Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 87-92*

On partitions into nonparallel Hamming codes

Olof Heden olohed@kth.se
Royal Institute of Technology, Stockholm, SWEDEN

Faina I. Solov'eva sol@math.nsc.ru
Sobolev Institute of Mathematics and Novosibirsk State University,
Novosibirsk, RUSSIA

Abstract. Let F denote the finite field with two elements. We describe a construction of partitions of F^n, for $n = 2^m - 1, m \geq 4$, into cosets of pairwise distinct Hamming codes (we call such codes *nonparallel*) of length n. We give a lower bound for the number of different such partitions.

1 Introduction

We describe a method to construct partitions of the set F^n of all binary vectors of length n into cosets of pairwise distinct (we call them *nonparallel*) Hamming codes of length n. In the case of length $n = 7$, Phelps [8] found a family of Hamming codes satisfying this property. Using his result we can produce rather many such families of Hamming codes for lengths greater than $n = 7$. For example for length $n = 15$ we show that the number of distinct partitions of F^{15} into cosets of nonparallel Hamming codes is greater than $1.93 \cdot 2^{54}$.

A Hamming code is a linear perfect code, i.e. a subspace of F^n, such that every word of length n differs in at most one coordinate position from a unique word of H. Let e_i, for $i = 1, 2, \ldots, n$, denote the word with just one non zero coordinate, the ith coordinate. If a word x does not belong to H then this word x belongs to exactly one of the cosets $e_i + H$, $i = 1, 2, \ldots, n$, of H, or equivalently that the sets in the family $\mathcal{P} = \{H, e_1 + H, e_2 + H, \ldots, e_n + H\}$, partition the set F^n.

The problem of the classification of all partitions of the set F_q^n of all q-ary vectors of length n, $q \geq 2$, into perfect codes is closely related to the classical problem to classify all perfect codes. Note that the case $q = 2$ is investigated much more deeply than the case $q > 2$. Constructions of partitions, see the list of references, can also be useful to create new classes of codes, in particular perfect. In Ch. 11, [4], a good survey of the constructions of perfect q-ary codes is presented. One can find there several constructions using some partitions of F_q^n into perfect codes. Two constructions of partitions of F^n into perfect codes are given in [10]. For any admissible $n > 15$ one of these construction allowed to get not less than $2^{2^{(n-1)/2}}$ different partitions of F^n into perfect binary codes of

length n, see [11, 1], the exact number of different partitions for the case $n = 7$ can easily be obtained from [8], for the case $n = 15$ the bound is also valid, see [14]. In [1] a switching construction of the partitions of F^n into pairwise nonequivalent perfect binary codes of length n is presented for any $n = 2^k - 1$, $k \geq 5$.

2 Preliminaries

We will be concerned with the dual space of a Hamming code. The *scalar product* of two vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ of F^n is defined as $x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n \pmod 2$. The *dual space* $V^\perp$ of a subspace V of F^n is $V^\perp = \{\ x \in F^n \ \mid \ x \cdot c = 0 \quad \text{for all} \quad c \in V\ \}$. Every Hamming code H is the dual space of its parity check matrix $\mathbf{H}$.

We remind that the row space of the parity check matrix of any Hamming code is a *simplex code* S of length $n = 2^m - 1$, i.e. a subspace of F^n with the property that every non zero word of S has weight $(n + 1)/2$. Let us give an example of a Hamming code H given by its parity check matrix

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}. \tag{1}$$

This particulary Hamming code H we will essentially use below.

Lemma 1 *If H and H' are Hamming codes of any length n such that $H + e_i = H' + e_j$, then $H = H'$ and $i = j$.*

Corollary 1 *Assume that $\mathcal{P}$ and $\mathcal{P}'$ are two partitions of F^n into cosets of the set of Hamming codes in the two families $\mathcal{H} = \{H_0, H_1, H_2, \ldots, H_n\}$ and $\mathcal{H}' = \{H'_0, H'_1, H'_2, \ldots, H'_n\}$ respectively. If $\mathcal{H} \neq \mathcal{H}'$, then $\mathcal{P} \neq \mathcal{P}'$.*

Lemma 2 *For any two codes C and D of length n, if $v = (v_1, v_2, \ldots, v_n) \in < C >^\perp \cap < D >^\perp$ then, from $v_i \neq v_j$ follows $(e_i + C) \cap (e_j + D) = \emptyset$, and from $v_i \neq 0$ we have $C \cap (e_i + D) = \emptyset$.*

To get the lower bound for the number of partitions F^n into cosets of non-parallel Hamming codes, we will use a partition $\mathcal{P}_{Ph}$ of F^7 found by Phelps [8]. We describe the partition by giving a set of generators for the dual code of each of these Hamming codes:

$H_0 =< 0111100, 1101010, 1011001 >^\perp$, $H_1 =< 1110100, 0111010, 1011001 >^\perp$,
$H_2 =< 0111100, 1110010, 1010101 >^\perp$, $H_3 =< 1111000, 1010110, 0110101 >^\perp$,
$H_4 =< 1110100, 1101010, 0111001 >^\perp$, $H_5 =< 1011100, 0101110, 1100101 >^\perp$,
$H_6 =< 0111010, 1100110, 1010011 >^\perp$, $H_7 =< 0101101, 0110011, 1001011 >^\perp$.

It is easy to check, e.g. using Lemma 2, that the codes in the family $\mathcal{H}_{Ph} = \{H_0, H_1, H_2, \ldots, H_7\}$, are nonparallel and give a partition of F^7. We also observe that the words of weight four, that are not contained in any of the dual spaces of the Hamming codes H_i, for $i = 0, 1, 2, \ldots, 7$, will be exactly the words of weight four in the dual space of the Hamming code H given in equation (1) of the introduction. So if W_4 denotes the set of words of weight four in F^7, then

$$H^{\perp} \setminus \{0\} = W_4 \setminus (\bigcup_{i=0}^{7} H_i^{\perp} \setminus \{0\}). \tag{2}$$

Let $\mathcal{S}_7$ denote the set of all permutations of the set of the seven coordinate positions and let $GL(m, 2)$ denote the general linear group. Taking into account that the automorphism group of a Hamming code of length 7 is isomorphic to GL$(3, 2)$ of order 168 and the well known fact that the Hamming code H is unique up to isomorphism we immediately get the following

Proposition 1 *For each $i = 0, 1, 2, \ldots, 7$ there are 168 distinct permutations π in $\mathcal{S}_7$ that maps the Hamming code H of length 7 onto the Hamming code H_i of length 7 in $\mathcal{H}_{Ph}$:* $|\{\ \pi \in \mathcal{S}_7 \ \mid\ \pi(H) = H_i\ \}| = 168$.

Denote by Π the set of all possible 1344 such permutations, i.e.

$$\Pi = \cup_{i=0}^{7} \{\pi \in \mathcal{S}_7 \mid \pi(H) = H_i\},$$

where H is the Hamming code given by the parity check matrix (1).

Proposition 2 *For any $\pi \in \Pi$ and for any $i = 0, 1, 2, \ldots, 7$, $\pi(H_i) \notin \mathcal{H}_{Ph}$.*

3 Construction

In this section we will give some more necessary lemmas. In lemmas 3–5 we will construct families $\mathcal{H}$ of Hamming codes of length n of which certain cosets will constitute a partition of F^n into perfect codes. By Corollary 1, different such families will give different partitions. Using this construction we will calculate the number of different such partitions.

For each family $\mathcal{H}$ of nonparallel Hamming codes of length n, that will appear here, we take a simplex code $S = S_{\mathcal{H}}$ of length n, dimension $\log_2(n + 1) - 3$, such that

$$\bigcap_{H \in \mathcal{H}} H^{\perp} = S. \tag{3}$$

Let us fix a simplex code S of length n and dimension $\log_2((n+1)/8)$. If a set of basis vectors for the simplex code S constitutes the rows of a matrix $\mathbf{M}$ then each possible non zero word of length $\log_2((n+1)/8)$ will appear as a column in this matrix exactly eight times and the zero column exactly seven times. Without loss of generality, and for the purpose to simplify the notation, we assume that the columns are placed in lexicographical order with the zero column first. When we will count the number of possibilities for partitions that we get by using this construction method, we will consider different distributions of these columns.

We now describe the Hamming codes of the family $\mathcal{H}$. We will use the following notation, related to the choice of ordering of the above set of n columns. For any word x of length n and $t = (n+1)/8 - 1$ we let

$$x = (x_{01}, x_{02}, \ldots, x_{07} \mid x_{10}, x_{11}, \ldots, x_{17} \mid x_{20}, x_{21}, \ldots, x_{27} \mid \cdots \mid x_{t0}, x_{t1}, \ldots, x_{t7}).$$

Let the codes in the family $\mathcal{H}$ be denoted by $H_{i,j}$, where $i = 0, 1, 2, \ldots, t$ and $j = 0, 1, 2, \ldots, 7$. The dual space of the Hamming code H_{ij} will be spanned by the rows of $\mathbf{M}$ and all words u that satisfy

$$u_{i0} = 0, \qquad i = 1, 2, \ldots, t;$$

$$(u_{i1}, u_{i2}, \ldots, u_{i7}) \in H_j^{\perp}, \qquad j = 0, 1, 2, \ldots, 7$$

and for $k \in \{0, 1, 2, \ldots, t\} \setminus \{i\}$, and some $\pi_k^i \in \Pi$:

$$(u_{k1}, u_{k2}, \ldots, u_{k7}) = \pi_k^i((u_{i1}, u_{i2}, \ldots, u_{i7})).$$

For i we put $\pi_i^i = \mathrm{id}$.

Lemma 3 *Every code $H_{i,j}$ for $i = 0, 1, 2, \ldots, t$ and $j = 0, 1, 2, \ldots, 7$ in the family $\mathcal{H}$, defined above, is a Hamming code of length n.*

Lemma 4 *The Hamming codes in the family $\mathcal{H}$ are nonparallel.*

Theorem 1 *The sets $e_{ij} + H_{ij}$, for $i = 0, 1, 2, \ldots, t$, and $j = 0, 1, 2, \ldots, 7$, constitute a partition of F^n into nonparallel Hamming codes.*

From all previous lemmas, propositions and Theorem 1 we get

Theorem 2 *For each $n = 2^m - 1$, where $m \geq 4$, the number of different partitions of F^n into nonparallel Hamming codes is at least*

$$(1344^t)^{t-1} \cdot \frac{(8t-1)!}{7! \cdot 8!^{t-1} \cdot |\mathrm{GL}(\log_2(t+1), 2)|}, \quad \textit{where} \quad t = (n+1)/8.$$

By more careful counting the bound given in Theorem 2 can be improved. We will thereby make use of the following

Lemma 5 *The number of different partitions of F^7 into cosets of nonparallel Hamming codes of length* 7 *is equal to* 1920.

¿From this lemma we deduce

Theorem 3 *The number of partitions of F^{15} into cosets of nonparallel Hamming codes is at least*

$$1,93 \cdot 2^{54}.$$

References

[1] S. V. Avgustinovich, O. Heden, F. I. Solov'eva, On partitions of n-cube into nonequivalent perfect codes, *Probl. Inform. Transm.* 43(4), 2007, 45-50.

[2] S. V. Avgustinovich, A. Lobstein, F. I. Solov'eva, Intersection matrices for partitions by binary perfect codes, *IEEE Trans. Inform. Theory* 47, 2001, 1621-1624.

[3] J. Borges, C. Fernandez, J. Rifa, M. Villanueva, Constructions of 1-perfect partitions on the n-cube $(Z/2)^n$, Techn. rep. PIRDI 1/01, ETSE, July 2001.

[4] G. Cohen, I. Honkala, A. Lobstein, S. Litsyn, *Covering codes*, Elsevier, 1998.

[5] T. Etzion, A. Vardy, Perfect binary codes and tilings: problems and solutions, *SIAM J. Discr. Math.* 11, 1998, 205-223.

[6] K. T. Phelps, A combinatorial construction of perfect codes, *SIAM J. Alg. Discr. Math.* 4, 1983, 398-403.

[7] K. T. Phelps, A general product construction for error correcting codes, *SIAM J. Algebr. Discr. Methods* 5, 1984, 224-228.

[8] K. T. Phelps, An enumeration of 1-perfect binary codes of length 15, *Australas. J. Combin.* 21, 2000, 287-298.

[9] J. Rifa, J. Pujol, J. Borges, 1-perfect uniform and distance invariant partitions, *Appl. Alg. Engin., Commun. Comput.* 11, 2001, 297-311.

[10] F. I. Solov'eva, On binary nongroup codes, *Meth. Discr. Analiza* 37, 1981, 65-76 (in Russian).

[11] F. I. Solov'eva, On perfect codes and related topics, *Com^{2}Mac Lect. Note Series* 13, Pohang, 2004.

[12] F. I. Solov'eva, On transitive partitions of n-cube into codes, *Probl. Inform. Transm.* 45(1), 2009, to appear.

[13] F. I. Solov'eva, A. V. Los', On constructions of partitions into perfect q-ary codes, *Discr. Anal. Oper. Res.*, 2009, to appear.

[14] F. I. Solov'eva, G. K. Guskov, On partitions of vertex-transitive partitions, *Siber. Math. J.*, submitted.