On the Preparata-like codes

D. V. Zinoviev dzinov@iitp.ru
V. A. Zinoviev zinov@iitp.ru
A.A. Kharkevich Institute for Problems of Information Transmission, Moscow, Russia

Abstract. A class of Preparata-like group codes is considered. It was suggested by Baker, van Lint and Wilson and re-stated in a different form by Ericson. We show that all such codes are inside the Hamming code providing its partition into the cosets of the Preparata-like codes. This partition induces 2-resolvable Steiner quadruple systems.

1 Introduction

Let $E$ be the binary alphabet $E = \{0, 1\}$. A code $C$ is any subset of $E^n$. Denote a binary code $C$ of length $n$ with the minimum (Hamming) distance $d$ and cardinality $N$ as an $(n, d, N)$-code. Denote by $\text{wt}(x)$ the Hamming weight of vector $x$ over $E$, and by $d(x, y)$ the Hamming distance between the vectors $x, y \in E^n$.

A Steiner system $S(v, k, t)$ is a pair $(X, B)$ where $X$ is a $v$-set and $B$ is a collection of $k$-subsets (blocks) of $X$ such that every $t$-subset of $X$ is contained in exactly one block of $B$. A system $S(v, 4, 3)$ is called a Steiner quadruple system.

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.

For a code $C$ and an arbitrary binary vector $x$ define the distance between $x$ and $C$

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

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

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

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

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

1This work has been partially supported by the Russian fund of fundamental researches (under the project No. 12 - 01 - 00905).
Definition 1. Let \( n = 2^m \), \( m = 2, 3, \ldots \) A binary \((n, 6, 2^{n-4m})\)-code is called a Preparata-like code and denoted \( P \).

Let \( n = 2^m \), \( m = 2, 3, \ldots \) A binary \((n, 4, 2^{n-m-1})\)-code is called a Hamming-like code and denoted \( H \).

We assume that any Preparata-like code \( P \) or any Hamming-like code \( H \) contains the zero vector \( 0 = (0, \ldots, 0) \). Alternatively, denote by \( P(i) \), the Preparata-like code which contains a codeword of weight \( i \) and no codewords of a smaller weight. Thus \( P(0) = P \). For any code \( C \), let \( C_j \) be the set of its codewords of weight \( j \).

Two binary codes \( C \) and \( C' \) with the same parameters are equivalent if and only if there exists a binary vector \( x \) and a permutation \( \sigma \) (of coordinate set \( J \)) such that

\[
C + x = \sigma(C').
\]

It was shown in [1] (and independently in [2]) that the original Preparata codes \( P \) (i.e. codes that were constructed by Preparata [3]) of length \( n = 4^m \), \( m = 2, 3, \ldots \) define a 2-resolvable Steiner quadruple system \( S(n, 4, 3) \) (which corresponds to the words of weight four of the binary extended Hamming code \( H \) which contains \( P \)). The partition of code \( H \) into the shifts of \( P \) induce a 2-resolvable system \( S(n, 4, 3) \). Same results were obtained independently in [4] and [5] for the generalized Preparata codes. The \( \mathbb{Z}_4 \)-linear Preparata codes were constructed in [6]. They turned out to be non-equivalent to the earlier known Preparata codes and also induce the 2-resolvable Steiner systems \( S(n, 4, 3) \). An infinite class of 2-resolvable Steiner systems \( S(n, 4, 3) \), where \( n \) is not a power of 4 was given in [7].

The goal of this paper is to consider the group structure of the Preparata-like codes of [5] (see also [12] and [13]). Any such code lies in the linear Hamming code and induces its partition into the cosets by this code. This induces the new partitions of Steiner systems \( S(n, 4, 3) \) into disjoint systems \( S(n, 4, 2) \).

2 Preliminary Results

We will recall some known results.

Lemma 1. [9]. For any extended Hamming-like code \( H \) of length \( n \), the set \( H_4 \) is a Steiner system \( S(n, 4, 3) \).

Lemma 2. [1]. For any extended Preparata-like code \( P \) there exists an extended Hamming-like code \( H \) which contains it, i.e. \( P \subset H \). Moreover the code \( H \) is obtained by adding all vectors \( x \in E^n \) to the set \( P \) lying at a distance 4 from it, namely

\[
H = P \cup P(4).
\]
Lemma 3. [10]. Let $P$ be a Preparata-like code of length $n$. Let $P^{(4)}$ be its shift by a word of weight four. Then, the set $P^{(4)}_4$ (the words of $P^{(4)}$ of weight four) is a Steiner system $S(n, 4, 2)$.

According to Lemma 1 the set $H_4$ is the Steiner system $S(n, 4, 3)$. Using the last two lemmas we obtain the following result.

Theorem 1. [1, 2]. For any $m$, $m = 2, 3, \ldots$, there exists a $2$-resolvable Steiner system $S(4^m, 4, 3)$.

It turned out [4 – 6] that for all constructed Preparata-like codes $P$ the corresponding Hamming-like codes $H$, which contain codes $P$, partitioned into the shifts of the code $P$. These partitions induce the $2$-resolvable Steiner systems $S(n, 4, 3)$. The same is true, of course, for any $\mathbb{Z}_4$-linear Preparata-like codes of [11].

3 Main results

We consider a class of the Preparata-like codes of [5] presented in a different form of [13]. Let $\mu \geq 3$ be an odd number and consider the functions $z : \mathbb{F}_{2^\mu} \rightarrow \mathbb{F}_4$. Let $\text{Tr}(z) = z + z^2$ be a trace function from $\mathbb{F}_4$ into $\mathbb{F}_2$. For $z \in \mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, where $\omega^2 = \omega + 1$, define $x, y \in \mathbb{F}_2$ as follows:

\[ x = \text{Tr}(\omega z) = z \omega + z^2 \omega^2, \quad y = \text{Tr}(\omega^2 z) = z \omega^2 + z^2 \omega, \]

Note that

\[ z = x \omega + y \omega^2, \quad z^2 = x \omega^2 + y \omega, \]

and

\[ z^3 = x + y + xy = \begin{cases} 0, & z = 0, \\ 1, & z \neq 0. \end{cases} \]

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 $\rho$ of $\mathbb{F}_4$, induced by the following weight function $w_{t_4}$:

\[ w_{t_4}(0) = 0, \quad w_{t_4}(\omega) = w_{t_4}(\omega^2) = 1, \quad w_{t_4}(1) = 2. \]

so that $\rho(a, b) = w_{t_4}(a + b)$. Since $\mu$ is odd, the field $\mathbb{F}_4$ is not contained in $\mathbb{F}_{2^\mu}$ and in particular the elements $\omega$ and $\omega^2$ are not contained in $\mathbb{F}_{2^\mu}$. Thus any function $z : \mathbb{F}_{2^\mu} \rightarrow \mathbb{F}_4$ is of the form $z(u) = z_1(u) \omega + z_2(u) \omega^2$. Extend the weight function $w_{t_4}$ to the set $\mathcal{F}$ in a natural way:

\[ w_{t_4}(z) = \sum_{u \in \mathbb{F}_{2^\mu}} w_{t_4}(z(u)). \]
Let $\mathcal{F}$ be the set of functions $z : \mathbb{F}_{2^\mu} \to \mathbb{F}_4$ which satisfy the following equalities:

$$\sum_u z(u) = 0 \quad (1)$$

$$\sum_u u(z_1(u) + z_2(u)) = 0 \quad (2)$$

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

Let $\sigma$ be a power of 2, so that $2 \leq \sigma \leq 2^\mu - 1$ and $(\sigma \pm 1, 2^\mu) = 1$ (note that Ericson [13] considered the case $\sigma = 2$). Let $\mathcal{F}_\sigma$ be the subset of functions of $\mathcal{F}$, which satisfy the following equality:

$$\sum_u u^{\sigma+1}(z_1(u) + z_2(u)) = \left(\sum_u uz(u)\right)^{\sigma+1}, \quad (3)$$

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

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

$$\lambda_z = \sum_{u \in \mathbb{F}_{2^\mu}} u z(u). \quad (4)$$

Note that since $\omega + \omega^2 = 1$, the condition (2) implies that

$$\lambda_z = \sum_{u \in \mathbb{F}_{2^\mu}} u(z_1(u)\omega + z_2(u)\omega^2) = \sum_{u \in \mathbb{F}_{2^\mu}} uz_1(u) = \sum_{u \in \mathbb{F}_{2^\mu}} uz_2(u).$$

Now one can 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

$$c = a \star b = c_1\omega + c_2\omega^2, \quad (5)$$

where

$$c_1(u) = a_1(u + \lambda_b) + b_1(u),$$

$$c_2(u) = a_2(u) + b_2(u).$$

It is shown in [13] for the case $\sigma = 1$, and one can do it for $\sigma > 1$ that the set $\mathcal{F}$ with the $\star$ operation is a non-commutative group and $\mathcal{F}_\sigma$ is a subgroup of $\mathcal{F}$, for any $1 \leq \sigma \leq \mu - 1$. One can show that $[\mathcal{F} : \mathcal{F}_\sigma]$ is equal to $2^\mu$ and we have that

$$\mathcal{F} = \bigcup_{i=1}^{2^\mu} \mathcal{F}_\sigma \star f_i, \quad (6)$$

where $f_1, \ldots, f_{2^\mu} \in \mathcal{F}$ are the coset representatives.
Clearly, the identity element of $F_\sigma$ is the zero function denoted by $0$. The inverse $z^{-1}(u)$ to $z(u)$ is the function such that $z_1^{-1}(u + \lambda z) = z_1(u)$, i.e. $z_1^{-1}(u) = z_1(u + \lambda z)$ and $z_2^{-1}(u) = z_2(u)$. Note that if $c \in F$, then it is easy to check that multiplication by $c$ on the right is distance preserving. Thus

$$\rho(a \ast c, b \ast c) = \rho(a, b) = \rho(0, b \ast a^{-1}) = \text{wt}_4(b \ast a^{-1}).$$  \hfill (7)

For a given positive odd number $\mu$, $\mu \in \{3, 5, 7, \ldots\}$, and $\sigma = 2, \ldots, 2^{\mu-1}$, $(\sigma \pm 1, 2^\mu) = 1$ define a non-commutative Preparata-like code of Ericson [13] type as a binary code of length $n = 2^m$, where $m = \mu + 1$. It is viewed as the set of values $z(u) \to [x(u), y(u)]$ of the functions $z \in F_\sigma$.

Equations (1) and (2) given in terms of the functions $z \in F$ can be written in terms of their values $x$ and $y$ as follows:

$$\sum_{u \in \mathbb{F}_{2^\mu}} x(u) = \sum_{u \in \mathbb{F}_{2^\mu}} y(u) = 0 \quad (8)$$

$$\sum_{u \in \mathbb{F}_{2^\mu}} u \cdot x(u) = \sum_{u \in \mathbb{F}_{2^\mu}} u \cdot y(u) = \lambda \quad (9)$$

Equation (3) given in terms of the functions $z \in F_\sigma$ can be written (in addition to (8) and (9)) in terms of their values $x$ and $y$ as follows:

$$\sum_{u \in \mathbb{F}_{2^\mu}} u^{\sigma+1} x(u) + \sum_{u \in \mathbb{F}_{2^\mu}} u^{\sigma+1} y(u) = \lambda^{\sigma+1}. \quad (10)$$

Note that the first two conditions define the linear Hamming code $H$ of length $n = 2^{\mu+1}$. The Preparata-like codes in this form were presented in [5].

**Theorem 2.** [5] Let $P_\sigma$ be a code of length $n = 2^{\mu+1}$, given by equations (1)-(3). For any odd number $\mu \geq 3$ and any $\sigma = 2, \ldots, 2^{\mu-1}$, $(\sigma \pm 1, 2^\mu) = 1$ 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.

Since $P_\sigma$ is a non-commutative group, it follows that for any $\mu$ and $\sigma$ these codes are different from the known Preparata-like codes. In particular they are different from the Preparata-like $\mathbb{Z}_4$-linear codes, which for $n \geq 64$ are the subcodes of the corresponding $\mathbb{Z}_4$-linear Hamming-like codes [11] (and are defined by the commutative group over $\mathbb{Z}_4$). We are not aware of any other group structures for the other known Preparata-like codes [3-5] (which are all subcodes of the Hamming codes).

Moreover, let $P_{\sigma,i}$ be the set of values of the functions $F_\sigma \ast f_i$. Due to (7), the minimal distance of $P_{\sigma,i}$ is 6. Taking into account (6), we have:
Theorem 3. The code $P_\sigma$ 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 $P_\sigma$, i.e. we have

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

According to Lemma 3 the set of codewords of weight 4 of $P_{\sigma,i}$ forms a Steiner system $S(n,4,2)$. Hence from the partition of $H$ into subcodes $P_{\sigma,i}$ of Theorem 3 we obtain the following result. 

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

**References.**