Affine 3-Nonsystematic Codes

S. A. Malyugin¹,²*

¹Sobolev Institute of Mathematics, pr. Akad. Koptyuga 4, Novosibirsk, 630090 Russia
²Novosibirsk State University, ul. Pirogova 2, Novosibirsk, 630090 Russia

Received December 23, 2013; in final form, January 17, 2014

Abstract—A perfect binary code \( C \) of length \( n = 2^k - 1 \) is called affine 3-systematic if in \( \{0, 1\}^n \) there exists a 3-dimensional subspace \( L \) such that the intersection of its every coset \( L + u \) with \( C \) is either empty or a singleton. Otherwise, \( C \) is called affine 3-nonsystematic. In this article we construct affine 3-nonsystematic codes of length \( n = 2^k - 1 \) for \( k > 4 \).

DOI: 10.1134/S1990478914040127

Keywords: perfect code, Hamming code, nonsystematic code, affine nonsystematic code, affine 3-nonsystematic code, component

INTRODUCTION

Let \( \{0, 1\}^n \) stand for the vector space over the field with the two elements 0 and 1. By definition, this space consists of all sequences \( u = (u_1, \ldots, u_n) \), where \( u_i \in \{0, 1\} \). The sum of two vectors \( u, v \in \{0, 1\}^n \) is defined as \( u + v = (u_1 \oplus v_1, \ldots, u_n \oplus v_n) \), where \( u = (u_1, \ldots, u_n) \), \( v = (v_1, \ldots, v_n) \), and \( u_i \oplus v_i \) is the sum of elements \( u_i, v_i \in \{0, 1\} \) in the Galois field \( GF(2) \). Further, we always consider the standard basis \( e_1, \ldots, e_n \) for \( \{0, 1\}^n \), where \( e_i = (0, \ldots, 1, \ldots, n) \).

The zero vector and all-one vector are denoted by 0 and 1. The number of nonzero entries of a vector \( u \) is called the weight of \( u \). The support of \( u \in \{0, 1\}^n \) is denoted by \([u]\) (i.e., the set of indices \( i \) such that \( u_i = 1 \)).

Consider in the Hamming code \( H^n \) the subspace \( R_i \) generated by all vectors of weight 3 with the \( i \)-th entry equal to 1. All possible cosets \( R_i^u = R_i + u \), where \( u \in H^n \), are called \( i \)-components of \( H^n \) for \( i = 1, \ldots, n \). Consider some family

\[ \mathcal{B} = \{R_{i_1}^{u_1}, \ldots, R_{i_m}^{u_m}\} \]

of pairwise disjoint \( i_p \)-entries, where \( u_p \in H^n, p = 1, \ldots, m \). One of the main constructions of nonlinear perfect binary codes is as follows: We translate in \( H^n \) by \( i_p \), all components of \( \mathcal{B} \); i.e., the set

\[ H^n(\mathcal{B}) = \left( H^n \setminus \bigcup_{p=1}^{m} R_{i_p}^{u_p} \right) \bigcup \left( \bigcup_{p=1}^{m} (R_{i_p}^{u_p} \oplus e_{i_p}) \right) \]  \hspace{1cm} (1)

is a perfect code [1, 6, 9, 11]. We will say further that \( H^n(\mathcal{B}) \) is obtained from \( H^n \) by switching all components of \( \mathcal{B} \).

A perfect binary code \( C \subseteq \{0, 1\}^n \) of length \( n = 2^k - 1 \) is called systematic if there exists some \( k \)-element subset \( K \subseteq \{1, \ldots, n\} \) such that every two nonequal vectors \( u, v \in C \) differ in at least one entry with the index not in \( K \). Otherwise, \( C \) is called nonsystematic. Nonsystematic perfect binary codes of length \( n \geq 255 \) were constructed first in [1] by switching the \( i \)-components of \( H^n \) for \( i \) varying in all values of \( \{1, \ldots, n\} \). In [10], some modification of the construction of [1] was proposed that allows

\*E-mail: mal@math.nsc.ru
us to construct such codes for all \( n \geq 63 \). For \( n = 15 \) and \( n = 31 \), the nonsystematic codes were found in [6, 10] by computer facilities.

In this article, we consider an essentially stronger notion of nonsystematicity.

**Definition 1.** A perfect binary code \( C \) of length \( n = 2^k - 1 \) is called affine \( t \)-systematic if there exists a \( t \)-dimensional subspace \( L \) in \( \{0, 1\}^n \) such that the intersection of its every coset \( L + u \) with \( C \) is either empty or a singleton. Otherwise, \( C \) is called affine \( t \)-nonsystematic.

It is easy that a perfect binary code \( C \) is affine \( t \)-systematic if and only if there exists a \( t \)-dimensional subspace \( L \subset \{0, 1\}^n \) such that \( L \cap (C + C) = \{0\} \).

If \( t = k = \log(n + 1) \) then an affine \( t \)-systematic (affine \( t \)-nonsystematic) code is called simply affine systematic (affine nonsystematic). The definition of affine systematicity was proposed by S. V. Avgustinovich. This property is an affine invariant of the code; i.e., it is invariant under every nondegenerate affine transformation of \( \{0, 1\}^n \). Avgustinovich also posed the question of existence of affine nonsystematic codes. The answer to this question was announced in [3]. In [4], the affine nonsystematic codes were constructed for all \( n = 2^k - 1 \) with \( k \geq 4 \). It follows from Definition 1 that each affine \( t \)-nonsystematic code is also affine \( t' \)-nonsystematic for every \( t' \geq t \). If \( t > k \) \((t < 3)\) then all perfect codes of length \( n = 2^k - 1 \) are affine \( t \)-nonsystematic (affine \( t \)-systematic). Therefore, it is reasonable to consider only the nontrivial cases of \( 3 \leq t \leq k \). The case \( t = k \) (of affine nonsystematicity) was studied in [4]. In this article, we study another extreme case \( t = 3 \).

### 1. Construction of Affine 3-Nonsystematic Codes

In the set of indices \( \{0, 1, \ldots, n\} \) with \( n = 2^k - 1 \), we can introduce the structure of a linear space as follows: Let \( i = i_1 \ldots i_k \) be the binary representation of a number \( 0 \leq i \leq n \). By the binary sum \( i \oplus j \) of \( 0 \leq i, j \leq n \) we call the number whose binary representation is the bit sum of the binary representations of \( i \) and \( j \). Thus, the set of indices \( \{0, 1, \ldots, n\}, n = 2^k - 1 \), is endowed with the structure of a linear space. The Hamming code \( H^n \) is defined in this case as the set of all vectors \( u = (u_1, \ldots, u_n) \in \{0, 1\}^n \) for which

\[
\bigoplus_{i=1}^{n} u_i = 0.
\]

A \( k \)-dimensional subspace \( Q \subset \{0, 1\}^n \) is called complementary to \( H^n \) if \( Q \cap H^n = \{0\} \). Since \( Q + H^n = \{0, 1\}^n \), the complementary subspace \( Q \) intersects each coset \( H^n + e_i \) in a single nonzero element \( q_i, i = 1, \ldots, n \).

Let \( Q = \{q_0, q_1, \ldots, q_n\} \) be a complementary subspace to \( H^n \), where \( q_0 = 0 \) and \( q_i \in H^n + e_i, 1 \leq i \leq n \). Then \( q_{i,j} = q_i + q_j \) for all \( 1 \leq i, j \leq n \) (see [4, Lemma 1]).

**Definition 2.** A set of indices \( I = \{i_1, \ldots, i_m\} \subset \{1, \ldots, n\} \) is called affine systematic if there exists a \( k \)-dimensional subspace \( Q = \{q_0, q_1, \ldots, q_n\} \) \((q_0 = 0)\) complementary to the Hamming code such that

\[ q_i \in H^n + e_i, \quad i = 1, \ldots, n, \quad q_{i,s} \in R_{i,s} + e_s, \quad s = 1, \ldots, m, \]

where \( R_s \) are the \( i_s \)-entries of the Hamming code containing the zero vector, \( s = 1, \ldots, m \). Otherwise, we call \( I \) affine nonsystematic.

The set of all vectors of \( \{0, 1\}^n \) splits into the orbits relative to the group of permutational automorphisms \( \text{Sym}(H^n) \) of \( H^n \). In Definition 3 of [2], the orbit of the vectors whose supports are systematic sets was called systematic, and the orbit, lacking this property, nonsystematic. According to this terminology, we call the orbit of the vectors whose supports are affine systematic sets affine systematic, and the orbit lacking this property, affine nonsystematic.

As was mentioned, the set of indices \( \{0, \ldots, n\} \) is also a linear space of dimension \( k, n = 2^k - 1 \), which we denote, for brevity, by \( \{0, 1\}^k \). Take a subset \( I = \{i_1, \ldots, i_m\} \) of rank \( r \leq k \) in this space. Let us select in \( I \) some basis family \( \{i_1, \ldots, i_r\} \) and consider the subspace \( M \in \{0, 1\}^k \) spanned by