Linear coordinates for perfect codes and Steiner triple systems

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

Sobolev Institute of Mathematics,
Novosibirsk State University

Presented at ALCOMA-2015
March 15 - 20, 2015, Kloster Banz, Germany

Perfect codes and Steiner triple systems

A *perfect code* of length n with the minimum distance 3 is a collection of binary vectors of length n such that any binary vector is at distance at most 1 from some codeword.

Remark: Further all codes contain the all-zero vector.

A Steiner triple system A STS is a collection of blocks (subsets) of size 3 of the n-element point set $P(S)$, such that any pair of distinct elements is exactly in one block.

STS of a perfect code we denote by $STS(C)$.

Perfect codes and Steiner triple systems

A *perfect code* of length n with the minimum distance 3 is a collection of binary vectors of length n such that any binary vector is at distance at most 1 from some codeword.
Remark: Further all codes contain the all-zero vector.

A Steiner triple system A STS is a collection of blocks (subsets) of size 3 of the n-element point set $P(S)$, such that any pair of distinct elements is exactly in one block.

STS of a perfect code we denote by $STS(C)$.

Perfect codes and Steiner triple systems

A *perfect code* of length n with the minimum distance 3 is a collection of binary vectors of length n such that any binary vector is at distance at most 1 from some codeword.
Remark: Further all codes contain the all-zero vector.

A Steiner triple system A STS is a collection of blocks (subsets) of size 3 of the n-element point set $P(S)$, such that any pair of distinct elements is exactly in one block.

STS of a perfect code we denote by $STS(C)$.

Perfect codes and Steiner triple systems

A *perfect code* of length n with the minimum distance 3 is a collection of binary vectors of length n such that any binary vector is at distance at most 1 from some codeword.
Remark: Further all codes contain the all-zero vector.

A Steiner triple system A STS is a collection of blocks (subsets) of size 3 of the n-element point set $P(S)$, such that any pair of distinct elements is exactly in one block.

STS of a perfect code we denote by $STS(C)$.

Steiner quasigroup

Let S be STS on the point set $P(S) = \{1, \ldots, n\}$.

For $x, y \in \{1, \ldots, n\}$ define an operation $\cdot$ as
$i \cdot j = k$, if (i, j, k) is a triple of S,
$i \cdot i = i$.

Then $(P(S), \cdot)$ is *the Steiner quasigroup* associated with S.

Steiner quasigroup

Let S be STS on the point set $P(S) = \{1, \dots, n\}$.

For $x, y \in \{1, \dots, n\}$ define an operation $\cdot$ as
$i \cdot j = k$, if (i, j, k) is a triple of S,
$i \cdot i = i$.

Then $(P(S), \cdot)$ is *the Steiner quasigroup* associated with S.

Steiner quasigroup

Let S be STS on the point set $P(S) = \{1, \ldots, n\}$.

For $x, y \in \{1, \ldots, n\}$ define an operation $\cdot$ as
$i \cdot j = k$, if (i, j, k) is a triple of S,
$i \cdot i = i$.

Then $(P(S), \cdot)$ is *the Steiner quasigroup* associated with S.

ν-linearity and Pasch configurations

For a STS S on points $\{1,\dots,n\}$ and $i\in\{1,\dots,n\}$, define $\nu_i(S)$ to be the number of different *Pasch configurations*, incident to i, i.e. the collection of triples $\{(i,j,k),(i,j_1,k_1),(i_1 j,j_1),(i_1,k,k_1)\}$.

We say that a point $i\in\{1,\dots,n\}$ is ν-*linear* for a STS S of order n if $\nu_i(S)$ takes the maximal possible value, i.e. $(n-1)(n-3)/4$.

ν-linearity and Pasch configurations

For a STS S on points $\{1, \ldots, n\}$ and $i \in \{1, \ldots, n\}$, define $\nu_i(S)$ to be the number of different *Pasch configurations*, incident to i, i.e. the collection of triples $\{(i, j, k), (i, j_1, k_1), (i_1 j, j_1), (i_1, k, k_1)\}$.

We say that a point $i \in \{1, \ldots, n\}$ is ν-*linear* for a STS S of order n if $\nu_i(S)$ takes the maximal possible value, i.e. $(n-1)(n-3)/4$.

The symmetry group of a code

$Ker(C) = \{k \in C : k + C = C\}$ is *the kernel* of a code C.

For a coordinate position i we define $\mu_i(C)$ to be the number of a perfect code C triples, containing i from $Ker(C)$ of the code C: $\mu_i(C) = |\{x \in \mathrm{STS}(C) \cap \mathrm{Ker}(C) : i \in supp(x)\}|$.

The symmetry group of a code

$Ker(C) = \{k \in C : k + C = C\}$ is *the kernel* of a code C.

For a coordinate position i we define $\mu_i(C)$ to be the number of a perfect code C triples, containing i from $Ker(C)$ of the code C: $\mu_i(C) = |\{x \in \mathrm{STS}(C) \cap \mathrm{Ker}(C) : i \in supp(x)\}|$.

μ-linearity

We say that a coordinate i is μ-*linear* for a code C of length n if $\mu_i(C)$ takes the maximal possible value, i.e. $(n-1)/2$.

Obviously, two coordinate positions i, j of S or C are in different orbits by symmetry groups of S or C respectively if $\nu_i(S) \neq \nu_j(S)$ or $\mu_i(C) \neq \mu_j(C)$ respectively.

μ-linearity

We say that a coordinate i is μ-*linear* for a code C of length n if $\mu_i(C)$ takes the maximal possible value, i.e. $(n-1)/2$.

Obviously, two coordinate positions i, j of S or C are in different orbits by symmetry groups of S or C respectively if $\nu_i(S) \neq \nu_j(S)$ or $\mu_i(C) \neq \mu_j(C)$ respectively.

The symmetry group of a code

Given a code C on the coordinate positions $\{1, \ldots, n\}$, define its *symmetry group* $Sym(C) = \{\pi \in S_n : \pi(C) = C\}$.

Hamming code

A linear (over F_2) perfect code is called *a Hamming code*.

Given codes C and D if $dim(Ker(C)) \neq dim(Ker(D))$ then C and D are inequivalent (up to an element of $Sym(n)$).

A STS S of order n is called *projective* if $STS(C) = S$ for a Hamming code C.

Hamming code

A linear (over F_2) perfect code is called *a Hamming code*.

Given codes C and D if $dim(Ker(C)) \neq dim(Ker(D))$ then C and D are inequivalent (up to an element of $Sym(n)$).

A STS S of order n is called *projective* if $STS(C) = S$ for a Hamming code C.

Hamming code

A linear (over F_2) perfect code is called *a Hamming code*.

Given codes C and D if $dim(Ker(C)) \neq dim(Ker(D))$ then C and D are inequivalent (up to an element of $Sym(n)$).

A STS S of order n is called *projective* if $STS(C) = S$ for a Hamming code C.

Linear coordinates of a perfect code and STS

By $Lin_\nu(S)$ and $Lin_\mu(C)$ we denote the sets of ν-linear coordinates of S and μ-linear coordinates of C respectively.

$Lin_\nu(S)$ and $Lin_\mu(C)$ are characteristics of a proximity of a STS S and a perfect code C to projective STS and the Hamming code respectively.

Linear coordinates of a Steiner triple system

Property

A perfect code C of length n is Hamming iff $Lin_\mu(C) = \{1, \dots, n\}$

Property

A STS S on n points is projective iff $Lin_\nu(S) = \{1, \dots, n\}$.

Linear coordinates of a Steiner triple system

Property

A perfect code C of length n is Hamming iff $Lin_{\mu}(C) = \{1, \ldots, n\}$

Property

A STS S on n points is projective iff $Lin_{\nu}(S) = \{1, \ldots, n\}$.

Theorem

1. Let C be a perfect code. Then we have $Lin_{\mu}(C) \subseteq Lin_{\nu}(STS(C))$.
2. A subdesign of a STS S on the points $Lin_{\nu}(S)$ is projective.
3. A subcode of a perfect code C on the coordinates $Lin_{\mu}(C)$ is a Hamming code.

Theorem

1. Let C be a perfect code. Then we have $Lin_\mu(C) \subseteq Lin_\nu(STS(C))$.
2. A subdesign of a STS S on the points $Lin_\nu(S)$ is projective.
3. A subcode of a perfect code C on the coordinates $Lin_\mu(C)$ is a Hamming code.

Theorem

1. Let C be a perfect code. Then we have $Lin_{\mu}(C) \subseteq Lin_{\nu}(STS(C))$.
2. A subdesign of a STS S on the points $Lin_{\nu}(S)$ is projective.
3. A subcode of a perfect code C on the coordinates $Lin_{\mu}(C)$ is a Hamming code.

These two characteristics for perfect codes and Steiner triple systems allowed us to investigate the symmetry group of certain Mollard codes and solve the problem of the existence of transitive nonpropeliner perfect codes.

Mollard code

Let C and D be two codes of lengths t and m.

The coordinate positions of the Mollard code $M(C,D)$ are $\{(r,s) : r \in \{0,\dots,t\}, s \in \{0,\dots,m\}\} \setminus (0,0)$.

For $z \in F_2^{tm+t+m}$ with the coordinates indexed by elements of $\{(r,s) : r \in \{0,\dots,t\}, s \in \{0,\dots,m\}\} \setminus (0,0)$ define

$$p_1(z) = (\sum_{s=0}^{m} z_{1,s}, \dots, \sum_{s=0}^{m} z_{t,s}),$$

$$p_2(z) = (\sum_{r=0}^{t} z_{r,1}, \dots, \sum_{r=0}^{t} z_{r,m}).$$

The *Mollard code* (with all-zero function) $M(C,D)$ is $\{z \in F_2^{tm+t+m} : p_1(z) \in C, p_2(z) \in D\}$.

Mollard code

Let C and D be two codes of lengths t and m.
The coordinate positions of the Mollard code $M(C,D)$ are $\{(r,s) : r \in \{0,\ldots,t\}, s \in \{0,\ldots,m\}\} \setminus (0,0)$.

For $z \in F_2^{tm+t+m}$ with the coordinates indexed by elements of $\{(r,s) : r \in \{0,\ldots,t\}, s \in \{0,\ldots,m\}\} \setminus (0,0)$ define

$$p_1(z) = (\sum_{s=0}^{m} z_{1,s}, \ldots, \sum_{s=0}^{m} z_{t,s}),$$

$$p_2(z) = (\sum_{r=0}^{t} z_{r,1}, \ldots, \sum_{r=0}^{t} z_{r,m}).$$

The *Mollard code* (with all-zero function) $M(C,D)$ is $\{z \in F_2^{tm+t+m} : p_1(z) \in C, p_2(z) \in D\}$.

Mollard code

Let C and D be two codes of lengths t and m.
The coordinate positions of the Mollard code $M(C,D)$ are $\{(r,s) : r \in \{0,\dots,t\}, s \in \{0,\dots,m\}\} \setminus (0,0)$.

For $z \in F_2^{tm+t+m}$ with the coordinates indexed by elements of $\{(r,s) : r \in \{0,\dots,t\}, s \in \{0,\dots,m\}\} \setminus (0,0)$ define

$$p_1(z) = (\sum_{s=0}^{m} z_{1,s}, \dots, \sum_{s=0}^{m} z_{t,s}),$$

$$p_2(z) = (\sum_{r=0}^{t} z_{r,1}, \dots, \sum_{r=0}^{t} z_{r,m}).$$

The *Mollard code* (with all-zero function) $M(C,D)$ is $\{z \in F_2^{tm+t+m} : p_1(z) \in C, p_2(z) \in D\}$.

Mollard code

Let C and D be two codes of lengths t and m.
The coordinate positions of the Mollard code $M(C,D)$ are $\{(r,s) : r \in \{0,\dots,t\}, s \in \{0,\dots,m\}\} \setminus (0,0)$.

For $z \in F_2^{tm+t+m}$ with the coordinates indexed by elements of $\{(r,s) : r \in \{0,\dots,t\}, s \in \{0,\dots,m\}\} \setminus (0,0)$ define

$$p_1(z) = (\sum_{s=0}^{m} z_{1,s}, \dots, \sum_{s=0}^{m} z_{t,s}),$$

$$p_2(z) = (\sum_{r=0}^{t} z_{r,1}, \dots, \sum_{r=0}^{t} z_{r,m}).$$

The *Mollard code* (with all-zero function) $M(C,D)$ is $\{z \in F_2^{tm+t+m} : p_1(z) \in C, p_2(z) \in D\}$.

Perfect Mollard code

Property

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

Subcodes of Mollard code

For $x \in C$ define $x^1 \in M(C,D)$: $x^1_{r,0} = x_r$, $x^1_{r,s} = 0$ otherwise.
For $y \in D$ define $y^2 \in M(C,D)$: $y^1_{0,s} = y_s$, $y^1_{r,s} = 0$ otherwise.

$C^1 = \{x^1 : x \in C\}$, $D^2 = \{y^2 : y \in D\}$ are subcodes of $M(C,D)$ isomorphic to C and D respectively.

Subcodes of Mollard code

For $x \in C$ define $x^1 \in M(C, D)$: $x^1_{r,0} = x_r$, $x^1_{r,s} = 0$ otherwise.
For $y \in D$ define $y^2 \in M(C, D)$: $y^1_{0,s} = y_s$, $y^1_{r,s} = 0$ otherwise.

$C^1 = \{x^1 : x \in C\}$, $D^2 = \{y^2 : y \in D\}$ are subcodes of $M(C, D)$ isomorphic to C and D respectively.

Problem statement

Describe $Stab_{D^2}Sym(M(C,D))$.

Avgustinovich, Heden, Solov'eva, 2005

Description is obtained for $Stab_{n+1}Sym(V(C))$, where $V(C)$ is the Vasiliev code applied to C with the zero function.

Problem statement

Describe $Stab_{D^2}Sym(M(C, D))$.

Avgustinovich, Heden, Solov'eva, 2005

Description is obtained for $Stab_{n+1}Sym(V(C))$, where $V(C)$ is the Vasiliev code applied to C with the zero function.

Main results

Theorem

Let C and D be two reduced perfect codes. Then

$$Stab_{D^2}(Sym(M(C,D))) =$$
$$(\mathcal{D}ub_1(Sym(C)) \leftthreetimes < Ort_{Lin_\mu(D)}(C^\perp) >) \times \mathcal{D}ub_2(Sym(D)).$$

Theorem

Let S_1 and S_2 be two STS (Steiner triple system treated as STS with all-zero vector). Then $Stab_{S_2^2}(Sym(M(S_1,S_2))) =$

$$(\mathcal{D}ub_1(Sym(S_1)) \leftthreetimes < Ort_{Lin_\nu(S_2)}(S_1^\perp) >) \times \mathcal{D}ub_2(Sym(S_2)).$$

I. Yu. Mogilnykh, F. I. Solov'eva, On symmetry group of Mollard code, submitted to Electronic Journal of Combin.

Main results

Theorem

Let C and D be two reduced perfect codes. Then

$$Stab_{D^2}(Sym(M(C,D))) =$$
$$(\mathcal{D}ub_1(Sym(C)) \leftthreetimes < Ort_{Lin_\mu(D)}(C^\perp) >) \times \mathcal{D}ub_2(Sym(D)).$$

Theorem

Let S_1 and S_2 be two STS (Steiner triple system treated as STS with all-zero vector). Then $Stab_{S_2^2}(Sym(M(S_1,S_2))) =$

$$(\mathcal{D}ub_1(Sym(S_1)) \leftthreetimes < Ort_{Lin_\nu(S_2)}(S_1^\perp) >) \times \mathcal{D}ub_2(Sym(S_2)).$$

I. Yu. Mogilnykh, F. I. Solov'eva, On symmetry group of Mollard code, submitted to Electronic Journal of Combin.

The automorphism group of the code

An automorphism of F_2^n is an isometry of the Hamming space.
Let $\pi \in S_n$ 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 $(\{(x, \pi) : x \in F_2^n, \pi \in S_n\}, \cdot)$

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 $\pi \in S_n$ 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 $(\{(x, \pi) : x \in F_2^n, \pi \in S_n\}, \cdot)$

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 $\pi \in S_n$ 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 $(\{(x, \pi) : x \in F_2^n, \pi \in S_n\}, \cdot)$

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 $\pi \in S_n$ 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
$(\{(x, \pi) : x \in F_2^n, \pi \in S_n\}, \cdot)$

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 $\pi \in S_n$ 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
$(\{(x, \pi) : x \in F_2^n, \pi \in S_n\}, \cdot)$

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.

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

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.

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

[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: 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 $2^r - 1, r \geq 8$.

See the details in

I. Yu. Mogilnykh, F. I. Solov'eva, Transitive propelinear perfect codes, Discrete Mathematics. 2015. V. 338. P. 174–182.

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 $2^r - 1, r \geq 8$.

See the details in

I. Yu. Mogilnykh, F. I. Solov'eva, Transitive propelinear perfect codes, Discrete Mathematics. 2015. V. 338. P. 174–182.

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 $2^r - 1, r \geq 8$.

See the details in
I. Yu. Mogilnykh, F. I. Solov'eva, Transitive propelinear perfect codes, Discrete Mathematics. 2015. V. 338. P. 174–182.

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 $2^r - 1, r \geq 8$.

See the details in

I. Yu. Mogilnykh, F. I. Solov'eva, Transitive propelinear perfect codes, Discrete Mathematics. 2015. V. 338. P. 174–182.

THANK YOU FOR YOUR ATTENTION