On uniform transitive partitions of F^n into Hamming 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

11 August 2018

Presented at the International Conference "Graphs and Groups, Representations and Relations" G2R2

Academgorodok, Novosibirsk, Russia, August 6-19, 2018

Outline

General definitions

- F^n is the vector space of dimension n over the Galois field $GF(2)$ equipped with the Hamming metric.
- Any subset of F^n is called a *binary code* of length n.
- C is called a *perfect binary single-error-correcting code* (briefly *perfect*) if for any vector $x \in F^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.
- A perfect linear code is called the *Hamming code*.

General definitions

- F^n is the vector space of dimension n over the Galois field $GF(2)$ equipped with the Hamming metric.
- Any subset of F^n is called a *binary code* of length n.
- C is called a *perfect binary single-error-correcting code* (briefly *perfect*) if for any vector $x \in F^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.
- A perfect linear code is called the *Hamming code*.

General definitions

- F^n is the vector space of dimension n over the Galois field $GF(2)$ equipped with the Hamming metric.
- Any subset of F^n is called a *binary code* of length n.
- C is called a *perfect binary single-error-correcting code* (briefly *perfect*) if for any vector $x \in F^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.
- A perfect linear code is called the *Hamming code*.

General definitions

- F^n is the vector space of dimension n over the Galois field $GF(2)$ equipped with the Hamming metric.
- Any subset of F^n is called a *binary code* of length n.
- C is called a *perfect binary single-error-correcting code* (briefly *perfect*) if for any vector $x \in F^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$.
- A perfect linear code is called the *Hamming code*.

Definition (Isometry)

Isometries of F^n:

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

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

Definition (Automorphism group)

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

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

Definition (Isometry)

Isometries of F^n:

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

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

Definition (Automorphism group)

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

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

Definition (Equivalent partitions)

We call two partitions *equivalent* if there exists an isometry of the space F^n that transforms one partition into another one.

Definition (Automorphism group of a partition)

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

Definition (Equivalent partitions)

We call two partitions *equivalent* if there exists an isometry of the space F^n that transforms one partition into another one.

Definition (Automorphism group of a partition)

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

Definition (Transitive family of codes)

A family of codes P^n is *transitive* if its automorphism group acts transitively on the elements (the codes) of the family.

Definition (Transitive family of codes)

A family of codes P^n is *transitive* if its automorphism group acts transitively on the elements (the codes) of the family.

Definition (2-transitive family of codes)

A family of codes $P^n = \{C_0, C_1, \ldots, C_n\}$ of F^n is called *2-transitive*, if for any two subsets $\{i_1, i_2\}$ and $\{j_1, j_2\}$ of $\{0, 1, \ldots, n\}$, there exists an automorphism σ from $Aut(P^n)$ such that $\sigma(C_{i_t}) = C_{j_t}, t \in \{1, 2\}$.

Definition (uniform partition)

A partition $P^n = \{H_0, H_1 + e_1, \ldots, H_n + e_n\}$ of F^n into cosets of Hamming codes $H_0, H_1, \ldots, H_n$ of length n is called *uniform* if any two Hamming codes H_i, H_j, $i, j \in I$, satisfy $\eta_n = |H_i \bigcap H_j| = \text{const}$.

Definition (2-transitive family of codes)

A family of codes $P^n = \{C_0, C_1, \ldots, C_n\}$ of F^n is called *2-transitive*, if for any two subsets $\{i_1, i_2\}$ and $\{j_1, j_2\}$ of $\{0, 1, \ldots, n\}$, there exists an automorphism σ from $Aut(P^n)$ such that $\sigma(C_{i_t}) = C_{j_t}, t \in \{1, 2\}$.

Definition (uniform partition)

A partition $P^n = \{H_0, H_1 + e_1, \ldots, H_n + e_n\}$ of F^n into cosets of Hamming codes $H_0, H_1, \ldots, H_n$ of length n is called *uniform* if any two Hamming codes H_i, H_j, $i, j \in I$, satisfy $\eta_n = |H_i \bigcap H_j| = \text{const}$.

The connection of the classification problem of all partitions with analogous problem for perfect binary codes.
It is known that the limit for the relation of double logarithms of the numbers of different perfect binary codes and different partitions equals 1, although the number of nonequivalent partitions significantly exceed the number of nonequivalent codes.
There are also tight connections between partitions of F^n into Hamming codes and Reed – Muller codes of order 1 related to these Hamming codes. An intersection of two Hamming codes often gives a good cyclic code.

The connection of the classification problem of all partitions with analogous problem for perfect binary codes.
It is known that the limit for the relation of double logarithms of the numbers of different perfect binary codes and different partitions equals 1, although the number of nonequivalent partitions significantly exceed the number of nonequivalent codes.
There are also tight connections between partitions of F^n into Hamming codes and Reed – Muller codes of order 1 related to these Hamming codes. An intersection of two Hamming codes often gives a good cyclic code.

Some other motivations to construct and study partitions of F^n into codes (not necessarily perfect) can be given by the following connection of partitions with vertex coloring problems in the space F^n:

a partition of F^n into codes induces colorings associated with fibre optic nets,

with perfect colorings called also regular codes, partition designs or equitable partitions.

Some other motivations to construct and study partitions of F^n into codes (not necessarily perfect) can be given by the following connection of partitions with vertex coloring problems in the space F^n:

a partition of F^n into codes induces colorings associated with fibre optic nets,

with perfect colorings called also regular codes, partition designs or equitable partitions.

Some other motivations to construct and study partitions of F^n into codes (not necessarily perfect) can be given by the following connection of partitions with vertex coloring problems in the space F^n:
a partition of F^n into codes induces colorings associated with fibre optic nets,
with perfect colorings called also regular codes, partition designs or equitable partitions.

Short overview

Applying some switching or concatenation approaches it is possible to construct partitions of F^n into perfect codes and investigate some properties of the partitions.

A good survey of some known results till 1998 how to use partitions to construct q-ary perfect codes can be found in

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

Covering codes, Elsevier, 1998.

A survey concerning some recent results on partitions and all other necessary definitions and notions can be found in

S.

Survey on perfect codes, *Mathematical Problems of Cybernetics*, V. 18, 2013.

Short overview

Applying some switching or concatenation approaches it is possible to construct partitions of F^n into perfect codes and investigate some properties of the partitions.
A good survey of some known results till 1998 how to use partitions to construct q-ary perfect codes can be found in

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

Covering codes, Elsevier, 1998.

A survey concerning some recent results on partitions and all other necessary definitions and notions can be found in

S.

Survey on perfect codes, *Mathematical Problems of Cybernetics*, V. 18, 2013.

Short overview

Applying some switching or concatenation approaches it is possible to construct partitions of F^n into perfect codes and investigate some properties of the partitions.
A good survey of some known results till 1998 how to use partitions to construct q-ary perfect codes can be found in

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

Covering codes, Elsevier, 1998.

A survey concerning some recent results on partitions and all other necessary definitions and notions can be found in

S.

Survey on perfect codes, *Mathematical Problems of Cybernetics*, V. 18, 2013.

Short overview

S., 1981: two methods of constructing partitions of F^n into perfect binary codes are given:

first one is done using the concatenation construction (S. 1981) for perfect binary codes,

another one is done using the well known Vasil'ev switching construction 1962 for perfect binary codes.

Short overview

S., 1981: two methods of constructing partitions of F^n into perfect binary codes are given:
first one is done using the concatenation construction (S. 1981) for perfect binary codes,
another one is done using the well known Vasil'ev switching construction 1962 for perfect binary codes.

Short overview

S., 1981: two methods of constructing partitions of F^n into perfect binary codes are given:
first one is done using the concatenation construction (S. 1981) for perfect binary codes,
another one is done using the well known Vasil'ev switching construction 1962 for perfect binary codes.

Short overview

The lower bound of different partitions $\mathcal{M}_n$ constructed by using the Vasil'ev's construction (1981 by S.) satisfies the lower bound

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

for every admissible $n \geq 31$.

In 2000 Phelps classified partitions of F^7 into perfect codes of length 7. Despite of the fact that a Hamming code is unique (up to equivalence) there are 11 such nonequivalent partitions, two of them are uniform.

Short overview

The lower bound of different partitions $\mathcal{M}_n$ constructed by using the Vasil'ev's construction (1981 by S.) satisfies the lower bound

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

for every admissible $n \geq 31$.

In 2000 Phelps classified partitions of F^7 into perfect codes of length 7. Despite of the fact that a Hamming code is unique (up to equivalence) there are 11 such nonequivalent partitions, two of them are uniform.

Short overview

S. and Gus'kov, 2009, proved that the number of different partitions of F^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 $n = 2^m - 1,\ m \geq 3$.

Lemma (S. and Gus'kov, 2009)

Among 11 nonequivalent partitions of F^7 into the cosets of Hamming codes there are seven transitive partitions, two of them are 2-transitive and uniform.

Using the Vasil'ev's construction 1962 and also the Mollard's construction 1986 it is possible to construct the large classes of transitive partitions of F^n into transitive binary codes (not necessarily into the cosets of Hamming codes).

Lemma (S. and Gus'kov, 2009)

Among 11 nonequivalent partitions of F^7 into the cosets of Hamming codes there are seven transitive partitions, two of them are 2-transitive and uniform.

Using the Vasil'ev's construction 1962 and also the Mollard's construction 1986 it is possible to construct the large classes of transitive partitions of F^n into transitive binary codes (not necessarily into the cosets of Hamming codes).

The Mollard's construction

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

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

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

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

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

Theorem 1, Construction B (S. 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 family of codes of length $n = tm + t + m$, correcting single errors, where

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

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

Theorem 2 (S. and Gus'kov, 2009)

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

Uniform partitions of F^n into cosets of Hamming codes with the smallest possible size of η_n were constructed for length $n = 7$ by Phelps in 2000 and for any $n = 2^m - 1$ for odd $m > 3$, using the Gold function by Krotov in 2014.

Exploiting Lemma, the construction B, theorems 1–2 and uniform partitions presented by Phelps and Krotov we give the recursive construction of the class of 2-transitive uniform partitions into Hamming codes.

Uniform partitions of F^n into cosets of Hamming codes with the smallest possible size of η_n were constructed for length $n = 7$ by Phelps in 2000 and for any $n = 2^m - 1$ for odd $m > 3$, using the Gold function by Krotov in 2014.

Exploiting Lemma, the construction B, theorems 1–2 and uniform partitions presented by Phelps and Krotov we give the recursive construction of the class of 2-transitive uniform partitions into Hamming codes.

Let e_i be a binary vector in F^n of weight 1 with one in the ith coordinate position.

Theorem 3 (S. 2018)

For any $n = 2^m - 1$, $m > 2$ and $e = 1, 2, \ldots, [(m+1)/2]$, with the exception $m = 4$, $e = 1$, there exists a 2-transitive uniform partition $P^n = \{H_0, H_1 + e_1, \ldots, H_n + e_n\}$ of F^n into cosets of Hamming codes $H_0, H_1, \ldots, H_n$ of length n for η_n satisfying

$$\log_2 \eta_n = \log_2(|H_i \cap H_j|) = n - 2m + 2e - \delta(m),$$

where $\delta(m) = \begin{cases} 1 \text{ for } m \equiv 1 (\mathrm{mod}\ 2); \\ 0 \text{ for } m \equiv 0 (\mathrm{mod}\ 2). \end{cases}$

Let e_i be a binary vector in F^n of weight 1 with one in the ith coordinate position.

Theorem 3 (S. 2018)

For any $n = 2^m - 1$, $m > 2$ and $e = 1, 2, \ldots, [(m+1)/2]$, with the exception $m = 4$, $e = 1$, there exists a 2-transitive uniform partition $P^n = \{H_0, H_1 + e_1, \ldots, H_n + e_n\}$ of F^n into cosets of Hamming codes $H_0, H_1, \ldots, H_n$ of length n for η_n satisfying

$$\log_2 \eta_n = \log_2(|H_i \cap H_j|) = n - 2m + 2e - \delta(m),$$

where $\delta(m) = \begin{cases} 1 \text{ for } m \equiv 1 (\text{mod } 2); \\ 0 \text{ for } m \equiv 0 (\text{mod } 2). \end{cases}$

Corollary (S. 2018)

For any $n = 2^m - 1$, $m > 2$ there exist at least $[(m+1)/2]$ nonequivalent 2-transitive uniform partitions of F^n into cosets of Hamming codes of length n.

Open Problems

- It should be noted that this theorem covers a half of possible values of the numbers η_n. Another part is still open.
- Find the description of all nonequivalent uniform partitions of F^n into cosets of Hamming codes of length n.
- Find the classification of all nonequivalent partitions into perfect codes in n-dimensional vector space F_q^n over $GF(q)$, $q = p^m, p \geq 2, m \geq 2$.
- Find the classification of all nonequivalent partitions into perfect codes in F^{15} (into extended perfect codes in F^{16}).

Open Problems

- It should be noted that this theorem covers a half of possible values of the numbers η_n. Another part is still open.
- Find the description of all nonequivalent uniform partitions of F^n into cosets of Hamming codes of length n.
- Find the classification of all nonequivalent partitions into perfect codes in n-dimensional vector space F_q^n over $GF(q)$, $q = p^m, p \geq 2, m \geq 2$.
- Find the classification of all nonequivalent partitions into perfect codes in F^{15} (into extended perfect codes in F^{16}).

Open Problems

- It should be noted that this theorem covers a half of possible values of the numbers η_n. Another part is still open.
- Find the description of all nonequivalent uniform partitions of F^n into cosets of Hamming codes of length n.
- Find the classification of all nonequivalent partitions into perfect codes in n-dimensional vector space F_q^n over $GF(q)$, $q = p^m, p \geq 2, m \geq 2$.
- Find the classification of all nonequivalent partitions into perfect codes in F^{15} (into extended perfect codes in F^{16}).

Open Problems

- It should be noted that this theorem covers a half of possible values of the numbers η_n. Another part is still open.
- Find the description of all nonequivalent uniform partitions of F^n into cosets of Hamming codes of length n.
- Find the classification of all nonequivalent partitions into perfect codes in n-dimensional vector space F_q^n over $GF(q)$, $q = p^m, p \geq 2, m \geq 2$.
- Find the classification of all nonequivalent partitions into perfect codes in F^{15} (into extended perfect codes in F^{16}).

Conclusion

- The problem of the existence of uniform partitions of the set F^n of all binary vectors of length n into cosets of Hamming codes is discussed.
- It is proved that for any $n = 2^m - 1$, $m > 2$ there exist at least $[(m+1)/2]$ nonequivalent 2-transitive uniform partitions of F^n into cosets of Hamming codes of length n.

Conclusion

- The problem of the existence of uniform partitions of the set F^n of all binary vectors of length n into cosets of Hamming codes is discussed.
- It is proved that for any $n = 2^m - 1$, $m > 2$ there exist at least $[(m+1)/2]$ nonequivalent 2-transitive uniform partitions of F^n into cosets of Hamming codes of length n.

Thank you for your attention!