Hamming codes avoiding Hamming subcodes

Josep Rifà, Faina Solov'eva, Merce Villanueva

Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain
e-mails: josep.rifa,merce.villanueva@autonoma.edu

Sobolev Institute of Mathematics
Novosibirsk State University
pr. ac. Koptyuga 4, Novosibirsk 630090, Russia
e-mail: sol@math.nsc.ru

6 September 2010

Presented at Twelfth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT2010

Academgorodok, Novosibirsk, Russia, September 05-11, 2010

Outline

1. Preliminaries
   - General definitions
   - Problem formulation
2. Hamming codes avoiding Hamming subcodes
3. Conclusion

General definitions

Let $\mathbb{F}^n$ be the vector space of length n over the binary field $\mathbb{F}$.

Any subset of F^n is called a *code* of length n.

General definitions

Let $\mathbb{F}^n$ be the vector space of length n over the binary field $\mathbb{F}$.

Any subset of F^n is called a *code* of length n.

Denote by $\mathbf{0}$ the all-zero vector.

General definitions

Let $\mathbb{F}^n$ be the vector space of length n over the binary field $\mathbb{F}$.

Any subset of F^n is called a *code* of length n.

Denote by $\mathbf{0}$ the all-zero vector.

General definitions

Let $\mathcal{S}_n$ be the symmetric group of permutations of length n.

Two binary codes C_1 and C_2 of length n are said to be *isomorphic* if there exists a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{\pi(x) \; : \; x \in C_1\}$.

General definitions

Let $\mathcal{S}_n$ be the symmetric group of permutations of length n.

Two binary codes C_1 and C_2 of length n are said to be *isomorphic* if there exists a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{\pi(x) \ : \ x \in C_1\}$.

They are said to be *equivalent* if there exists a vector $y \in \mathbb{F}^n$ and a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{y + \pi(x) \ : \ x \in C_1\}$.

General definitions

Let $\mathcal{S}_n$ be the symmetric group of permutations of length n.

Two binary codes C_1 and C_2 of length n are said to be *isomorphic* if there exists a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{\pi(x) \ : \ x \in C_1\}$.

They are said to be *equivalent* if there exists a vector $y \in \mathbb{F}^n$ and a coordinate permutation $\pi \in \mathcal{S}_n$ such that $C_2 = \{y + \pi(x) \ : \ x \in C_1\}$.

General definitions

Given a binary code C and a subcode C' of C, the *support of* C' is the set of coordinates where not all codewords of C' are zero, and is denoted by $\mathrm{supp}(C')$.

General definitions

C is called *perfect* if for any vector $x \in F^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.

The linear 1-perfect codes are unique up to equivalence and are the well known *Hamming codes*.

General definitions

C is called *perfect* if for any vector $x \in F^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.

The linear 1-perfect codes are unique up to equivalence and are the well known *Hamming codes*.

The columns in the parity check matrix H_n of a binary Hamming code $\mathcal{H}^n$ of length n, $n = 2^m - 1$, are all the nonzero vectors in $\mathbb{F}^m$. We can associate each one of the elements in the set $N = \{1, 2, \ldots, n\}$ to each one of the columns in H_n.

General definitions

C is called *perfect* if for any vector $x \in F^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.

The linear 1-perfect codes are unique up to equivalence and are the well known *Hamming codes*.

The columns in the parity check matrix H_n of a binary Hamming code $\mathcal{H}^n$ of length n, $n = 2^m - 1$, are all the nonzero vectors in $\mathbb{F}^m$. We can associate each one of the elements in the set $N = \{1, 2, \ldots, n\}$ to each one of the columns in H_n.

General definitions

Consider the $(m-1)$-dimensional projective geometry over $\mathbb{F}$, denoted by $PG(m-1,2)$.

The points of $PG(m-1,2)$ are the 1-dimensional subspaces of $\mathbb{F}^m$, so they can be associated with the columns in H_m, or equivalently, the elements of N.

General definitions

Consider the $(m-1)$-dimensional projective geometry over $\mathbb{F}$, denoted by $PG(m-1,2)$.
The points of $PG(m-1,2)$ are the 1-dimensional subspaces of $\mathbb{F}^m$, so they can be associated with the columns in H_m, or equivalently, the elements of N.
The lines in $PG(m-1,2)$ are the set of points such that the corresponding columns conform 2-dimensional subspaces in $\mathbb{F}^m$.

General definitions

Consider the $(m-1)$-dimensional projective geometry over $\mathbb{F}$, denoted by $PG(m-1,2)$.
The points of $PG(m-1,2)$ are the 1-dimensional subspaces of $\mathbb{F}^m$, so they can be associated with the columns in H_m, or equivalently, the elements of N.
The lines in $PG(m-1,2)$ are the set of points such that the corresponding columns conform 2-dimensional subspaces in $\mathbb{F}^m$.

General definitions

A line (ab) through two distinct points $a, b \in N$ will be denoted by (a, b, c).

The $(k-1)$-flats in $PG(m-1, 2)$ correspond to the sets of columns conforming k-dimensional subspaces in $\mathbb{F}^m$. A 1-flat is a line and a 0-flat is a point.

General definitions

A line (ab) through two distinct points $a, b \in N$ will be denoted by (a, b, c).
The $(k-1)$-flats in $PG(m-1, 2)$ correspond to the sets of columns conforming k-dimensional subspaces in $\mathbb{F}^m$. A 1-flat is a line and a 0-flat is a point.

General definitions

A line (ab) through two distinct points $a, b \in N$ will be denoted by (a, b, c).
The $(k-1)$-flats in $PG(m-1, 2)$ correspond to the sets of columns conforming k-dimensional subspaces in $\mathbb{F}^m$. A 1-flat is a line and a 0-flat is a point.

General definitions

Any Hamming subcode of the code can be defined by some subbasis of the basis of the code from the codewords of weight 3.

The same is true for the corresponding projective geometries.

General definitions

Any Hamming subcode of the code can be defined by some subbasis of the basis of the code from the codewords of weight 3. The same is true for the corresponding projective geometries.

It is well known that all codewords of weight 3 from any binary 1-perfect code C^n of length n containing the all-zero vector define a Steiner triple system of order n, called briefly $STS(C^n)$.

General definitions

Any Hamming subcode of the code can be defined by some subbasis of the basis of the code from the codewords of weight 3. The same is true for the corresponding projective geometries.
It is well known that all codewords of weight 3 from any binary 1-perfect code C^n of length n containing the all-zero vector define a Steiner triple system of order n, called briefly $STS(C^n)$.

Definition ($STS(n)$)

Steiner triple system of order n is a family of 3-element subsets (also called *blocks* or *triples*) of the set N, such that each not ordered pair of elements of N appears in exactly one subset.

For a Hamming code $\mathcal{H}^n$, we denote the corresponding Steiner triple system by $STS(\mathcal{H}^n)$.

Definition ($STS(n)$)

Steiner triple system of order n is a family of 3-element subsets (also called *blocks* or *triples*) of the set N, such that each not ordered pair of elements of N appears in exactly one subset.

For a Hamming code $\mathcal{H}^n$, we denote the corresponding Steiner triple system by $STS(\mathcal{H}^n)$. A codeword $x \in \mathcal{H}^n$ of weight 3 with $\mathrm{supp}(x) = \{a, b, c\}$ corresponds to the line (ab) in the corresponding $PG(m-1, 2)$. This codeword will also be denoted by the triple (a, b, c).

Definition ($STS(n)$)

Steiner triple system of order n is a family of 3-element subsets (also called *blocks* or *triples*) of the set N, such that each not ordered pair of elements of N appears in exactly one subset.

For a Hamming code $\mathcal{H}^n$, we denote the corresponding Steiner triple system by $STS(\mathcal{H}^n)$. A codeword $x \in \mathcal{H}^n$ of weight 3 with $\mathrm{supp}(x) = \{a, b, c\}$ corresponds to the line (ab) in the corresponding $PG(m-1, 2)$. This codeword will also be denoted by the triple (a, b, c).

Problem formulation

Given a binary Hamming code $\mathcal{H}^n$ of length $n = 2^m - 1$, $m \geq 3$, or equivalently a $PG(m-1, 2)$, find permutations $\pi \in \mathcal{S}_n$, such that $\mathcal{H}^n$ and $\pi(\mathcal{H}^n)$ do not have any Hamming subcode with the same support.

Problem formulation

We will further call such a pair of Hamming codes, $\mathcal{H}^n$ and $\pi(\mathcal{H}^n)$, *Hamming codes avoiding Hamming subcodes*, and the corresponding pair of projective geometries, $PG(m-1,2)$ and $\pi(PG(m-1,2))$, *projective geometries avoiding flats*.

This problem can be also reformulated as follows: Given a Hamming Steiner triple system $STS(\mathcal{H}^n)$, find a permutation $\pi \in \mathcal{S}_n$, such that $STS(\mathcal{H}^n)$ and $\pi(STS(\mathcal{H}^n))$ do not have any common supports for subsystems, which are $STS(\mathcal{H}^r)$ for all $r = 2^k - 1$, $1 < k < m$.

Problem formulation

We will further call such a pair of Hamming codes, $\mathcal{H}^n$ and $\pi(\mathcal{H}^n)$, *Hamming codes avoiding Hamming subcodes*, and the corresponding pair of projective geometries, $PG(m-1,2)$ and $\pi(PG(m-1,2))$, *projective geometries avoiding flats*.

This problem can be also reformulated as follows: Given a Hamming Steiner triple system $STS(\mathcal{H}^n)$, find a permutation $\pi \in \mathcal{S}_n$, such that $STS(\mathcal{H}^n)$ and $\pi(STS(\mathcal{H}^n))$ do not have any common supports for subsystems, which are $STS(\mathcal{H}^r)$ for all $r = 2^k - 1$, $1 < k < m$.

Note that if the Hamming codes do not have common triples, then they do not have common Hamming subcodes, but they can have different Hamming subcodes with the same supports.

We will prove that given a binary Hamming code $\mathcal{H}^n$ of length $n = 2^m - 1$, $m \geq 3$, there exists a permutation $\pi \in \mathcal{S}_n$, such that the Hamming codes $\mathcal{H}^n$ and $\pi(\mathcal{H}^n)$ avoid Hamming subcodes.

We use the iterative *Vasil'ev construction* 1962 for a binary Hamming code $\mathcal{H}^n$ of length n, given by

$$\mathcal{H}^n = \{(x+y, |x|, x) \; : \; x \in \mathbb{F}^{\frac{n-1}{2}}, y \in \mathcal{H}^{\frac{n-1}{2}}\},$$

where $\mathcal{H}^{\frac{n-1}{2}}$ is a Hamming code of length $(n-1)/2$, $n = 2^m - 1$, $m \geq 2$.

We use the iterative *Vasil'ev construction* 1962 for a binary Hamming code $\mathcal{H}^n$ of length n, given by

$$\mathcal{H}^n = \{(x+y, |x|, x) \ : \ x \in \mathbb{F}^{\frac{n-1}{2}}, y \in \mathcal{H}^{\frac{n-1}{2}}\},$$

where $\mathcal{H}^{\frac{n-1}{2}}$ is a Hamming code of length $(n-1)/2$, $n = 2^m - 1$, $m \geq 2$.

The first Hamming code in this family of Hamming codes is

$$\mathcal{H}^3 = \{(0,0,0), (1,1,1)\}.$$

We use the iterative *Vasil'ev construction* 1962 for a binary Hamming code $\mathcal{H}^n$ of length n, given by

$$\mathcal{H}^n = \{(x+y, |x|, x) \ : \ x \in \mathbb{F}^{\frac{n-1}{2}}, y \in \mathcal{H}^{\frac{n-1}{2}}\},$$

where $\mathcal{H}^{\frac{n-1}{2}}$ is a Hamming code of length $(n-1)/2$, $n = 2^m - 1$, $m \geq 2$.
The first Hamming code in this family of Hamming codes is

$$\mathcal{H}^3 = \{(0,0,0), (1,1,1)\}.$$

The binary Hamming code of length n constructed by (5) has the following parity check matrix H_n, given in lexicographical order:

$$H_n = \left[\begin{array}{c|c|c} 0\cdots 0 & 1 & 1\cdots 1 \\ \hline H_{\frac{n-1}{2}} & 0 & H_{\frac{n-1}{2}} \end{array}\right].$$

For $n = 7$:

$$\begin{array}{ll} \pi_1 = (1,2,3,4,5,6), & \pi_5 = (3,4,5,6), \\ \pi_2 = \pi_1^{-1} = (6,5,4,3,2,1), & \pi_6 = (3,4,5,7), \\ \pi_3 = (1,7)(2,5)(3,6), & \pi_7 = (3,4,6,5), \\ \pi_4 = (1,7)(2,3)(5,6), & \pi_8 = (3,4)(5,6,7). \end{array}$$

Lemma 1.

Let $N = \{1, 2, \ldots, n\}$ and $N' = \{1, 2, \ldots, (n-1)/2)\}$, where $n = 2^m - 1$, $m \geq 3$. The support of any Hamming subcode of length $r = 2^k - 1$, $1 < k \leq m$, in the Hamming code $\mathcal{H}^n$ contains either all r coordinate positions in N', or $(r-1)/2$ coordinate positions in N' and the others $(r+1)/2$ coordinate positions in $N \setminus N'$.

Lemma 2.

Let (a, b, c) be a triple in the Hamming code $\mathcal{H}^{(n-1)/2}$, where $n = 2^m - 1$, $m \geq 3$. Then, the triples in the Hamming code $\mathcal{H}^n$ are

$$(a, b, c), (a, b + \tfrac{n+1}{2}, c + \tfrac{n+1}{2}),$$
$$(a + \tfrac{n+1}{2}, b, c + \tfrac{n+1}{2}), (a + \tfrac{n+1}{2}, b + \tfrac{n+1}{2}, c);$$

$$\text{and } (s, \frac{n+1}{2}, s + \frac{n+1}{2}) \text{ for any } s \in \{1, 2, \ldots, \frac{n-1}{2}\}.$$

Lemma 3.

Let $\mathcal{H}^r$ be a Hamming subcode of length $r \geq 3$, in the Hamming code $\mathcal{H}^n$ of length $n = 2^m - 1$, $m \geq 3$, such that $n \in \text{supp}(\mathcal{H}^r)$. If $a \in \text{supp}(\mathcal{H}^r) \cap N'$, where $N' = \{1, 2, \ldots, (n-1)/2\}$, then $n - a \in \text{supp}(\mathcal{H}^r)$.

Let π_1 be the permutation

$$\pi_1 = (1, 2, \ldots, n-1)(n). \tag{1}$$

Proposition 1.

Consider the permutation π_1 defined above. Then, the Hamming codes $\mathcal{H}^n$ and $\pi_1(\mathcal{H}^n)$ do not have common triples.

Let π_1 be the permutation

$$\pi_1 = (1, 2, \ldots, n-1)(n). \tag{1}$$

Proposition 1.

Consider the permutation π_1 defined above. Then, the Hamming codes $\mathcal{H}^n$ and $\pi_1(\mathcal{H}^n)$ do not have common triples.

Corollary 1.

If the Hamming codes do not have common triples, then they do not have common Hamming subcodes.

Remark. It should be noted that the Hamming codes mentioned in the last corollary can have different Hamming subcodes with the same supports.

Corollary 1.

If the Hamming codes do not have common triples, then they do not have common Hamming subcodes.

Remark. It should be noted that the Hamming codes mentioned in the last corollary can have different Hamming subcodes with the same supports.

Theorem.

For any Hamming code of length $n = 2^m - 1$, $m \geq 3$, there exists another Hamming code of the same length such that they avoid Hamming subcodes.

Corollary 2.

For any projective geometry $PG(m-1,2)$, $m \geq 3$, there exists another projective geometry with the same points and the same dimension such that they avoid flats.

Corollary 3.

For any Hamming Steiner triple system $STS(\mathcal{H}^n)$ of order $n = 2^m - 1, m \geq 3$, there exists another Hamming Steiner triple system $\pi(STS(\mathcal{H}^n))$ such that they do not have any common subsystems, which are $STS(\mathcal{H}^r)$ for some $r = 2^k - 1$, $1 < k < m$.

Corollary 2.

For any projective geometry $PG(m-1,2)$, $m \geq 3$, there exists another projective geometry with the same points and the same dimension such that they avoid flats.

Corollary 3.

For any Hamming Steiner triple system $STS(\mathcal{H}^n)$ of order $n = 2^m - 1, m \geq 3$, there exists another Hamming Steiner triple system $\pi(STS(\mathcal{H}^n))$ such that they do not have any common subsystems, which are $STS(\mathcal{H}^r)$ for some $r = 2^k - 1$, $1 < k < m$.

Proposition 2.

Consider the permutation π_1. Then, the linear code $\mathcal{H}^n \cap \pi_1(\mathcal{H}^n)$ of length $n = 2^m - 1$, has dimension $n - 2m$ and minimum distance 4, for all $m \geq 4$.

Proposition 3.

Let σ be a permutation such that the Hamming codes $\mathcal{H}^n$ and $\sigma(\mathcal{H}^n)$ avoid Hamming subcodes. Then, the Hamming codes $\mathcal{H}^n$ and $\sigma^{-1}(\mathcal{H}^n)$ avoid Hamming subcodes.

The permutation $\pi_2 = \pi_1^{-1} = (1, 2, \ldots, n-1)^{-1} = (n-1, n-2, \ldots, 1)$ also satisfies that the Hamming codes $\mathcal{H}^n$ and $\pi_2(\mathcal{H}^n)$ avoid Hamming subcodes by Proposition 3.

Proposition 2.

Consider the permutation π_1. Then, the linear code $\mathcal{H}^n \cap \pi_1(\mathcal{H}^n)$ of length $n = 2^m - 1$, has dimension $n - 2m$ and minimum distance 4, for all $m \geq 4$.

Proposition 3.

Let σ be a permutation such that the Hamming codes $\mathcal{H}^n$ and $\sigma(\mathcal{H}^n)$ avoid Hamming subcodes. Then, the Hamming codes $\mathcal{H}^n$ and $\sigma^{-1}(\mathcal{H}^n)$ avoid Hamming subcodes.

The permutation
$\pi_2 = \pi_1^{-1} = (1, 2, \ldots, n-1)^{-1} = (n-1, n-2, \ldots, 1)$ also satisfies that the Hamming codes $\mathcal{H}^n$ and $\pi_2(\mathcal{H}^n)$ avoid Hamming subcodes by Proposition 3.

We showed the existence of Hamming codes avoiding Hamming subcodes for any admissible length. The problem of finding such pairs of Hamming codes

(or pairs of finite geometries of the same dimension avoiding flats,

We showed the existence of Hamming codes avoiding Hamming subcodes for any admissible length. The problem of finding such pairs of Hamming codes
(or pairs of finite geometries of the same dimension avoiding flats, or pairs of corresponding Hamming Steiner triple systems not having any common subsystems) is interesting not only from coding, combinatorial, geometrical point of view, but also from cryptographic.

We showed the existence of Hamming codes avoiding Hamming subcodes for any admissible length. The problem of finding such pairs of Hamming codes
(or pairs of finite geometries of the same dimension avoiding flats, or pairs of corresponding Hamming Steiner triple systems not having any common subsystems) is interesting not only from coding, combinatorial, geometrical point of view, but also from cryptographic.

The codes $\mathcal{H}^n \cap \pi_i(\mathcal{H}^n)$, $i \in \{1, 2\}$ of length $n = 2^m - 1$, have dimension $n - 2m$ and minimum distance 4, for all $m \geq 4$. Therefore, these permutations π_1 and π_2 are not APN (almost perfect nonlinear) functions.

Let $F : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ be any bijective function such that $F(0) = 0$.
Let H_F be the matrix

$$H_F = \left(\begin{array}{c} H_m \\ H_m^{(F)} \end{array} \right) = \left(\begin{array}{ccc} \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{array} \right), \qquad (2)$$

where $0 \neq x \in \mathbb{F}^m$, and let C_F be the linear code admitting H_F as a parity check matrix. Note that C_F is a subcode of the Hamming code $\mathcal{H}^\backslash$ (defined by the parity check matrix H_m).

APN function

Let $F : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ be any function such that $F(0) = 0$. Let C_F be the linear code admitting H_F, defined in (2), as a parity check matrix.

Definition

A function F is called *APN (almost perfect nonlinear)* if all equations:

$$F(x) + F(x + a) = b;\;\; a, b \in \mathbb{F}^m;\;\; a \neq 0$$

have no more than two solutions in $\mathbb{F}^m$.

We proved that the bijective APN functions give the Hamming codes avoiding Hamming subcodes for $m \leq 6$. For $m = 7$ we showed that there exists APN function which give the Hamming codes which do not avoid Hamming subcodes.

Conclusions

We showed in the paper the existence of Hamming codes avoiding Hamming subcodes for any admissible length,

Conclusions

We showed in the paper the existence of Hamming codes avoiding Hamming subcodes for any admissible length,

pairs of finite geometries of the same dimension avoiding flats

Conclusions

We showed in the paper the existence of Hamming codes avoiding Hamming subcodes for any admissible length,

pairs of finite geometries of the same dimension avoiding flats

or pairs of corresponding Hamming Steiner triple systems not having any common subsystems.

Conclusions

We showed in the paper the existence of Hamming codes avoiding Hamming subcodes for any admissible length,
pairs of finite geometries of the same dimension avoiding flats
or pairs of corresponding Hamming Steiner triple systems not having any common subsystems.

Thank you for your attention!