New infinite families of 3-designs from preparata codes over $\mathbb{Z}_4$\(^1\)

Tor Helleseth\(^a\), Chunming Rong\(^a,*\), Kyeongcheol Yang\(^b\)

\(^a\) Department of Informatics, University of Bergen, Haytekologisenteret, N-5020 Bergen, Norway
\(^b\) Department of Electronic Communication Engineering, Hanyang University, Seoul 133-791, South Korea

Received 7 October 1997; accepted 5 January 1998

Abstract

We consider $t$-designs constructed from codewords in the Preparata code $\mathcal{P}_m$ over $\mathbb{Z}_4$. A new approach is given to prove that the support (size 5) of minimum Lee weight codewords form a simple 3-design for any odd integer $m \geq 3$. We also show that the support of codewords with support size 6 form four new families of simple 3-designs, with parameters $(2^m, 6, 2^m - 8)$, $(2^m, 6, 5 \cdot (2^{m-1} - 4))$, $(2^m, 6, 20 \cdot (2^{m-1} - 4)/3)$ and $(2^m, 6, 18 \cdot (2^{m-1} - 4))$, for any odd integer $m \geq 5$. Codewords with support size 7 are also investigated by computer search. © 1999 Elsevier Science B.V. All rights reserved

Keywords: Linear codes over $\mathbb{Z}_4$; Preparata codes; $t$-Designs

1. Introduction

A $t$-$(v, k, \lambda)$ design is a pair $(\mathcal{X}, \mathcal{B})$ where $\mathcal{X}$ is a $v$-element set of points and $\mathcal{B}$ is a collection of $k$-element subsets of $\mathcal{X}$ (called blocks) with the property that every $t$-element subset of $\mathcal{X}$ is contained in exactly $\lambda$ blocks. A design is simple if no two blocks are identical. Many designs can be constructed from codes over a finite field $F_q$ with $q$ elements. The Assmus–Mattson theorem [1] gives necessary conditions for the support of the codewords of constant weight in a code to form a $t$-design.

For codes over $\mathbb{Z}_4$ (the ring of integers modulo 4) no similar theorem has been found. Recently, Harada [4] was able to construct new 5-designs from the lifted Golay code over $\mathbb{Z}_4$. These designs were constructed by a computer search. In Helleseth

\(^1\) This work was supported in part by the Korea Science and Engineering Foundation (KOSEF) under Grant Number 981-0916-080-2, and by the Norwegian Research Council under Grant Numbers 107542/410 and 107623/420.

* Corresponding author. E-mail: chunming.rong@ii.uib.no.
et al. [7], an infinite family of 3-(2\(^m\), 5, 10) design is given for any odd integer \(m \geq 3\) by using the support (size 5) of minimum Lee weight codewords in the Preparata code over \(\mathbb{Z}_4\).

In this paper, we consider also the codewords of the Preparata code over \(\mathbb{Z}_4\). First, the infinite family of 3-(2\(^m\), 5, 10) design given by Helleseth et al. [7], is reproved by a different approach. Second, four more new infinite families of 3-designs, from the support of codewords with support size 6 are constructed. Third, some possible 3-designs from the support of codewords with support size 7 are also investigated by computer search.

A linear code \(\mathcal{C}\) over \(\mathbb{Z}_4\) with block length \(n\) is an additive subgroup of \(\mathbb{Z}_4^n\). The Lee weights of the elements 0, 1, 2, 3 in \(\mathbb{Z}_4\) are 0, 1, 2, 1, respectively. The Lee weight of a vector \(a \in \mathbb{Z}_4^n\) is defined to be the sum of the Lee weights of its components. The Gray map \(\phi: \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^4\) is defined by \(\phi(0) = 00\), \(\phi(1) = 01\), \(\phi(2) = 11\), and \(\phi(3) = 10\). In general, the binary code defined by \(C = \phi(\mathcal{C})\) is a nonlinear binary code of length 2\(n\).

Let \(R_m\) be a Galois ring of characteristic 4 with 4\(^m\) elements and \(\mathbb{R}_m^*\) be the set of units of \(\mathbb{R}_m\). \(\mathbb{R}_m^*\) has a multiplicative cyclic subgroup of order 2\(^m\) - 1. Let \(\mathcal{F}_m = \{0, 1, \beta, \ldots, \beta^{2^m - 2}\}\), where \(\beta \in \mathbb{R}_m^*\) is an element of order 2\(^m\) - 1. Any element \(z \in \mathbb{R}_m\) can be expressed uniquely as \(z = A + 2B\) for \(A, B \in \mathcal{F}_m\). Let \(\mu\) denote the modulo-2 reduction map. Note that \(\mu(\beta)\) is a primitive element in the finite field \(\mathbb{F}_{2^m}\) with 2\(^m\) elements, thus \(\mu(\mathcal{F}_m) = F_{2^m}\) (see [3,9] for details). The Frobenius map \(\sigma\) from \(R_m\) to \(R_m\) is defined by \(\sigma(z) = A^2 + 2B^2\) and the trace map from \(R_m\) to \(\mathbb{Z}_4\) is defined by

\[
T(z) = \sum_{j=0}^{m-1} \sigma^j(z). \tag{1}
\]

Obviously, \(T(\cdot)\) is linear over \(\mathbb{Z}_4\). Let \(\text{tr}(x)\) denote the trace function from \(\mathbb{GF}(2^m)\) to \(\mathbb{GF}(2)\). The commutativity relationship between \(T(\cdot)\) and \(\text{tr}(\cdot)\) is

\[
\mu(T(z)) = \text{tr}(\mu(z)). \tag{2}
\]

The Kerdock code \(\mathcal{K}_m\) of length 2\(^m\) over \(\mathbb{Z}_4\) is defined [3] by

\[
\mathcal{K}_m = \{c(\gamma, \xi) | \gamma \in R_m, \xi \in \mathbb{Z}_4\}
\]

where \(c(\gamma, \xi)\) is a vector in \(\mathbb{Z}_4^{2^m}\) indexed by the elements of \(\mathcal{F}_m\) such that \(c(\gamma, \xi)_x = T(\gamma X) + \xi\) for all \(X \in \mathcal{F}_m\). Clearly, \(\mathcal{K}_m\) has 4\(^{m+1}\) codewords.

The Lee weight of \(\xi \in \mathbb{Z}_4\) is related to the real part of \(i\xi\) via \(w_L(\xi) = 1 - \text{Re}(i\xi)\), where \(i = \sqrt{-1}\) and \(\text{Re}(i\xi)\) is the real part of \(i\xi\). Hence we have

\[
w_L(c(\gamma, \xi)) = 2^m - \text{Re} \left( i^\xi \sum_{x \in \mathcal{F}_m} i^{T(\gamma X)} \right)
\]

\[
= 2^m - \text{Re}(i^\xi \Gamma(\gamma)) \tag{3}
\]

where

\[
\Gamma(\gamma) = \sum_{X \in \mathcal{F}_m} i^{T(\gamma X)}. \tag{4}
\]
Hence, the distribution of the exponential sum $F(y)$ determines the Lee weight distribution of $\mathcal{K}_m$. The Lee weight distribution of $\mathcal{K}_m$ is well known in [3]. For $c(\gamma, \zeta) \in \mathcal{K}_m$, the set of values for $i^2 F(y)$ is $\{0, e^{\sqrt{q}, e^{3\sqrt{q}}, e^{e^{5\sqrt{q}}, e^{7\sqrt{q}}, \pm iq, \pm q}\}$. See [13] or [6] for more detailed properties of $F(y)$.

The Preparata code $P_m$ of length $2^m$ over $\mathbb{Z}_4$ is the code over $\mathbb{Z}_4$, whose parity-check matrix is given by

$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \beta^2 & \cdots & \beta^{2^m-2} \end{bmatrix}. \quad (5)$$

In [3], it is shown that if $m$ is odd, then $P_m$ has minimum Lee weight 6 and its Gray map $P_m = \phi(P_m)$ gives a $(2^{m+1}, 2^{m+1} - 2^{m-2}, 6)$ binary nonlinear code. The binary code $P_m$ has the same Hamming weight distribution as the original Preparata code [10].

The support of a vector $e = (c_1, c_2, \ldots, c_n)$ is the subset of $\{1, 2, \ldots, n\}$ given by $\{j \mid c_j \neq 0\}$. From codewords of the same support size $k$ in a code, it may be possible to construct $t$-designs with $v = n$ for an integer $t$.

It is known that the nonlinear binary Preparata code contains 3-designs ([11] or [10, p. 473]). However, those 3-designs have different parameters than the 3-designs obtained from $P_m$ in this paper.

In [2], all known infinite families of simple $t$-designs with $t \geq 3$ are listed. The parameters, $(2^m, 6, 2^m - 8), (2^m, 6, 5 \cdot (2^{m-1} - 4)), (2^m, 6, 20 \cdot (2^{m-1} - 4)/3)$ and $(2^m, 6, 18 \cdot (2^{m-1} - 4))$, for any odd integer $m \geq 5$, of the four infinite families of simple 3-designs given in this paper are not listed in [2] and therefore are new. Also the constructions of these 3-designs are new.

2. Some useful lemmas

Let $(c_X)_{X \in \mathcal{F}_n}$ be a codeword of the Preparata code $P_m$. Then it must satisfy

$$\sum_{X \in \mathcal{F}_n} c_X = 0 \quad \text{and} \quad \sum_{X \in \mathcal{F}_n} c_X X = 0.$$

These relations give an invariant property of $P_m$.

**Lemma 1** (Hammons et al. [3]). *The Preparata code defined in (5) is invariant under the doubly transitive group of ‘affine’ permutations of the form $X \rightarrow (AX + B)^{2^m}$ where $A, B \in \mathcal{F}_m$ and $A \neq 0$.**

The next lemma shows how an equation over $R_m$ can be represented as two equivalent equations over $F_{2^m}$.


Lemma 2 (Helleseth and Kumar [5]). Let $e = (e_X)_{X \in \mathcal{F}_m}$ and let $E_j = \{X \mid e_X = j\}$ for $j = 0, 1, 2, 3$. The equation given by
\[ \sum_{X \in \mathcal{F}_m} e_X X = A + 2B, \quad A, B \in \mathcal{F}_m, \quad e_X \in \mathbb{Z}_4 \]
is equivalent to the two binary equations
\[ a = \sum_{X \in E_1 \cup E_3} x, \quad b^2 = \sum_{X \in E_2 \cup E_3} x^2 + \sum_{X \leq Y} xy, \]
where $x, y, a, b$ are the modulo-2 reductions of $X, Y, A, B$, respectively, and $<$ is any ordering of the elements in $\mathcal{F}_m$.

The next lemma is used to determine the solvability of a quadratic equation over $\mathbb{F}_{2^m}$.

Lemma 3 (MacWilliams and Sloane [10, p. 278]). Let $a \neq 0$, $b \in \mathbb{F}_{2^m}$. The quadratic equation $x^2 + ax + b = 0$ has two roots in $\mathbb{F}_{2^m}$ if and only if $tr(b/a^2) = 0$.

3. 3-Designs in Preparata code over $\mathbb{Z}_4$

3.1. 3-Designs from codewords of minimum Lee weight

A vector is denoted to be of the type $1^n 2^m 3^t 0^g$ if $j$ occurs $n_j$ times, $j = 0, 1, 2, 3$, as a component. The codewords of minimum Lee weight in the Preparata code $\mathcal{P}_m$ for any odd integer $m$ are of the type $1^3 2^1 3^1 0^m$ or $1^1 2^1 3^3 0^{m-1}$. Changing the sign of a codeword leads to a codeword with the same support. Hence, to construct simple designs (designs without repeated blocks), we only consider the former type. Note that the codewords of minimal Lee weight have Hamming weight 5. In [7], it is shown that the support of these minimum Lee weight codewords form a simple 3-(2, 5, 10) design. In the following, we give a different proof that these minimum Lee weight codewords form a simple 3-(2, 5, $\lambda$) design for an integer $\lambda$.

Theorem 1. The support of the codewords of the type $1^3 2^1 3^1 0^{m-5}$ (or $1^1 2^1 3^3 0^{m-5}$) in the Preparata code $\mathcal{P}_m$ over $\mathbb{Z}_4$ form a 3-(2, 5, $\lambda$) design for an integer $\lambda$ and any odd integer $m \geq 3$.

Proof. We denote the codewords of the type $1^3 2^1 3^1 0^{m-5}$ as minimal and will show that for any three coordinates $X_1, X_2$ and $X_3$ in $\mathcal{F}_m$, there are exactly the same number, say $\lambda$, of minimal codewords with nonzero support at these coordinates. Since the Preparata code is invariant under the doubly transitive group of ‘affine’ permutations by Lemma 1, we can assume without loss of generality that the first two coordinates are $X_1 = 0$ and $X_2 = 1$. Furthermore, the third coordinate is chosen arbitrary to be $X_3 = A \in \mathcal{F}_m \setminus \{0, 1\}$. Let $a = \mu(A)$.
Let $C$ be the punctured code from the Preparata code $\mathcal{P}_m$ over $\mathbb{Z}_4$ at the coordinates 0, 1, and $A$. Let $c(\gamma, \xi) = (c_0, c_1, c_2, \ldots, c_{3^m-2}) \in \mathcal{X}_m = \mathcal{P}_m^\perp$, where $c_X = T(\gamma X) + \xi$ for $\forall X \in \mathcal{F}_m$. Let

$$\mathcal{H}' = \{ c(\gamma, 0) \mid T(\gamma) = T(\gamma A) = 0 \}$$

be the set of codewords with $c_0 = c_1 = c_A = 0$ in $\mathcal{X}_m$. The dual of $C$, denoted by $C^\perp$, is obtained by puncturing these three coordinates from $\mathcal{H}'$.

Consider the complete weight distribution of $C^\perp$. The cardinality $N$ of $C^\perp$ is

$$N = | \{ \gamma \in R_m \mid T(\gamma) = T(\gamma A) = 0 \} |.$$

Consider the following equality:

$$16N = \sum_{\gamma \in R_m} \left( \sum_{v_1 \in \mathbb{Z}_4} i^{v_1 T(\gamma)} \right) \left( \sum_{v_2 \in \mathbb{Z}_4} i^{v_2 T(\gamma A)} \right). \quad (6)$$

Exchanging the orders of the sum and collecting exponents of $i$ in (6), we have

$$16N = \sum_{v_1, v_2 \in \mathbb{Z}_4} \sum_{\gamma \in R_m} i^{T(v_1 + v_2 A) \gamma}. \quad (7)$$

Since

$$\sum_{\gamma \in R_m} i^{T(\gamma)} = \begin{cases} 0 & \text{if } t \neq 0 \\ 4^m & \text{if } t = 0 \end{cases}$$

and $A \in \mathcal{F}_m \setminus \{0, 1\}$, the only non-zero contribution in the right hand side sum of (7) is when $v_1 = v_2 = 0$. Therefore, $16N = 4^m$, i.e., $N = 4^{m-2}$.

Let $c(\gamma, 0) \in \mathcal{H}'$. Then, $c_X = T(\gamma X)$. Consider the $I(\gamma)$ defined in (4). Since $\mathcal{H}'$ has no codewords with all 1 or all 2 or all 3, we have $I(\gamma) \not\in \{-2^m, \pm i2^m\}$. On the other hand, $I(\gamma)$ may have value in $\{0, \sqrt[4]{2^m}, \sqrt[4]{2^m}, \sqrt[4]{2^m}, \sqrt[4]{2^m}, \sqrt[4]{2^m}, \sqrt[4]{2^m}, \sqrt[4]{2^m}, \sqrt[4]{2^m}, 2^m\}$ and let $N_2, N_1, N_3, N_5, N_7, N_0$ denote respectively the number of the corresponding codewords in $\mathcal{H}'$. Hence,

$$N = 4^{m-2} = N_1 + N_3 + N_5 + N_7 + N_2 + N_0. \quad (8)$$

We will show in the following that $N_2, N_1, N_3, N_5, N_7, N_0$ are all independent of the choice of $A$.

First, we have $N_0 = 1$ since only $c(0, 0)$ in $\mathcal{H}'$ gives $I(\gamma) = 2^m$.

Second, we compute $N_2$. Since $I(\gamma) = 0$ only if $\gamma = 2\gamma^*$ for some $\gamma^* \in \mathcal{F}_m \setminus \{0\}$, we have

$$N_2 = | \{ \gamma \in R_m \mid T(\gamma) = T(\gamma A) = 0 \text{ and } \gamma = 2\gamma^* \text{ for } \gamma^* \in \mathcal{F}_m \setminus \{0\} \} |$$

$$= | \{ \tilde{\gamma} \in \mathcal{F}_{2^m} \mid \text{tr}(\tilde{\gamma}) = \text{tr}(\tilde{\gamma} A) = 0 \} |$$

$$= | \{ \tilde{\gamma} \in \mathcal{F}_{2^m} \mid \text{tr}(\tilde{\gamma}) = 0 \} |.$$
where \( \bar{\gamma} = \mu(\gamma^*) \) and \( F_{2n}^* = F_{2n} \setminus \{0\} \). Consider the following equality:

\[
4N_2 = \sum_{\bar{\gamma} \in F_{2n}^*} \left( \sum_{x_1=0}^{1} (-1)^{x_1 \text{tr}((\bar{\gamma}))} \right) \left( \sum_{x_2=0}^{1} (-1)^{x_2 \text{tr}((\bar{\gamma}))} \right)
\]

\[
= \sum_{x_1, x_2 \in \mathbb{Z}_2} \sum_{\bar{\gamma} \in F_{2n}^*} (-1)^{\text{tr}((x_1 + x_2 \bar{\gamma}))}
\]

\[
= 2^m - 4.
\]

Hence, \( N_2 = 2^m - 2 - 1 \).

Then, we need four equations in order to solve the numbers \( N_1, N_3, N_5 \) and \( N_7 \). By Eq. (8), we have the first equation

\[
N_1 + N_3 + N_5 + N_7 = 4^m - 2 - 2^m - 2.
\]

Let \( B \in \mathcal{F}_m \setminus \{0, 1, A\} \) and \( N_{B_B} \) denote the number of codewords in \( \mathcal{X}' \) with value \( j \) at coordinate \( B \). By the same arguments as above, we have the equality:

\[
64N_{B_0} = \sum_{v_1, v_2, v_3 \in \mathbb{Z}_4} \sum_{\bar{\gamma} \in F_{2n}} i_{\bar{\gamma}}^{T((v_1 + v_2 A + v_3 B)\bar{\gamma})} = 4^m.
\]

Hence, \( N_{B_0} = 4^{m-3} \neq N \) and there is no column with all 0 in \( \mathcal{C}^\perp \). Furthermore, it can be shown accordingly that \( N_{B_1} = N_{B_2} = N_{B_3} = N_{B_0} = 4^{m-3} \). In other words, if we put all codewords of \( \mathcal{C}^\perp \) together, each element of \( \mathbb{Z}_4 \) appears exactly \( 4^{m-3} \) times in each column. Consider the following sum:

\[
S_1 = \sum_{c(\gamma, 0) \in \mathcal{X}'} \sum_{X \in \mathcal{X}_n} i^{cX} = \sum_{c(\gamma, 0) \in \mathcal{X}'} \sum_{X \in \mathcal{X}_n} i^{T(\gamma X)}.
\]

Exchanging the order of the sum in (10), we have

\[
S_1 = \sum_{X \in \mathcal{X}_n} \sum_{c(\gamma, 0) \in \mathcal{X}'} i^{cX} = 3 \cdot 4^{m-2} + (2^m - 3)4^{m-3}(i^0 + i^1 + i^2 + i^3) = 3 \cdot 4^{m-2}.
\]

Using the definition of \( \Gamma(\gamma) \) in (4), the sum \( S_1 \) in (10) becomes

\[
S_1 = \sum_{c(\gamma, 0) \in \mathcal{X}'} \Gamma(\gamma) = \sqrt{2^m(N_1 \varepsilon + N_3 \varepsilon^3 + N_5 \varepsilon^5 + N_7 \varepsilon^7)} + N_2 \cdot 0 + N_0 \cdot 2^m.
\]

From Eqs. (11) and (12), we obtain the following equality:

\[
(N_1 - N_3) \varepsilon + (N_3 - N_7) \varepsilon^3 = (3 \cdot 2^{2m-4} - 2^m)/\sqrt{2^m}.
\]

Substituting \( \varepsilon = (1 + i)/\sqrt{2} \) into the last equation and comparing the real part and the imaginary part of both sides, we obtain two more needed equations:

\[
N_1 - N_5 - N_3 + N_7 = 2^{m+1}(3 \cdot 2^{m-4} - 1),
\]

\[
N_1 - N_5 + N_3 - N_7 = 0.
\]
The last needed equation is obtained by considering the sum $S_2$, where

$$S_2 = \sum_{c(\gamma, 0) \in \mathcal{F}} \left( \langle T(\gamma) \rangle^2 \sum_{c(\gamma, 0) \in \mathcal{F}} \left( \sum_{X \in \mathcal{F}} i^{T(\gamma; X)} \right)^2 \right)$$

$$= \sum_{c(\gamma, 0) \in \mathcal{F}} \sum_{X, Y \in \mathcal{F}} i^{T(\gamma; X + Y + 2\sqrt{XY} + 2\gamma\sqrt{XY})} \quad \text{where } Z = X + Y + 2\sqrt{XY}$$

$$= \sum_{c(\gamma, 0) \in \mathcal{F}} \sum_{X, Z \in \mathcal{F}} i^{T(\gamma; X + Z + 2\gamma^2 X Z)}$$

$$= \sum_{c(\gamma, 0) \in \mathcal{F}} \sum_{Z \in \mathcal{F}} i^{T(\gamma; Z)} \sum_{X \in \mathcal{F}} (-1)^{\text{tr}(\mu(\gamma + \gamma^2 Z)X))}$$

$$= 2^m \sum_{T(\gamma) = 0} \sum_{Z \in \mathcal{F}} i^{T(\gamma; Z)} \quad \text{where } \mu(\gamma + \gamma^2 Z) = 0$$

Let $\gamma = \eta + 2\delta$ for $\eta, \delta \in \mathcal{F}_m$. Since $\mu(\gamma + \gamma^2 Z) = 0$ for $Z \in \mathcal{F}_m$, we have

$$\eta(1 + \eta Z) = 0 \mod 2.$$

Thus, $\eta = 0$ or $\eta = \frac{1}{2}$ (if $Z \neq 0$), i.e., $\gamma = 2\delta$ or $\gamma = \frac{1}{2} + 2\delta$ (if $Z \neq 0$). Hence,

$$S_2 = 2^m \sum_{\delta \in \mathcal{F}_m} \sum_{Z \in \mathcal{F}_m} i^{T(2\delta Z)} + 2^m \sum_{\delta \in \mathcal{F}_m} \sum_{Z \in \mathcal{F}_m \setminus \{0\}} \sum_{T(\gamma) = 0} \sum_{T(\gamma') = 0} \sum_{T((\gamma + \gamma^2 Z) = 0)} (-1)^{\text{tr}(\mu(Z\delta))}$$

$$= 2^m + 2^m i^{T(1)} \sum_{Z \in \mathcal{F}_m \setminus \{0\}} \sum_{\delta \in \mathcal{F}_m} \sum_{\text{tr}(\mu(\delta)) = \mu(\frac{1}{2} T(\frac{1}{2})) \text{ or } \text{tr}(\mu(\delta)) = \mu(\frac{1}{2} T(\frac{1}{2}))} (-1)^{\text{tr}(\mu(Z\delta))}$$

$$= 2^m$$

since for all $k_1, k_2 \in F_2$, \[ \sum_{\text{tr}(x) = k_1, \text{tr}(by) = k_2} (-1)^{\text{tr}(xy)} = 0 \]

if $y, b$ and 1 are linearly independent over $F_2^m$. We notice that $\mu(Z), a$ and 1 are linearly independent over $F_2^m$, since $T(\frac{1}{2} + 2\delta) = T((\frac{1}{2} + 2\delta)A) = 0$, i.e. $\text{tr}(\frac{1}{\mu(Z)}) = \text{tr}(\frac{a}{\mu(Z)}) = 0$. On the other hand, since

$$S_2 = 2^m(N_1 e^2 + N_3 e^6 + N_5 e^{10} + N_7 e^{14}) + N_2 \cdot 0 + N_0 \cdot 2^{2m},$$

we have $2^{2m} = 2^m(N_1 - N_3 + N_5 - N_7)i + 2^{2m}$, which then leads us to the last needed equation:

$$N_1 - N_3 + N_5 - N_7 = 0. \quad (15)$$
From Eqs. (9), (13)–(15), we obtain easily

\[ N_1 = N_7 = 4^{m-3} - 2^{m-4} + 2^{\frac{m-3}{2}} (3 \cdot 2^{m-4} - 1), \]
\[ N_3 = N_5 = 4^{m-3} - 2^{m-4} - 2^{\frac{m-3}{2}} (3 \cdot 2^{m-4} - 1), \]

while \( N_2 = 2^{m-2} - 1 \) and \( N_0 = 1 \). They are all independent of \( A \).

For each value of \( \Gamma(Y) = \eta + i\delta \), there is a corresponding codeword \( c(\gamma, 0) \in \mathcal{C}' \) with type \( 1^n 2^n 3^n 0^n 6 \), where \( n_1, n_2, n_3, n_0 \) can be obtained from the following:

\[ n_0 + n_1 + n_2 + n_3 = 2^m, \]
\[ n_0 + n_1i + n_2 i^2 + n_3 i^3 = \eta + i\delta, \]
\[ n_1 + n_3 = 2^{m-1}. \]

The first two equations come straightforwardly from the definition of \( \Gamma(Y) \) while the last equation is because of \( \mu(c(\gamma, 0)) \) is a codeword in the binary Hamming code. Therefore, the complete weight distribution of \( \mathcal{C}' \) is independent of the choice of \( A \). According to the MacWilliams transform [10], the complete weight distribution of \( \mathcal{C}' \) can be then obtained and also independent of the choice of \( A \).

A codeword of support size 2 in \( \mathcal{C} \), except those with support type 22, corresponds to a codeword of type \( 1^3 2^1 3^1 0^n 5 \) or \( 1^1 2^1 3^3 0^n 5 \) in \( \mathcal{R}_m \). Since changing the sign of a codeword of type \( 1^3 2^1 3^1 0^n 5 \) leads to a codeword of type \( 1^1 2^1 3^3 0^n 5 \). Hence, the number, say \( \lambda \), of minimal codewords (type \( 1^3 2^1 3^1 0^n 5 \)) with nonzero support at coordinates 0, 1 and \( A \) is equal to half of the number of codewords of support size 2, except those with support type 22, in \( \mathcal{C} \). Note that \( \lambda \) is independent of the choice of \( A \). Therefore, minimal codewords in \( \mathcal{R}_m \) form a \( 3-(2^m, 6, \lambda) \) design. \( \square \)

Actually, according to Table 1 derived from Helleseth et al. [7], we also know that \( \lambda = 10 \) in Theorem 1.

### 3.2. 3-Designs from codewords of support size 6

The codewords of support size 6 in the Preparata code \( \mathcal{R}_m \) for any odd integer \( m \) are of the type \( 1^3 2^0 3^1 0^n 6 \) or \( 1^4 2^2 3^0 0^n 6 \) or \( 1^3 2^0 3^3 0^n 6 \) or \( 1^2 2^2 3^0 0^n 6 \). From these codewords, we construct four new infinite families of simple 3-designs.

**Theorem 2.** The support of the codewords of type \( 1^5 2^0 3^1 0^n 6 \) in the Preparata code \( \mathcal{R}_m \) over \( \mathbb{Z}_4 \) form a \( 3-(2^m, 6, 2^m - 8) \) design for any odd integer \( m \geq 5 \).

**Theorem 3.** The support of the codewords of type \( 1^4 2^2 3^0 0^n 6 \) in the Preparata code \( \mathcal{R}_m \) over \( \mathbb{Z}_4 \) form a \( 3-(2^m, 6, 5 \cdot (2^m - 1 - 4)) \) design for any odd integer \( m \geq 5 \).

**Theorem 4.** The support of the codewords of type \( 1^3 2^0 3^3 0^n 6 \) in the Preparata code \( \mathcal{R}_m \) over \( \mathbb{Z}_4 \) form a \( 3-(2^m, 6, 20 \cdot (2^m - 1 - 4)/3) \) design for any odd integer \( m \geq 5 \).
Table 1
Number of codewords with a given support of size 5

<table>
<thead>
<tr>
<th>Case</th>
<th>0 1 a x x5</th>
<th># codewords</th>
<th>0 1 a x x5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 1 1 3 2</td>
<td>1</td>
<td>3 3 3 2 1</td>
</tr>
<tr>
<td>2</td>
<td>3 1 1 1 2</td>
<td>1</td>
<td>1 3 3 3 2</td>
</tr>
<tr>
<td>3</td>
<td>1 3 1 1 2</td>
<td>1</td>
<td>3 1 3 3 2</td>
</tr>
<tr>
<td>4</td>
<td>1 1 3 1 2</td>
<td>1</td>
<td>3 3 1 3 2</td>
</tr>
<tr>
<td>5</td>
<td>3 1 1 3 1</td>
<td>1</td>
<td>2 3 3 1 3</td>
</tr>
<tr>
<td>6</td>
<td>1 2 1 3 1</td>
<td>1</td>
<td>3 2 3 1 3</td>
</tr>
<tr>
<td>7</td>
<td>1 1 2 3 1</td>
<td>1</td>
<td>3 3 2 3 1</td>
</tr>
<tr>
<td>8a</td>
<td>2 1 3 1 1</td>
<td>1 if (\text{tr} \left( \frac{1}{a+1} \right) = 0)</td>
<td>2 3 1 3 3</td>
</tr>
<tr>
<td>8b</td>
<td>2 3 1 1 1</td>
<td>1 if (\text{tr} \left( \frac{1}{a+1} \right) = 1)</td>
<td>2 1 3 3 3</td>
</tr>
<tr>
<td>9a</td>
<td>1 2 3 1 1</td>
<td>1 if (\text{tr} \left( \frac{1}{a} \right) = 0)</td>
<td>3 2 1 3 3</td>
</tr>
<tr>
<td>9b</td>
<td>3 2 1 1 1</td>
<td>1 if (\text{tr} \left( \frac{1}{a} \right) = 1)</td>
<td>1 2 3 3 3</td>
</tr>
<tr>
<td>10a</td>
<td>1 3 2 1 1</td>
<td>1 if (\text{tr}(a) = 0)</td>
<td>3 1 2 3 3</td>
</tr>
<tr>
<td>10b</td>
<td>3 1 2 1 1</td>
<td>1 if (\text{tr}(a) = 1)</td>
<td>1 3 2 3 3</td>
</tr>
</tbody>
</table>

Theorem 5. The support of the codewords of type \(1^22^23^20^{n-6}\) in the Preparata code \(\mathcal{P}_m\) over \(\mathbb{Z}_4\) form a \(3-(2^n, 6, 18 \cdot (2^{m-1} - 4))\) design for any odd integer \(m \geq 5\).

In this paper, we give two methods to prove Theorem 2. The proofs of Theorem 3, Theorem 4 and Theorem 5 follow the same way. For full details, the reader is referred to [8].

Proof of Theorem 2. In the Preparata code \(\mathcal{P}_m\), we consider the codewords of type \(1^52^30^{n-6}\) with support \(\{X_1, \ldots, X_6\} \subset \mathcal{F}_m\). We will show that for any distinct coordinates \(X_1, X_2\) and \(X_3\), there are exactly \(2^m - 8\) codewords of this type. Since the Preparata code is invariant under the doubly-transitive group of 'affine' permutations by Lemma 1, we can assume without loss of generality that \(X_1 = 0\) and \(X_2 = 1\). Furthermore, we choose arbitrarily \(X_3 = A \in \mathcal{F}_m \setminus \{0, 1\}\). Let \(x_j = \mu(X_j)\) and \(a = \mu(A)\). Hence, \(x_1 = 0\), \(x_2 = 1\) and \(x_3 = a\). Let \(x_4 = x\).

Let \(U_{X_i}\) denote the nonzero values of such a codeword at the six corresponding locations \(X_i\) for \(i = 1, 2, \ldots, 6\). We will discuss the conditions for a codeword to have this support. For a such codeword, there are 4 possible ways for the values \(U_0, U_1\) and \(U_a\).

Note that \(X_1, X_2, \ldots, X_6\) are distinct elements of \(\mathcal{F}_m\) and \(0, 1, a, x, x_5, x_6\) are therefore distinct elements of \(F_{2^m}\).

Method 1: Merge coordinates and refer to lower support size.

Case 1: Let \(U_0 = U_1 = U_a = 1\). We will determine the number of codewords such that \(U_{X_4} = 3\) and \(U_{X_5} = U_{X_6} = 1\). Since they are codewords in the Preparata code, we have

\[X_1 + X_2 + X_3 + 3X_4 + X_5 + X_6 = 0.\]
Lemma 2 shows that this is equivalent to the following equations over $F_{2^m}$:

$$
1 + a + x + x_5 + x_6 = 0,
$$

$$
x^2 + a + x + x_5 + x_6 + ax + ax_5 + ax_6 + xx_5 + xx_6 + x_5x_6 = 0.
$$

Eliminating $x_5$ from the second equation by using the first equation, we obtain a quadratic equation in $x_6$:

$$
x_6^2 + (1 + a + x)x_6 + a + x + a^2 x + 1 + a^2 = 0. \quad (16)
$$

By Lemma 3, Eq. (16) has two distinct roots in $F_{2^m}$ if and only if $S = 0$, where

$$
S = \text{tr} \left( \frac{1 + a + a^2 + (1 + a)x}{1 + a^2 + x^2} \right)
$$

$$
= \text{tr} \left( \frac{1 + a + a^2}{1 + a^2 + x^2} + \frac{(1 + a + x)x}{1 + a^2 + x^2} + \frac{x^2}{1 + a^2 + x^2} \right)
$$

$$
= \text{tr} \left( \frac{1 + a + a^2}{1 + a^2 + x^2} \right). \quad (17)
$$

Note that $a^2 + a + 1 \neq 0$ since $a \in F_{2^m}$ and $m$ is odd. If $x$ runs through all elements of $F_{2^n}\{a+1\}$, there are exactly $2^{m-1} - 1$ of them that satisfy the trace condition $S = 0$ in (17). If $x = a + 1$, there is only one solution of Eq. (16). Hence, there are total $2(2^{m-1} - 1) + 1$ solutions.

However, we have to exclude codewords with support size smaller than 6, which occurs if 0, 1, $a, x, x_5, x_6$ are not distinct. All codewords with support size 5 is listed in Table 1, and the only codeword with support size 4 is of type $1^0 2^4 3^0 0^n - 4$. Because $a$ is chosen to be different from 0 and 1, we need only to check that $x, x_5, x_6$ are distinct and different from 0, 1, $a$. It is straightforward to verify that merging coordinates in this case does not give a codeword with support size 4. Hence, we need only to consider codewords with support size 5 from Table 1. Finally, because of the symmetry between $x_5$ and $x_6$, the total number is divided by 2 and is then equal to $2^{m-1} - 4$ according to Table 2.

Case 2a: Let $U_0 = 3, \ U_1 = U_4 = 1$. We will determine the number of codewords such that $U_{x_4} = U_{x_5} = U_{x_6} = 1$. Since they are codewords in the Preparata code, we have

$$
3X_1 + X_2 + X_3 + X_4 + X_5 + X_6 = 0.
$$

Lemma 2 shows that this is equivalent to the following equations over $F_{2^m}$:

$$
1 + a + x + x_5 + x_6 = 0,
$$

$$
a + x + x_5 + x_6 + ax + ax_5 + ax_6 + xx_5 + xx_6 + x_5x_6 = 0.
$$

Eliminating $x_5$ from the second equation by using the first equation, we obtain a quadratic equation in $x_6$:

$$
x_6^2 + (1 + a + x)x_6 + a + x + a^2 + x^2 = 0. \quad (18)
$$
Table 2
Count codewords in Case 1 by merging coordinates

<table>
<thead>
<tr>
<th>Case</th>
<th>0 1 a x x5 x6</th>
<th>(x, x5, x6) sol. cond.</th>
<th>Exception</th>
<th>Excl. vectors</th>
<th>#Excl. sol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 1 1 3 1 1</td>
<td>x = 0</td>
<td>0 1 1 1 1</td>
<td>1 0 1 1 1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>x = 1</td>
<td>1 1 0 1 1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>x = a</td>
<td>1 1 0 1 1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>tr( 1 + a + x^2 ) 0</td>
<td>x5 or x6 = x</td>
<td>1 1 1 0 1</td>
<td>1 0 1 1 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>x5 or x6 = 0</td>
<td>2 1 1 3 1</td>
<td>2 1 1 3 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>x5 or x6 = 1</td>
<td>1 2 1 3 1</td>
<td>2 1 1 3 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>x5 or x6 = a</td>
<td>1 1 2 3 1</td>
<td>2 1 1 3 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>x5 = x6</td>
<td>1 1 1 3 2</td>
<td>1 1 1 3 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total #sol.: (2(2^m-1) - 1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total #excl. sol.: 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>#codewd.: ((2^m-8)/2 = 2^{m-1} - 4)</td>
</tr>
</tbody>
</table>

By Lemma 3, this equation has two distinct roots in \(F_{2^m}\) if and only if \(S = 0\), where

\[
S = \text{tr} \left( \frac{1 + a + x + a(x + a) + x^2}{1 + a^2 + x^2} \right)
\]

\[
= \text{tr} \left( \frac{1}{1 + a + x} + \frac{a(x + a + 1)}{1 + a^2 + x^2} + \frac{a}{1 + a^2 + x^2} + \frac{x^2}{1 + a^2 + x^2} \right)
\]

\[
= \text{tr} \left( \frac{a + 1}{1 + a + x} + \frac{a + a^2 + 1}{1 + a^2 + x^2} + \frac{x^2 + a^2 + 1}{1 + a^2 + x^2} \right)
\]

\[
= \text{tr} \left( \frac{a}{1 + a^2 + x^2} \right) + 1. \quad (19)
\]

**Case 2b:** Let \(U_0 = 1\), \(U_1 = 3\), \(U_A = 1\). We will determine the number of codewords such that \(U_{X_4} = U_{X_5} = U_{X_6} = 1\). Since they are codewords in the Preparata code, we have

\[
X_1 + 3X_2 + X_3 + X_4 + X_5 + X_6 = 0.
\]

Lemma 2 shows that this is equivalent to the following equations over \(F_{2^m}\):

\[
1 + a + x + x_5 + x_6 = 0,
\]

\[
1 + a + x + x_5 + x_5 + ax + ax_5 + ax_6 + x x_5 + x x_6 + x_5 x_6 = 0.
\]

Eliminating \(x_5\) from the second equation by using the first equation, we obtain a quadratic equation in \(x_6\):

\[
x_6^2 + (1 + a + x)x_6 + a + x + ax + a^2 + x^2 = 0. \quad (20)
\]
By Lemma 3, this equations has two distinct roots in $F_{2^m}$ if and only if $S = 0$, where

$$S = \text{tr} \left( \frac{x(1 + a + x) + a + a^2}{1 + a^2 + x^2} \right)$$

$$= \text{tr} \left( \frac{x}{1 + a + x} + \frac{a}{1 + a + x} + \frac{a}{1 + a^2 + x^2} \right)$$

$$= \text{tr} \left( \frac{x + a + 1}{1 + a + x} + \frac{a + 1}{1 + a^2 + x^2} \right)$$

$$= \text{tr} \left( \frac{a + 1}{1 + a^2 + x^2} \right) + 1. \quad (21)$$

Case 2c: Let $U_0 = 1$, $U_1 = 1$, $U_A = 3$. We will determine the number of codewords such that $U_{x_1} = U_{x_5} = U_{x_6} = 1$. Since they are codewords in the Preparata code, we have

$$x_1 + x_2 + 3x_3 + x_4 + x_5 + x_6 = 0.$$}

Lemma 2 shows that this is equivalent to the following equations over $F_{2^m}$:

$$1 + a + x + x_5 + x_6 = 0,$$

$$a^2 + a + x + x_5 + x_6 + ax + ax_5 + ax_6 + xx_5 + xx_6 + x_5x_6 = 0.$$}

Eliminating $x_5$ from the second equation by using the first equation, we obtain a quadratic equation in $x_6$:

$$x_6^2 + (1 + a + x)x_6 + a + x + ax + 1 + x^2 = 0. \quad (22)$$

By Lemma 3, this equations has two distinct roots in $F_{2^m}$ if and only if $S = 0$, where

$$S = \text{tr} \left( \frac{x(1 + a + x) + a + 1}{1 + a^2 + x^2} \right)$$

$$= \text{tr} \left( \frac{x + a + 1}{1 + a + x} + \frac{a^2 + 1 + a + 1}{1 + a^2 + x^2} \right)$$

$$= \text{tr} \left( \frac{a^2 + a}{1 + a^2 + x^2} \right) + 1. \quad (23)$$

Table 3 summarizes Cases 2a–2c. Note that $a \notin \{0, 1\}$. By the same argument as in Case 1, there are totally $2(2^{m-1} - 1) + 1$ solutions for each case. However, we have to exclude 21 codewords with support size smaller than 6. Furthermore, because of the symmetry between $x, x_5$ and $x_6$, the total number is divided by 6 and is then equal to $2^{m-1} - 4$. 
Table 3
Count codewords in Case 2a, 2b and 2c by merging coordinates

<table>
<thead>
<tr>
<th>Case</th>
<th>x=0</th>
<th>x=1</th>
<th>a or x5 or x6 = x</th>
<th>x5 or x6 = 0</th>
<th>x5 or x6 = a</th>
<th>x5 = x6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2a</td>
<td>x=0</td>
<td>x=1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>when x ≠ a + 1</td>
<td>two distinct sol. iff.</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2 if tr(\frac{1}{a}) = 1</td>
</tr>
<tr>
<td></td>
<td>tr(\frac{a+1}{1+a^2+a^x}) = 1</td>
<td>x5 or x6 = x</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2 if tr(\frac{1}{a}) = 1</td>
</tr>
<tr>
<td></td>
<td>x5 or x6 = 0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>when x = a + 1</td>
<td>one sol.</td>
<td>x5 or x6 = 1</td>
<td>3</td>
<td>1</td>
<td>2 if tr(\frac{1}{a}) = 1</td>
</tr>
<tr>
<td></td>
<td>x5 or x6 = a</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2 if tr(\frac{1}{a}) = 1</td>
</tr>
<tr>
<td></td>
<td>x5 = x6</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2b</td>
<td>x=0</td>
<td>x=1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>when x ≠ a + 1</td>
<td>two distinct sol. iff.</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2 if tr(\frac{1}{a}) = 0</td>
</tr>
<tr>
<td></td>
<td>tr(\frac{a+1}{1+a^2+a^x}) = 1</td>
<td>x5 or x6 = x</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2 if tr(\frac{1}{a}) = 0</td>
</tr>
<tr>
<td></td>
<td>x5 or x6 = 0</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2 if tr(\frac{1}{a}) = 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>when x = a + 1</td>
<td>one sol.</td>
<td>x5 or x6 = 1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>x5 or x6 = a</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>x5 = x6</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2c</td>
<td>x=0</td>
<td>x=1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>when x ≠ a + 1</td>
<td>two distinct sol. iff.</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>2 if tr(\frac{1}{a}) = 0</td>
</tr>
<tr>
<td></td>
<td>tr(\frac{a+1}{1+a^2+a^x}) = 1</td>
<td>x5 or x6 = x</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2 if tr(\frac{1}{a}) = 0</td>
</tr>
<tr>
<td></td>
<td>x5 or x6 = 0</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2 if tr(\frac{1}{a}) = 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>when x = a + 1</td>
<td>one sol.</td>
<td>x5 or x6 = 1</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>x5 or x6 = a</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>x5 = x6</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Total #sol.:</td>
<td>3(2(2^m-1) + 1)</td>
<td>Total #excl. sol.:</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>#codewd.:</td>
<td>3(2^m - 8)/6 = 2^m-1 - 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The total number of codewords in all the cases of this proof is 2(2^m-1 - 4) = 2^m - 8. We complete the proof by showing that the block size b of this 3-(2^m, 6, 2^m-8) design is an integer, where

\[ b = \frac{(2^m - 8)2^m(2^m - 1)(2^m - 2)}{6 \cdot 5 \cdot 4} = \frac{2^{m+1}(2^m - 1)(2^{m-1} - 1)(2^{m-3} - 1)}{3 \cdot 5}. \]

Since 5|2^l - 1 if and only if l ≡ 0 (mod 4) and 3|2^l - 1 if and only if l is even, it follows that b is an integer if and only if m ≡ 0, 1 or 3 (mod 4), which is always satisfied by our precondition of odd m ≥ 5.
**Method 2: DIRECT TRACE FUNCTION ANALYSIS.**

**Case 1:** Let $U_0 = U_1 = U_A = 1$. We will determine the number of codewords such that $U_{X_4} = 3$ and $U_{X_5} = U_{X_6} = 1$. Use the equation system in Method 1 and trace function $S$ in (17). Since $0, 1, a, x, x_5, x_6$ are distinct, we have to exclude the following cases:

- $x = 0$, which gives $S = \text{tr} \left( \frac{1 + a + a^2}{1 + a^2 + \frac{1 + a^2}{a^2}} \right) = 1 + \text{tr} \left( \frac{1 + a + \frac{1 + a^2}{a^2}}{1 + a^2 + \frac{1 + a^2}{a^2}} \right) = 1$.
- $x = 1$, which gives $S = \text{tr} \left( \frac{1 + a + a^2}{1 + a^2 + \frac{1 + a^2}{a^2}} \right) = 1 + \text{tr} \left( \frac{1}{1 + a^2 + \frac{1 + a^2}{a^2}} \right) = 1$.
- $x = a$, which gives $S = \text{tr} (1 + a + a^2) = 1 + \text{tr} (a + a^2) = 1$.
- $x_5 = x_6 \Rightarrow x = a + 1$, which have already been excluded in counting.
- $x_5$ or $x_6 = 0 \Rightarrow x = \frac{1 + a + a^2}{1 + a^2}$, which gives

$$S = \text{tr} \left( \frac{1 + a + a^2}{1 + a^2 + \frac{1 + a^2}{a^2}} \right) = \text{tr} \left( \frac{(1 + a + a^2)(1 + a^2)}{a^2} \right) = \text{tr} \left( a^2 + \frac{1}{a^2} + a + \frac{1}{a} \right) = 0.$$

- $x_5$ or $x_6 = 1 \Rightarrow x = \frac{1 + a^2}{a}$, which gives

$$S = \text{tr} \left( \frac{1 + a + a^2}{1 + a^2 + \frac{1 + a^2}{a^2}} \right) = \text{tr} \left( \frac{a^2(1 + a^2) + a(a^2 + 1) + a}{1 + a^2} \right) = \text{tr} \left( \frac{1 + a + 1}{1 + a^2} \right) = 0.$$

- $x_5$ or $x_6 = a \Rightarrow x = 1 + a^2$, which gives

$$S = \text{tr} \left( \frac{1 + a + a^2}{a^2(1 + a^2)} \right) = \text{tr} \left( \frac{1}{a^2(1 + a^2)} + \frac{1}{1 + a} \right) = \text{tr} \left( \frac{1 + a}{a^2(1 + a)} \right) = \text{tr} \left( \frac{1}{a^2} + \frac{1}{a} \right) = 0.$$

- $x_5$ or $x_6 = x \Rightarrow a^2 + a + 1 = 0$, which is impossible, since $m \geq 5$.

Three of the above cases satisfy trace condition $S = 0$ in (17) and should therefore be excluded from counting as the possible $x$. Hence, the total number of possible codewords in this case is $2^m - 4$ according to Table 4.

The remaining Cases 2a–2c form their own class. Each case does not give a constant number of codewords for each choice of $A$. However, all the cases in the class together give $2^m - 4$ codewords independent of the choice of $A$.

**Case 2a:** Let $U_0 = 3$, $U_1 = U_A = 1$. We will determine the number of codewords such that $U_{X_4} = U_{X_5} = U_{X_6} = 1$. Use the equation system in Method 1 and trace function $S$ in (19). Since $0, 1, a, x, x_5, x_6$ are distinct, we have to exclude the following cases:

- $x = 0$, which gives

$$S = \text{tr} \left( \frac{a}{1 + a^2} \right) + 1 = \text{tr} \left( \frac{a + 1 + a^2}{1 + a^2} + \frac{1}{1 + a^2} \right) + 1 = 1.$$
Table 4
Count codewords in Case 1 by trace analysis

<table>
<thead>
<tr>
<th>Case</th>
<th>0</th>
<th>1</th>
<th>a</th>
<th>x</th>
<th>x5</th>
<th>x6</th>
<th>x exception</th>
<th>#Excl. sol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>two distinct</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>sol. iff.</th>
<th>(x = \frac{1-a+a^2}{1+a^2}) always</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\text{tr}(\frac{1-a+a^2}{1+a^2}) = 0)</td>
<td>(x = 1+a^2) always</td>
</tr>
<tr>
<td>(x = 1)</td>
<td>always</td>
</tr>
<tr>
<td>(3 \cdot 2)</td>
<td>(6)</td>
</tr>
</tbody>
</table>

Total #sol.: \(2 \cdot (2^m - 1)\)
Total #excl. sol.: 6

#codewd.: \(\frac{2(2^m - 4)}{2} = 2^{m-1} - 4\)

- \(x = 1\), which gives \(S = \text{tr}(a/a^2) + 1 = \text{tr}(1/a) + 1\).
- \(x = a\), which gives \(S = \text{tr}(a) + 1\).
- \(x_5 = x_6 \Rightarrow x = a + 1\), which have already been excluded in counting.
- \(x_5 = x_6 = 0 \Rightarrow x^2 + (a + 1)x + a^2 + a + 1 = 0\), which has no solutions since

\[
\text{tr}\left(\frac{a^2 + a + 1}{a^2 + 1}\right) = \text{tr}\left(1 + \frac{a}{a^2 + 1}\right) = 1.
\]

- \(x_5 = x_6 = 1 \Rightarrow x^2 + ax + a^2 + 1 = 0\), which gives

\[
S = \text{tr}\left(\frac{a+x+1}{1+a^2+x^2} + \frac{1}{1+a^2+x^2} + \frac{x}{1+a^2+x^2}\right) + 1
\]

\[
= \text{tr}\left(1 + \frac{1}{a}\right) + 1.
\]

- \(x_5 = x_6 = a \Rightarrow x^2 + x + a^2 + 1 = 0\), which has solutions of \(x\) if and only if \(\text{tr}(a) + 1 = 0\). Thus,

\[
S = \text{tr}\left(\frac{a+x+1}{1+a^2+x^2} + \frac{x+1}{1+a^2+x^2}\right) + 1
\]

\[
= \text{tr}\left(\frac{1}{1+a+x} + \frac{x^2+a^2}{1+a^2+x^2}\right) + 1 = 0.
\]

- \(x_5 = x_6 = x \Rightarrow x^2 + 1 + a + a^2\), which gives \(S = \text{tr}(a/a) + 1 = 0\).

**Case 2b**: Let \(U_0 = 1\), \(U_1 = 3\), \(U_a = 1\). We will determine the number of codewords such that \(U_{x_5} = U_{x_5} = U_{x_6} = 1\). Use the equation system in Method 1 and trace function \(S\) in (21). Since 0, 1, a, x, x5, x6 are distinct, we have to exclude the following cases:

- \(x = 0\), which gives \(S = \text{tr}((a + 1)/(1 + a^2)) + 1 - \text{tr}(1/(1 + a)) + 1\).
- \(x = 1\), which gives \(S = \text{tr}((a + 1)/a^2) + 1 = \text{tr}(1/a) + (1/a^2) + 1 = 1\).
- \(x = a\), which gives \(S = \text{tr}(a + 1) + 1 = \text{tr}(a)\).
- \(x_5 = x_6 \Rightarrow x = a + 1\), which have already been excluded in counting.
\begin{itemize}
  \item $x_5$ or $x_6 = 0 \Rightarrow x^2 + (a + 1)x + a^2 + a = 0$, which has solutions of $x$ if and only if $\text{tr}((a + a^2)/(1 + a^2)) = \text{tr}(1/(1 + a)) + 1 = 0$ since $a + 1 \neq 0$. Thus,
  \[ S = \text{tr} \left( \frac{a + 1 + x}{1 + a^2 + x^2} + \frac{x}{1 + a^2 + x^2} \right) + 1 \]
  \[ = \text{tr} \left( \frac{1}{1 + a + x} + \frac{x^2 + a(x + a + 1)}{1 + a^2 + x^2} \right) + 1 = 0. \]

  \item $x_5$ or $x_6 = 1 \Rightarrow x^2 + ax + a^2 = 0$, which has no solution of $x$ since $\text{tr}(a^2/(a^2)) = 1$.

  \item $x_5$ or $x_6 = a \Rightarrow x^2 + x + a^2 = 0$, which has solutions of $x$ if and only if $\text{tr}(a) = 0$. Thus,
  \[ S = \text{tr} \left( \frac{a + 1 + x}{1 + a^2 + x^2} + \frac{x}{1 + a^2 + x^2} \right) + 1 \]
  \[ = \text{tr} \left( \frac{1}{1 + a + x} + \frac{x^2 + a^2}{1 + a^2 + x^2} \right) + 1 = 0. \]

  \item $x_5$ or $x_6 = x \Rightarrow x^2 = a + a^2$, which gives $S = \text{tr}((a + 1)/(1 + a)) + 1 = 0$.

  \textbf{Case 2c:} Let $U_0 = 1$, $U_1 = 1$, $U_4 = 3$. We will determine the number of codewords such that $U_{x_5} = U_{x_6} = U_{x_5} = 1$. Use the equation system in Method 1 and trace function $S$ in (23). Since 0, 1, $a, x, x_5, x_6$ are distinct, we have to exclude the following cases:
  \item $x = 0$, which gives
  \[ S = \text{tr} \left( \frac{a^2 + 1 + a + 1}{1 + a^2 + x^2} \right) + 1 = \text{tr} \left( \frac{1}{1 + a} \right). \]

  \item $x = 1$, which gives $S = \text{tr}((a^2 + a)/a^2) + 1 = \text{tr}(1/a))$.

  \item $x = a$, which gives $S = \text{tr}(a^2 + a) + 1 = 1$.

  \item $x_5 = x_6 \Rightarrow x = a + 1$, which have already been excluded in counting.

  \item $x_5$ or $x_6 = 0 \Rightarrow x^2 + (a + 1)x + a + 1 = 0$, which has solutions of $x$ if and only if $\text{tr}((1 + a)/(1 + a^2)) = \text{tr}(1/(1 + a)) = 0$ since $a + 1 \neq 0$. Thus,
  \[ S = \text{tr} \left( \frac{(a + x + 1) + a^2 + (x + 1)}{1 + a^2 + x^2} \right) + 1 \]
  \[ = \text{tr} \left( \frac{1 + a^2 + x^2 + ax + a}{1 + a^2 + x^2} \right) + 1 = \text{tr} \left( \frac{a(x + 1 + a) + a^2}{1 + a^2 + x^2} \right) = 0. \]

  \item $x_5$ or $x_6 = 1 \Rightarrow x^2 + ax + 1 = 0$, which has solutions of $x$ if and only if $\text{tr}(1/(a^2)) = \text{tr}(1/a) = 0$. Thus,
  \[ S = \text{tr} \left( \frac{a^2 + x^2 + 1 + a + x^2 + 1}{1 + a^2 + x^2} \right) + 1 \]
  \[ = \text{tr} \left( \frac{a + ax}{1 + a^2 + x^2} \right) = \text{tr} \left( \frac{a(1 + x + a) + a^2}{1 + a^2 + x^2} \right) = 0. \]

  \item $x_5$ or $x_6 = a \Rightarrow x^2 + x + 1 = 0$, which has no solution of $x$ since $\text{tr}(1) = 1$.
\end{itemize}
Table 5
Count codewords in Cases 2a–2c by trace analysis

<table>
<thead>
<tr>
<th>Case</th>
<th>0</th>
<th>1</th>
<th>a</th>
<th>x5</th>
<th>x6</th>
<th>x5 sol. cond.</th>
<th>x6 sol. cond.</th>
<th>x exception</th>
<th>#Excl. sol.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2a</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>x = 1 if ( \text{tr}(\alpha) = 1 )</td>
<td>( x = a ) if ( \text{tr}(\alpha) = 1 )</td>
<td>( x = 1 ) if ( \text{tr}(\alpha) = 1 )</td>
</tr>
<tr>
<td>2b</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>( x = 0 ) if ( \text{tr}(\alpha) = 1 )</td>
<td>( x = a ) if ( \text{tr}(\alpha) = 1 )</td>
<td>( x = 0 ) if ( \text{tr}(\alpha) = 1 )</td>
</tr>
<tr>
<td>2c</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>( x = 0 ) if ( \text{tr}(\alpha) = 1 )</td>
<td>( x = 1 ) if ( \text{tr}(\alpha) = 1 )</td>
<td>( x = 0 ) if ( \text{tr}(\alpha) = 1 )</td>
</tr>
</tbody>
</table>

Total #sol.: 3 \cdot 2 \cdot (2^m - 1)  
Total #excl. sol.: 18

#codewd.: \( \frac{6(2^m - 1) - 1}{6} = 2^m - 4 \)

- \( x_5 \) or \( x_6 = x \Rightarrow x^2 = a + 1 \), which gives \( S = \text{tr}((a^2 + a)/(a^2 + a)) + 1 = 0 \).

Table 5 summarizes Cases 2a–2c and conclude that the total number of possible codewords is \( 2^{m-1} - 4 \).

The total number of codewords in all the cases of this proof is \( 2(2^{m-1} - 4) = 2^m - 8 \).

As shown in Method 1, the proof is now completed by showing the block size \( b \) of this \( 3-(2^m, 6, 2^m - 8) \) design is an integer. \( \square \)

3.3. 3-designs from codewords of support size 7

The codewords of support size 7 in the Preparata code \( \mathcal{P}_m \) for any odd integer \( m \) are of the type \( 1^62^13^00^{n-6} \) or \( 1^42^13^20^{n-6} \) or \( 1^12^33^10^{n-6} \). From these codewords, we construct three simple 3-designs for \( m = 5 \) by computer search.

**Theorem 6.** The support of the codewords of type \( 1^62^13^00^{n-6} \) in the Preparata code \( \mathcal{P}_5 \) over \( \mathbb{Z}_4 \) form a \( 3-(2^5, 7, 154) \) design.

**Theorem 7.** The support of the codewords of type \( 1^42^13^20^{n-6} \) in the Preparata code \( \mathcal{P}_5 \) over \( \mathbb{Z}_4 \) form a \( 3-(2^5, 7, 2838) \) design.
Theorem 8. The support of the codewords of type $1^32^31^0n^{-6}$ in the Preparata code $P_n$ over $\mathbb{Z}_4$ form a 3-(2$^2$, 7, 3535) design.

Conjecture 1. The support of the codewords of type $1^62^13^00^1n^{-6}$, type $1^42^13^20^1n^{-6}$ and type $1^32^31^0n^{-6}$ in the Preparata code $P_m$ over $\mathbb{Z}_4$ form three infinite families of 3-designs for $m \geq 5$.

4. Conclusions

We have considered $t$-designs constructed from codewords in the Preparata code $P_n$ over $\mathbb{Z}_4$. The infinite family of 3-(2$^m$, 5, 10) design, for any odd integer $m \geq 3$, given in [7] is reproved by a different approach in this paper. Four new families of simple 3-designs, with parameters $(2^m, 6, 2^m - 8)$, $(2^m, 6, 5 \cdot (2^m - 4))$, $(2^m, 6, 20 \cdot (2^m - 4)/3)$ and $(2^m, 6, 18 \cdot (2^m - 4))$, for any odd integer $m \geq 5$, are constructed from the support of codewords with support size 6. Several new simple 3-designs from the support of codewords with support size 7 are also investigated by computer search. The parameters of the simple 3-designs constructed in this paper are new in the sense that they are not found in Colbourn and Dinitz [2], where all known infinite families of simple $t$-designs with $t \geq 3$ are listed.

References