Existence of Transitive Partitions into Binary 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

12 June 2008

Presented at the International Conference on Algebraic and Combinatorial Coding Theory ACCT2008

Outline

General definitions

- F_2^n is the set of all binary vectors of length n.
- Any subset of F_2^n is called a *binary code* of length n.
- C is called *perfect* if for any vector $x \in F_2^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.

General definitions

- F_2^n is the set of all binary vectors of length n.
- Any subset of F_2^n is called a *binary code* of length n.
- C is called *perfect* if for any vector $x \in F_2^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.

General definitions

- F_2^n is the set of all binary vectors of length n.
- Any subset of F_2^n is called a *binary code* of length n.
- C is called *perfect* if for any vector $x \in F_2^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.

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 (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 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 (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.

Short overview

- S., 2004: several methods to construct transitive binary codes are given;
- a class of perfect and extended perfect transitive codes for any admissible length $n \geq 31$;
- the number of nonequivalent perfect transitive codes of length $n = 2^k - 1$ and distance 3 is not less than $\lfloor k/2 \rfloor^2$.
- An analogous estimate is true for extended perfect transitive codes.
- Transitive perfect codes have different ranks, for example, for $n = 16^l - 1, l > 0$ the ranks vary from $n - \log(n+1)$ (the rank of the Hamming code of length n) to $n - \frac{\log(n+1)}{4}$.

Short overview

- S., 2004: several methods to construct transitive binary codes are given;
- a class of perfect and extended perfect transitive codes for any admissible length $n \geq 31$;
- the number of nonequivalent perfect transitive codes of length $n = 2^k - 1$ and distance 3 is not less than $\lfloor k/2 \rfloor^2$.
- An analogous estimate is true for extended perfect transitive codes.
- Transitive perfect codes have different ranks, for example, for $n = 16^l - 1, l > 0$ the ranks vary from $n - \log(n+1)$ (the rank of the Hamming code of length n) to $n - \frac{\log(n+1)}{4}$.

Short overview

- S., 2004: several methods to construct transitive binary codes are given;
- a class of perfect and extended perfect transitive codes for any admissible length $n \geq 31$;
- the number of nonequivalent perfect transitive codes of length $n = 2^k - 1$ and distance 3 is not less than $\lfloor k/2 \rfloor^2$.
- An analogous estimate is true for extended perfect transitive codes.
- Transitive perfect codes have different ranks, for example, for $n = 16^l - 1, l > 0$ the ranks vary from $n - \log(n+1)$ (the rank of the Hamming code of length n) to $n - \frac{\log(n+1)}{4}$.

Short overview

- S., 2004: several methods to construct transitive binary codes are given;
- a class of perfect and extended perfect transitive codes for any admissible length $n \geq 31$;
- the number of nonequivalent perfect transitive codes of length $n = 2^k - 1$ and distance 3 is not less than $\lfloor k/2 \rfloor^2$.
- An analogous estimate is true for extended perfect transitive codes.
- Transitive perfect codes have different ranks, for example, for $n = 16^l - 1, l > 0$ the ranks vary from $n - \log(n+1)$ (the rank of the Hamming code of length n) to $n - \frac{\log(n+1)}{4}$.

Short overview

- S., 2004: several methods to construct transitive binary codes are given;
- a class of perfect and extended perfect transitive codes for any admissible length $n \geq 31$;
- the number of nonequivalent perfect transitive codes of length $n = 2^k - 1$ and distance 3 is not less than $\lfloor k/2 \rfloor^2$.
- An analogous estimate is true for extended perfect transitive codes.
- Transitive perfect codes have different ranks, for example, for $n = 16^l - 1, l > 0$ the ranks vary from $n - \log(n+1)$ (the rank of the Hamming code of length n) to $n - \frac{\log(n+1)}{4}$.

Short overview

- Malyugin, 2004, investigated transitive perfect binary codes of length 15 and extended such codes of length 16.
- Potapov, 2006, found the exponential number of transitive extended perfect codes of small rank.

Short overview

- Malyugin, 2004, investigated transitive perfect binary codes of length 15 and extended such codes of length 16.
- Potapov, 2006, found the exponential number of transitive extended perfect codes of small rank.

Observation

Applying some switching constructions of partitions of the set F_2^n of all binary vectors of length n into perfect binary codes given in 1981 by S. (using Vasil'ev construction 1962) and also using Mollard construction 1986 we construct transitive partitions of F_2^n into transitive binary codes.

Phelps, 2000, classified all partitions of F_2^7 into Hamming codes of length 7. Regardless of the fact that the Hamming code is unique (up to equivalence) there are 11 such nonequivalent partitions.

Proposition

There exist transitive partitions of F_2^7 and a transitive partition of F_2^7 into pairwise nonparallel Hamming codes of length 7.

Theorem 1.

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 1.

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

Corollary 2.

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 1 is a transitive partition of the space F_2^{2n+1} into perfect binary codes of length $2n+1$.

Theorem 2.

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

Corollary 3.

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

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

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

The generalized parity-check functions $p_1(x)$ and $p_2(x)$ are defined by $p_1(x) = (\sigma_1, \sigma_2, \ldots, \sigma_t) \in F_2^t$, $p_2(x) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in F_2^m$, 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.

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 4.

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 $n = tm + t + m$.

Definition (Automorphism group)

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 4.

Let $\mathcal{P}^t = \{H_0^t, H_1^t, \ldots, H_t^t\}$ and $\mathcal{P}^m = \{H_0^m, H_1^m, \ldots, H_m^m\}$ be any transitive partitions into pairwise nonparallel Hamming codes, $t = 2^r - 1$, $r \geq 3$, and $m = 2^l - 1$, $l \geq 3$. Then the family of the codes

$$H_{ij}^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in F_2^{tm}, y \in H_i^t, z \in H_j^m\},$$

$i = 0, 1, \ldots, t$, $j = 0, 1, \ldots, m$, is a transitive partition of F_2^n into pairwise nonparallel Hamming codes of length $n = tm + t + m$.

Conclusions

- Two constructions of transitive partitions of the set F_2^n into binary codes are presented.
- It is established that for any admissible $n \geq 7$, there exist transitive partitions of F_2^n into perfect binary transitive codes of length n and distance 3.
- For any $m = 2^k - 1$, $l \geq 6$ there exist transitive partitions into pairwise nonparallel Hamming codes of length n.

Thank you for your attention!