Steiner triple (quadruple) systems of small ranks embedded into perfect (extended perfect) binary codes

Darya Kovalevskaya, Faina Solov'eva, Elena Filimonova

Sobolev Institute of Mathematics
Novosibirsk State University, Russia
e-mails: daryik@rambler.ru, sol@math.nsc.ru, FilimonovaES@yandex.ru

16 June 2012

Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT2012

Pomorie, Bulgaria, June 15-21, 2012

Outline

Definitions

F^n – the n-dimensional metric space over the Galois field $GF(2)$.

C – a perfect code of length $n = 2^r - 1$, $r \geq 2$.

Definitions

F^n – the n-dimensional metric space over the Galois field $GF(2)$.

C – a perfect code of length $n = 2^r - 1$, $r \geq 2$.

$\bar{C}$ – any extended perfect code of length $N = n + 1 = 2^r$, obtained from C by parity checking.

Definitions

F^n – the n-dimensional metric space over the Galois field $GF(2)$.

C – a perfect code of length $n = 2^r - 1$, $r \geq 2$.

$\bar{C}$ – any extended perfect code of length $N = n + 1 = 2^r$, obtained from C by parity checking.

Definitions

A *t-$(v, k, 1)$-design* – a family of k-element subsets (blocks) of the set V, $|V| = v$, such that every t-element subset is contained in exactly one block.

Steiner triple system $STS(n)$ of order n – 2-$(n, 3, 1)$-design, $n = 1, 3(mod\ 6)$.

Definitions

A *t-$(v, k, 1)$-design* – a family of k-element subsets (blocks) of the set V, $|V| = v$, such that every t-element subset is contained in exactly one block.

Steiner triple system $STS(n)$ of order n – 2-$(n, 3, 1)$-design, $n \equiv 1, 3(mod\ 6)$.

Steiner quadruple system $SQS(N)$ of order N – 3-$(N, 4, 1)$-design, $N \equiv 2, 4(mod\ 6)$.

Definitions

A *t-$(v, k, 1)$-design* – a family of k-element subsets (blocks) of the set V, $|V| = v$, such that every t-element subset is contained in exactly one block.

Steiner triple system $STS(n)$ of order n – 2-$(n, 3, 1)$-design, $n \equiv 1, 3(mod\ 6)$.

Steiner quadruple system $SQS(N)$ of order N – 3-$(N, 4, 1)$-design, $N \equiv 2, 4(mod\ 6)$.

Definitions

The set of all vectors of weight 3 in C of length n defines a Steiner triple system of order n.

A Steiner triple system of order n corresponding to a binary Hamming code $\mathcal{H}^n$, is called *Hamming Steiner triple system* $STS(\mathcal{H}^n)$.

Definitions

The set of all vectors of weight 3 in C of length n defines a Steiner triple system of order n.

A Steiner triple system of order n corresponding to a binary Hamming code $\mathcal{H}^n$, is called *Hamming Steiner triple system* $STS(\mathcal{H}^n)$.

The set of all vectors of weight 4 in $\bar{C}$ defines a Steiner quadruple system of order N.

Definitions

The set of all vectors of weight 3 in C of length n defines a Steiner triple system of order n.

A Steiner triple system of order n corresponding to a binary Hamming code $\mathcal{H}^n$, is called *Hamming Steiner triple system* $STS(\mathcal{H}^n)$.

The set of all vectors of weight 4 in $\bar{C}$ defines a Steiner quadruple system of order N.

A Steiner quadruple system of order N, corresponding to a binary extended Hamming code $\mathcal{H}^N$, is called *Hamming Steiner quadruple system* $SQS(\mathcal{H}^N)$.

Definitions

The set of all vectors of weight 3 in C of length n defines a Steiner triple system of order n.

A Steiner triple system of order n corresponding to a binary Hamming code $\mathcal{H}^n$, is called *Hamming Steiner triple system* $STS(\mathcal{H}^n)$.

The set of all vectors of weight 4 in $\bar{C}$ defines a Steiner quadruple system of order N.

A Steiner quadruple system of order N, corresponding to a binary extended Hamming code $\mathcal{H}^N$, is called *Hamming Steiner quadruple system* $SQS(\mathcal{H}^N)$.

Definitions

A code $C' = (C \backslash M) \cup M'$ is obtained by a *switching* of some set M with a set M' in a binary code C if the code C' has the same parameters as C.

M – *component* of C.

Definitions

A code $C' = (C \setminus M) \cup M'$ is obtained by a *switching* of some set M with a set M' in a binary code C if the code C' has the same parameters as C.

M – *component* of C.

If $M' = M \oplus e_i$ for some $i \in \{1, 2, \ldots, n\}$, where $e_i = (0^{i-1}10^{n-i})$, then M – *i-component* of C of length n.

Definitions

A code $C' = (C \backslash M) \cup M'$ is obtained by a *switching* of some set M with a set M' in a binary code C if the code C' has the same parameters as C.

M – *component* of C.

If $M' = M \oplus e_i$ for some $i \in \{1, 2, \ldots, n\}$, where $e_i = (0^{i-1}10^{n-i})$, then M – *i-component* of C of length n.

The set M – *ijk-component* of C, if M is an i-component, j-component and k-component.

Definitions

A code $C' = (C \backslash M) \cup M'$ is obtained by a *switching* of some set M with a set M' in a binary code C if the code C' has the same parameters as C.

M – *component* of C.

If $M' = M \oplus e_i$ for some $i \in \{1, 2, \ldots, n\}$, where $e_i = (0^{i-1}10^{n-i})$, then M – *i-component* of C of length n.

The set M – *ijk-component* of C, if M is an i-component, j-component and k-component.

Definitions

Two sets R and R', composed of k-element subsets of the set V, $|V| = v$, are *balanced with each other*, if every t-element unordered set from the k-element subsets of R can also be found in the k-element subsets of R'.

A t-$(v, k, 1)$-design $A' = (A \setminus R) \cup R'$ is obtained by a *switching* of a block set R with a block set R' in a t-$(v, k, 1)$-design A, if R and R' are balanced with each other.

Definitions

Two sets R and R', composed of k-element subsets of the set V, $|V| = v$, are *balanced with each other*, if every t-element unordered set from the k-element subsets of R can also be found in the k-element subsets of R'.

A t-$(v, k, 1)$-design $A' = (A \backslash R) \cup R'$ is obtained by a *switching* of a block set R with a block set R' in a t-$(v, k, 1)$-design A, if R and R' are balanced with each other.

The set R (and R') is also called a *component*.

Definitions

Two sets R and R', composed of k-element subsets of the set V, $|V| = v$, are *balanced with each other*, if every t-element unordered set from the k-element subsets of R can also be found in the k-element subsets of R'.

A t-$(v, k, 1)$-design $A' = (A \setminus R) \cup R'$ is obtained by a *switching* of a block set R with a block set R' in a t-$(v, k, 1)$-design A, if R and R' are balanced with each other.

The set R (and R') is also called a *component*.

The *rank* of a code C in the vector space F^n – the dimension of the subspace $< C >$ spanned by vectors from C.

Definitions

Two sets R and R', composed of k-element subsets of the set V, $|V| = v$, are *balanced with each other*, if every t-element unordered set from the k-element subsets of R can also be found in the k-element subsets of R'.

A t-$(v, k, 1)$-design $A' = (A \backslash R) \cup R'$ is obtained by a *switching* of a block set R with a block set R' in a t-$(v, k, 1)$-design A, if R and R' are balanced with each other.

The set R (and R') is also called a *component*.

The *rank* of a code C in the vector space F^n – the dimension of the subspace $< C >$ spanned by vectors from C.

Definitions

A *Pasch configuration* – a collection of 4 triples of a Steiner triple system, isomorphic to (a, b, c), (a, y, z), (x, b, z) and (x, y, c).

Switchings: $a \leftrightarrow x,\ b \leftrightarrow y,\ c \leftrightarrow z.$

Definitions

A *Pasch configuration* – a collection of 4 triples of a Steiner triple system, isomorphic to (a, b, c), (a, y, z), (x, b, z) and (x, y, c).

Switchings: $a \leftrightarrow x$, $b \leftrightarrow y$, $c \leftrightarrow z$.

$$\{(a, b, c), (a, y, z), (x, b, z), (x, y, c)\}$$

Definitions

A *Pasch configuration* – a collection of 4 triples of a Steiner triple system, isomorphic to (a, b, c), (a, y, z), (x, b, z) and (x, y, c).

Switchings: $a \leftrightarrow x,\ b \leftrightarrow y,\ c \leftrightarrow z.$

$$\{(a, b, c),\ (a, y, z),\ (x, b, z),\ (x, y, c)\}$$

$$\Downarrow a \leftrightarrow x$$

Definitions

A *Pasch configuration* – a collection of 4 triples of a Steiner triple system, isomorphic to (a, b, c), (a, y, z), (x, b, z) and (x, y, c).

Switchings: $a \leftrightarrow x,\ b \leftrightarrow y,\ c \leftrightarrow z.$

$$\{(a, b, c),\ (a, y, z),\ (x, b, z),\ (x, y, c)\}$$

$$\Downarrow\ a \leftrightarrow x$$

$$\{(x, b, c),\ (x, y, z),\ (a, b, z),\ (a, y, c)\}$$

Definitions

A *Pasch configuration* – a collection of 4 triples of a Steiner triple system, isomorphic to (a, b, c), (a, y, z), (x, b, z) and (x, y, c).

Switchings: $a \leftrightarrow x,\ b \leftrightarrow y,\ c \leftrightarrow z.$

$$\{(a, b, c), (a, y, z), (x, b, z), (x, y, c)\}$$

$$\Downarrow a \leftrightarrow x$$

$$\{(x, b, c), (x, y, z), (a, b, z), (a, y, c)\}$$

Well-known constructions

Vasil'ev construction of perfect codes:

Well-known constructions

Vasil'ev construction of perfect codes:

$$V^n = \{(x, |x| + \lambda(y), x + y) \mid x \in F^{\frac{n-1}{2}}, y \in \mathcal{H}^{\frac{n-1}{2}}, \lambda : \mathcal{H}^{\frac{n-1}{2}} \to \{0,1\}\}$$

Well-known constructions

Vasil'ev construction of perfect codes:

$$V^n = \{(x, |x| + \lambda(y), x + y) \mid x \in F^{\frac{n-1}{2}}, y \in \mathcal{H}^{\frac{n-1}{2}}, \lambda : \mathcal{H}^{\frac{n-1}{2}} \to \{0, 1\}\}$$

Method of ijk-components:

Well-known constructions

Vasil'ev construction of perfect codes:

$$V^n = \{(x, |x|+\lambda(y), x+y) \mid x \in F^{\frac{n-1}{2}}, y \in \mathcal{H}^{\frac{n-1}{2}}, \lambda : \mathcal{H}^{\frac{n-1}{2}} \to \{0,1\}\}$$

Method of ijk-components:

Theorem*

(S. V. Avgustinovich, F. I. Solov'eva) Every binary Hamming code of length n can be presented as a union of disjoint ijk-components R^t_{ijk}. Each of them can be represented as a union of disjoint i-components R^{pt}_i:
$\mathcal{H}^n = \bigcup_{t=1}^{N_2} R^t_{ijk} = \bigcup_{t=1}^{N_2} \bigcup_{p=1}^{N_1} R^{pt}_i$, where $N_1 = 2^{(n-3)/4}$, $N_2 = 2^{(n+5)/4-log(n+1)}$.

Well-known constructions

Vasil'ev construction of perfect codes:

$$V^n = \{(x, |x| + \lambda(y), x + y) \mid x \in F^{\frac{n-1}{2}}, y \in \mathcal{H}^{\frac{n-1}{2}}, \lambda : \mathcal{H}^{\frac{n-1}{2}} \to \{0, 1\}\}$$

Method of ijk-components:

Theorem*

(S. V. Avgustinovich, F. I. Solov'eva) Every binary Hamming code of length n can be presented as a union of disjoint *ijk*-components R^t_{ijk}. Each of them can be represented as a union of disjoint *i*-components R^{pt}_i:
$\mathcal{H}^n = \bigcup_{t=1}^{N_2} R^t_{ijk} = \bigcup_{t=1}^{N_2} \bigcup_{p=1}^{N_1} R^{pt}_i$, where $N_1 = 2^{(n-3)/4}$,
$N_2 = 2^{(n+5)/4 - log(n+1)}$.

Ranks of codes

The Hamming code $\mathcal{H}^n$: rank $= n - log(n+1)$.

A perfect binary code of length n given by Vasil'ev construction from $\mathcal{H}^{\frac{n-1}{2}}$: rank $= n - log(n+1) + 1$.

A perfect binary code of length n constructed by switchings of ijk-components from $\mathcal{H}^n$: rank $= n - log(n+1) + 2$.

Construction

$M = \{1, 2, 3, \dots, m\}$, $m \equiv 1, 3 (mod\ 6)$, $n = 4m + 3 > 7$
$\{i, j, k\} \cap M = \emptyset$

$\mathbf{S}(\mathbf{T}, \mathbf{n})$, $T =$

	1	2	...	a	b	c	...	m
i	i_1	i_2	...	i_a	i_b	i_c	...	i_m
j	j_1	j_2	...	j_a	j_b	j_c	...	j_m
k	k_1	k_2	...	k_a	k_b	k_c	...	k_m

1.(i, j, k)
2.$\forall a \in M : (i, j_a, k_a)\,(i, a, i_a)\,(j, a, j_a)\,(j, i_a, k_a)\,(k, i_a, j_a)\,(k, a, k_a)$
3.$\forall (a, b, c) \in STS(m) :$

$$\begin{aligned} &(a, b, c)\ \ (a, j_b, j_c)\ \ (j_a, j_b, c)\ \ (j_a, b, j_c) \\ &(a, i_b, i_c)\,(a, k_b, k_c)\,(j_a, k_b, i_c)\,(j_a, i_b, k_c) \\ &(i_a, b, i_c)\,(i_a, j_b, k_c)\,(k_a, j_b, i_c)\,(k_a, b, k_c) \\ &(i_a, i_b, c)\,(i_a, k_b, j_c)\,(k_a, k_b, c)\,(k_a, i_b, j_c) \end{aligned} \quad (1)$$

Theorem 1.

The set $S(T, n)$ is a Steiner triple system of order $n = 4m + 3$.

Corollary.

Let $STS(m)$ be the Hamming Steiner triple system of order m. Then $S(T, n)$ is the Hamming Steiner triple system of order $n = 4m + 3$.

Theorem 1.

The set $S(T, n)$ is a Steiner triple system of order $n = 4m + 3$.

Corollary.

Let $STS(m)$ be the Hamming Steiner triple system of order m. Then $S(T, n)$ is the Hamming Steiner triple system of order $n = 4m + 3$.

Switchings of the construction

A. $\forall a \in M$

$$\{(i, j_a, k_a), (i, a, i_a), (j, a, j_a), (j, i_a, k_a), (k, i_a, j_a), (k, a, k_a)\}$$

Three Pasch configurations:

$\{(i, j_a, k_a),\ (i, a, i_a),\ (j, a, j_a),\ (j, i_a, k_a)\}$	$i \leftrightarrow j$
$\{(i, j_a, k_a),\ (i, a, i_a),\ (k, i_a, j_a),\ (k, a, k_a)\}$	$i \leftrightarrow k$
$\{(j, a, j_a),\ (j, i_a, k_a),\ (k, i_a, j_a),\ (k, a, k_a)\}$	$j \leftrightarrow k$

B. $\forall (a, b, c) \in STS(m)$

i – columns from (1):	$a \leftrightarrow i_a$	$a \leftrightarrow i_a$	$j_a \leftrightarrow k_a$	$j_a \leftrightarrow k_a$
j – rows from (1):	$a \leftrightarrow j_a$	$a \leftrightarrow j_a$	$i_a \leftrightarrow k_a$	$i_a \leftrightarrow k_a$
k – transversals from (1):	$a \leftrightarrow k_a$	$a \leftrightarrow k_a$	$j_a \leftrightarrow i_a$	$j_a \leftrightarrow i_a$

B1. i or j, or k

B2. $i + j$ (k) or $j + i$ (k) or $k + i$ (j)

Theorem 2.

The class of Steiner triple systems of order $n = 4m + 3$, obtained by the switching construction of Theorem 1 using the Hamming Steiner triple system $STS(\mathcal{H}^m)$ of order m, coincides with the class of Steiner triple systems of order $n = 4m + 3$, embedded into the class of perfect binary codes, constructed by the method of *ijk*-components from the binary Hamming code of length n.

$$|Sym(\mathcal{H}^n)| = |GL(log(n+1), 2)|$$

Theorem 3.

Any $STS(n)$ of rank $n - log(n+1) + 1$ is embedded in some perfect code of length n and the same rank, the code is given by Vasil'ev construction from the Hamming code of length $(n-1)/2$. The number of such different $STS(n)$ equals to $(2^{|STS(\frac{n-1}{2})| - \frac{n-1}{2}} - \frac{2}{n+1}) \cdot n!/|Sym(\mathcal{H}^{\frac{n-1}{2}})|$.

$$R(H, n) = n!/|Sym(\mathcal{H}^n)|$$

Theorem 4.

The number $R_2(n)$ of different Steiner triple systems of order $n = 4m + 3$ of rank not more than $n - log(n+1) + 2$, embedded into perfect binary codes of the same rank, satisfies the following inequalities:

$$4^{(n-3)/4} \cdot 130^{(n-3)(n-7)/3 \cdot 2^5} \cdot n(n-1)/6 \cdot R(\mathcal{H}, (n-3)/4) \leq$$
$$\leq R_2(n) \leq 4^{(n-3)/4} \cdot 130^{(n-3)(n-7)/3 \cdot 2^5} \cdot n(n-1)/6 \cdot R(\mathcal{H}, n).$$

Theorem 5.

The number $R(n)$ of different Steiner triple systems $STS(n)$ of order $n = 4m+3$, obtained from the all switchings of the construction, is at least
$((n+1)\cdot 4^{(n-7)/4}+n-3)\cdot 310^{(n-3)(n-7)/3\cdot 2^5}\cdot n(n-1)/6\cdot R((n-3)/4)$.

Theorem 6.

The number $R'(n)$ of different Steiner triple systems $STS(n)$ of order $n = 4m+3$, $m \geq 255$, which are not embedded into perfect binary codes constructed by the method of *ijk*-components from the binary Hamming code, is at least
$R'(n) \geq ((n+1)\cdot 4^{(n-7)/4} + n - 3)\cdot 310^{(n-3)(n-7)/3\cdot 2^5}\cdot n(n-1)/6\cdot R((n-3)/4) - 4^{(n-3)/4}\cdot 130^{(n-3)(n-7)/3\cdot 2^5}\cdot n(n-1)/6\cdot R(\mathcal{H}, n)$,
where $R((n-3)/4)$ is the number of different $STS((n-3)/4)$.

Theorem 5.

The number $R(n)$ of different Steiner triple systems $STS(n)$ of order $n = 4m + 3$, obtained from the all switchings of the construction, is at least $((n+1)\cdot 4^{(n-7)/4} + n - 3)\cdot 310^{(n-3)(n-7)/3\cdot 2^5}\cdot n(n-1)/6\cdot R((n-3)/4)$.

Theorem 6.

The number $R'(n)$ of different Steiner triple systems $STS(n)$ of order $n = 4m + 3$, $m \geq 255$, which are not embedded into perfect binary codes constructed by the method of *ijk*-components from the binary Hamming code, is at least

$R'(n) \geq ((n+1)\cdot 4^{(n-7)/4} + n - 3)\cdot 310^{(n-3)(n-7)/3\cdot 2^5}\cdot n(n-1)/6\cdot R((n-3)/4) - 4^{(n-3)/4}\cdot 130^{(n-3)(n-7)/3\cdot 2^5}\cdot n(n-1)/6\cdot R(\mathcal{H}, n)$,

where $R((n-3)/4)$ is the number of different $STS((n-3)/4)$.

Theorem 7.

The number of different Steiner triple systems of order $n = 2^r - 1$, $r \geq 4$, of rank not more than $n - \log(n+1) + 2$, is at most $2^{(4n-7)(n-3)/6} \cdot R(\mathcal{H}, n)$.

Theorem 8.

The class of Steiner quadruple systems, constructed by the switching method of *ijkl*-components from the Hamming Steiner quadruple system $SQS(\mathcal{H}^N)$, coincides with the class of Steiner quadruple systems of order N, embedded into extended perfect binary code, constructed by the method of *ijkl*-components from the extended binary Hamming code.

Theorem 9.

Any $SQS(N)$ of rank $N - logN$ is embedded in some extended perfect code of length N and the same rank, the code is given by extended Vasil'ev construction from the Hamming code of length $N/2 - 1$. The number of such different $SQS(n)$ equals to $(2^{|SQS(\frac{N}{2})| - \frac{N}{2}} - \frac{1}{N}) \cdot N!/|Sym(\bar{\mathcal{H}}^{\frac{N}{2}})|$.

$$R(H, N/4) = (N/4)!/((N/4-1)(N/4-2)(N/4-2^2)\cdot \ldots \cdot (N/4)/2)$$

Theorem 10.

The number of different Steiner quadruple systems $SQS(N)$ of order N of rank not more than $N - logN + 1$, embedded into perfect extended binary codes of the same rank, constructed by the method of $ijkl$-components from $\mathcal{H}^N$, is at least

$$(3^2 \cdot 2^8 - 8)^{N(N-4)(N-8)/(3\cdot 2^9)} \cdot (2^{N(N-4)/2^5} - 1) \cdot \frac{N(N-1)(N-2)}{2^3} \cdot R(H, N/4)$$

Theorem 9.

Any $SQS(N)$ of rank $N - logN$ is embedded in some extended perfect code of length N and the same rank, the code is given by extended Vasil'ev construction from the Hamming code of length $N/2-1$. The number of such different $SQS(n)$ equals to $(2^{|SQS(\frac{N}{2})|-\frac{N}{2}} - \frac{1}{N}) \cdot N!/|Sym(\bar{\mathcal{H}}^{\frac{N}{2}})|$.

$$R(H, N/4) = (N/4)!/((N/4-1)(N/4-2)(N/4-2^2)\cdot \ldots \cdot (N/4)/2)$$

Theorem 10.

The number of different Steiner quadruple systems $SQS(N)$ of order N of rank not more than $N - logN + 1$, embedded into perfect extended binary codes of the same rank, constructed by the method of *ijkl*-components from $\mathcal{H}^N$, is at least

$$(3^2 \cdot 2^8 - 8)^{N(N-4)(N-8)/(3\cdot 2^9)} \cdot (2^{N(N-4)/2^5} - 1) \cdot \frac{N(N-1)(N-2)}{2^3} \cdot R(H, N/4).$$

Futher research

- An exact estimation for the number of $STS(n)$ of rank $n - log(n+1) + 2$, embedded into perfect codes of the same rank.

- An exact estimation for the number of $SQS(N)$ of rank $N - logN + 1$, embedded into extended perfect codes of the same rank.

Conclusion

- Classification of $STS(n)$ of rank $n - log(n+1) + 1$ and $n - log(n+1) + 2$, embedded into perfect codes of the same rank:

– construction

– the number of $STS(n)$ of rank $n - log(n+1) + 1$

– the bounds of the number of $STS(n)$ of rank $n - log(n+1) + 2$

$+$

– the upper bound of the whole number of $STS(n)$ of rank $n - log(n+1) + 2$

- Classification of $SQS(N)$ of rank $N - logN$ and $N - logN + 1$, embedded into extended perfect codes of the same rank:

– construction

– the number of $SQS(N)$ of rank $N - logN$

– the bound of the number of $SQS(n)$ of rank $N - logN + 1$

Thank you for your attention!