On regular subgroups of the automorphism group of the Hamming code of length 15

I.Yu. Mogilnykh

Sobolev Institute of Mathematics
Tomsk State University

Presented at G2R2

Codes in Hamming space

The Hamming space F_2^n is the n-dimensional vector space over $GF(2)$ with the *Hamming metric*

$$d(x, y) = |\{i \in \{1, \ldots, n\} : x_i \neq y_i\}|.$$

A subset C of F_2^n is a binary *code*.
The minimum distance of a code is $min_{x,y \in C: x \neq y} d(x, y)$.

Codes in Hamming space

The Hamming space F_2^n is the n-dimensional vector space over $GF(2)$ with the *Hamming metric*

$$d(x, y) = |\{i \in \{1, \ldots, n\} : x_i \neq y_i\}|.$$

A subset C of F_2^n is a binary *code*.
The minimum distance of a code is $min_{x,y \in C: x \neq y} d(x, y)$.

Codes in Hamming space

The Hamming space F_2^n is the n-dimensional vector space over $GF(2)$ with the *Hamming metric*

$$d(x, y) = |\{i \in \{1, \ldots, n\} : x_i \neq y_i\}|.$$

A subset C of F_2^n is a binary *code*.
The minimum distance of a code is $min_{x,y \in C : x \neq y} d(x, y)$.

Perfect codes

A code with minimum distance 3 is *perfect* (1-perfect) if it attains the Hamming bound, i.e.

$$|C| = 2^n/(n+1).$$

These codes exist for length $n = 2^r - 1$, size 2^{n-r} and minimum distance 3 for any $r \geq 2$.

A Hamming code is a perfect code which is a linear subspace of F_2^n.

Perfect codes

A code with minimum distance 3 is *perfect* (1-perfect) if it attains the Hamming bound, i.e.

$$|C| = 2^n/(n+1).$$

These codes exist for length $n = 2^r - 1$, size 2^{n-r} and minimum distance 3 for any $r \geq 2$.

A Hamming code is a perfect code which is a linear subspace of F_2^n.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

$Aut(F_2^n)$ w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

$Aut(F_2^n)$ w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

$Aut(F_2^n)$ w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

$Aut(F_2^n)$ w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

$Aut(F_2^n)$ w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

The automorphism group of the code

An automorphism of F_2^n is an isometry of Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

$$(x, \pi) : y \to x + (y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}), y \in F_2^n.$$

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi\pi').$$

$Aut(F_2^n)$ w.t.r. $\cdot$ is $(\{(x, \pi) : x \in F_2^n, \pi \in Sym(n)\}, \cdot)$

The *automorphism group* of a code C is $Stab_C(Aut(F_2^n))$, denoted by $Aut(C)$.

Propelinear codes

A code C is called *propelinear* [1], [2] if there is a subgroup $G < Aut(C)$ acting regularly on the codewords, i.e.:

$$\forall x, y \in C \quad \exists! g \in G : g(x) = y$$

The automorphism group of a propelinear code can have many regular subgroups.

[1] Rifà J., Basart J.M., Huguet L.: On completely regular propelinear codes. Proc. 6th Int. Conference, AAECC-6. LNCS. 357 (1989) 341–355

[2] Phelps K. T., Rifà J.: On binary 1-perfect additive codes: some structural properties. IEEE Trans. Inform. Theory. 48 (2002) 2587–2592.

Propelinear codes

A code C is called *propelinear* [1], [2] if there is a subgroup $G < Aut(C)$ acting regularly on the codewords, i.e.:

$$\forall x, y \in C \quad \exists! g \in G : g(x) = y$$

The automorphism group of a propelinear code can have many regular subgroups.

[1] Rifà J., Basart J.M., Huguet L.: On completely regular propelinear codes. Proc. 6th Int. Conference, AAECC-6. LNCS. 357 (1989) 341–355

[2] Phelps K. T., Rifà J.: On binary 1-perfect additive codes: some structural properties. IEEE Trans. Inform. Theory. 48 (2002) 2587–2592.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has an element of order 4.
$(G',\cdot) \cong Z_4$.

$Aut(C)$ has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has an element of order 4.
$(G',\cdot) \cong Z_4$.

$Aut(C)$ has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has an element of order 4.
$(G',\cdot) \cong Z_4$.

$Aut(C)$ has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has an element of order 4.
$(G',\cdot) \cong Z_4$.

$Aut(C)$ has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has an element of order 4.
$(G',\cdot) \cong Z_4$.

$Aut(C)$ has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has an element of order 4.
$(G',\cdot) \cong Z_4$.

$Aut(C)$ has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Example

$C = F_2^2 = \{(0,0),(1,0),(0,1),(1,1)\}$.
$Aut(C) = \{(x,\pi) : x \in C, \pi \in S_2\}$

Regular subgroup 1

$G = \{(x, id) : x \in C\}$, $(G,\cdot)$ is a regular subgroup of $Aut(C)$.
$(G,\cdot) \cong Z_2^2$.

Regular subgroup 2

$G' = \{((0,0), id), ((1,1), id), ((0,1),(1,2)), ((1,0),(1,2))\}$.
$((0,1),(1,2))^2 = ((1,1), id)$, so G' has an element of order 4.
$(G',\cdot) \cong Z_4$.

$Aut(C)$ has two *nonisomorphic* regular subgroups: $G \ncong G'$.

Propelinear codes

Linear codes [Hamming, 1949]

Z4-linear Preparata codes [Hammons, Kumar, Calderbank, Sloane, Sole, 1994]

Z4-linear perfect and Hadamard codes [Rifa, Pujol, Borges 1997], [Krotov, 2001]

Vasiliev and Mollard can be used to construct propelinear perfect codes [Borges, M., Rifa, Solov'eva, 2012]

Malygin and Potapov codes are propelinear [Borges, M., Rifa, Solov'eva, 2013]

Propelinear Vasil'ev perfect codes from quadratic functions [Krotov, Potapov, 2013]

There are 5983 classes of perfect codes of length 15 [Ostergard, Pottonen, 2009], 200 of which are propelinear

Propelinear codes

Linear codes [Hamming, 1949]

Z4-linear Preparata codes [Hammons, Kumar, Calderbank, Sloane, Sole, 1994]

Z4-linear perfect and Hadamard codes [Rifa, Pujol, Borges 1997], [Krotov, 2001]

Vasiliev and Mollard can be used to construct propelinear perfect codes [Borges, M., Rifa, Solov'eva, 2012]

Malygin and Potapov codes are propelinear [Borges, M., Rifa, Solov'eva, 2013]

Propelinear Vasil'ev perfect codes from quadratic functions [Krotov, Potapov, 2013]

There are 5983 classes of perfect codes of length 15 [Ostergard, Pottonen, 2009], 200 of which are propelinear

Propelinear codes

Linear codes [Hamming, 1949]

Z4-linear Preparata codes [Hammons, Kumar, Calderbank, Sloane, Sole, 1994]

Z4-linear perfect and Hadamard codes [Rifa, Pujol, Borges 1997], [Krotov, 2001]

Vasiliev and Mollard can be used to construct propelinear perfect codes [Borges, M., Rifa, Solov'eva, 2012]

Malygin and Potapov codes are propelinear [Borges, M., Rifa, Solov'eva, 2013]

Propelinear Vasil'ev perfect codes from quadratic functions [Krotov, Potapov, 2013]

There are 5983 classes of perfect codes of length 15 [Ostergard, Pottonen, 2009], 200 of which are propelinear

Propelinear codes

Linear codes [Hamming, 1949]
Z4-linear Preparata codes [Hammons, Kumar, Calderbank, Sloane, Sole, 1994]
Z4-linear perfect and Hadamard codes [Rifa, Pujol, Borges 1997], [Krotov, 2001]
Vasiliev and Mollard can be used to construct propelinear perfect codes [Borges, M., Rifa, Solov'eva, 2012]
Malygin and Potapov codes are propelinear [Borges, M., Rifa, Solov'eva, 2013]
Propelinear Vasil'ev perfect codes from quadratic functions [Krotov, Potapov, 2013]
There are 5983 classes of perfect codes of length 15 [Ostergard, Pottonen, 2009], 200 of which are propelinear

Propelinear codes

Linear codes [Hamming, 1949]
Z4-linear Preparata codes [Hammons, Kumar, Calderbank, Sloane, Sole, 1994]
Z4-linear perfect and Hadamard codes [Rifa, Pujol, Borges 1997], [Krotov, 2001]
Vasiliev and Mollard can be used to construct propelinear perfect codes [Borges, M., Rifa, Solov'eva, 2012]
Malygin and Potapov codes are propelinear [Borges, M., Rifa, Solov'eva, 2013]
Propelinear Vasil'ev perfect codes from quadratic functions [Krotov, Potapov, 2013]
There are 5983 classes of perfect codes of length 15 [Ostergard, Pottonen, 2009], 200 of which are propelinear

Propelinear codes

Linear codes [Hamming, 1949]
Z4-linear Preparata codes [Hammons, Kumar, Calderbank, Sloane, Sole, 1994]
Z4-linear perfect and Hadamard codes [Rifa, Pujol, Borges 1997], [Krotov, 2001]
Vasiliev and Mollard can be used to construct propelinear perfect codes [Borges, M., Rifa, Solov'eva, 2012]
Malygin and Potapov codes are propelinear [Borges, M., Rifa, Solov'eva, 2013]
Propelinear Vasil'ev perfect codes from quadratic functions [Krotov, Potapov, 2013]
There are 5983 classes of perfect codes of length 15 [Ostergard, Pottonen, 2009], 200 of which are propelinear

Propelinear codes

Linear codes [Hamming, 1949]
Z4-linear Preparata codes [Hammons, Kumar, Calderbank, Sloane, Sole, 1994]
Z4-linear perfect and Hadamard codes [Rifa, Pujol, Borges 1997], [Krotov, 2001]
Vasiliev and Mollard can be used to construct propelinear perfect codes [Borges, M., Rifa, Solov'eva, 2012]
Malygin and Potapov codes are propelinear [Borges, M., Rifa, Solov'eva, 2013]
Propelinear Vasil'ev perfect codes from quadratic functions [Krotov, Potapov, 2013]
There are 5983 classes of perfect codes of length 15 [Ostergard, Pottonen, 2009], 200 of which are propelinear

Solov'eva-Topalova[3]

The order of the automorphism group of the Hamming code of length n is the largest among the automorphism groups of the perfect codes of length n

Question

Does the Hamming code of length n has the maximum number of regular subgroups among all propelinear perfect codes of length n.

Let $\mathcal{H}$ be the Hamming code of length 15. Then $|\mathcal{H}| = 2^{11}$ and $|Aut(\mathcal{H})| = |\mathcal{H}||GL(4,2)| > 41000000$.
Too large

[3]F. I. Solov'eva, S. Topalova, On automorphism groups of perfect binary codes and Steiner triple systems. *Problems of Information Transmission* **36(4)** (2000) 331–335.

Solov'eva-Topalova[3]

The order of the automorphism group of the Hamming code of length n is the largest among the automorphism groups of the perfect codes of length n

Question

Does the Hamming code of length n has the maximum number of regular subgroups among all propelinear perfect codes of length n.

Let $\mathcal{H}$ be the Hamming code of length 15. Then $|\mathcal{H}| = 2^{11}$ and $|Aut(\mathcal{H})| = |\mathcal{H}||GL(4,2)| > 41000000$.
Too large

[3]F. I. Solov'eva, S. Topalova, On automorphism groups of perfect binary codes and Steiner triple systems. *Problems of Information Transmission* **36(4)** (2000) 331–335.

Solov'eva-Topalova[3]

The order of the automorphism group of the Hamming code of length n is the largest among the automorphism groups of the perfect codes of length n

Question

Does the Hamming code of length n has the maximum number of regular subgroups among all propelinear perfect codes of length n.

Let $\mathcal{H}$ be the Hamming code of length 15. Then $|\mathcal{H}| = 2^{11}$ and $|Aut(\mathcal{H})| = |\mathcal{H}||GL(4,2)| > 41000000$.

Too large

[3]F. I. Solov'eva, S. Topalova, On automorphism groups of perfect binary codes and Steiner triple systems. *Problems of Information Transmission* **36(4)** (2000) 331–335.

Solov'eva-Topalova[3]

The order of the automorphism group of the Hamming code of length n is the largest among the automorphism groups of the perfect codes of length n

Question

Does the Hamming code of length n has the maximum number of regular subgroups among all propelinear perfect codes of length n.

Let $\mathcal{H}$ be the Hamming code of length 15. Then $|\mathcal{H}| = 2^{11}$ and $|Aut(\mathcal{H})| = |\mathcal{H}||GL(4,2)| > 41000000$.
Too large

[3]F. I. Solov'eva, S. Topalova, On automorphism groups of perfect binary codes and Steiner triple systems. *Problems of Information Transmission* **36(4)** (2000) 331–335.

Extension in narrow sense

Let $G < Aut(F^n)$. Denote by $\Pi_G = \{\pi : (x, \pi) \in G\}$.

Let $G, H < Aut(F^n)$. The group G is called *extended in narrow sense* to H if $G < H$ and $\Pi_G = \Pi_H$.

Extension in narrow sense

Let $G < Aut(F^n)$. Denote by $\Pi_G = \{\pi : (x, \pi) \in G\}$.

Let $G, H < Aut(F^n)$. The group G is called *extended in narrow sense* to H if $G < H$ and $\Pi_G = \Pi_H$.

Finding regular subgroups of $Aut(\mathcal{H})$:idea

Let C be a propelinear subcode of the Hamming code of length 15 $\mathcal{H}$, $Aut(C)$ is extended in narrow sense to $Aut(\mathcal{H})$.

Obtain the classification of regular subgroups of $Aut(C)$

Find all regular subgroups of $Aut(\mathcal{H})$ that are extensions of the regular subgroups of $Aut(C)$ in narrow sense.

Finding regular subgroups of $Aut(\mathcal{H})$:idea

Let C be a propelinear subcode of the Hamming code of length 15 $\mathcal{H}$, $Aut(C)$ is extended in narrow sense to $Aut(\mathcal{H})$.

Obtain the classification of regular subgroups of $Aut(C)$

Find all regular subgroups of $Aut(\mathcal{H})$ that are extensions of the regular subgroups of $Aut(C)$ in narrow sense.

Finding regular subgroups of $Aut(\mathcal{H})$:idea

Let C be a propelinear subcode of the Hamming code of length 15 $\mathcal{H}$, $Aut(C)$ is extended in narrow sense to $Aut(\mathcal{H})$.

Obtain the classification of regular subgroups of $Aut(C)$

Find all regular subgroups of $Aut(\mathcal{H})$ that are extensions of the regular subgroups of $Aut(C)$ in narrow sense.

A subcode of the Hamming code: the Hadamard code

Let $\mathcal{H}$ denote the Hamming code of length $2^r - 1$.

The *Hadamard code* $\mathcal{A}$ is $\{x : cx^T = 0 \text{ for all } c \in \mathcal{H}\}$.

$Aut(\mathcal{A})$ is extended to $Aut(\mathcal{H})$ in narrow sense.

Proposition

$Aut(\mathcal{A}) \cong GA(r, 2)$
The regular subgroups of $Aut(\mathcal{A})$ correspond to the regular subgroups of $GA(r, 2)$ w.r.t. action on vectors of F_2^r.

A subcode of the Hamming code: the Hadamard code

Let $\mathcal{H}$ denote the Hamming code of length $2^r - 1$.

The *Hadamard code* $\mathcal{A}$ is $\{x : cx^T = 0 \text{ for all } c \in \mathcal{H}\}$.

$Aut(\mathcal{A})$ is extended to $Aut(\mathcal{H})$ in narrow sense.

Proposition

$Aut(\mathcal{A}) \cong GA(r, 2)$
The regular subgroups of $Aut(\mathcal{A})$ correspond to the regular subgroups of $GA(r, 2)$ w.r.t. action on vectors of F_2^r.

A subcode of the Hamming code: the Hadamard code

Let $\mathcal{H}$ denote the Hamming code of length $2^r - 1$.

The *Hadamard code* $\mathcal{A}$ is $\{x : cx^T = 0 \text{ for all } c \in \mathcal{H}\}$.

$Aut(\mathcal{A})$ is extended to $Aut(\mathcal{H})$ in narrow sense.

Proposition

$Aut(\mathcal{A}) \cong GA(r, 2)$
The regular subgroups of $Aut(\mathcal{A})$ correspond to the regular subgroups of $GA(r, 2)$ w.r.t. action on vectors of F_2^r.

A subcode of the Hamming code: the Hadamard code

Let $\mathcal{H}$ denote the Hamming code of length $2^r - 1$.

The *Hadamard code* $\mathcal{A}$ is $\{x : cx^T = 0 \text{ for all } c \in \mathcal{H}\}$.

$Aut(\mathcal{A})$ is extended to $Aut(\mathcal{H})$ in narrow sense.

Proposition

$Aut(\mathcal{A}) \cong GA(r, 2)$

The regular subgroups of $Aut(\mathcal{A})$ correspond to the regular subgroups of $GA(r, 2)$ w.r.t. action on vectors of F_2^r.

A subcode of the Hamming code: the Hadamard code

Let $\mathcal{H}$ denote the Hamming code of length $2^r - 1$.

The *Hadamard code* $\mathcal{A}$ is $\{x : cx^T = 0 \text{ for all } c \in \mathcal{H}\}$.

$Aut(\mathcal{A})$ is extended to $Aut(\mathcal{H})$ in narrow sense.

Proposition

$Aut(\mathcal{A}) \cong GA(r, 2)$
The regular subgroups of $Aut(\mathcal{A})$ correspond to the regular subgroups of $GA(r, 2)$ w.r.t. action on vectors of F_2^r.

A subcode of the Hamming code: the Nordstrom-Robinson code

Let $\mathcal{H}$ denote the Hamming code of length 15.

Let $\mathcal{NR}$ denote *the Nordstrom-Robinson code*[4] of length 15. The code $\mathcal{NR}$ has parameters $(15, 256, 5)$. Any code with the same parameters is equivalent to $\mathcal{NR}$ w.r.t. an automorphism[5].

The linear span of $\mathcal{NR}$ is $\mathcal{H}$[6].

[4] Nordstrom, A.W. and Robinson, J.P., An Optimum Nonlinear Code, Inform. Control, 1967, vol. 11, no. 5-6, pp. 613-616.

[5] S. L. Snover, "The uniqueness of the Nordstrom-Robinson and the Golay binary codes," Ph.D. dissertation, Math. Dep., Michigan State Univ., 1973.

[6] Semakov, N.V. and Zinoviev, V.A., Complete and Quasi-complete Balanced Codes, Probl. Peredachi Inf., 1969, vol. 5, no. 2, pp. 11–13].

A subcode of the Hamming code: the Nordstrom-Robinson code

Let $\mathcal{H}$ denote the Hamming code of length 15.

Let $\mathcal{NR}$ denote *the Nordstrom-Robinson code*[4] of length 15. The code $\mathcal{NR}$ has parameters $(15, 256, 5)$. Any code with the same parameters is equivalent to $\mathcal{NR}$ w.r.t. an automorphism[5].

The linear span of $\mathcal{NR}$ is $\mathcal{H}$[6].

[4] Nordstrom, A.W. and Robinson, J.P., An Optimum Nonlinear Code, Inform. Control, 1967, vol. 11, no. 5-6, pp. 613-616.

[5] S. L. Snover, "The uniqueness of the Nordstrom-Robinson and the Golay binary codes," Ph.D. dissertation, Math. Dep., Michigan State Univ., 1973.

[6] Semakov, N.V. and Zinoviev, V.A., Complete and Quasi-complete Balanced Codes, Probl. Peredachi Inf., 1969, vol. 5, no. 2, pp. 11-13]

A subcode of the Hamming code: the Nordstrom-Robinson code

Let $\mathcal{H}$ denote the Hamming code of length 15.

Let $\mathcal{NR}$ denote *the Nordstrom-Robinson code*[4] of length 15. The code $\mathcal{NR}$ has parameters $(15, 256, 5)$. Any code with the same parameters is equivalent to $\mathcal{NR}$ w.r.t. an automorphism[5].

The linear span of $\mathcal{NR}$ is $\mathcal{H}$[6].

[4]Nordstrom, A.W. and Robinson, J.P., An Optimum Nonlinear Code, Inform. Control, 1967, vol. 11, no. 5-6, pp. 613-616.

[5]S. L. Snover, "The uniqueness of the Nordstrom-Robinson and the Golay binary codes," Ph.D. dissertation, Math. Dep., Michigan State Univ., 1973.

[6]Semakov, N.V. and Zinoviev, V.A., Complete and Quasi-complete Balanced Codes, Probl. Peredachi Inf., 1969, vol. 5, no. 2, pp. 11-13]

A subcode of the Hamming code: the Nordstrom-Robinson code

A (15,256,5) code is $\mathcal{NR}$[4] unique up to an automorphism[5].

The linear span of $\mathcal{NR}$ is $\mathcal{H}$[6].

The Nordstrom-Robinson code is propelinear[7].

$Aut(\mathcal{NR})$ is extended to $Aut(\mathcal{H})$ in narrow sense

[4]Nordstrom, A.W. and Robinson, J.P., An Optimum Nonlinear Code, Inform. Control, 1967, vol. 11, no. 5-6, pp. 613-616.

[5]S. L. Snover, "The uniqueness of the Nordstrom-Robinson and the Golay binary codes," Ph.D. dissertation, Math. Dep., Michigan State Univ., 1973.

[6]Semakov, N.V. and Zinoviev, V.A., Complete and Quasi-complete Balanced Codes, Probl. Peredachi Inf., 1969, vol. 5, no. 2, pp. 11-13]

[7]Hammons, A. R., Jr, Kumar, P. V., Calderbank, A. R., Sloan e, N. J. A., Sole, P. The Z4-linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. Vol. 40, 2. P. 301-319.

A subcode of the Hamming code: the Nordstrom-Robinson code

A (15,256,5) code is $\mathcal{NR}$[4] unique up to an automorphism[5].

The linear span of $\mathcal{NR}$ is $\mathcal{H}$[6].

The Nordstrom-Robinson code is propelinear[7].

$Aut(\mathcal{NR})$ is extended to $Aut(\mathcal{H})$ in narrow sense

[4]Nordstrom, A.W. and Robinson, J.P., An Optimum Nonlinear Code, Inform. Control, 1967, vol. 11, no. 5-6, pp. 613-616.

[5]S. L. Snover, "The uniqueness of the Nordstrom-Robinson and the Golay binary codes," Ph.D. dissertation, Math. Dep., Michigan State Univ., 1973.

[6]Semakov, N.V. and Zinoviev, V.A., Complete and Quasi-complete Balanced Codes, Probl. Peredachi Inf., 1969, vol. 5, no. 2, pp. 11-13]

[7]Hammons, A. R., Jr, Kumar, P. V., Calderbank, A. R., Sloan e, N. J. A., Sole, P. The Z4-linearity of Kerdock, Preparata, Goethals, and related codes // IEEE Trans. Inform. Theory. 1994. Vol. 40, 2. P. 301-319.

Subcodes of the Hamming code

$\mathcal{NR}$ is a nonlinear propelinear code, $\mathcal{A}$, $\mathcal{H}$ are linear codes.

$Aut(\mathcal{NR}), Aut(\mathcal{A})$ are extended to $Aut(\mathcal{H})$ in narrow sense
$\mathcal{A} \subset \mathcal{NR}$, but $Aut(\mathcal{A}) \not\leq Aut(\mathcal{H})$

Main Results

There are 73 and 39 conjugacy classes of regular subgroups of the $Aut(\mathcal{NR})$ and $Aut(\mathcal{A})$ that fall into 45 and 11 isomorphism classes respectively.

The regular subgroups of $Aut(\mathcal{NR})$ are extended in narrow sense to 605 conjugacy classes of regular subgroups of $Aut(\mathcal{H})$, which fall into at least 219 isomorphism classes.

The regular subgroups of $Aut(\mathcal{A})$ are extended in narrow sense to 1207 conjugacy classes of regular subgroups of $Aut(\mathcal{H})$, which fall into at least 48 isomorphism classes.

[8]Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24 (1997) 235-265.

Main Results

There are 73 and 39 conjugacy classes of regular subgroups of the $Aut(\mathcal{NR})$ and $Aut(\mathcal{A})$ that fall into 45 and 11 isomorphism classes respectively.

The regular subgroups of $Aut(\mathcal{NR})$ are extended in narrow sense to 605 conjugacy classes of regular subgroups of $Aut(\mathcal{H})$, which fall into at least 219 isomorphism classes.

The regular subgroups of $Aut(\mathcal{A})$ are extended in narrow sense to 1207 conjugacy classes of regular subgroups of $Aut(\mathcal{H})$, which fall into at least 48 isomorphism classes.

[8]Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24 (1997) 235-265.

Proposition

Let C be a subcode of D.

Let G' be a regular subgroup of $Aut(C)$ that is an extension of a regular subgroup G of $Aut(D)$ in narrow sense.

Then for any $x \in G'$

$$\{c : (c, \pi) \in xG\}$$

is a translation of C.The cosets of G in G' induce a partition of C' into translations of C.

Exploit the partition into translations of the subcode in finding the extensions in narrow sense.

We need the partitions of $\mathcal{H}$ into translations of $\mathcal{NR}$.

Proposition

Let C be a subcode of D.
Let G' be a regular subgroup of $Aut(C)$ that is an extension of a regular subgroup G of $Aut(D)$ in narrow sense.
Then for any $x \in G'$

$$\{c : (c, \pi) \in xG\}$$

is a translation of C.The cosets of G in G' induce a partition of C' into translations of C.

Exploit the partition into translations of the subcode in finding the extensions in narrow sense.

We need the partitions of $\mathcal{H}$ into translations of $\mathcal{NR}$.

Proposition

Let C be a subcode of D.
Let G' be a regular subgroup of $Aut(C)$ that is an extension of a regular subgroup G of $Aut(D)$ in narrow sense.
Then for any $x \in G'$

$$\{c : (c, \pi) \in xG\}$$

is a translation of C. The cosets of G in G' induce a partition of C' into translations of C.

Exploit the partition into translations of the subcode in finding the extensions in narrow sense.

We need the partitions of $\mathcal{H}$ into translations of $\mathcal{NR}$.

Proposition

Let C be a subcode of D.
Let G' be a regular subgroup of $Aut(C)$ that is an extension of a regular subgroup G of $Aut(D)$ in narrow sense.
Then for any $x \in G'$

$$\{c : (c, \pi) \in xG\}$$

is a translation of C.The cosets of G in G' induce a partition of C' into translations of C.

Exploit the partition into translations of the subcode in finding the extensions in narrow sense.

We need the partitions of $\mathcal{H}$ into translations of $\mathcal{NR}$.

Proposition

Let C be a subcode of D.
Let G' be a regular subgroup of $Aut(C)$ that is an extension of a regular subgroup G of $Aut(D)$ in narrow sense.
Then for any $x \in G'$

$$\{c : (c, \pi) \in xG\}$$

is a translation of C.The cosets of G in G' induce a partition of C' into translations of C.

Exploit the partition into translations of the subcode in finding the extensions in narrow sense.

We need the partitions of $\mathcal{H}$ into translations of $\mathcal{NR}$.

Proposition

Let C be a subcode of D.
Let G' be a regular subgroup of $Aut(C)$ that is an extension of a regular subgroup G of $Aut(D)$ in narrow sense.
Then for any $x \in G'$

$$\{c : (c, \pi) \in xG\}$$

is a translation of C.The cosets of G in G' induce a partition of C' into translations of C.

Exploit the partition into translations of the subcode in finding the extensions in narrow sense.

We need the partitions of $\mathcal{H}$ into translations of $\mathcal{NR}$.

Characterization of partitions of $\mathcal{H}$ into translations of $\mathcal{NR}$

Theorem

$\mathcal{NR} = \mathcal{A} \cup \bigcup_{i=1,\dots,7} \mathcal{A} + a_i$.

Any partition of the Hamming code into translations of $\mathcal{NR}$ could be described as follows: for any Fano plane S on the points $\{1, \dots, 7\}$

$$\bigcup_{\{i,j,k\} \in S} (a_i + a_j + a_k + \mathcal{NR})$$

Characterization of partitions of $\mathcal{H}$ into translations of $\mathcal{NR}$

Theorem

$\mathcal{NR} = \mathcal{A} \cup \bigcup_{i=1,\dots,7} \mathcal{A} + a_i$.
Any partition of the Hamming code into translations of $\mathcal{NR}$ could be described as follows: for any Fano plane S on the points $\{1, \dots, 7\}$

$$\bigcup_{\{i,j,k\} \in S} (a_i + a_j + a_k + \mathcal{NR})$$

THANK YOU FOR YOUR ATTENTION