Separability of homogeneous perfect codes from transitive

Ivan Yu. Mogilnykh, Faina I. Solov'eva

Novosibirsk State University
Sobolev Institute of Mathematics

Presented at the 15th International Workshop on Algebraic and Combinatorial Coding Theory
18-24.06.2016, Albena, Bulgaria

Definitions

The automorphism group (the isometry group) $\mathrm{Aut}(GF(2^m))$ of the binary vector space $GF(2^m)$ with respect to the Hamming metric is the group of all transformations (x, π) fixing $GF(2^m)$ with respect to the composition

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

The automorphism group $\mathrm{Aut}(C)$ of a binary code C is the setwise stabilizer of C in $\mathrm{Aut}(GF(2^m))$.

The symmetry group $\mathrm{Sym}(C)$ of a code C is defined as $\mathrm{Sym}(C) = \{\pi \in S_n : \pi(C) = C\}$.

Definitions

The automorphism group (the isometry group) $\mathrm{Aut}(GF(2^m))$ of the binary vector space $GF(2^m)$ with respect to the Hamming metric is the group of all transformations (x,π) fixing $GF(2^m)$ with respect to the composition

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

The automorphism group $\mathrm{Aut}(C)$ of a binary code C is the setwise stabilizer of C in $\mathrm{Aut}(GF(2^m))$.

The symmetry group $\mathrm{Sym}(C)$ of a code C is defined as $\mathrm{Sym}(C)=\{\pi\in S_n:\pi(C)=C\}$.

Definitions

The automorphism group (the isometry group) $\mathrm{Aut}(GF(2^m))$ of the binary vector space $GF(2^m)$ with respect to the Hamming metric is the group of all transformations (x, π) fixing $GF(2^m)$ with respect to the composition

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

The automorphism group $\mathrm{Aut}(C)$ of a binary code C is the setwise stabilizer of C in $\mathrm{Aut}(GF(2^m))$.

The symmetry group $\mathrm{Sym}(C)$ of a code C is defined as $\mathrm{Sym}(C) = \{\pi \in S_n : \pi(C) = C\}$.

Definitions, transitive and propelinear codes

A code C is called *transitive* if there is a subgroup H of $\mathrm{Aut}(C)$ acting transitively on the codewords of C.

If we additionally require that for any $x, y \in C$, $x \neq y$ there is a unique element h of H such that $h(x) = y$, then H acting on C is called a *regular group* [Phelps, Rifa, 2002] and the code C is called *propelinear* (for the original definition see [Rifa, Basart and Huguet, 1989])

Definitions, transitive and propelinear codes

A code C is called *transitive* if there is a subgroup H of $\mathrm{Aut}(C)$ acting transitively on the codewords of C.

If we additionally require that for any $x, y \in C$, $x \neq y$ there is a unique element h of H such that $h(x) = y$, then H acting on C is called a *regular group* [Phelps, Rifa, 2002] and the code C is called *propelinear* (for the original definition see [Rifa, Basart and Huguet, 1989])

Definitions, propelinear codes

In this case the order of H is equal to the size of C.

Each regular subgroup $H < \mathrm{Aut}(C)$ naturally induces a group operation on the codewords of C defined in the following way: $x * y := h_x(y)$, such that the codewords of C form a group with respect to the operation $*$, isomorphic to H: $(C, *) \cong H$, which is called a *propelinear structure* on C.

Definitions, propelinear codes

In this case the order of H is equal to the size of C.

Each regular subgroup $H < \mathrm{Aut}(C)$ naturally induces a group operation on the codewords of C defined in the following way: $x * y := h_x(y)$, such that the codewords of C form a group with respect to the operation $*$, isomorphic to H: $(C, *) \cong H$, which is called a *propelinear structure* on C.

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.

Steiner triple systems and perfect codes

Recall that a *Steiner triple system* (briefly STS) is a collection of blocks (subsets) of size 3 of an n-element set such that any unordered pair of distinct elements is exactly in one block.

The set of codewords of weight 3 of a perfect code C that contains the all-zero word is a Steiner triple system, which we denote by $\mathrm{STS}(C)$.

Steiner triple systems and perfect codes

Recall that a *Steiner triple system* (briefly STS) is a collection of blocks (subsets) of size 3 of an n-element set such that any unordered pair of distinct elements is exactly in one block.

The set of codewords of weight 3 of a perfect code C that contains the all-zero word is a Steiner triple system, which we denote by $\mathrm{STS}(C)$.

Steiner triple systems and perfect codes

The set $supp(x) = \{i : x_i = 1\}$ is called the *support* of the vector x. The set $\{supp(x + y) : x \in C, d(x, y) = 3\}$ for a codeword $y \in C$ we denote by $STS(C, y)$.

A code C is called *homogeneous* if for any codeword $y \in C$ the system $\mathrm{STS}(C, y)$ is isomorphic to $\mathrm{STS}(C, 0^n)$, i.e. there exists a permutation $\pi \in S_n$ such that $\pi(STS(C, y)) = STS(C, 0^n)$. It is easy to see that any transitive code is homogeneous.

Steiner triple systems and perfect codes

The set $supp(x) = \{i : x_i = 1\}$ is called the *support* of the vector x. The set $\{supp(x + y) : x \in C, d(x, y) = 3\}$ for a codeword $y \in C$ we denote by $STS(C, y)$.

A code C is called *homogeneous* if for any codeword $y \in C$ the system $\mathrm{STS}(C, y)$ is isomorphic to $\mathrm{STS}(C, 0^n)$, i.e. there exists a permutation $\pi \in S_n$ such that $\pi(STS(C, y)) = STS(C, 0^n)$. It is easy to see that any transitive code is homogeneous.

Propelinear perfect codes: existence

Linear codes [Hamming, 1949]

Z_2Z_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]

Propelinear perfect codes: existence

Linear codes [Hamming, 1949]

Z_2Z_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]

Propelinear perfect codes: existence

Linear codes [Hamming, 1949]
Z_2Z_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]

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]

Propelinear perfect codes: existence

Linear codes [Hamming, 1949]

Z_2Z_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]

Propelinear perfect codes: existence

Linear codes [Hamming, 1949]
Z_2Z_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]

Transitive nonropelinear perfect codes: existence

Theorem [Mogilnykh, S., 2014]

For any admissible length there exist transitive nonpropelinear perfect codes.

Problem statement

Does there exist a *homogenious nontransitive perfect* code?

More definitions

The dimension of the linear span of a code C is called its *rank*.

Define the *translator* $Tr(C)$ of a code C:

$$\mathrm{Tr}(C) = \{y \in C \mid \exists \pi \in S_n : (y, \pi) \in \mathrm{Aut}(C)\}.$$

The linear span over codewords of weight 3 of a code C of length n containing i, $i \in \{1, 2, \ldots, n\}$ is called the *linear i-component* (in what follows *i-component*) and denoted R_i^n. If C is the Hamming code of length n than R_i^n is its linear subcode.

More definitions

The dimension of the linear span of a code C is called its *rank*.

Define the *translator* $Tr(C)$ of a code C:

$$\mathrm{Tr}(C) = \{y \in C \mid \exists \pi \in S_n : (y, \pi) \in \mathrm{Aut}(C)\}.$$

The linear span over codewords of weight 3 of a code C of length n containing i, $i \in \{1, 2, \dots, n\}$ is called the *linear i-component* (in what follows *i-component*) and denoted R_i^n. If C is the Hamming code of length n than R_i^n is its linear subcode.

More definitions

The dimension of the linear span of a code C is called its *rank*.

Define the *translator* $Tr(C)$ of a code C:

$$\mathrm{Tr}(C) = \{y \in C \mid \exists \pi \in S_n : (y, \pi) \in \mathrm{Aut}(C)\}.$$

The linear span over codewords of weight 3 of a code C of length n containing i, $i \in \{1, 2, \ldots, n\}$ is called the *linear i-component* (in what follows *i-component*) and denoted R_i^n. If C is the Hamming code of length n than R_i^n is its linear subcode.

More definitions

Let C be any perfect code of length n, $n = 2^k - 1$, $\lambda : C \to \{0,1\}$ be any function satisfying $\lambda(0^n) = 0$.

$C_\lambda = \{(y, \lambda(y), 0^n) \mid y \in C\}$,
$R_{n+1}^{2n+1} = \{(x, |x|, x) \mid x \in F^n\}$, where $|x| = x_1 + \ldots + x_n (\text{mod } 2)$.
Both codes have length $2n+1$ and R_{n+1}^{2n+1} is an $(n+1)$-component.

Vasil'ev code:

$$V_C^\lambda = C_\lambda + R_n^{2n+1} = \{(x+y, |x| + \lambda(y), x) \mid x \in F^n, y \in C\}.$$

More definitions

Let C be any perfect code of length n, $n = 2^k - 1$, $\lambda : C \to \{0, 1\}$ be any function satisfying $\lambda(0^n) = 0$.

$C_\lambda = \{(y, \lambda(y), 0^n) \mid y \in C\}$,
$R_{n+1}^{2n+1} = \{(x, |x|, x) \mid x \in F^n\}$, where $|x| = x_1 + \ldots + x_n \pmod 2$.
Both codes have length $2n + 1$ and R_{n+1}^{2n+1} is an $(n + 1)$-component.

Vasil'ev code:

$$V_C^\lambda = C_\lambda + R_n^{2n+1} = \{(x + y, |x| + \lambda(y), x) \mid x \in F^n, y \in C\}.$$

Transitivity criterion for perfect codes of small rank

Theorem

Let λ be a nonlinear Boolean function on the Hamming code H of length n.Then the vector $(y' + x, \lambda(y') + |x|, x)$ belongs to $Tr(V_H^\lambda)$ of the Vasil'ev code V_H^λ of length $2n+1$ for any $x \in F^n$ if and only if there exist $\pi_{y'} \in Sym(H)$ and $u \in F^n$ such that for all $y \in H$ we have

$$\lambda(y') + \lambda(y) + \lambda(y' + \pi_{y'}(y)) = u \cdot y,$$

where $u \cdot y$ is a scalar product of the vectors u and y in F^n.

Homogenious nontransitive perfect code of length 15: algebraic property

Let H be the Hamming code of length 7 generated by the vectors

$$\{1,2,3\},\ \{1,4,5\},\ \{1,6,7\},\ \{2,4,6\}.$$

The code $V22^1$ is the Vasil'ev code V_H^λ such that

$$\lambda(0^7) = \lambda(\{1,6,7\}) = \lambda(\{1,3,5,7\}) = \lambda(1^7) = 0,$$

for other codewords in H the value of λ is 1. Here 1^7 is the all-one vector of length 7.

The code $V3^11$ is the Vasil'ev code V_H^λ where

$$\lambda(0^7) = \lambda(\{1,6,7\}) = \lambda(\{2,4,6\}) = \lambda(\{4,5,6,7\}) = 0,$$

and λ is equal to 1 for other codewords from H.

The code $V22^1$ is the Vasil'ev code V_H^λ such that

$$\lambda(0^7) = \lambda(\{1,6,7\}) = \lambda(\{1,3,5,7\}) = \lambda(1^7) = 0,$$

for other codewords in H the value of λ is 1. Here 1^7 is the all-one vector of length 7.

The code $V3^11$ is the Vasil'ev code V_H^λ where

$$\lambda(0^7) = \lambda(\{1,6,7\}) = \lambda(\{2,4,6\}) = \lambda(\{4,5,6,7\}) = 0,$$

and λ is equal to 1 for other codewords from H.

Homogenious nontransitive perfect code of length 15: algebraic property

Proposition

The codes $V22^1$ and $V3^11$ are nonequivalent homogeneous nontransitive perfect codes of length 15.

Exploiting the Vasil'ev's construction with the function $\lambda \equiv 0$ we obtain

Theorem

If C is any homogeneous perfect code than the Vasil'ev code V_C^λ with $\lambda \equiv 0$ is homogeneous.

Homogenious nontransitive perfect code of length 15: algebraic property

Proposition

The codes $V22^1$ and $V3^11$ are nonequivalent homogeneous nontransitive perfect codes of length 15.

Exploiting the Vasil'ev's construction with the function $\lambda \equiv 0$ we obtain

Theorem

If C is any homogeneous perfect code than the Vasil'ev code V_C^{λ} with $\lambda \equiv 0$ is homogeneous.

Homogenious nontransitive perfect code of length 15: algebraic property

Proposition

The codes $V22^1$ and $V3^11$ are nonequivalent homogeneous nontransitive perfect codes of length 15.

Exploiting the Vasil'ev's construction with the function $\lambda \equiv 0$ we obtain

Theorem

If C is any homogeneous perfect code than the Vasil'ev code V_C^λ with $\lambda \equiv 0$ is homogeneous.

Main result

In order to separate the class of homogeneous perfect codes from transitive for any lengthy $n > 15$ we iteratively apply appropriate times the Vasil'ev's construction with the Boolean function $\lambda \equiv 0$ to these homogeneous nontransitive Vasil'ev codes $V22^1$ and $V3^11$ of length 15.

As the result we get

Theorem

For any $n \geq 15$ there exist perfect binary homogeneous nontransitive codes for any admissible length $n > 7$.

Main result

In order to separate the class of homogeneous perfect codes from transitive for any lengthy $n > 15$ we iteratively apply appropriate times the Vasil'ev's construction with the Boolean function $\lambda \equiv 0$ to these homogeneous nontransitive Vasil'ev codes $V22^1$ and $V3^11$ of length 15.

As the result we get

Theorem

For any $n \geq 15$ there exist perfect binary homogeneous nontransitive codes for any admissible length $n > 7$.

Main result

$$\mathbf{L} \subset \mathbf{Prl} \subset \mathbf{Tr} \subset \mathbf{Hom},$$

here
L is the class of linear codes,
Prl is the class of propelinear codes,
Tr is the class of transitive codes,
Hom is the class of homogeneous codes.

THANK YOU FOR YOUR ATTENTION