Transitive codes

Faina I. Solov'eva

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

16 April 2010

Presented at ALCOMA2010

Thurnay, Germany, April 11-18, 2010

Outline

General definitions

- F_q^n is the set of all q-ary vectors of length n.
- Any subset of F_q^n is called a *q-ary code* of length n.

General definitions

- F_q^n is the set of all q-ary vectors of length n.
- Any subset of F_q^n is called a *q-ary code* of length n.
- C is called *perfect* if for any vector $x \in F_q^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.

General definitions

- F_q^n is the set of all q-ary vectors of length n.
- Any subset of F_q^n is called a *q-ary code* of length n.
- C is called *perfect* if for any vector $x \in F_q^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.

Observation

Codes and partitions of the set F_q^n of all q-ary vectors into codes of length n are closely related with each other.

$$F_q^n \quad \Longrightarrow \quad F_2^n.$$

For example, a good survey of some known results how to use partitions to construct q-ary perfect codes can be found in the book of

Cohen G., Honkala I., Lobstein A., Litsyn S.

Covering codes, Elsevier, 1998.

Definition (Isometry)

Isometry of F_2^n:

$$\mathrm{Aut}(F_2^n) = F_2^n \leftthreetimes S_n = \{(v,\pi) \mid v \in F_2^n, \pi \in S_n\},$$

where $\leftthreetimes$ denotes a semidirect product, S_n is a group of symmetry of order n.

Definition (Automorphism group)

The *automorphism group* $\mathrm{Aut}(C) \longrightarrow$ all the isometries of F_2^n that transform the code into itself:

$$\mathrm{Aut}(C) = \{(v,\pi) \mid v + \pi(C) = C\}.$$

Definition (Isometry)

Isometry of F_2^n:

$$\mathrm{Aut}(F_2^n) = F_2^n \leftthreetimes S_n = \{(v, \pi) \mid v \in F_2^n, \pi \in S_n\},$$

where $\leftthreetimes$ denotes a semidirect product, S_n is a group of symmetry of order n.

Definition (Automorphism group)

The *automorphism group* $\mathrm{Aut}(C) \longrightarrow$ all the isometries of F_2^n that transform the code into itself:

$$\mathrm{Aut}(C) = \{(v, \pi) \mid v + \pi(C) = C\}.$$

Definition (Automorphism group of a family of codes)

The automorphism group of any family of codes $\mathcal{P} = \{C_0, C_1, \ldots, C_m\}$, $\mathcal{P} \subseteq F_2^n$, $m \leq n$, is a group of isometries of F_2^n that transform the set $\mathcal{P}$ into itself such that for any $i \in M = \{0, 1, \ldots, m\}$ there exists $j \in M$, $v \in F_2^n$, $\pi \in S_n$ satisfying $v + \pi(C_i) = C_j$.

Definition (Automorphism group of a family of codes)

Every such isometry induces a permutation τ on the index set M that permutes the codes in the partition $\mathcal{P}$:

$$\tau(\{C_0, C_1, \ldots, C_m\}) = \{C_{\tau(0)}, C_{\tau(1)}, \ldots, C_{\tau(m)}\},$$

i. e. the automorphism group of the family $\mathcal{P}$ is isomorphic to some subgroup of the group S_{m+1}.

Definition (Transitive codes)

A code C is said to be *transitive* if its automorphism group acts transitively on all codewords.

Without loss of generality we can investigate only reduced codes, i.e., the codes containing the all-zero vector $\mathbf{0}^n$ of length n.

For such codes it is convenient to use the following definition, which is equivalent to the definition given above:

Definition (Transitive codes)

For every codeword $v \in C$ there exists a permutation $\pi \in S_n$ such that $(v, \pi) \in \mathrm{Aut}(C)$, which means $v + \pi(C) = C$ and π may not belong to the set $\mathrm{Sym}(C)$.

Overview

Many classes of known codes are transitive, for example all linear, all important classes of Z_4-linear binary codes, all additive codes.

In 2004 Malyugin enumerated perfect transitive codes of length 15 which belong to the switching class of the Hamming code.

Overview

Many classes of known codes are transitive, for example all linear, all important classes of Z_4-linear binary codes, all additive codes.

In 2004 Malyugin enumerated perfect transitive codes of length 15 which belong to the switching class of the Hamming code.

In 2009 Östergård and Pottonen classified all perfect codes of length 15 (there are 5983 non equivalent such codes) and all extended perfect codes of length 16 (there are 2165 non equivalent such codes) and among them they listed all transitive such codes.

Overview

Many classes of known codes are transitive, for example all linear, all important classes of Z_4-linear binary codes, all additive codes.

In 2004 Malyugin enumerated perfect transitive codes of length 15 which belong to the switching class of the Hamming code.
In 2009 Östergård and Pottonen classified all perfect codes of length 15 (there are 5983 non equivalent such codes) and all extended perfect codes of length 16 (there are 2165 non equivalent such codes) and among them they listed all transitive such codes.

There are two different kinds of additive extended perfect codes. Borges, Rifa in 1998 (for the case Z_2Z_4) and Krotov in 2001 (for the case Z_4) proved that for any $m \geq 2$ there are exactly $\lfloor \frac{m+1}{2} \rfloor$ nonequivalent Z_2Z_4-linear extended perfect codes C of binary length $n = 2^m$.

Puyol, Rifa, S. (2009):
For $m \geq 1$, there exists the quaternary linear Reed-Muller family of codes $\{\mathcal{RM}_s(r,m)\}$, $0 \leq s \leq \lfloor \frac{m-1}{2} \rfloor$, $0 \leq r \leq m$, s.t.:

1. binary length $n = 2^m$, $m \geq 1$;
2. minimum distance $d = 2^{m-r}$;
3. number of codewords 2^k where $k = \sum_{i=0}^{r} \binom{m}{i}$;
4. each code $\mathcal{RM}_s(r-1,m)$ is a subcode of $\mathcal{RM}_s(r,m)$;
5. the $\mathcal{RM}_s(1,m)$ code is a Hadamard quaternary linear code and $\mathcal{RM}_s(m-2,m)$ is an extended quat. linear perfect code;
6. the $\mathcal{RM}_s(r,m)$ code is the dual code of $\mathcal{RM}_s(m-1-r,m)$ for $-1 \leq r \leq m$.

Observation

Applying some well-known constructions, namely Vasil'ev, Plotkin and Mollard, generalized Phelps to known binary transitive codes of some lengths and using some additional conditions it is possible to get infinite classes of transitive binary codes of greater lengths.

Let B and C be arbitrary binary codes of length n with code distance d_1 and d_2 respectively, where d_1 is odd. Let λ be any function from the code C into the set $\{0, 1\}$ and $|x| = x_1 + \ldots + x_n (\bmod 2)$, where $x = (x_1, \ldots, x_n)$. The code

$$C^{2n+1} = \{(x, |x| + \lambda(y), x + y) \mid x \in B, y \in C\}$$

we will call Vasil'ev code. It has length $2n + 1$, size $|B| \cdot |C|$ and code distance $d = \min\{2d_1 + 1, d_2\}$.

Theorem 1, 2005.

Let C be a transitive code with parameters $(n, |C|, d_2)$, B be any linear code with parameters $[n, |B|, d_1]$ such that for any automorphism $(y, \pi) \in \mathrm{Aut}\,(C)$ it is true that $\pi \in \mathrm{Sym}\,(B)$. Then the Vasil'ev code C^{2n+1} with the function $\lambda \equiv 0$ is transitive.

Let D and C be arbitrary binary codes of length n with code distances d_1 and d_2 respectively. The code

$$C^{2n} = \{(x, x+y) \mid x \in D, y \in C\}$$

is known Plotkin code of length $2n$, size $|D| \cdot |C|$ and code distance $d = \min\{2d_1, d_2\}$.

Theorem 2, 2005.

Let C be any transitive code with parameters $(n, |C|, d_2)$ and D be any linear code with parameters $[n, |D|, d_1]$ such that for any automorphism $(y, \pi) \in \mathrm{Aut}\,(C)$ it is true that $\pi \in \mathrm{Sym}\,(D)$. Then the Plotkin code C^{2n} is transitive.

Mollard construction

Let P^t and C^m be any two binary codes of lengths t and m respectively with code distances not less than 3. Let

$$x = (x_{11}, x_{12}, \dots, x_{1m}, x_{21}, \dots, x_{2m}, \dots, x_{t1}, \dots, x_{tm}) \in F_2^{tm}.$$

The generalized parity-check functions $p_1(x)$ and $p_2(x)$ are defined by $p_1(x) = (\sigma_1, \sigma_2, \dots, \sigma_t) \in F_2^t$, $p_2(x) = (\sigma'_1, \sigma'_2, \dots, \sigma'_m) \in F_2^m$, where $\sigma_i = \sum_{j=1}^m x_{ij}$ and $\sigma'_j = \sum_{i=1}^t x_{ij}$. The set

$$C^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in F_2^{tm}, y \in P^t, z \in C^m\}$$

is a binary Mollard code of length $n = tm + t + m$ correcting single errors.

Theorem 3, 2005.

Let P^t and C^m be arbitrary binary transitive codes of lengths t and m respectively. Then the Mollard code

$$C^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in F^{tm}, y \in P^t, z \in C^m\}$$

is a binary transitive code of length $n = tm + t + m$ correcting single errors.

Corollary

Let P^t and C^m be any two perfect binary transitive codes of lengths t and m respectively containing the all-zero vectors. Then the Mollard code C^n is a transitive perfect code of length $n = tm + t + m$.

Theorem 4, 2005.

The number of nonequivalent perfect transitive codes of length $n = 2^k - 1, k \geq 4$ is at least $\lfloor k/2 \rfloor^2$.

Theorem 5, 2005.

For any $n = 16^l - 1$, $l \geq 1$ for each integer δ satisfying

$$1 \leq \delta \leq \frac{3}{4}\log(n+1)$$

there exists a perfect transitive code of length n with the rank $n - \log_2(n_1) + \delta$.

Solov'eva F.I., On construction of transitive codes. Problems of Inform. Transm. (41) 3 (2005) 23-31.

Theorem 5, 2005.

For any $n = 16^l - 1$, $l \geq 1$ for each integer δ satisfying

$$1 \leq \delta \leq \frac{3}{4}\log(n+1)$$

there exists a perfect transitive code of length n with the rank $n - \log_2(n_1) + \delta$.

Solov'eva F.I., On construction of transitive codes. Problems of Inform. Transm. (41) 3 (2005) 23-31.

Theorem 6, Potapov, 2006.

For $n \longrightarrow \infty$ there exist at least

$$\frac{1}{8n^2\sqrt{3}}\, e^{\pi\sqrt{2n/3}}(1 + o(1))$$

pairwise nonequivalent transitive extended perfect codes of length $4n$.

These transitive codes are given constructively using well known Phelps construction-1984. All such transitive codes of length n have rank $n - \log_2 n$. It should be noted that these codes can be represented by extended Vasil'ev construction.

V. N. Potapov, On the lower bound of transitive perfect codes, Diskretn. Anal. Issled. Oper. Ser. 1 13 (2006) No. 4, 49-59 (in Russian).

These transitive codes are given constructively using well known Phelps construction-1984. All such transitive codes of length n have rank $n - \log_2 n$. It should be noted that these codes can be represented by extended Vasil'ev construction.
V. N. Potapov, On the lower bound of transitive perfect codes, Diskretn. Anal. Issled. Oper. Ser. 1 13 (2006) No. 4, 49-59 (in Russian).

Definition (Equivalent partitions of codes)

Two partitions we call *equivalent* if there exists an isometry of the space F_2^n that transforms one partition into another one.

Definition (Transitive family of codes)

A family of codes $\mathcal{P}$ is *transitive* if its automorphism group acts transitively on the elements (the codes) of the family.

Definition (Equivalent partitions of codes)

Two partitions we call *equivalent* if there exists an isometry of the space F_2^n that transforms one partition into another one.

Definition (Transitive family of codes)

A family of codes $\mathcal{P}$ is *transitive* if its automorphism group acts transitively on the elements (the codes) of the family.

Definition (k-transitive family of codes)

A family of the codes $P^n = \{C_0, C_1, \ldots, C_n\}$ of F^n we call *k-transitive*, $1 \leq k \leq n$, if for any two subsets $\{i_1, \ldots, i_k\}$ and $\{j_1, \ldots, j_k\}$ of $I = \{0, 1, \ldots, n\}$, there exists an automorphism σ from $Aut(P^n)$ such that $\sigma(C_{i_t}) = C_{j_t}, t = 1, \ldots, k$.

Definition (Vertex-transitive family of codes)

A family of codes P^n we call *vertex-transitive*, if for any two vectors $u \in C_i$ and $v \in C_j$ there exists an automorphism σ from $\mathrm{Aut}(P^n)$ such that $\sigma(u) = v$.

Definition (k-transitive family of codes)

A family of the codes $P^n = \{C_0, C_1, \ldots, C_n\}$ of F^n we call *k-transitive*, $1 \leq k \leq n$, if for any two subsets $\{i_1, \ldots, i_k\}$ and $\{j_1, \ldots, j_k\}$ of $I = \{0, 1, \ldots, n\}$, there exists an automorphism σ from $Aut(P^n)$ such that $\sigma(C_{i_t}) = C_{j_t}, t = 1, \ldots, k$.

Definition (Vertex-transitive family of codes)

A family of codes P^n we call *vertex-transitive*, if for any two vectors $u \in C_i$ and $v \in C_j$ there exists an automorphism σ from $\mathrm{Aut}(P^n)$ such that $\sigma(u) = v$.

Short overview

- S., 1981: two methods to construct partitions of F_2^n into perfect binary codes are given:
- first one is done using the S-1981 construction for perfect binary codes,

Short overview

- S., 1981: two methods to construct partitions of F_2^n into perfect binary codes are given:
- first one is done using the S-1981 construction for perfect binary codes,
- another one is done using well known Vasil'ev construction for perfect binary codes.

F.I.Solov'eva, On binary nongroup codes, Methody Discretnogo Analiza, 37 (1981) 65-75.

Short overview

- S., 1981: two methods to construct partitions of F_2^n into perfect binary codes are given:
- first one is done using the S-1981 construction for perfect binary codes,
- another one is done using well known Vasil'ev construction for perfect binary codes.

F.I.Solov'eva, On binary nongroup codes, Methody Discretnogo Analiza, 37 (1981) 65-75.

In 2000 Phelps classified partitions of F_2^7 into perfect codes of length 7. Regardless of the fact that the Hamming code is unique (up to equivalence) there are 11 such nonequivalent partitions. Also Phelps proved that there are 10 nonequivalent partitions of F_2^8 into extended perfect codes.

Proposition (S. and Gus'kov, 2009)

Among 11 nonequivalent partitions of F_2^7 into the Hamming codes there are seven transitive partitions, six of which are vertex-transitive, two of them are 2-transitive; there are no k-transitive partitions for $k \geq 3$.

Using Vasil'ev construction 1962 and also Mollard construction 1986 we construct transitive partitions of F_2^n into transitive binary codes.

Theorem 7, Construction A, 2009.

Let $\mathcal{P}^n = \{C_0^n, C_1^n, \ldots, C_m^n\}$ be a transitive family of binary codes of length n;
let B^n be any binary linear code of length n with odd code distance such that for any automorphism $(y, \pi) \in \mathrm{Aut}(\mathcal{P}^n)$ it holds $\pi \in \mathrm{Sym}(B^n)$.
Then the family of the codes
$\mathcal{P}^{2n+1} = \{C_0^{2n+1}, C_1^{2n+1}, \ldots, C_{2m+1}^{2n+1}\}$:
$C_i^{2n+1} = \{(x, |x|, x + y) : x \in B^n, y \in C_i^n\}$,
$C_{m+i+1}^{2n+1} = C_i^{2n+1} + e_{n+1}$,
where $i = 0, 1, \ldots, m$, is transitive.

Corollary 3.

If every code in the family $\mathcal{P}^n$ is transitive than every code of the family $\mathcal{P}^{2n+1}$ from Theorem 7 is transitive.

Corollary 4.

Let $\mathcal{P}^n = \{C_0^n, C_1^n, \ldots, C_n^n\}$ be a transitive partition of F_2^n into perfect binary codes of length n. Then the family of the codes from Theorem 7 is a transitive partition of the space F_2^{2n+1} into perfect binary codes of length $2n+1$.

Theorem 8. (S. and Gus'kov, 2009)

There exist transitive partitions of F_2^n into transitive perfect codes of length n for any $n = 2^m - 1,\ m \geq 3$.

Theorem 9. (S. and Gus'kov, 2009)

Let P^n be a vertex-transitive partition (a 2-transitive partition) of F_2^n into perfect codes of length n. Then the family of the codes P^{2n+1}, defined by Construction A using a partition P^n, is a vertex-transitive partition (a 2-transitive partition) of F_2^{2n+1} into perfect codes of length $2n+1$.

Corollary 5.

There exist transitive partitions of full-even binary code into extended transitive perfect codes of length n for any $n = 2^m,\ m \geq 4$.

F.I. Solov'eva and G.K. Gus'kov, On constructions of vertex-transitive partitions of F_2^n into perfect codes, Discrete Analysis and Oper. Research, accepted, 2010.

Corollary 5.

There exist transitive partitions of full-even binary code into extended transitive perfect codes of length n for any $n = 2^m, \; m \geq 4$.

F.I. Solov'eva and G.K. Gus'kov, On constructions of vertex-transitive partitions of F_2^n into perfect codes, Discrete Analysis and Oper. Research, accepted, 2010.

Theorem 10. Construction B (2009).

Let $\mathcal{P}^t = \{C_0^t, C_1^t, \ldots, C_t^t\}$ and $\mathcal{P}^m = \{D_0^m, D_1^m, \ldots, D_m^m\}$ be any transitive families of the codes of length t and m respectively correcting single errors. Then the family of the codes

$$\mathcal{P}^n = \{C_{00}^n, C_{01}^n, \ldots, C_{tm}^n\}$$

is transitive class of codes of length $n = tm + t + m$, correcting single errors, where

$$C_{ij}^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in F_2^{tm}, y \in C_i^t, z \in D_j^m\}$$

is Mollard code, $i = 0, 1, \ldots, t;\ j = 0, 1, \ldots, m$.

Corollary 6.

Let $\mathcal{P}^t$ and $\mathcal{P}^m$ be any transitive partitions of F_2^t and F_2^m into perfect transitive codes of length $t = 2^r - 1$, $r \geq 3$, and $m = 2^l - 1$, $l \geq 3$, respectively. Then the construction B gives a transitive partition of F_2^n into perfect binary transitive codes of length $n = tm + t + m$.

Theorem 11. (S. and Gus'kov, 2009)

If P^t and P^m are vertex-transitive partitions, then the family P^n of the perfect codes of length n, defined by Construction B from the partitions P^t and P^m, is vertex-transitive.

In the case of 2-transitive partitions it is true

Theorem 12. (S. and Gus'kov, 2009)

If P^t and P^m are 2-transitive partitions, then the family P^n of the perfect codes of length n, given by Construction B from the partitions P^t and P^m, is 2-transitive.

Theorem 11. (S. and Gus'kov, 2009)

If P^t and P^m are vertex-transitive partitions, then the family P^n of the perfect codes of length n, defined by Construction B from the partitions P^t and P^m, is vertex-transitive.

In the case of 2-transitive partitions it is true

Theorem 12. (S. and Gus'kov, 2009)

If P^t and P^m are 2-transitive partitions, then the family P^n of the perfect codes of length n, given by Construction B from the partitions P^t and P^m, is 2-transitive.

F.I. Solov'eva and G.K. Gus'kov, On constructions of vertex-transitive partitions of F_2^n into perfect codes, Discrete Analysis and Oper. Research, accepted, 2010.

Theorem 11. (S. and Gus'kov, 2009)

If P^t and P^m are vertex-transitive partitions, then the family P^n of the perfect codes of length n, defined by Construction B from the partitions P^t and P^m, is vertex-transitive.

In the case of 2-transitive partitions it is true

Theorem 12. (S. and Gus'kov, 2009)

If P^t and P^m are 2-transitive partitions, then the family P^n of the perfect codes of length n, given by Construction B from the partitions P^t and P^m, is 2-transitive.

F.I. Solov'eva and G.K. Gus'kov, On constructions of vertex-transitive partitions of F_2^n into perfect codes, Discrete Analysis and Oper. Research, accepted, 2010.

Theorem 13. (S. and Gus'kov, 2009)

For every $n = 2^k - 1$, $k > 20$, the number of nonequivalent transitive, vertex-transitive and 2-transitive partitions of F^n into perfect codes of length n satisfies the following lower bounds respectively:

- a) $R_{n;trans} \geq n + 1$;
- b) $R_{n;vertex-trans} \geq \frac{n+1}{2}$;
- c) $R_{n;2-trans} \geq \frac{n+1}{3}$.

For small lengths $n = 2^k - 1$, where $3 \leq k \leq 20$:

- a) $R_{n;trans} \geq (n + 1)/2$;
- b) $R_{n;vertex-trans} \geq (n + 1)/3$;
- c) $R_{n;2-trans} \geq (n + 1)/4$.

Definition (Nonparallel Hamming codes)

Two Hamming codes of length n are called *nonparallel* if they can not be obtained from each other using a translation by a vector of F_2^n.

Theorem 14. (Heden and S., 2009)

For each $n = 2^m - 1$, $m \geq 4$, the number of different partitions of F_2^n into non-parallel Hamming codes is at least

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

Definition (Strongly nonparallel partitions)

A pair $\mathcal{P}_1^n = \{\bar{H}_0, \bar{H}_1, \ldots, \bar{H}_n\}$ and $\mathcal{P}_2^n = \{\bar{H}'_0, \bar{H}'_1, \ldots, \bar{H}'_n\}$ of partitions into non-parallel Hamming codes is called *strongly nonparallel* if $H_i \neq H'_j$ for any $i \neq j$ $(i, j \in N)$, where $H_i = e_i + \bar{H}_i$, $H'_j = e_j + \bar{H}'_j$ are the linear Hamming codes corresponding to $\bar{H}_i$ and $\bar{H}'_j$, respectively.

Proposition

There exist $1920 \cdot 1344$ different pairs of strongly non-parallel partitions of F_2^7 into Hamming codes of length 7.

Theorem 15. (Heden and S., 2009)

If $\mathcal{P}_1^n = \{\bar{H}_0, \bar{H}_1, \ldots, \bar{H}_n\}$, $\mathcal{P}_2^n = \{\bar{H}'_0, \bar{H}'_1, \ldots, \bar{H}'_n\}$ is any pair of strongly non-parallel partitions into Hamming codes and δ, δ', ψ, ψ' are any permutations in $\mathcal{S}_n$, then the family of codes

$$\bar{H}_i^{2n+1} = \{(\delta(x), |x|, \psi(x) + y) : x \in F_2^n, y \in \bar{H}_i\},$$
$$\bar{H}_{n+i+1}^{2n+1} = \{(\delta'(x'), |x'| + 1, \psi'(x') + y') : x' \in F_2^n, y' \in \bar{H}'_i\},$$
$$i \in N,$$

defines a partition $\mathcal{P}^{2n+1}$ of F_2^{2n+1} into non-parallel Hamming codes of length $2n+1$.

Theorem 16. (Heden and S., 2009)

Let $\mathcal{P}^t = \{\bar{H}^t_0, \bar{H}^t_1, \ldots, \bar{H}^t_t\}$ and $\mathcal{P}^s = \{\bar{H}^s_0, \bar{H}^s_1, \ldots, \bar{H}^s_s\}$ be any two partitions such that at least one of them is a partition into non-parallel Hamming codes, where $t = 2^l - 1$, $l > 2$, and $s = 2^p - 1$, $p > 2$. Let τ be any permutation in the symmetric group of degree ts. Then the family of codes

$$\bar{H}^n_{ij} = \{(\tau(x), p_1(x) + y, p_2(x) + z) \colon x \in F_2^{st}, y \in \bar{H}^t_i, z \in \bar{H}^s_j\},$$

where $i = 0, 1, \ldots, t$ and $j = 0, 1, \ldots, s$, define a partition $\mathcal{P}^n$ of F_2^n into non-parallel Hamming codes of length $n = st + s + t$.

Heden O., Solov'eva F.I. Partitions of F^n into nonparallel Hamming codes, Advances Math. Commun., 2009, V. 3, N 4, P. 385-397.

Theorem 16. (Heden and S., 2009)

Let $\mathcal{P}^t = \{\bar{H}_0^t, \bar{H}_1^t, \ldots, \bar{H}_t^t\}$ and $\mathcal{P}^s = \{\bar{H}_0^s, \bar{H}_1^s, \ldots, \bar{H}_s^s\}$ be any two partitions such that at least one of them is a partition into non-parallel Hamming codes, where $t = 2^l - 1$, $l > 2$, and $s = 2^p - 1$, $p > 2$. Let τ be any permutation in the symmetric group of degree ts. Then the family of codes

$$\bar{H}_{ij}^n = \{(\tau(x), p_1(x) + y, p_2(x) + z) \colon x \in F_2^{st}, y \in \bar{H}_i^t, z \in \bar{H}_j^s\},$$

where $i = 0, 1, \ldots, t$ and $j = 0, 1, \ldots, s$, define a partition $\mathcal{P}^n$ of F_2^n into non-parallel Hamming codes of length $n = st + s + t$.

Heden O., Solov'eva F.I. Partitions of F^n into nonparallel Hamming codes, Advances Math. Commun., 2009, V. 3. N 4, P. 385-397.

Theorem 17. (S. and Los', 2009)

The number of different partitions of the space F_q^N into perfect q-ary codes is at least

$$\left(\frac{(L(p))^{p^{r-1}}}{p!}\right)^{K(N-1)} \cdot \frac{\left((L(p))^{p^{r-1}}\right)^{K}}{p!}, \qquad (1)$$

where $K = p^{n(2r-1)-r(m-1)}$.

Here $L(p)$ denote the number of different Latin squares of order $p \times p$. It is known that $L(p) > p^{p^2(1-o(1))}$.

Solov'eva F. I., Los' A.V., On constructing of partitions of F_q^n into q-ary perfect codes, J. of Applied and Industrial Mathematics: V. 4, Iss. 1 (2010) 136-146.

Theorem 17. (S. and Los', 2009)

The number of different partitions of the space F_q^N into perfect q-ary codes is at least

$$\left(\frac{(L(p))^{p^{r-1}}}{p!}\right)^{K(N-1)} \cdot \frac{\left((L(p))^{p^{r-1}}\right)^{K}}{p!}, \quad (1)$$

where $K = p^{n(2r-1)-r(m-1)}$.

Here $L(p)$ denote the number of different Latin squares of order $p \times p$. It is known that $L(p) > p^{p^2(1-o(1))}$.
Solov'eva F. I., Los' A.V., On constructing of partitions of F_q^n into q-ary perfect codes, J. of Applied and Industrial Mathematics: V. 4, Iss. 1 (2010) 136-146.

The lower bound of different partitions $\mathcal{M}_n$ given by Vasil'ev construction was proven in 1981 by S. to satisfy the lower bound

$$\mathcal{M}_n \geq 2^{2^{\frac{(n-1)}{2}}}$$

for every admissible $n \geq 31$.

Definition

Let $P^n = \{C_0, \ldots, C_n\}$ be any partition of F^n into the perfect binary codes C_i, $i = 0, 1, \ldots, n$. Then the following is the partition P^{2n+1} of F^{2n+1} into perfect binary Vasil'ev codes of length $2n+1$:

$$\begin{cases} C_i^{2n+1} = & \{(\tau(x)+y, |x|+\lambda_i(y), \sigma(x))\}, \\ C_{n+1+i}^{2n+1} = & \{(\tau(x)+y, |x|+\lambda_i(y)+1, \sigma(x))\}; \end{cases} \quad (2)$$

where $x \in F^n$, $y \in C_i^n$, τ, σ are arbitrary permutations from S_n, $i = 0, 1, \ldots, n$, and λ_i is any binary function defined on the vertices from C_i^n, such that $\lambda_i(e_i) = 0$, $i = 0, \ldots, n$. Here e_i is the vector from F^n of weight 1 having unit only in the ith coordinate position and $e_0 = \mathbf{0}^n$ is the vector from F^n having all zero coordinates.

Lemma

Let $P_1^n = \{C_0, \ldots, C_n\}$ and $P_2^n = \{C'_0, \ldots, C'_n\}$ be any two different partitions of F^n. Then the partitions P_1^{2n+1} and P_2^{2n+1}, obtained by the construction (2) from P_1^n and P_2^n, functions λ_i and λ'_i and permutations $\sigma, \sigma' \in S_n$, respectively, are different.

Lemma

The number of different partitions of F^{15} into perfect binary codes $\mathcal{M}_{15}$ satisfies

$$\mathcal{M}_{15} > 2^{147}.$$

Theorem 18. (S. and Gus'kov)

The number of different partitions of F_2^n into perfect codes of length n satisfies the lower bound

$$2^{2^{\frac{(n-1)}{2}}} \cdot 2^{2^{\frac{(n-3)}{4}}}$$

for every $n = 2^m - 1, \; m \geq 3.$

Corollary

For every $n = 2^m - 1, \; m \geq 6$ there are not less than $2^{2^{\frac{n-1}{2}}}$ nonequivalent partitions of F^n into perfect codes of length n.

Theorem 18. (S. and Gus'kov)

The number of different partitions of F_2^n into perfect codes of length n satisfies the lower bound

$$2^{2^{\frac{(n-1)}{2}}} \cdot 2^{2^{\frac{(n-3)}{4}}}$$

for every $n = 2^m - 1, \ m \geq 3$.

Corollary

For every $n = 2^m - 1, \ \ m \geq 6$ there are not less than $2^{2^{\frac{n-1}{2}}}$ nonequivalent partitions of F^n into perfect codes of length n.

Corollary

The number of nonequivalent partitions of F^{15} into perfect binary codes $\mathcal{M}'_{15}$ satisfies

$$\mathcal{M}'_{15} > 2^{91}.$$

In 2009 Östergård and Pottonen:
there are 5983 nonequivalent perfect codes of length 15, which is less than 2^{13}.

Corollary

The number of nonequivalent partitions of F^{15} into perfect binary codes $\mathcal{M}'_{15}$ satisfies

$$\mathcal{M}'_{15} > 2^{91}.$$

In 2009 Östergård and Pottonen:
there are 5983 nonequivalent perfect codes of length 15, which is less than 2^{13}.

Definition

Let $P_1^n = \{C_0, \ldots, C_n\}$ and $P_2^n = \{C'_0, \ldots, C'_n\}$ be any two partitions of F^n into perfect binary codes of length $n = 2^m - 1, m \geq 3$, where $e_i \in C_i$. The following set of codes defines the partition of F^N, $N = 2^m$ into extended codes

$$\left\{ \begin{array}{rcl} C_i^{2n+2} & = & \{(u, |u|) \mid u \in C_i^{2n+1}\}, \;\; i = 0, 1, \ldots, n, \\ C_{n+1+i}^{2n+2} & = & \{(u', |u'|) \mid u' \in C_{n+1+i}^{2n+1}\}, \;\; i = 0, 1, \ldots, n; \\ \bar{C}_j^{2n+2} & = & \{(v, |v| + 1) \mid v \in C_j^{2n+1}\}, \;\; j = 0, 1, \ldots, n, \\ \bar{C}_{n+1+j}^{2n+2} & = & \{(v', |v'| + 1) \mid v' \in C_{n+1+j}^{2n+1}\}, \;\; j = 0, 1, \ldots, n; \end{array} \right. \tag{3}$$

where C_i^{2n+1} and C_{n+1+i}^{2n+1} are from (2) and

$$C_j^{2n+1} = \{(\theta(x) + y, |x| + \mu_j(y), \pi(x)) \mid, \ \ x \in F^n, \ \ y \in C_j'\},$$

$$C_{n+1+j}^{2n+1} = \{(\theta(x) + y, |x| + \mu_j(y) + 1, \pi(x)) \mid, \ \ x \in F^n, \ \ y \in C_j'\},$$

$$\theta, \pi \in S_n; i, j = 0, 1, \ldots, n.$$

$$C_i \in P_1^n, \ \ C_j' \in P_2^n$$

λ_i and μ_j are two arbitrary binary functions defined as mappings from C_i, C_j' into the set $\{0, 1\}$ respectively, such that $\lambda_i(e_i) = \mu_j(e_j) = 0$.

Lemma

The number of different partitions of F^{16} into extended perfect codes satisfies the following lower bound:

$$\mathcal{R}_{16} > 2^{281}.$$

Theorem 19

The number of different partitions of $F^N, N = 2^m, m \geq 4$ into extended perfect binary codes satisfies the following lower bound:

$$\mathcal{R}_N \geq 2^{2^{\frac{N}{2}}} \cdot 2^{2^{\frac{N-4}{4}}}.$$

Corollary

The number of nonequivalent partitions of F^{16} into perfect binary codes satisfies the following lower bound

$$\mathcal{R}'_{16} > 2^{220}. \tag{4}$$

In 2009 Östergård and Pottonen:
there are 2165 nonequivalent extended perfect codes of length 16, which is less than 2^{12}.

Corollary

The number of nonequivalent partitions of F^{16} into perfect binary codes satisfies the following lower bound

$$\mathcal{R}'_{16} > 2^{220}. \tag{4}$$

In 2009 Östergård and Pottonen:
there are 2165 nonequivalent extended perfect codes of length 16, which is less than 2^{12}.

Open Problems

- Find new transitive perfect (extended) codes in $F_q^n, q \geq 2$.
- Find the lower and upper bounds of all transitive perfect (extended perfect) codes in F_2^n.

Open Problems

- Find new transitive perfect (extended) codes in $F_q^n, q \geq 2$.
- Find the lower and upper bounds of all transitive perfect (extended perfect) codes in F_2^n.
- Find the classification of all transitive perfect (extended) codes in $F_q^n, q \geq 2$.

Open Problems

- Find new transitive perfect (extended) codes in $F_q^n, q \geq 2$.
- Find the lower and upper bounds of all transitive perfect (extended perfect) codes in F_2^n.
- Find the classification of all transitive perfect (extended) codes in $F_q^n, q \geq 2$.
- Find the classification of all transitive partitions into perfect (extended perfect) codes in F_2^{15} (F_2^{16}).

Open Problems

- Find new transitive perfect (extended) codes in $F_q^n, q \geq 2$.
- Find the lower and upper bounds of all transitive perfect (extended perfect) codes in F_2^n.
- Find the classification of all transitive perfect (extended) codes in $F_q^n, q \geq 2$.
- Find the classification of all transitive partitions into perfect (extended perfect) codes in F_2^{15} (F_2^{16}).

Conclusions

- Several methods to construct transitive codes and transitive partitions are presented in the talk.
- Some lower bounds of the number of transitive perfect, extended transitive perfect codes are given.

Conclusions

- Several methods to construct transitive codes and transitive partitions are presented in the talk.
- Some lower bounds of the number of transitive perfect, extended transitive perfect codes are given.
- The lower bound on the number of nonequivalent transitive, vertex-transitive and 2-transitive partitions of $\mathbb{F}_2^n$ into perfect binary codes is done, and also

Conclusions

- Several methods to construct transitive codes and transitive partitions are presented in the talk.
- Some lower bounds of the number of transitive perfect, extended transitive perfect codes are given.
- The lower bound on the number of nonequivalent transitive, vertex-transitive and 2-transitive partitions of $\mathbb{F}_2^n$ into perfect binary codes is done, and also
- The lower bound on the number of different partitions of $\mathbb{F}_2^n$ into nonparallel Hamming codes is given.

Conclusions

- Several methods to construct transitive codes and transitive partitions are presented in the talk.
- Some lower bounds of the number of transitive perfect, extended transitive perfect codes are given.
- The lower bound on the number of nonequivalent transitive, vertex-transitive and 2-transitive partitions of $\mathbb{F}_2^n$ into perfect binary codes is done, and also
- The lower bound on the number of different partitions of $\mathbb{F}_2^n$ into nonparallel Hamming codes is given.
- The problem of the enumeration and the classification of all partitions of the set $\mathbb{F}_q^n$ of all q-ary $(q \geq 2)$ vectors of length n into perfect codes is discussed. The lower bound on the number of different partitions of $\mathbb{F}_q^n$ into perfect codes is done.

Conclusions

- Several methods to construct transitive codes and transitive partitions are presented in the talk.
- Some lower bounds of the number of transitive perfect, extended transitive perfect codes are given.
- The lower bound on the number of nonequivalent transitive, vertex-transitive and 2-transitive partitions of $\mathbb{F}_2^n$ into perfect binary codes is done, and also
- The lower bound on the number of different partitions of $\mathbb{F}_2^n$ into nonparallel Hamming codes is given.
- The problem of the enumeration and the classification of all partitions of the set $\mathbb{F}_q^n$ of all q-ary $(q \geq 2)$ vectors of length n into perfect codes is discussed. The lower bound on the number of different partitions of $\mathbb{F}_q^n$ into perfect codes is done.

Thank you for your attention!