Symmetries of a q-ary Hamming Code

Evgeny V. Gorkunov

Novosibirsk State University
<evgumin@gmail.com>

Algebraic and Combinatorial Coding Theory
Akademgorodok, Novosibirsk, Russia
September 5–11, 2010

Notation

- $\mathbb{F}_q = GF(q)$ – the Galois field of order $q = p^r$
- $\mathbb{F}_q^n$ – the n-dimensional vector space over $\mathbb{F}_q$
- $d(x, y) = \#\{i\colon x_i \neq y_i\}$ – the Hamming distance
- $w(x) = \#\{i\colon x_i \neq 0\}$ – weight of $x \in \mathbb{F}_q^n$
- $\mathrm{supp}(x) = \{i\colon x_i \neq 0\}$ – the support of $x \in \mathbb{F}_q^n$
- $C \subseteq \mathbb{F}_q^n$ – a q-ary code of length n;
- $d(C) = \min\{d(x, y)\colon x, y \in C, x \neq y\}$ – the minimum distance of C

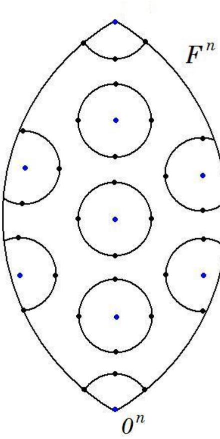
Novosibirsk State University

Definitions

Code equivalence

Two codes are equivalent if there is an isometry of $\mathbb{F}_q^n$ that maps one of the codes into the other one

Definitions



Perfect codes

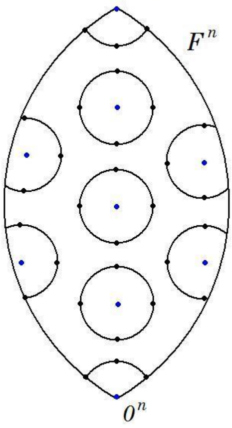
The balls with radius 1 centred at the codewords partition the space $\mathbb{F}_q^n$

Such codes have the minimum distance $d = 3$

Golay codes

Binary and ternary Golay codes and codes equivalent to them have $d = 7$ and $d = 5$

Definitions



Perfect codes

The balls with radius 1 centred at the codewords partition the space $\mathbb{F}_q^n$

Such codes have the minimum distance $d = 3$

Golay codes

Binary and ternary Golay codes and codes equivalent to them have $d = 7$ and $d = 5$

Faces of regularity

- Linearity
- Rank of a code
- Dimension of the kernal of a code
- Perfect and uniformly packed codes
- Distance invariance
- Complete regularity
- Regular properties of minimal distance graph
- Other extremal properties

Automorphisms and symmetries

Automorphism group of a code C

The group of isometries of the space $\mathbb{F}_q^n$ that map the code C into itself

Symmetry group of a code C

The group of automorphisms of C that fix the vector 0.

Examples

Permutation

$\pi \in S_n$ – a permutation on coordinate positions,

$$n = 3: \quad (x_1, x_2, x_3)(123) = (x_3, x_1, x_2)$$

Configuration

$\sigma = (\sigma_1, \ldots, \sigma_n) \in S_q^n$ – n permutations on elements of $\mathbb{F}_q$,

$$n = 3: \quad (x_1, x_2, x_3)\sigma = (x_1\sigma_1, x_2\sigma_2, x_3\sigma_3)$$

Isometries of the space $\mathbb{F}_q^n$

Theorem (Markov, 1956)

The group of isometries of the space $\mathbb{F}_q^n$ is

$$\mathrm{Aut}(\mathbb{F}_q^n) = S_n \leftthreetimes S_q^n = \{(\pi;\sigma)\colon \pi \in S_n, \sigma \in S_q^n\}$$

with multiplication given by

$$(\pi;\sigma)(\tau;\delta) = (\pi\tau;\sigma\tau \cdot \delta)$$

Kinds of isometries: $q = 2$

Permutation automorphisms

$\pi \in S_n \longrightarrow \mathrm{PAut}(\mathbb{F}_2) = \mathrm{Sym}(\mathbb{F}_2)$

All configurations are translations

S_2 acts on $\mathbb{F}_2$:
$e \to \beta + 0$
$(0\,1) \to \beta + 1$

$x \in \mathbb{F}_2, \sigma \in S_2^n$
$x\sigma = x + v$
for some $v \in \mathbb{F}_2$

Kinds of isometries: $q = 3$

Permutation automorphisms

$\pi \in S_n \longrightarrow \mathrm{PAut}(\mathbb{F}_3) \subset \mathrm{Sym}(\mathbb{F}_3)$

Monomial configurations

S_3 acts on $\mathbb{F}_3$:

$e \to 1 \cdot \beta$

$(1\,2) \to 2\beta$

$x \in \mathbb{F}_3, \sigma$ – multiplying

$x\sigma = xD$

for some diagonal matrix D

Monomial automorphisms

$x \in \mathbb{F}_3, \pi \in S_n, \sigma$ – multiplying

$x(\pi;\sigma) = xPD = xM$ $\longrightarrow$ $\mathrm{MAut}(\mathbb{F}_3) = \mathrm{Sym}(3)$

for some monomial matrix M

Kinds of isometries: $q \geq 4$

Permutation automorphisms

$\pi \in S_n \longrightarrow \mathrm{PAut}(\mathbb{F}_q^n) \subset \mathrm{Sym}(\mathbb{F}_q^n)$

Configurations

- $q = 4$
  $\mathrm{Gal}(\mathbb{F}_4), \times, +$
  $(0\ \alpha^2\ 1\ \alpha) \to (\beta + \alpha)^2,$ where α – primitive element of $\mathbb{F}_4$
  no matrix representation for all!
- $q \geq 5$
  no field operations for all!

Linear and semilinear transformations of $\mathbb{F}_q^n$

General linear group

$\mathrm{GL}_n(q)$
$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$
for all $x, y \in \mathbb{F}_q^n$ and $\alpha, \beta \in \mathbb{F}_q$

General semilinear group

$\Gamma\mathrm{L}_n(q) = \mathrm{Gal}(\mathbb{F}_q) \ltimes \mathrm{GL}_n(q)$
$f(\alpha x + \beta y) = \gamma(\alpha) f(x) + \gamma(\beta) f(y)$
for all $x, y \in \mathbb{F}_q^n$, all $\alpha, \beta \in \mathbb{F}_q$, and some $\gamma \in \mathrm{Gal}(\mathbb{F}_q)$

But not all of them are isometries of $\mathbb{F}_q^n$!

MacWilliams' theorem

Theorem (MacWilliams, 1962)

Two linear codes are monomially equivalent iff there exists an isomorphism between them (as linear spaces) preserving the weight of each vector

Corollary 1

$\mathrm{MAut}(\mathbb{F}_q^n)$ – all linear symmetries of $\mathbb{F}_q^n$

Corollary 2

$\mathrm{Gal}(\mathbb{F}_q) \leftthreetimes \mathrm{MAut}(\mathbb{F}_q^n)$ – all semilinear symmetries of $\mathbb{F}_q^n$

The automorphism group of a linear code

Proposition

If a code $C \subseteq \mathbb{F}_q^n$ is linear, then

$$\mathrm{Aut}(C) \cong \mathrm{Sym}(C) \ltimes C$$

Theorem

- *C is an $[n, n-m, d \geq 3]_q$-code*

$\Rightarrow$ *The semilinear symmetry group of C is isomorphic to some subgroup of $\Gamma\mathrm{L}_m(q)$*

Semilinear automorphisms of $\mathcal{H}$

Theorem

The semilinear symmetry group of a q-ary Hamming code $\mathcal{H}$ of length $n = \frac{q^m-1}{q-1}$ is isomorphic to $\Gamma\mathrm{L}_m(q)$

- $q = 2, 3$ – all symmetries of $\mathbb{F}_q^n$ are linear
  $\mathrm{Aut}(\mathcal{H}) \cong \mathrm{GL}_m(q) \leftthreetimes \mathcal{H}$
- $q \geq 4$ – not all symmetries of $\mathbb{F}_q^n$ are semilinear
  $\mathrm{Aut}(\mathcal{H}) \cong \Gamma\mathrm{L}_m(q) \leftthreetimes \mathcal{H}$ – ?

Is there anything to doubt?

Example

- $C \subset \mathbb{F}_q^n$ is the linear code with $H = [1\,1\,\ldots\,1]$
- $A \in S_q$ is a linear transformation of $\mathbb{F}_q$ as a vector space over the subfield $\mathbb{F}_p$

$\Rightarrow$ $(e, (A, A, \ldots, A)) \in \mathrm{Aut}(C)$

$\Rightarrow$ for $q \geq 8$ there exists A such that this automorphism of C is neither linear nor semilinear

Collinear triples

- $T = \{x \in \mathcal{H} \colon w(x) = 3\}$
- $\mathrm{Sym}(\mathcal{H}) \leq \mathrm{Sym}(T)$

Lemma

- $x, y \in T$
- $\mathrm{supp}(x) = \mathrm{supp}(y)$

$\Rightarrow$ $y = \mu x$ *for some* $\mu \in \mathbb{F}_q^*$

Symmetries of Hamming triples

Lemma (saving collinearity)

- $(\pi;\sigma) \in \mathrm{Sym}(T)$

$\Rightarrow$ $(\pi;\sigma)$ *preserves collinearity of vectors from* $\mathbb{F}_q^n$

Lemma (saving sum)

- $(\pi;\sigma) \in \mathrm{Sym}(T)$

$\Rightarrow$ $(\pi;\sigma)$ *preserves sum of vectors from* $\mathbb{F}_q^n$

Lemma

- $(\pi;\sigma) \in \mathrm{Sym}(T)$

$\Rightarrow$ $(\pi;\sigma)$ *is a semilinear transformation of* $\mathbb{F}_q^n$

The automorphism group of $\mathcal{H}$

Theorem

For any q-ary Hamming code $\mathcal{H}$ of length $n = \frac{q^m-1}{q-1}$, where $q, m \geq 2$, it is true

$$\mathrm{Aut}(\mathcal{H}) \cong \Gamma\mathrm{L}_m(q) \leftthreetimes \mathcal{H}$$

Conclusion

We proved that

- all symmetries of the Hamming code are semilinear
- the same can be said about the triple system of a q-ary Hamming code