1996, Lecture Notes in Statistics* **127**(1997),221-231.

[2] K. M. Lawrence: *A combinatorial characterization of* (t,m,s)*-nets in base* b*, Journal of Combinatorial Designs* **4** (1996),275-293.

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

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

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

[6] H.Niederreiter: *Constructions of* (t, m, s)*-nets,*
Monte Carlo and quasi-Monte Carlo methods 1998 (H.Niederreiter and *J.Spainier,eds),* pp. 70-85, Springer Berlin 2000.

[7] W.C.Schmid: (T, M, S)*-nets: digital construction and combinatorial aspects,* PhD dissertation, Salzburg (Austria), 1995.