On the Preparata-like codes

D.V. Zinoviev, V.A. Zinoviev

A.A. Kharkevich Institute for Problems of Information Transmission, Moscow, Russia

ACCT-2014 Svetlogorsk, Russia, September 7-13, 2014

Outline

Let $E = \{0, 1\}$.

Let $E = \{0, 1\}$. As usual, by (n, d, N) denote a binary code $C \subseteq E^n$ of length n, cardinality N and minimum (Hamming) distance d.

Let $E = \{0, 1\}$. As usual, by (n, d, N) denote a binary code $C \subseteq E^n$ of length n, cardinality N and minimum (Hamming) distance d.
Let $n = 2^{2\,m}$, $m = 2, 3, \ldots$.

Let $E = \{0, 1\}$. As usual, by (n, d, N) denote a binary code $C \subseteq E^n$ of length n, cardinality N and minimum (Hamming) distance d.
Let $n = 2^{2m}$, $m = 2, 3, \ldots$.
A binary $(n, 6, 2^{n-4m})$-code is called a **Preparata-like** code and denoted P.

Let $E = \{0, 1\}$. As usual, by (n, d, N) denote a binary code $C \subseteq E^n$ of length n, cardinality N and minimum (Hamming) distance d.
Let $n = 2^{2m}$, $m = 2, 3, \ldots$.
A binary $(n, 6, 2^{n-4m})$-code is called a **Preparata-like** code and denoted P.
A binary $(n, 4, 2^{n-m-1})$-code is called a **Hamming-like** code and denoted H.

Let $E = \{0, 1\}$. As usual, by (n, d, N) denote a binary code $C \subseteq E^n$ of length n, cardinality N and minimum (Hamming) distance d.
Let $n = 2^{2m}$, $m = 2, 3, \ldots$.
A binary $(n, 6, 2^{n-4m})$-code is called a **Preparata-like** code and denoted P.
A binary $(n, 4, 2^{n-m-1})$-code is called a **Hamming-like** code and denoted H.

Assume that any Preparata-like code P and any Hamming-like code H contains the zero vector $\mathbf{0} = (0, \ldots, 0)$.

For a binary code $C \subset E^n$ and an arbitrary binary vector $\mathbf{x} \in E^n$ define the distance between $\mathbf{x}$ and C

$$d(\mathbf{x}, C) \;=\; \min\{d(\mathbf{x}, \mathbf{c}) : \; \mathbf{c} \in C\}.$$

For a binary code $C \subset E^n$ and an arbitrary binary vector $\mathbf{x} \in E^n$ define the distance between $\mathbf{x}$ and C

$$d(\mathbf{x}, C) \;=\; \min\{d(\mathbf{x}, \mathbf{c}) :\; \mathbf{c} \in C\}.$$

For a binary code $C \subset E^n$ let $C(i)$ be the set of vectors of E^n, at a distance i from C, i.e.

$$C(i) \;=\; \{\mathbf{x} \in E^n :\; d(\mathbf{x}, C) = i\}.$$

For a binary code $C \subset E^n$ and an arbitrary binary vector $\mathbf{x} \in E^n$ define the distance between $\mathbf{x}$ and C

$$d(\mathbf{x}, C) \;=\; \min\{d(\mathbf{x}, \mathbf{c}) : \; \mathbf{c} \in C\}.$$

For a binary code $C \subset E^n$ let $C(i)$ be the set of vectors of E^n, at a distance i from C, i.e.

$$C(i) \;=\; \{\mathbf{x} \in E^n : \; d(\mathbf{x}, C) = i\}.$$

Define the covering radius of a code C, $\rho = \rho(C)$, the smallest positive integer ρ such that

$$E^n \;=\; \bigcup_{i=0}^{\rho} C(i).$$

A Steiner system $S(v,k,t)$ is a pair (X,B), X is a v-set (i.e. $|X| = v$) and B – the collection of k-subsets of X (called blocks) such that every t-subset (of t elements) of X is contained in exactly one block of B.

A Steiner system $S(v,k,t)$ is a pair (X,B), X is a v-set (i.e. $|X| = v$) and B – the collection of k-subsets of X (called blocks) such that every t-subset (of t elements) of X is contained in exactly one block of B.

A Steiner system $S(v,4,3)$ is a Steiner quadruple system SQS(v).

A Steiner system $S(v,k,t)$ is a pair (X,B), X is a v-set (i.e. $|X| = v$) and B – the collection of k-subsets of X (called blocks) such that every t-subset (of t elements) of X is contained in exactly one block of B.

A Steiner system $S(v,4,3)$ is a Steiner quadruple system SQS(v).

A Steiner system $S(v,4,3)$ is called 2-resolvable if it can be split into mutually non-overlapping $S(v,4,2)$ Steiner systems.

[*Zaitsev, Zinoviev, Semakov* (1971)] and [*Baker* (1975)]: the original Preparata codes P of length $n = 4^m,\ m = 2, 3, \ldots$ define a 2-resolvable $S(n, 4, 3)$

[*Zaitsev, Zinoviev, Semakov* (1971)] and [*Baker* (1975)]: the original Preparata codes P of length $n = 4^m,\ m = 2, 3, \ldots$ define a 2-resolvable $S(n, 4, 3)$
It is obtained by the partition of code H into the shifts of P.

[*Zaitsev, Zinoviev, Semakov* (1971)] and [*Baker* (1975)]: the original Preparata codes P of length $n = 4^m,\ m = 2, 3, \dots$ define a 2-resolvable $S(n, 4, 3)$
It is obtained by the partition of code H into the shifts of P.

[*Dumer* (1976)] and [*Baker, van Lint, Wilson* (1983)]: Same results were obtained for the generalized Preparata codes and for Z_4-linear Preparata-like codes [*Hammons, Kumar, Calderbank, Sloane, Sole* (1994)]

[*Zaitsev, Zinoviev, Semakov* (1971)] and [*Baker* (1975)]: the original Preparata codes P of length $n = 4^m$, $m = 2, 3, \dots$ define a 2-resolvable $S(n, 4, 3)$
It is obtained by the partition of code H into the shifts of P.

[*Dumer* (1976)] and [*Baker, van Lint, Wilson* (1983)]: Same results were obtained for the generalized Preparata codes and for Z_4-linear Preparata-like codes [*Hammons, Kumar, Calderbank, Sloane, Sole* (1994)]
We consider the group structure of the Preparata-like codes of [*Baker, van Lint, Wilson*] (also considered by [*Rifa, Pujol* (1997)] and [*Ericson* (2009)] presented them in a slightly different form).

Let $\mu \geq 3$ be an odd number and consider the functions $z: \mathbb{F}_{2^\mu} \to \mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, where $\omega^2 = \omega + 1$.

Let $\mu \geq 3$ be an odd number and consider the functions $z: \mathbb{F}_{2^\mu} \rightarrow \mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, where $\omega^2 = \omega + 1$.

Let $\mathrm{Tr}(z) = z + z^2$ be a trace function from $\mathbb{F}_4$ into $\mathbb{F}_2$. For $z \in \mathbb{F}_4$ define $x, y \in \mathbb{F}_2$ as follows:

$$x = \mathrm{Tr}(\omega z) = z\omega + z^2\omega^2, \;\; y = \mathrm{Tr}(\omega^2 z) = z\omega^2 + z^2\omega,$$

Note that $z = x\omega + y\omega^2$ and $z^2 = x\omega^2 + y\omega$.

Let $\mu \geq 3$ be an odd number and consider the functions $z: \mathbb{F}_{2^\mu} \to \mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, where $\omega^2 = \omega + 1$.

Let $\mathrm{Tr}(z) = z + z^2$ be a trace function from $\mathbb{F}_4$ into $\mathbb{F}_2$. For $z \in \mathbb{F}_4$ define $x, y \in \mathbb{F}_2$ as follows:

$$x = \mathrm{Tr}(\omega z) = z\omega + z^2\omega^2, \;\; y = \mathrm{Tr}(\omega^2 z) = z\omega^2 + z^2\omega,$$

Note that $z = x\omega + y\omega^2$ and $z^2 = x\omega^2 + y\omega$.

These equalities establish an isomorphism between $\mathbb{F}_4$ and $\mathbb{F}_2^2$. In this case the Hamming metric of $\mathbb{F}_2^2$ corresponds to the metric ρ of $\mathbb{F}_4$, induced by the following weight function wt_4:

$$\mathrm{wt}_4(0) = 0, \;\; \mathrm{wt}_4(\omega) = \mathrm{wt}_4(\omega^2) = 1, \;\; \mathrm{wt}_4(1) = 2.$$

so that $\rho(a, b) = \mathrm{wt}_4(a + b)$. Since μ is odd, the field $\mathbb{F}_4$ is not contained in $\mathbb{F}_{2^\mu}$ and in particular the elements ω and ω^2 are not contained in $\mathbb{F}_{2^\mu}$.

Let $\mathcal{F}$ be the set of functions $z : \mathbb{F}_{2^\mu} \to \mathbb{F}_4$ which satisfy the following equalities:

$$\sum_u z(u) = 0, \qquad \sum_u u(z_1(u) + z_2(u)) = 0, \tag{1}$$

where $z(u) = z_1(u)\omega + z_2(u)\omega^2$ and u runs over the whole field $\mathbb{F}_{2^\mu}$.

Let $\mathcal{F}$ be the set of functions $z : \mathbb{F}_{2^\mu} \to \mathbb{F}_4$ which satisfy the following equalities:

$$\sum_u z(u) = 0, \qquad \sum_u u(z_1(u) + z_2(u)) = 0, \qquad (1)$$

where $z(u) = z_1(u)\omega + z_2(u)\omega^2$ and u runs over the whole field $\mathbb{F}_{2^\mu}$.

Let σ be a power of 2, so that $2 \leq \sigma \leq 2^{\mu-1}$ and $(\sigma \pm 1, 2^\mu - 1) = 1$ (*Ericson* considered the case $\sigma = 2$). Let $\mathcal{F}_\sigma$ be the subset of functions of $\mathcal{F}$, which satisfy the following equality:

$$\sum_u u^{\sigma+1}(z_1(u) + z_2(u)) = \left(\sum_u uz(u)\right)^{\sigma+1}, \qquad (2)$$

where u runs over the whole field $\mathbb{F}_{2^\mu}$.

For an arbitrary function $z \in \mathcal{F}$ set

$$\lambda_z = \sum_{u \in \mathbb{F}_{2^\mu}} u z(u).$$

For an arbitrary function $z \in \mathcal{F}$ set

$$\lambda_z = \sum_{u \in \mathbb{F}_{2^\mu}} u z(u).$$

Define a binary operation $\star$ on the set $\mathcal{F}$, so that for any $a = a_1\omega + a_2\omega^2$ and $b = b_1\omega + b_2\omega^2$ from $\mathcal{F}$, we have

$$c = a \star b = c_1\omega + c_2\omega^2, \tag{3}$$

where $c_1(u) = a_1(u + \lambda_b) + b_1(u)$ and $c_2(u) = a_2(u) + b_2(u)$.

For an arbitrary function $z \in \mathcal{F}$ set

$$\lambda_z = \sum_{u \in \mathbb{F}_{2^\mu}} u z(u).$$

Define a binary operation $\star$ on the set $\mathcal{F}$, so that for any $a = a_1\omega + a_2\omega^2$ and $b = b_1\omega + b_2\omega^2$ from $\mathcal{F}$, we have

$$c = a \star b = c_1\omega + c_2\omega^2, \tag{3}$$

where $c_1(u) = a_1(u + \lambda_b) + b_1(u)$ and $c_2(u) = a_2(u) + b_2(u)$.

The set $\mathcal{F}$ with this operation $\star$ is a non-commutative group and $\mathcal{F}_\sigma$ is a subgroup of $\mathcal{F}$. One can show that $[\mathcal{F} : \mathcal{F}_\sigma]$ is equal to 2^μ and we have that

$$\mathcal{F} = \bigcup_{i=1}^{2^\mu} \mathcal{F}_\sigma \star f_i, \tag{4}$$

where $f_1, \ldots, f_{2^\mu} \in \mathcal{F}$ are coset representatives.

Note that if $c \in \mathcal{F}$, then it is easy to check that multiplication by c on the right (but not on the left) is distance preserving. Thus

$$\rho(a \star c, b \star c) = \rho(a, b) = \rho(\mathbf{0}, b \star a^{-1}) = \mathrm{wt}_4(b \star a^{-1}). \quad (5)$$

Note that if $c \in \mathcal{F}$, then it is easy to check that multiplication by c on the right (but not on the left) is distance preserving. Thus

$$\rho(a \star c, b \star c) = \rho(a, b) = \rho(\mathbf{0}, b \star a^{-1}) = \mathrm{wt}_4(b \star a^{-1}). \quad (5)$$

For a given positive odd number $\mu \geq 3$, and $\sigma = 2, \ldots, 2^{\mu-1}$, $(\sigma \pm 1, 2^{\mu} - 1) = 1$ define a non-commutative Preparata-like code of **Ericson-type** as a binary code of length $n = 2^m$, $(m = \mu + 1)$ viewed as the set of values $z(u) \to [x(u), y(u)]$ of the functions $z \in \mathcal{F}_{\sigma}$.

Note that if $c \in \mathcal{F}$, then it is easy to check that multiplication by c on the right (but not on the left) is distance preserving. Thus

$$\rho(a \star c, b \star c) = \rho(a, b) = \rho(\mathbf{0}, b \star a^{-1}) = \mathrm{wt}_4(b \star a^{-1}). \quad (5)$$

For a given positive odd number $\mu \geq 3$, and $\sigma = 2, \dots, 2^{\mu-1}$, $(\sigma \pm 1, 2^{\mu} - 1) = 1$ define a non-commutative Preparata-like code of **Ericson-type** as a binary code of length $n = 2^m$, $(m = \mu + 1)$ viewed as the set of values $z(u) \to [x(u), y(u)]$ of the functions $z \in \mathcal{F}_{\sigma}$.

Equations (1) becomes (u runs over $F_{2^{\mu}}$):

$$\sum x(u) = \sum y(u) = 0, \qquad \sum u \cdot x(u) = \sum u \cdot y(u) = \lambda$$

Note that if $c \in \mathcal{F}$, then it is easy to check that multiplication by c on the right (but not on the left) is distance preserving. Thus

$$\rho(a \star c, b \star c) = \rho(a, b) = \rho(\mathbf{0}, b \star a^{-1}) = \mathrm{wt}_4(b \star a^{-1}). \quad (5)$$

For a given positive odd number $\mu \geq 3$, and $\sigma = 2, \ldots, 2^{\mu-1}$, $(\sigma \pm 1, 2^{\mu} - 1) = 1$ define a non-commutative Preparata-like code of **Ericson-type** as a binary code of length $n = 2^m$, $(m = \mu + 1)$ viewed as the set of values $z(u) \to [x(u), y(u)]$ of the functions $z \in \mathcal{F}_\sigma$.

Equations (1) becomes (u runs over F_{2^μ}):

$$\sum x(u) = \sum y(u) = 0, \qquad \sum u \cdot x(u) = \sum u \cdot y(u) = \lambda$$

Equation (2) becomes:

$$\sum u^{\sigma+1} x(u) + \sum u^{\sigma+1} y(u) = \lambda^{\sigma+1}.$$

Theorem 1.

Let $\mathcal{P}_\sigma$ be a code of length $n = 2^{\mu+1}$, given by equations (1)-(2). For any odd number $\mu \geq 3$ and any $\sigma = 2, \ldots, 2^{\mu-1}$, $(\sigma \pm 1, 2^\mu - 1) = 1$ this code has the following parameters

$$n = 2^m, \quad N = 2^{n-2m}, \quad d = 6,$$

i.e. is the non-commutative Preparata-like group code.

Theorem 1.

Let $\mathcal{P}_\sigma$ be a code of length $n = 2^{\mu+1}$, given by equations (1)-(2). For any odd number $\mu \geq 3$ and any $\sigma = 2, \dots, 2^{\mu-1}$, $(\sigma \pm 1, 2^\mu - 1) = 1$ this code has the following parameters

$$n = 2^m, \;\; N = 2^{n-2m}, \;\; d = 6,$$

i.e. is the non-commutative Preparata-like group code.

Ericson (for $\sigma = 2$)

Let $\mathcal{P}_{\sigma,i}$ be the set of values of functions $\mathcal{F}_\sigma \star f_i$. It follows that minimum distance of $\mathcal{P}_{\sigma,i}$ is 6.

Let $\mathcal{P}_{\sigma,i}$ be the set of values of functions $\mathcal{F}_\sigma \star f_i$. It follows that minimum distance of $\mathcal{P}_{\sigma,i}$ is 6.

Theorem 2.

The code $\mathcal{P}_\sigma$ of length $n = 2^{\mu+1}$ is a subcode of the Hamming code H of length n and induce a partition of H into the cosets of the code $\mathcal{P}_\sigma$, i.e. we have

$$H = \bigcup_{i=1}^{n/2} \mathcal{P}_{\sigma,i}.$$

Main Results

According to [*Zaitsev, Zinoviev, Semakov* (1971)] the set of codewords of weight 4 of $P_{\sigma,i}$, $i = 1, \ldots, n/2 - 1$, forms a Steiner system $S(n, 4, 2)$.

Main Results

According to [*Zaitsev, Zinoviev, Semakov* (1971)] the set of codewords of weight 4 of $P_{\sigma,i}$, $i = 1, \ldots, n/2 - 1$, forms a Steiner system $S(n, 4, 2)$. Recall that the codeowrds of weight 4 of H forms $S(n, 4, 3)$ [*Assmuss, Mattson*, (1967)].

Main Results

According to [*Zaitsev, Zinoviev, Semakov* (1971)] the set of codewords of weight 4 of $P_{\sigma,i}$, $\; i = 1, \ldots, n/2-1$, forms a Steiner system $S(n,4,2)$. Recall that the codeowrds of weight 4 of H forms $S(n,4,3)$ [*Assmuss, Mattson*, (1967)]. Hence from the partition of H into subcodes $P_{\sigma,i}$ of Theorem 2 we obtain

Main Results

According to [*Zaitsev, Zinoviev, Semakov* (1971)] the set of codewords of weight 4 of $P_{\sigma,i},\ \ i = 1, \dots, n/2-1$, forms a Steiner system $S(n,4,2)$. Recall that the codeowrds of weight 4 of H forms $S(n,4,3)$ [*Assmuss, Mattson*, (1967)]. Hence from the partition of H into subcodes $P_{\sigma,i}$ of Theorem 2 we obtain

Theorem 3.

For any $\sigma = 2, \dots, 2^{\mu-1}$, $(\sigma \pm 1, 2^{\mu}) = 1$, *the partition of* H *into* $P_{\sigma,i}$, $i = 1, \dots, n/2$, *induces the partition of* $S(n,4,3)$ *into the Steiner systems* $S_{\sigma,i} = S(n,4,2)$.