A family of binary (t, m, s)-nets of strength 5

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)

September 11, 2003

Abstract

$(t, m, s)-$nets were defined by Niederreiter [6], based on earlier work by Sobol [7], in the context of quasi-Monte Carlo methods of numerical integration. Formulated in combinatorial/coding theoretic terms a binary linear $(m-k, m, s)_2$-net is a family of ks vectors in $\mathbb{F}_2^m$ satisfying certain linear independence conditions (s is the **length,** m the **dimension** and k the **strength**: certain subsets of k vectors must be linearly independent). Helleseth-Kløve-Levenshtein [5] recently constructed $(2r-3, 2r+2, 2^r-1)_2$-nets for every r. In this paper we give a direct and elementary construction for $(2r-3, 2r+2, 2^r+1)_2$-nets based on a family of binary linear codes of minimum distance 6.

1 Introduction

Definition 1. *Let s, m, k be natural numbers and $X_i(w) \in \mathbb{F}_2^m$ for $w = 1, 2, \ldots, s,\ i = 1, 2, \ldots, k$. The $X_i(w)$ define a (binary) linear $(m-k, m, s)_2$-net if the following independence condition is satisfied:*
any subset F of k of the $X_i(w)$ is linearly independent provided $X_i(w) \in F$ implies $X_{i-1}(w) \in F$ for all w and $i > 1$.

This notion can be generalized so as to allow also non-linear nets and nets defined over arbitrary finite alphabets. The main application comes from the fact that a binary linear net as in Definition 1 can be used to define a set of 2^m points in the unit cube in Euclidean s-space with extremal uniformity properties, for use in numerical integration. We will work with Definition 1 exclusively. tms-nets are known under various names. They are special cases of ordered orthogonal arrays (for an introduction see [4]) and they are **hypercubic designs** (see [5]).

We will work with Definition 1 exclusively. The $X_i(w)$ for fixed w are said to form the elements of **block** $B(w)$. The **length** of a net is s, the **dimension** is m, the **strength** is k. The parameter $m-k$ is often denoted by the letter t.

Definition 1 implies that any k of the vectors $X_1(w)$ are linearly independent, in other words the $X_1(w)$ form the columns of a check matrix of a linear code $[s, s-m, k+1]_2$ (length s, codimension m, minimum distance larger than k). It is therefore natural to start from such a check matrix, use its columns as the first elements of the blocks and try to construct the remaining elements $X_2(w), \dots, X_k(w)$ such that a net is obtained. This is the problem of **net embeddability** of a linear code. A sufficient condition is the Gilbert-Varshamov bound, see [4]. Helleseth-Kløve-Levenshtein [5] constructed $(2r-3, 2r+2, 2^r-1)_2$-nets using a variant of net embedding of primitive BCH-codes. In this paper we give a direct and elementary construction for a family with slightly better parameters:

Theorem 1. *There is a linear* $(2r-3, 2r+2, 2^r+1)_2$*-net for every* $r > 1$.

The construction is explicit, based on a non-primitive BCH-code $[2^r+1, 2^r-2r, 6]_2$. It is similar to earlier constructions in [2, 3]. Theorem 1 is one of the results announced in [4]. In the next section we give the construction and proof.

2 Construction of the net

For arbitrary $r > 1$ consider the tower of finite fields

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

Let $q = 2^r$. The length is $s = 2^r + 1$. Let $W \subset F$ be the multiplicative subgroup of order s. As $gcd(2^r+1, 2^r-1) = 1$ we have $W \cap L = \{1\}$. Let the blocks be indexed by the elements $w \in W$.

Consider the BCH-code $\mathcal{C}$ with $A = \{0, 1\}$ as defining set. For information on cyclic codes consult for example [1]. As the Galois closure of A contains the interval $\{-2, -1, 0, 1, 2\}$ it follows from the theory of cyclic codes that $\mathcal{C}$ has minimum distance ≥ 6, equivalently that its dual has strength ≥ 5. This means that the family of vectors $(w, 1) \in \mathbb{F}_2^{2r+1}$ have the property that any 5 of them are linearly independent. Here w can be seen either as an element of $W \subset F$ or as an element of $\mathbb{F}_2^{2r}$, when expanded with respect to a basis of F over $\mathbb{F}_2$. We can use $(w, 1)$ as first element of a block and try to complete the net embedding. While we have not been able to construct such an embedding we do obtain a net embedding after introducing an additional coordinate.

Definition 2. *Let $w \in W$. Choose $\alpha \in L \setminus \mathbb{F}_2$ such that $\alpha^2 + 1$ is not of the form $w' + 1/w'$ for $w' \in W$. The block $X(w)$ is defined as follows:*

$$X_1(w) = (w, 1, 0),\ X_2(w) = (\alpha w, 0, 1),\ X_3(w) = (\mathbf{0}, 1, 1),\ X_4(w) = (\mathbf{0}, 0, 1)$$

and $X_5(w) = X_1(w')$ for some $w' \neq w$.

By Definition 1 we have to prove that any family F of 5 of the vectors $X_i(w) \in \mathbb{F}_2^{2r+2}$ is linearly independent provided F consists of the first n_1 vectors from some block, the first n_2 vectors from some other block and so forth, where $n_1 + n_2 + \cdots = 5$. Order the n_i such that $n_1 \geq n_2 \geq \ldots$ and call $(n_1, n_2, \ldots)$ the **type** of family F. The possible types are

$$(1,1,1,1,1),\ (2,1,1,1),\ (2,2,1),\ (3,1,1),\ (3,2),\ (4,1),\ (5).$$

As we chose the BCH-code as point of departure, type $(1,1,1,1,1)$ is independent. The last coordinate shows that type (2,1,1,1) is independent as well. Also, by the choice of $X_5(w)$, type (5) reduces to type $(4,1)$. It suffices to prove that families of types $(2,2,1)$ through $(4,1)$ are independent.

- Type $(2, 2, 1)$

Assume there is a linear combination of

$$(\alpha w_1, 0, 1), (\alpha w_2, 0, 1), (w_1, 1, 0), (w_2, 1, 0), (w_3, 1, 0)$$

with coefficients $\lambda_1, \ldots, \lambda_5$. As type $(2,1,1,1)$ has been considered already we can assume $\lambda_1 = \lambda_2 = 1$. The middle coordinate shows $\lambda_3 + \lambda_4 + \lambda_5 = 0$. Assume at first $\lambda_5 = 0$. Clearly $\lambda_3 = \lambda_4 = 1$. The first coordinate section yields the contradiction $w_1 = w_2$. We can therefore assume $\lambda_3 = \lambda_5 = 1, \lambda_4 = 0$. The equation is

$$(\alpha + 1)w_1 + \alpha w_2 + w_3 = 0.$$

Multiplication by w_1^{-1} shows that we can assume $w_1 = 1$. We have $\alpha + 1 = \alpha w_2 + w_3$. Raising to power q yields $\alpha + 1 = \alpha/w_2 + 1/w_3$, after multiplication $\alpha^2 + 1 = \alpha^2 + 1 + \alpha(w_2/w_3 + w_3/w_2)$. Let $x = w_2/w_3$. Then $1 \neq x \in W$ and $x + 1/x = 0$. This yields the contradiction $x^2 = 1$, hence $x = 1$.

- Type $(3, 2)$

The first coordinate section shows that there is no non-trivial linear combination of

$$(\mathbf{0}, 1, 1),\ (\alpha w_1, 0, 1),\ (\alpha w_2, 0, 1),\ (w_1, 1, 0),\ (w_2, 1, 0).$$

- Type $(3, 1, 1)$

Consider a linear combination of

$$(\mathbf{0}, 1, 1),\ (\alpha w_1, 0, 1),\ (w_1, 1, 0),\ (w_2, 1, 0),\ (w_3, 1, 0).$$

Clearly $\lambda_1 = 1$. The last coordinate shows $\lambda_2 = 1$. The first coordinate section shows $\lambda_4 = \lambda_5 = 1$. The middle coordinate yields $\lambda_3 = 1$. We have $(\alpha + 1)w_1 = w_2 + w_3$. As before we can assume $w_1 = 1$. Raising to power $q + 1$ we obtain $(\alpha + 1)^2 = w_2/w_3 + w_3/w_2$. Let $x = w_2/w_3$. By choice of α a contradiction is reached.

Type $(4, 1)$ is easy to check.

In order to complete the proof it remains to show that α can be chosen as required in Definition 2. Let r be odd. The function $T : W \rightarrow L$ defined by $T(x) = x + 1/x$ is the restriction of the trace $T : F \rightarrow L$ to W. We have $T(w) = 0$ if and only if $w = 1$. Moreover $T(w) = T(1/w)$. It follows that precisely 2^{r-1} nonzero elements of L have the form $T(w)$ for some $w \in W$. This shows that α can be chosen in the required way. The proof of Theorem 1 is complete.

References

[1] J.Bierbrauer: *The theory of cyclic codes and a generalization to additive codes, Designs, Codes and Cryptography* **25** (2001), 189-206.

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

[3] Y. Edel and J. Bierbrauer: *Families of ternary (t, m, s)-nets related to BCH-codes, Monatsh. Math.* **132** (2001), 99–103.

[4] J.Bierbrauer, Y.Edel and W.Ch.Schmid: *Coding-Theoretic constructions for tms-nets and ordered orthogonal arrays, Journal of Combinatorial Designs* **10** (2002), 403-418.

[5] T.Helleseth, T. Kløve and V. Levenshtein: *Hypercubic* 4*-and* 5*-designs from double-error-correcting BCH codes, Designs, Codes and Cryptography* **28** (2003), 265-282.

[6] H. Niederreiter: *Point sets and sequences with small discrepancy, Monatsh. Math.* **104** (1987), 273–337.

[7] I.M. Sobol: *Distribution of points in a cube and the approximate evaluation of integrals* (in Russian), *Zh. Vychisl.Mat. i Mat. Fiz* **7** (1967), 784-802.
English Translation in *USSR Comput. Math. Math. Phys* **7** (1967), 86-112.