Existence of transitive nonpropelinear perfect codes

I.Yu. Mogilnykh, F.I. Solov'eva

Novosibirsk State University
Sobolev Institute of Mathematics

Presented at the 14th International Workshop on Algebraic and Combinatorial Coding Theory
07-13.09.2014, Svetlogorsk, Russia

Perfect codes

A code with minimum distance 3 is called *perfect* (sometimes called 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 called *perfect* (sometimes called 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 the Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

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

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

Theorem

The group of automorphisms of F_2^n with respect to $\cdot$ 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 the Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

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

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

Theorem

The group of automorphisms of F_2^n with respect to $\cdot$ 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 the Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

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

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

Theorem

The group of automorphisms of F_2^n with respect to $\cdot$ 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 the Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

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

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

Theorem

The group of automorphisms of F_2^n with respect to $\cdot$ 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 the Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

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

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

Theorem

The group of automorphisms of F_2^n with respect to $\cdot$ 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 the Hamming space.
Let $\pi \in Sym(n)$ and $x \in F_2^n$.
Consider the transformation (x, π) of F_2^n:

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

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

Theorem

The group of automorphisms of F_2^n with respect to $\cdot$ 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 $Aut(C)$.

Transitive and propelinear codes

A code C is called *transitive* if there is a group $G < Aut(C)$ transitively acting on the codewords of C, i.e.

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

[Rifa, Phelps, 2002], original definition by [Rifa, Huguet, Bassart, 1989]

A code C is called *propelinear* if there is a subgroup $G < Aut(C)$ acting sharply transitive (regularly) on the codewords, i.e.

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

Transitive and propelinear codes

A code C is called *transitive* if there is a group $G < Aut(C)$ transitively acting on the codewords of C, i.e.

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

[Rifa, Phelps, 2002], original definition by [Rifa, Huguet, Bassart, 1989]

A code C is called *propelinear* if there is a subgroup $G < Aut(C)$ acting sharply transitive (regularly) on the codewords, i.e.

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

Propelinear perfect codes: existence

Linear codes [Hamming, 1949]

$Z_2 Z_4$ - linear perfect codes [Rifa, Pujol, 1999], Z_4 - linear perfect codes [Krotov, 2000]

Transitive Malyugin perfect codes of length 15, i.e. 1-step switchings of the Hamming code are propelinear [Borges, Mogilnykh, Rifa, S., 2012]

Vasil'ev and Mollard can be used to construct propelinear perfect codes [Borges, Mogilnykh, Rifa, S., 2012]

Potapov transitive extended perfect codes are propelinear [Borges, Mogilnykh, Rifa, S., 2013]

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

Problem statement

Does there exist a transitive nonpropelinear *perfect* code?

Transitive nonpropelinear perfect code of length 15: algebraic property

Proposition

There is a unique transitive nonpropelinear perfect code C of length 15.

Nonpropelinearity (The main key):

We cannot correctly define g^{-1} for some $g \in G$ (*incorrect inversion*): both g and g^{-1} send a codeword x to a codeword y.

Transitive nonpropelinear perfect code of length 15: algebraic property

Proposition

There is a unique transitive nonpropelinear perfect code C of length 15.

Nonpropelinearity (The main key):

We cannot correctly define g^{-1} for some $g \in G$ (*incorrect inversion*): both g and g^{-1} send a codeword x to a codeword y.

Transitive nonpropelinear perfect code of length 15: algebraic property

Proposition

There is a unique transitive nonpropelinear perfect code C of length 15.

Nonpropelinearity (The main key):

We cannot correctly define g^{-1} for some $g \in G$ (*incorrect inversion*): both g and g^{-1} send a codeword x to a codeword y.

Invariants for transitive perfect codes

$Ker(C) = \{k \in F_2^n : k + C = C\}$,
$Rank(C) = dim(< C >)$.
Denote by $\mu_i(C) = |\{Ker(C) \cap \Delta : \Delta \in STS(C), i \in \Delta\}|$,
$\mu(C) = \{*\mu_i(C) : i \in \{1, \ldots, n\}*\}$.

Invariants for transitive perfect codes

$Ker(C) = \{k \in F_2^n : k + C = C\}$,
$Rank(C) = dim(< C >)$.
Denote by $\mu_i(C) = |\{Ker(C) \cap \Delta : \Delta \in STS(C), i \in \Delta\}|$,
$\mu(C) = \{*\mu_i(C) : i \in \{1, \dots, n\}*\}$.

Invariants for transitive perfect codes

$Ker(C) = \{k \in F_2^n : k + C = C\}$,
$Rank(C) = dim(< C >)$.
Denote by $\mu_i(C) = |\{Ker(C) \cap \Delta : \Delta \in STS(C), i \in \Delta\}|$,
$\mu(C) = \{*\mu_i(C) : i \in \{1, \dots, n\}*\}$.

Invariants for transitive perfect codes

$Ker(C) = \{k \in F_2^n : k + C = C\}$,
$Rank(C) = dim(< C >)$.
Denote by $\mu_i(C) = |\{Ker(C) \cap \Delta : \Delta \in STS(C), i \in \Delta\}|$,
$\mu(C) = \{*\mu_i(C) : i \in \{1, \ldots, n\}*\}$.

Transitive nonpropelinear perfect code of length 15: a characterization via $\mu(C)$

Proposition(PC search)

The transitive nonpropelinear perfect code of length 15 is a unique transitive code with the property that $\mu(C) = 0^{15}$.

Invariants for transitive perfect codes

$$\mu_i(C) = |\{Ker(C) \cap \Delta : \Delta \in STS(C), i \in \Delta\}|,$$
$$\mu(C) = \{*\mu_i(C) : i \in \{1, \ldots, n\}*\}.$$

Some transitive perfect codes of length 15

Code number in Ostergard and Pottonen classification	Rank(C)	Dim(Ker(C))	$\lvert\mathrm{Sym}(C)\rvert$	$\mu(C)$	$\lvert\mathrm{Aut}(\mathrm{STS}(C))\rvert$
the Hamming code	11	11	20160	7^{15}	20160
51	13	7	8	$1^{13}3^{1}5^{1}$	8
694	13	8	32	$1^{8}3^{5}5^{2}$	32
724	13	8	32	$1^{13}3^{1}5^{1}$	96
771	13	8	96	$1^{12}3^{3}$	288
4918	14	6	4	$\mathbf{0}^{15}$	4

Main result

Theorem

1. There is exactly one transitive nonpropelinear perfect code among 201 transitive codes of length 15.

2. There is at least 1 transitive nonpropelinear perfect code of length $2^r - 1, 7 \geq r \geq 5$.

3. There are at least 5 pairwise inequivalent (up to transformation from $Aut(F_2^n)$) codes for length $2^r - 1, r \geq 8$.

Main result

Theorem

1. There is exactly one transitive nonpropelinear perfect code among 201 transitive codes of length 15.
2. There is at least 1 transitive nonpropelinear perfect code of length $2^r - 1, 7 \geq r \geq 5$.
3. There are at least 5 pairwise inequivalent (up to transformation from $Aut(F_2^n)$) codes for length $2^r - 1, r \geq 8$.

Main result

Theorem

1. There is exactly one transitive nonpropelinear perfect code among 201 transitive codes of length 15.
2. There is at least 1 transitive nonpropelinear perfect code of length $2^r - 1, 7 \geq r \geq 5$.
3. There are at least 5 pairwise inequivalent (up to transformation from $Aut(F_2^n)$) codes for length $2^r - 1, r \geq 8$.

Main result

Theorem

1. There is exactly one transitive nonpropelinear perfect code among 201 transitive codes of length 15.
2. There is at least 1 transitive nonpropelinear perfect code of length $2^r - 1, 7 \geq r \geq 5$.
3. There are at least 5 pairwise inequivalent (up to transformation from $Aut(F_2^n)$) codes for length $2^r - 1, r \geq 8$.

Keys to the proof

S., 2005

If C and D are transitive then $M(C,D)$ is transitive.

Borges, Mogilnykh, Rifa, S., 2012

If C and D are propelinear then $M(C,D)$ is propelinear.

Idea

C is a unique transitive nonpropelinear code of length 15, $\mu(C) = 0^{15}$.
Take a transitive code D: $\mu(D)$ does not contain 0, e.g. D is the Hamming code.
Then the Mollard code $M(C,D)$ is *transitive* and $Stab_{D_2}Sym(M(C,D)) = Sym(M(C,D))$. $M(C,D)$ is a *nonpropelinear code*, since it fulfills *incorrect inversion property*.

Keys to the proof

S., 2005

If C and D are transitive then $M(C,D)$ is transitive.

Borges, Mogilnykh, Rifa, S., 2012

If C and D are propelinear then $M(C,D)$ is propelinear.

Idea

C is a unique transitive nonpropelinear code of length 15, $\mu(C) = 0^{15}$.
Take a transitive code D: $\mu(D)$ does not contain 0, e.g. D is the Hamming code.
Then the Mollard code $M(C,D)$ is *transitive* and $Stab_{D_2}Sym(M(C,D)) = Sym(M(C,D))$. $M(C,D)$ is a *nonpropelinear code*, since it fulfills *incorrect inversion property*.

Keys to the proof

S., 2005

If C and D are transitive then $M(C, D)$ is transitive.

Borges, Mogilnykh, Rifa, S., 2012

If C and D are propelinear then $M(C, D)$ is propelinear.

Idea

C is a unique transitive nonpropelinear code of length 15, $\mu(C) = 0^{15}$.
Take a transitive code D: $\mu(D)$ does not contain 0, e.g. D is the Hamming code.
Then the Mollard code $M(C, D)$ is *transitive* and $Stab_{D_2}Sym(M(C, D)) = Sym(M(C, D))$. $M(C, D)$ is a *nonpropelinear code*, since it fulfills *incorrect inversion property*.

Keys to the proof

S., 2005

If C and D are transitive then $M(C, D)$ is transitive.

Borges, Mogilnykh, Rifa, S., 2012

If C and D are propelinear then $M(C, D)$ is propelinear.

Idea

C is a unique transitive nonpropelinear code of length 15, $\mu(C) = 0^{15}$.
Take a transitive code D: $\mu(D)$ does not contain 0, e.g. D is the Hamming code.
Then the Mollard code $M(C, D)$ is *transitive* and $Stab_{D_2} Sym(M(C, D)) = Sym(M(C, D))$. $M(C, D)$ is a *nonpropelinear code*, since it fulfills *incorrect inversion property*.

Keys to the proof

S., 2005

If C and D are transitive then $M(C, D)$ is transitive.

Borges, Mogilnykh, Rifa, S., 2012

If C and D are propelinear then $M(C, D)$ is propelinear.

Idea

C is a unique transitive nonpropelinear code of length 15, $\mu(C) = 0^{15}$.
Take a transitive code D: $\mu(D)$ does not contain 0, e.g. D is the Hamming code.
Then the Mollard code $M(C, D)$ is *transitive* and $Stab_{D_2}Sym(M(C, D)) = Sym(M(C, D))$. $M(C, D)$ is a *nonpropelinear code*, since it fulfills *incorrect inversion property*.

Keys to the proof

S., 2005

If C and D are transitive then $M(C,D)$ is transitive.

Borges, Mogilnykh, Rifa, S., 2012

If C and D are propelinear then $M(C,D)$ is propelinear.

Idea

C is a unique transitive nonpropelinear code of length 15, $\mu(C) = 0^{15}$.
Take a transitive code D: $\mu(D)$ does not contain 0, e.g. D is the Hamming code.
Then the Mollard code $M(C,D)$ is *transitive* and $Stab_{D_2}Sym(M(C,D)) = Sym(M(C,D))$. $M(C,D)$ is a *nonpropelinear code*, since it fulfills *incorrect inversion property*.

Keys to the proof

S., 2005

If C and D are transitive then $M(C,D)$ is transitive.

Borges, Mogilnykh, Rifa, S., 2012

If C and D are propelinear then $M(C,D)$ is propelinear.

Idea

C is a unique transitive nonpropelinear code of length 15, $\mu(C) = 0^{15}$.
Take a transitive code D: $\mu(D)$ does not contain 0, e.g. D is the Hamming code.
Then the Mollard code $M(C,D)$ is *transitive* and $Stab_{D_2} Sym(M(C,D)) = Sym(M(C,D))$. $M(C,D)$ is a *nonpropelinear code*, since it fulfills *incorrect inversion property*.

Keys to the proof

S., 2005

If C and D are transitive then $M(C,D)$ is transitive.

Borges, Mogilnykh, Rifa, S., 2012

If C and D are propelinear then $M(C,D)$ is propelinear.

Idea

C is a unique transitive nonpropelinear code of length 15, $\mu(C) = 0^{15}$.
Take a transitive code D: $\mu(D)$ does not contain 0, e.g. D is the Hamming code.
Then the Mollard code $M(C,D)$ is *transitive* and $Stab_{D_2}Sym(M(C,D)) = Sym(M(C,D))$. $M(C,D)$ is a *nonpropelinear code*, since it fulfills *incorrect inversion property*.

THANK YOU FOR YOUR ATTENTION