Two classes of ternary codes and their weight distributions

Cunsheng Ding[*], Torleiv Kløve[†], and Francesco Sica[‡]

Abstract

In this paper we describe two classes of ternary codes, determine their minimum weight and weight distribution, and prove their properties. We also present four classes of 1-designs that are based on the classes of ternary codes.

Keywords — Group character codes, ternary codes, designs.

1 Introduction

Ternary codes have been studied by many authors, see, for example, Bogdanova and Boukliev [2], Hamada, Helleseth and Ytrehus [5], Hill and Newton [6, 7], van Eupen [13, 14, 15], and van Eupen and van Lint [16]. Much of the study was concentrated on ternary codes of small dimensions.

A class of $[2^n, \sum_{i=0}^{k} \binom{n}{i}, 2^{n-r}]$ group character codes $C_q(r, n)$ over $GF(q)$, where q is odd, is described and analyzed by Ding, Kohel and Ling [3]. This class of codes contains the ternary codes $C_3(1, n)$. In this paper, we describe a new class of $[2^n, n+1]$ ternary codes and a class of $[2^n, n+2]$ ternary codes, and determine their weight distributions. The supports of the minimum weight codewords of these codes give 1-designs under certain conditions. The supports of all codewords of some other weight also give 1-designs. As byproducts we present here four classes of 1-designs that are based on the ternary codes.

[*]C. Ding is with the Department of Computer Science, National University of Singapore, Lower Kent Ridge Road, Singapore 119260. dingcs@comp.nus.edu.sg

[†]T. Kløve is with the Department of Informatics, University of Bergen, HIB, N-5020 Bergen, Norway. torleiv@ii.uib.no

[‡]F. Sica is with the Department of Computer Science, National University of Singapore, Lower Kent Ridge Road, Singapore 119260. sica@comp.nus.edu.sg

2 The class of ternary codes $C_3(r, n)$

Note that $(GF(2)^n, +)$ is an additive Abelian group of exponent 2 and order $N = 2^n$, with $\mathbf{0}$ as the identity element. From now on we assume that $n \geq 2$. Let M denote the multiplicative group of characters from $GF(2)^n$ to $GF(3)^*$. The group M is isomorphic non-canonically to $GF(2)^n$ [12, Chapter VI]. In particular we have $|M| = |GF(2)^n| = N = 2^n$. The set $GF(2)^n$ may be identified with the set of integers $\{i \ : \ 0 \leq i \leq 2^n - 1\}$: the element $(i_0, i_1, \ldots, i_{n-1})$ of $GF(2)^n$ is identified with $i = i_0 + i_1 2 + \cdots + i_{n-1} 2^{n-1}$, where each i_j is 0 or 1. We also say that $(i_0, i_1, \ldots, i_{n-1})$ is the binary representation of i. We define

$$f_i(y) = (-1)^{i_0 y_0 + i_1 y_1 + \cdots + i_{n-1} y_{n-1}}, \tag{1}$$

where $y = (y_0, y_1, \ldots, y_{n-1}) \in GF(2)^n$, and $(i_0, i_1, \ldots, i_{n-1})$ is the binary representation of i. It is easy to check that, for all i with $0 \leq i \leq 2^n - 1$, this gives all the 2^n characters from $GF(2)^n$ to $GF(3)^*$ with f_0 as the trivial character, so $M = \{f_0, f_1, \ldots, f_{2^n-1}\}$. Since we identify i and y with their respective binary representation, we have $f_i(y) = f_y(i)$. For any subset X of $GF(2)^n$, the group character code C_X over $GF(3)$ described by Ding, Kohel and Ling [3] is:

$$C_X = \Big\{(c_0, c_1, \ldots, c_{N-1}) \in GF(3)^N : \sum_{i=0}^{N-1} c_i f_i(x) = 0 \text{ for all } x \in X\Big\}.$$

Let $X = \{x_0, x_1, \ldots, x_{t-1}\}$ be a subset of $GF(2)^n$ and let X^c be the complement of X in $GF(2)^n$, indexed such that $GF(2)^n = \{x_0, x_1, \ldots, x_{N-1}\}$.

Proposition 1 [3] *Let X be as above. For $0 \leq i \leq N-1$, let $\mathbf{v}_i$ denote the vector*

$$(f_0(x_i), f_1(x_i), \ldots, f_{N-1}(x_i)).$$

Then the set $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{N-1}\}$ is linearly independent. In particular,

$$H = \Big[f_{j-1}(x_{i-1})\Big]_{1 \leq i \leq t,\ 1 \leq j \leq N}$$

has rank t and is a parity check matrix of C_X,

$$G = \Big[f_{j-1}(x_{t-1+i})\Big]_{1 \leq i \leq N-t,\ 1 \leq j \leq N}$$

has rank $N - t$ and is a generator matrix for C_X, so C_X is an $[N, N-t]$ linear code over $GF(3)$. Moreover, H is a generator matrix for C_{X^c} and $C_X \oplus C_{X^c} = GF(3)^N$.

The Hamming weight of a vector $\mathbf{a}$ of $GF(2)^n$, denoted $\mathrm{wt}(\mathbf{a})$, is defined to be the number of its nonzero coordinates. For $-1 \le r \le n$, let $X(r,n) = \{\mathbf{a} \in GF(2)^n : \mathrm{wt}(\mathbf{a}) > r\}$, and let $C_3(r,n)$ denote the code $C_{X(r,n)}$ over $GF(3)$. For a word $\mathbf{c} = (c_0, \ldots, c_{2^n-1})$ in $GF(3)^{2^n}$, let the support of $\mathbf{c}$ be defined as

$$\mathrm{Supp}(\mathbf{c}) = \{i : 0 \le i < 2^n, \text{ and } c_i \neq 0\}.$$

By convention we define the minimum distance of the zero code to be ∞, which we represent by any integer larger than the block length of the code.

Proposition 2 [3] *The following properties of the codes $C_3(r,n)$ are known:*

(A) *$C_3(r,n)$ is a $[2^n, \sum_{j=0}^{r} \binom{n}{j}, 2^{n-r}]$ ternary code.*

(B) *The minimum nonzero weight codewords generate $C_3(r,n)$.*

(C) *The dual code $C_3(r,n)^{\perp}$ is equivalent to $C_3(n-r-1,n)$.*

In the sequel we define $\mathbf{v}_0 = (1,1,\cdots,1) \in GF(3)^n$ and

$$\mathbf{v}_i = (f_0(\mathbf{e}_i), f_1(\mathbf{e}_i), \cdots, f_{N-1}(\mathbf{e}_i))$$

for all $1 \le i \le n$, where $\mathbf{e}_i$ is the vector of $GF(2)^n$ whose ith coordinate is 1 and other coordinates are all zero.

Proposition 3 [4] *For any integer $1 \le m \le n+1$, in the code $C_3(1,n)$ there are $\binom{n+1}{m}2^m$ codewords of the form $\sum_{j=0}^{m-1} a_j \mathbf{v}_{i_j}$ which have the same Hamming weight*

$$w(m) := 2^{n-m+1}\frac{2^m - (-1)^m}{3}, \tag{2}$$

where all $a_j \in GF(3)^*$, and $0 \le i_0 < i_1 < \cdots < i_{m-1} \le n$. The n weights $w(m)$ in (2) are pairwise distinct and satisfy

$$\begin{aligned} & w(2) < w(4) < w(6) < \cdots < w(2\lfloor n/2 \rfloor) < w(2\lfloor (n-1)/2 \rfloor + 1) < \\ < \;& w(2\lfloor (n-1)/2 \rfloor - 1) < \cdots < w(5) < w(3) < w(1). \end{aligned}$$

For a ternary $[N,K]$ code C, let $A_i = A_i(C)$, $i = 0, 1, \cdots, N$, be its weight distribution and let

$$A_C(x) = \sum_{i=0}^{N} A_i(C) x^i.$$

be its weight distribution function. Then $A_C(x)$ and $A_{C^\perp}(x)$ are related by the MacWilliams identity (see e.g. [11, p. 88])

$$A_{C^\perp}(x) = \frac{1}{3^K}\sum_{i=0}^{N} A_i(C)\,(1-x)^i(1+2x)^{N-i} = \frac{1}{3^K}(1+2x)^N A_C\Big(\frac{1-x}{1+2x}\Big). \tag{3}$$

From Proposition 3 we get

$$A_{C_3(1,n)}(x) = 1 + \sum_{m=1}^{n+1} \binom{n+1}{m} 2^m x^{w(m)}.$$

Combining this with (3) we get $A_{C_3(1,n)^\perp}(x)$. The explicit expressions for $A_i(C_3(1,n)^\perp)$ are quite complicated in general. However, we get $A_i(C_3(1,n)^\perp) = 0$ for $1 \le i \le 3$ (as we should since the code has minimum distance 4 by Proposition 3) and

$$A_4(C_3(1,n)^\perp) = \frac{6^n - 2 \cdot 4^n + 2^n}{4}. \tag{4}$$

In the rest of this section, we prove some auxiliary results for later sections and present a class of new 1-designs. The following lemma is a well-known result, known as the orthogonality relations in character theory [12, Chapter VI, Proposition 4].

Lemma 4 *Let A' be a finite additive Abelian group of order N' and let M' be the group of characters of A'. For characters f, g in M' and elements x, y in A', we have:*

1. $\sum_{x \in A'} f(x)g(x) = \begin{cases} N' & \text{if } f = g^{-1} \\ 0 & \text{if } f \neq g^{-1}. \end{cases}$

2. $\sum_{f \in M'} f(x)f(y) = \begin{cases} N' & \text{if } x = -y \\ 0 & \text{if } x \neq -y. \end{cases}$

Define $\mathbf{e}_0$ to be the zero vector of $GF(2)^n$. For each i with $1 \le i \le n$, $\mathbf{e}_i$ is defined as before. Let $\mathbf{e}_{n+1}, \mathbf{e}_{n+2}, \cdots, \mathbf{e}_{2^n-1}$ denote the elements of $GF(2)^n \setminus \{\mathbf{e}_0, \mathbf{e}_1, \cdots, \mathbf{e}_n\}$ with any order.

Define

$$\mathbf{v}_i = (f_0(\mathbf{e}_i), f_1(\mathbf{e}_i), \cdots, f_{N-1}(\mathbf{e}_i))$$

for all $0 \le i \le 2^n - 1$. By Lemma 4, the vectors $\mathbf{v}_0, \mathbf{v}_1, \cdots, \mathbf{v}_{2^n-1}$ are linearly independent over $GF(3)$. Take any $n+1$ vectors $\mathbf{v}_{j_0}, \mathbf{v}_{j_1}, \cdots, \mathbf{v}_{j_n}$, where $0 \le j_0 < j_1 < \cdots < j_n \le 2^n - 1$, we use $T_{j_0,j_1,\cdots,j_n}$ to denote the ternary code generated by $\mathbf{v}_{j_0}, \mathbf{v}_{j_1}, \cdots, \mathbf{v}_{j_n}$.

Proposition 5 *If $1 \le j_1 < j_2 < \cdots < j_n \le 2^n - 1$ and $\mathbf{e}_{j_1}, \mathbf{e}_{j_2}, \cdots, \mathbf{e}_{j_n}$ are linearly independent, then $T_{0,j_1,\cdots,j_n}$ is equivalent to $C_3(1,n)$ and has thus the same parameters and weight distribution as $C_3(1,n)$. That is, for any integer $1 \le m \le n+1$, in the code $T_{0,j_1,j_2,\cdots,j_n}$ there are $\binom{n+1}{m}2^m$ codewords of the form $\sum_{l=0}^{m-1} a_l \mathbf{v}_{j_{i_l}}$ which have the same Hamming weight $w(m)$, where $1 \le i_0 < i_1 < \cdots < i_{m-1} \le n$.*

Proof: Note that $C_3(1,n) = T_{0,1,\cdots,n}$. To prove the equivalence, we will show that by some column permutations a generator matrix of $T_{0,j_1,\cdots,j_n}$ gives a generator matrix of $T_{0,1,\cdots,n}$.

Consider the following matrices

$$M(j_1,\cdots,j_n) := [\mathbf{e}_l \mathbf{e}_{j_i}]_{1\le i\le n,\ 0\le l\le 2^n-1}$$

and

$$G(j_1,\cdots,j_n) := [(-1)^{\mathbf{e}_l \mathbf{e}_{j_i}}]_{0\le i\le n,\ 0\le l\le 2^n-1},$$

where $e_{j_1}, e_{j_2}, \cdots, e_{j_n}$ are linearly independent, and $\mathbf{e}_0\mathbf{e}_{j_1}$ denotes the standard inner product. Since $\mathbf{e}_{j_1}, \mathbf{e}_{j_2}, \cdots, \mathbf{e}_{j_n}$ are linearly independent over $GF(2)$, every vector of $GF(2)^n$ appears exactly once as column vectors of the matrix $M(j_1,\cdots,j_n)$. Hence by some column permutations, $M(j_1,\cdots,j_n)$ can be rearranged into $M(1,\cdots,n)$. Therefore the generate matrix $G(j_1,\cdots,j_n)$ of $T_{0,j_1,\cdots,j_n}$ can be rearranged into the generator matrix $G(1,\cdots,n)$ of $T_{0,1,\cdots,n}$ by the same column permutations. This proves the equivalence. □

Example 1 Consider the case $n = 3$. We take $\mathbf{e}_{j_1} = (1,0,0)$, $\mathbf{e}_{j_2} = (0,1,0)$, and $\mathbf{e}_{j_3} = (1,1,1)$. The three vectors are linearly independent. Then the code T_{0,j_1,j_2,j_3} has parameters $[8,4,4]$ and generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 2 & 2 & 1 & 2 \\ 1 & 1 & 2 & 1 & 2 & 1 & 2 & 2 \\ 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 \end{bmatrix}.$$

The weight enumerator of this code is $1 + 24x^4 + 16x^5 + 32x^6 + 8x^8$. This code is one of the best possible codes of this length and dimension.

Remark: The condition that $\mathbf{e}_{j_1}, \mathbf{e}_{j_2}, \cdots, \mathbf{e}_{j_n}$ are linearly independent in Proposition 5 is necessary to ensure that the minimum weight of the code $T_{0,j_1,\cdots,j_n}$ is 2^{n-1}. For example, in the case $n = 3$ if we take $\mathbf{e}_{j_1} = (0,1,0)$, $\mathbf{e}_{j_2} = (0,0,1)$, and $\mathbf{e}_{j_3} = (0,1,1)$. The three vectors are linearly dependent. Then the code T_{0,j_1,j_2,j_3} has parameters $[8,4,2]$ and generator matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 2 & 1 & 2 & 2 \\ 1 & 1 & 1 & 2 & 1 & 2 & 2 & 2 \\ 1 & 1 & 2 & 2 & 2 & 2 & 1 & 1 \end{bmatrix}.$$

The weight enumerator of this code is $1 + 8x^2 + 24x^4 + 32x^6 + 16x^8$. So the minimum distance is less than 2^{n-1}. □

Proposition 6 *The set of supports of the minimum nonzero weight codewords of $T_{0,j_1,j_2,\cdots,j_n}$ in Proposition 5 is a 1-$(2^n, 2^{n-1}, n(n+1)/2)$ design.*

Proof: This can be proved similarly as Corollary 17 in [3]. □

It is interesting to note that the code $T_{0,j_1,j_2,\cdots,j_n}$ in Proposition 5 has only one odd weight $w(n+1)$. Only codewords of form $\sum_{i=0}^{n} a_i \mathbf{v}_i$ have this odd weight, where each $a_i \neq 0$. We now prove that the supports of these codewords give 1-designs.

First we quote an old result of C. Ramus from 1834 which will be needed in the proof and also later.

Lemma 7 [10, p. 70] *Let m and μ be positive integers and $0 \leq i < \mu$. Then*

$$\Delta_{\mu,i}(m) \stackrel{\text{def}}{=} \sum_{\substack{0 \leq j \leq m \\ j \equiv i \bmod \mu}} \binom{m}{j} = \frac{1}{\mu} \sum_{l=0}^{\mu-1} \Big(2\cos\frac{l\pi}{\mu}\Big)^m \cos\frac{l(m-2i)\pi}{\mu}.$$

Proposition 8 *The set of supports of all the codewords $\sum_{i=0}^{n} a_i \mathbf{v}_i$, where each $a_i \neq 0$, in the code $T_{0,j_1,j_2,\cdots,j_n}$ of Proposition 5, is a 1-$(2^n, (2^{n+1} - (-1)^{n+1})/3, \lambda)$ design, where*

$$\lambda = \begin{cases} \frac{2^{n+1}+(-1)^{n/3}2}{3} & \text{if } n \equiv 0 \pmod 3, \\ \frac{2^{n+1}-(-1)^{(n-1)/3}}{3} & \text{if } n \equiv 1 \pmod 3, \\ \frac{2^{n+1}+(-1)^{(n-2)/3}}{3} & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Proof: A codeword covers another one if and only if the set of supports of the former contains that of the latter. We first prove that a codeword $\mathbf{x} := \sum_{i=0}^{n} a_i \mathbf{v}_i$ covers another one $\mathbf{y} := \sum_{i=0}^{n} b_i \mathbf{v}_i$ if and only if one is a nonzero multiple of the other, where each a_i and b_i are nonzero. We need only to prove one direction of this claim as the other is obvious.

Assume now that $\mathbf{x}$ covers $\mathbf{y}$. Then $\mathbf{x}$ covers both $\mathbf{x} \pm \mathbf{y}$. Let h denote the Hamming distance between $(a_0, \cdots, a_n)$ and $(b_0, \cdots, b_n)$. If $h = n+1$ or $h = 0$, then $\mathbf{x}$ is a multiple of $\mathbf{y}$. Suppose that $h \neq 0$ and $h \neq n+1$. Then $\mathbf{x} - \mathbf{y}$ is a linear combination of h vectors $\mathbf{v}_i$ and $\mathbf{x} + \mathbf{y}$ is a linear combination of $n - h$ vectors $\mathbf{v}_i$. If n is odd, one of h and $n - h$ is odd. If h is odd, by Proposition 5 the weight of $\mathbf{x} - \mathbf{y}$ is larger than that of $\mathbf{x}$, so $\mathbf{x}$ cannot cover $\mathbf{x} - \mathbf{y}$. If h is even, then $\mathbf{x}$ cannot cover $\mathbf{x} + \mathbf{y}$. If n is even, similarly we can prove that $\mathbf{x}$ cannot cover at least one of $\mathbf{x} \pm \mathbf{y}$. This leads to a contradiction. So h must be equal to one of 0 and $n+1$ and $\mathbf{x}$ must be a nonzero multiple of $\mathbf{y}$.

Hence all the codewords of the form $\sum_{i=0}^{n} a_i \mathbf{v}_i$, where $a_0 = 1$, give 2^n different supports. The weight of such a codeword is $w(n+1) = \frac{2^{n+1}-(-1)^{n+1}}{3}$. We now

consider the function $F_{d_1,\cdots,d_n}(x) := 1 + d_1x_1 + d_2x_2 + \cdots + d_nx_n$ from $(GF(3)^*)^n$ to $GF(3)$, where each d_i is a nonzero element of $GF(3)$ and $x = (x_1, \cdots, x_n)$. The weight of $F_{d_1,\cdots,d_n}(x)$ is defined to be the number of nonzero elements of $GF(3)$ this function takes on when x ranges over all elements of $(GF(3)^*)^n$. Since each d_i and x_i can be written in the form $(-1)^y$, where $y \in GF(2)$, the weight of $F_{d_1,\cdots,d_n}(x)$ does not depend on d_i. It then follows from the definition of these $\mathbf{v}_i$ that the set of supports of all these codewords is a 1-$(2^n, w(n+1), \lambda)$ design. It remains to determine λ. To this end, we need to consider the weight of $F_{1,\cdots,1}(x)$. It is seen that the weight of this function is

$$2^n - |\{z \in GF(2)^n : \mathrm{wt}(z) \equiv 2n - 1 \pmod 3\}| = 2^n - \Delta_{3,i}(n)$$

where $i \equiv 2n - 1 \pmod 3$. Then the λ, which is the weight of the function $F_{1,\cdots,1}(x)$, is given by Lemma 7. This completes the proof of this proposition. □

3 Another class of $[2^n, n+1]$ ternary codes

Let $\mathbf{e}_{2^n-1}$ denote the all-one vector $(1, 1, \cdots, 1)$ of $GF(2)^n$, and let

$$\mathbf{v}_{2^n-1} = (f_0(\mathbf{e}_{2^n-1}), f_1(\mathbf{e}_{2^n-1}), \cdots, f_{2^n-1}(\mathbf{e}_{2^n-1})).$$

Let $\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n$ be the n vectors as before. We use $T_{1,2,\cdots,n,2^n-1}$ to denote the linear code generated by $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n$ and $\mathbf{v}_{2^n-1}$. By Lemma 4, $T_{1,2,\cdots,n,2^n-1}$ has dimension $n+1$. We now determine the minimum weight and the weight distribution of this code.

Proposition 9 *The code $T_{1,2,\cdots,n,2^n-1}$ is a $[2^n, n+1, d]$ ternary code, where d is given below.*

If n is even, then the minimum weight d of this code is 2^{n-1}, and the weight distribution in this code is given in Table 1.

weight	*frequency*	*codewords*
$w(m)$ *where* $1 \le m \le n$	$\binom{n+1}{m}2^m$	$\sum_{l=0}^{m-1} a_l \mathbf{v}_{j_l}$, *where* $j_l \in \{1, \cdots, n, 2^n - 1\}$,
$\frac{2^{n+1}+1}{3}$	2^{n+1}	$\sum_{i=1}^{n} a_i \mathbf{v}_i + a\mathbf{v}_{2^n-1}$, $a_i \neq 0$, $a \neq 0$

Table 1: Weight distribution in $T_{1,2,\cdots,n,2^n-1}$ when n is even.

If n is odd, then the minimum weight d of this code is

$$\min\left\{2^{n-1}, \left[2^{n+1} - 1 - 3^{(n+1)/2}\right]/3\right\},$$

and the weight distribution in this code is given in Table 2.

weight	*frequency*	*codewords*
$w(m)$ *where* $1 \le m \le n$	$\binom{n+1}{m}2^m$	$\sum_{l=0}^{m-1} a_l \mathbf{v}_{j_l}$, *where* $j_l \in \{1, \cdots, n, 2^n - 1\}$,
$\frac{2^{n+1}-1-(-3)^{(n+1)/2}}{3}$	2^n	$\sum_{i=1}^{n} a_i \mathbf{v}_i + a\mathbf{v}_{2^n-1}$ *where* $\mathrm{wt}(\mathbf{h})$ *even,* $a_i \neq 0$, $a \neq 0$
$\frac{2^{n+1}-1+(-3)^{(n+1)/2}}{3}$	2^n	$\sum_{i=1}^{n} a_i \mathbf{v}_i + a\mathbf{v}_{2^n-1}$ *where* $\mathrm{wt}(\mathbf{h})$ *odd,* $a_i \neq 0$, $a \neq 0$

Table 2: Weight distribution in $T_{1,2,\cdots,n,2^n-1}$ when n is odd.

Case I

Since $\mathbf{u}$ and $a\mathbf{u}$ have the same Hamming weight if $a \neq 0$, we consider the weight of the following codeword

$$\mathbf{u} := \sum_{l=0}^{m-2} a_l \mathbf{v}_{j_l} + \mathbf{v}_{2^n-1}, \tag{5}$$

where $j_l \in \{1, 2, \cdots, n\}$, $m - 1 \le n$, and each $a_l \neq 0$.

Subcase I.1

We consider the vector $\mathbf{u}$ of (5) under the condition that $m - 1 < n$. Each $a_l = (-1)^{h_l}$, where $h_l = \{0, 1\}$. We now consider the following matrix

$$L := \begin{bmatrix} \mathbf{e}_0\mathbf{e}_{j_0} + h_0 & \mathbf{e}_1\mathbf{e}_{j_0} + h_0 & \cdots & \mathbf{e}_{2^n-1}\mathbf{e}_{j_0} + h_0 \\ \mathbf{e}_0\mathbf{e}_{j_1} + h_1 & \mathbf{e}_1\mathbf{e}_{j_1} + h_1 & \cdots & \mathbf{e}_{2^n-1}\mathbf{e}_{j_1} + h_1 \\ \vdots & \vdots & & \vdots \\ \mathbf{e}_0\mathbf{e}_{j_{m-2}} + h_{m-2} & \mathbf{e}_1\mathbf{e}_{j_{m-2}} + h_{m-2} & \cdots & \mathbf{e}_{2^n-1}\mathbf{e}_{j_{m-2}} + h_{m-2} \end{bmatrix}.$$

Since $\mathbf{e}_{j_0}, \mathbf{e}_{j_1}, \cdots, \mathbf{e}_{j_{m-2}}$ are linearly independent, each vector of $GF(2)^{m-1}$ appears exactly $2^{n-(m-1)}$ times as column vectors of L.

Let $j_{m-1}, j_m, \cdots, j_{n-1}$ be the elements of $\{1, 2, \cdots, n\} \setminus \{j_0, j_1, \cdots, j_{m-2}\}$. Consider now the following matrix

$$L_1 := \begin{bmatrix} \mathbf{e}_0\mathbf{e}_{j_0} + h_0 & \mathbf{e}_1\mathbf{e}_{j_0} + h_0 & \cdots & \mathbf{e}_{2^n-1}\mathbf{e}_{j_0} + h_0 \\ \mathbf{e}_0\mathbf{e}_{j_1} + h_1 & \mathbf{e}_1\mathbf{e}_{j_1} + h_1 & \cdots & \mathbf{e}_{2^n-1}\mathbf{e}_{j_1} + h_1 \\ \vdots & \vdots & & \vdots \\ \mathbf{e}_0\mathbf{e}_{j_{m-2}} + h_{m-2} & \mathbf{e}_1\mathbf{e}_{j_{m-2}} + h_{m-2} & \cdots & \mathbf{e}_{2^n-1}\mathbf{e}_{j_{m-2}} + h_{m-2} \\ \mathbf{e}_0\mathbf{e}_{j_{m-1}} & \mathbf{e}_1\mathbf{e}_{j_{m-1}} & \cdots & \mathbf{e}_{2^n-1}\mathbf{e}_{j_{m-1}} \\ \vdots & \vdots & & \vdots \\ \mathbf{e}_0\mathbf{e}_{j_{n-1}} & \mathbf{e}_1\mathbf{e}_{j_{n-1}} & \cdots & \mathbf{e}_{2^n-1}\mathbf{e}_{j_{n-1}} \end{bmatrix}.$$

Since $\mathbf{e}_{j_0}, \mathbf{e}_{j_1}, \cdots, \mathbf{e}_{j_{n-1}}$ are linearly independent, each vector of $GF(2)^{m-1}$ appears exactly once as a column vector of L_1.

Let $\mathbf{s}_0, \mathbf{s}_1, \cdots, \mathbf{s}_{2^{m-1}-1}$ be all the vectors of $GF(2)^{m-1}$, and we let $\mathbf{t}_0, \mathbf{t}_1, \cdots$, $\mathbf{t}_{2^{n-(m-1)}-1}$ be all the vectors of $GF(2)^{n-(m-1)}$. By permutations on columns, L_1 can be rearranged into the following matrix L_2:

$$\begin{bmatrix} \mathbf{s}_0 & \mathbf{s}_1 & \cdots & \mathbf{s}_{2^{m-1}-1} & \cdots & \mathbf{s}_0 & \mathbf{s}_1 & \cdots & \mathbf{s}_{2^{m-1}-1} \\ \mathbf{t}_0 & \mathbf{t}_0 & \cdots & \mathbf{t}_0 & \cdots & \mathbf{t}_{2^{n-(m-1)}-1} & \mathbf{t}_{2^{n-(m-1)}-1} & \cdots & \mathbf{t}_{2^{n-(m-1)}-1} \end{bmatrix}.$$

The weight of the codeword $\mathbf{u}$ in (5) can be determined by looking at the first $m-1$ rows of the matrix L_2. However, all the vectors $\mathbf{s}_i$ and $\mathbf{t}_i$ are needed to determine the corresponding coordinates of $\mathbf{v}_{2^n-1}$. This is because by definition $f_x(\mathbf{e}_{2^n-1}) = (-1)^{x_0+x_1+\cdots+x_{n-1}}$, where $(x_0, x_1, \cdots, x_{n-1})$ is the binary representation of the integer x.

Define $r = m \bmod 3$. We use $\mathbf{y}$ to denote one of the vectors $\mathbf{s}_i$ and $\mathbf{x}$ to denote one of the vectors $\mathbf{t}_i$. Then $(\mathbf{y}^T, \mathbf{x}^T)^T$ ranges over all column vectors of L_2 when $\mathbf{y}$ and $\mathbf{x}$ run over all vectors of $GF(2)^{m-1}$ and $GF(2)^{n-(m-1)}$ respectively, where $\mathbf{y}^T$ denotes the transpose of $\mathbf{y}$. Let w be the Hamming weight of $\mathbf{y}$. Suppose that $\mathbf{y}$ and $\mathbf{x}$ are in the ith column of L_2, then $(m-1-2w) \bmod 3$ is the corresponding entry of the codeword $\sum_{l=0}^{m-2} a_l \mathbf{v}_{j_l}$, and $(m-1-2w+(-1)^{w+\mathrm{wt}(\mathbf{x})}) \bmod 3$ is the corresponding entry of the codeword $\sum_{l=0}^{m-2} a_l \mathbf{v}_{j_l} + \mathbf{v}_{2^n-1}$. It is then seen that Table 3 gives the distribution of the elements $\{r, r-1, r-2\}$ of $GF(3)$ in the codeword $\mathbf{u}$ of (5).

By Table 3, we have the following frequency of appearance of the elements of $GF(3)$ in the codeword $\mathbf{u}$:

$r \in GF(3)$	frequency
r	$[\Delta_{6,0}(m-1) + \Delta_{6,5}(m-1) + \Delta_{6,2}(m-1) + \Delta_{6,3}(m-1)]2^{n-m}$
$r-1$	$[\Delta_{6,1}(m-1) + \Delta_{6,2}(m-1) + \Delta_{6,4}(m-1) + \Delta_{6,5}(m-1)]2^{n-m}$
$r-2$	$[\Delta_{6,3}(m-1) + \Delta_{6,4}(m-1) + \Delta_{6,0}(m-1) + \Delta_{6,1}(m-1)]2^{n-m}$

(6)

By Lemma 7 and (6), the frequency of appearance of the elements of $GF(3)$ in the codeword $\mathbf{u}$ is given in Table 4.

$w := \mathrm{wt}(\mathbf{y})$	g	entries of $\mathbf{u}$ $\mathrm{wt}(x)$ even	entries of $\mathbf{u}$ $\mathrm{wt}(x)$ odd	frequency
$w \equiv 0 \pmod 6$	$r-1$	r	$r-2$	$2^{n-m}\Delta_{6,0}(m-1)$
$w \equiv 1 \pmod 6$	r	$r-1$	$r-2$	$2^{n-m}\Delta_{6,1}(m-1)$
$w \equiv 2 \pmod 6$	$r-2$	$r-1$	r	$2^{n-m}\Delta_{6,2}(m-1)$
$w \equiv 3 \pmod 6$	$r-1$	$r-2$	r	$2^{n-m}\Delta_{6,3}(m-1)$
$w \equiv 4 \pmod 6$	r	$r-2$	$r-1$	$2^{n-m}\Delta_{6,4}(m-1)$
$w \equiv 5 \pmod 6$	$r-2$	r	$r-1$	$2^{n-m}\Delta_{6,5}(m-1)$

Table 3: Distribution of elements of $GF(3)$ in $\mathbf{u}$, where $g := (m-1-2w) \bmod 3$.

	r	$r-1$	$r-2$
$m-1=3k$	$\frac{2^m+(-1)^k}{3}2^{n-m}$	$\frac{2^m-(-1)^k 2}{3}2^{n-m}$	$\frac{2^m+(-1)^k}{3}2^{n-m}$
$m-1=3k+1$	$\frac{2^m-(-1)^k}{3}2^{n-m}$	$\frac{2^m-(-1)^k}{3}2^{n-m}$	$\frac{2^m+(-1)^k 2}{3}2^{n-m}$
$m-1=3k+2$	$\frac{2^m-(-1)^k 2}{3}2^{n-m}$	$\frac{2^m+(-1)^k}{3}2^{n-m}$	$\frac{2^m+(-1)^k}{3}2^{n-m}$

Table 4: The frequency distribution of the elements of $GF(3)$ in $\mathbf{u}$

With Table 4, we obtain that

$$\begin{aligned}
\mathrm{wt}(\mathbf{u}) &= \tfrac{2^{m+1}+(-1)^k 2}{3}2^{n-m} \quad \text{if } m-1=3k,\\
\mathrm{wt}(\mathbf{u}) &= \tfrac{2^{m+1}-(-1)^k 2}{3}2^{n-m} \quad \text{if } m-1=3k+1,\\
\mathrm{wt}(\mathbf{u}) &= \tfrac{2^{m+1}+(-1)^k 2}{3}2^{n-m} \quad \text{if } m-1=3k+2.
\end{aligned}$$

It is then easy to check that $\mathrm{wt}(\mathbf{u}) = w(m)$.

Subcase I.2

We consider the codeword $\mathbf{u}$ of (5) under the condition that $m-1=n$. Let $a_l = (-1)^{h_l}$, where $h_l \in \{0,1\}$. Define $\mathbf{h} = (h_0, h_1, \cdots, h_{m-2})$. To determine the weight of $\mathbf{u}$, we need the values of some $\Delta_{6,i}(n) + \Delta_{6,j}(n)$ given in Lemma 7. With an argument similar to that in Subcase I.1, we obtain the weight of $\mathbf{u}$ given in Table 5.

Case II

For any codeword

$$\mathbf{u} := \sum_{l=0}^{m-1} a_l \mathbf{v}_{j_l}, \tag{7}$$

	wt(**u**) (wt(**h**) even)	wt(**u**) (wt(**h**) odd)
n even	$\frac{2^{n+1}+1}{3}$	$\frac{2^{n+1}+1}{3}$
n odd	$\frac{2^{n+1}-1-(-3)^{(n+1)/2}}{3}$	$\frac{2^{n+1}-1+(-3)^{(n+1)/2}}{3}$

Table 5: The weight of **u** in Subcase I.2

where $j_l \in \{1, 2, \cdots, n\}$, the weight of **u** is $w(m)$ as described in Proposition 5.

Summarizing the discussion in the two cases proves the conclusion of this proposition. □

Lemma 10 *If $n \geq 13$ and n is odd, then*

$$2^{n-1} < \left[2^{n+1} - 1 - 3^{(n+1)/2}\right]/3.$$

If $n \geq 8$ and n is even, then

$$2^{n-1} < \left[2^{n+2} - 1 - 3^{(n+2)/2}\right]/6.$$

Proof: The two inequalities can be easily proved by induction on n. □

Remark: If n is even, then $A_{T_{1,2,\cdots,n,2^n-1}}(x) = A_{C_3(1,n)}(x)$. In particular, the minimum weight of the code $T_{1,2,\cdots,n,2^n-1}$ is 2^{n-1} and the minimum weight of the dual code is 4.

When n is odd, the minimum weight of the code $T_{1,2,\cdots,n,2^n-1}$ is

$$d = \min\left\{2^{n-1}, \left[2^{n+1} - 1 - 3^{(n+1)/2}\right]/3\right\} = \begin{cases} < 2^{n-1} & \text{if } n \leq 11, \\ = 2^{n-1} & \text{if } n \geq 13. \end{cases}$$

Using MacWilliams identity, we get

$$\begin{aligned} A_1(T^{\perp}_{1,2,\cdots,n,2^n-1}) &= 0, \\ A_2(T^{\perp}_{1,2,\cdots,n,2^n-1}) &= 2^n. \end{aligned}$$

In particular, the minimum weight of the dual code is 2.

Proposition 11 *If n is even or if $n \geq 13$ is odd, then the minimum weight codewords of $T_{1,2,\cdots,n,2^n-1}$ generate this code.*

Proof: By Proposition 9 and Lemma 10, in both cases the minimum weight codewords are of the form $a\mathbf{v}_i + b\mathbf{v}_j$, where $i < j$. Thus it suffices to prove that $\mathbf{v}_{2^n-1} + \mathbf{v}_{j_1}$, $\mathbf{v}_{2^n-1} + \mathbf{v}_{j_2}$, $\cdots$, $\mathbf{v}_{2^n-1} + \mathbf{v}_{j_n}$, and $\mathbf{v}_{2^n-1} - \mathbf{v}_{j_n}$ are linearly independent. This can be easily proved as $\mathbf{v}_{2^n-1}$, $\mathbf{v}_0$, $\mathbf{v}_1$, $\cdots$, $\mathbf{v}_n$ are linearly independent. □

Proposition 12 *The set of supports of the minimum nonzero weight codewords of $T_{1,2,\cdots,n,2^n-1}$ is a 1-$(2^n, 2^{n-1}, n(n+1)/2)$ design when n is even or $n \geq 13$ is odd.*

Proof: Note that the minimum weight codewords of $T_{1,2,\cdots,n,2^n-1}$ must be of the form $a\mathbf{v}_i + b\mathbf{v}_i$, where $i \neq j$, $a \neq 0$, and $b \neq 0$, when n is even or $n \geq 13$ is odd. This proposition can then be proved similarly as Corollary 17 in [3]. □

Example 2 Consider the case $n = 4$. We take $\mathbf{e}_{j_i} = \mathbf{e}_i$ for $i = 1, 2, 3, 4$. The four vectors are linearly independent. Then the code $T_{j_1,j_2,j_3,j_4,2^4-1}$ has parameters $[16, 5, 8]$ and generator matrix

$$\begin{bmatrix} 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 \\ 1 & 1 & 2 & 1 & 1 & 2 & 1 & 1 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 2 \\ 1 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & 2 & 1 & 2 & 2 & 2 & 2 \\ 1 & 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 1 \end{bmatrix}.$$

The weight enumerator of this code is $1 + 40x^8 + 80x^{10} + 32x^{11} + 80x^{12} + 10x^{16}$. The best ternary codes of length 16 and dimension 5 have minimum distance 9. So this is almost the best code of these parameters.

4 A class of $[2^n, n+2]$ ternary codes

Let $T_{0,1,2,\cdots,n,2^n-1}$ denote the code generated by $\mathbf{v}_0$, $\mathbf{v}_1$, $\cdots$, $\mathbf{v}_n$ and $\mathbf{v}_{2^n-1}$. Clearly, it has dimension $n + 2$. The minimum distance and weight distribution of this code is given in the following proposition.

Proposition 13 *The code $T_{0,1,2,\cdots,n,2^n-1}$ is a $[2^n, n+2, d]$ ternary code, where d is given below.*

If n is even, then the minimum weight d of this code is

$$\min\left\{2^{n-1}, \frac{1}{6}\left[2^{n+2} - 1 - (3)^{(n+2)/2}\right]\right\}$$

and the weight distribution in this code is given in Table 6.

weight	*frequency*	*codewords*
$w(m)$ *where* $1 \le m \le n$	$\binom{n+2}{m}2^m$	$\sum_{l=0}^{m-1} a_l \mathbf{v}_{j_l}$, *where* $j_l \in \{0, 1, \cdots, n, 2^n - 1\}$,
$w(n+1)$	$(n+1)2^{n+1}$	$\sum_{l=0}^{n} a_l \mathbf{v}_{j_l}$, $j_0 = 0$, $j_l \in \{0, 1, \cdots, n, 2^n - 1\}$
$\frac{2^{n+1}+1}{3}$	2^{n+1}	$\sum_{i=1}^{n} a_i \mathbf{v}_i + a\mathbf{v}_{2^n-1}$
$\frac{2^{n+2}-1+3(-3)^{n/2}}{6}$	2^{n+1}	$\sum_{l=0}^{n} a_l \mathbf{v}_l + a\mathbf{v}_{2^n-1}$
$\frac{2^{n+2}-1-3(-3)^{n/2}}{6}$	2^{n+1}	$\sum_{l=0}^{n} a_l \mathbf{v}_l + a\mathbf{v}_{2^n-1}$

Table 6: Weight distribution in $T_{0,1,2,\cdots,n,2^n-1}$ when n is even, where all a_i and a are nonzero.

If n is odd, then the minimum weight d of this code is

$$\min\left\{2^{n-1}, (2^{n+1} - 1 - 3^{(n+1)/2})/3\right\},$$

and the weight distribution in this code is given in Table 7.

weight	*frequency*	*codewords*
$w(m)$ *where* $1 \le m \le n$	$\binom{n+2}{m}2^m$	$\sum_{l=0}^{m-1} a_l \mathbf{v}_{j_l}$, *where* $j_l \in \{0, 1, \cdots, n, 2^n - 1\}$,
$w(n+1)$	$(n+1)2^{n+1}$	$\sum_{l=0}^{n} a_l \mathbf{v}_{j_l}$, $j_0 = 0$, $j_l \in \{0, 1, \cdots, n, 2^n - 1\}$
$\frac{2^{n+1}-1-(-3)^{(n+1)/2}}{3}$	2^n	$\sum_{i=1}^{n} a_i \mathbf{v}_i + a\mathbf{v}_{2^n-1}$
$\frac{2^{n+1}-1+(-3)^{(n+1)/2}}{3}$	2^n	$\sum_{i=1}^{n} a_i \mathbf{v}_i + a\mathbf{v}_{2^n-1}$
$\frac{2^{n+2}+1+(-3)^{(n+1)/2}}{6}$	2^{n+1}	$\sum_{l=0}^{n} a_l \mathbf{v}_l + a\mathbf{v}_{2^n-1}$
$\frac{2^{n+2}+1-(-3)^{(n+1)/2}}{6}$	2^{n+1}	$\sum_{l=0}^{n} a_l \mathbf{v}_l + a\mathbf{v}_{2^n-1}$

Table 7: Weight distribution in $T_{0,1,2,\cdots,n,2^n-1}$ when n is odd, where all a_l and a are nonzero.

Proof: Note that $T_{0,1,2,\cdots,n,2^n-1}$ contains both $T_{0,1,2,\cdots,n}$ and $T_{1,2,\cdots,n,2^n-1}$ as subcodes. We need only to consider the codewords

$$\mathbf{u} := a_0\mathbf{v}_0 + \sum_{l=1}^{m-2} a_l\mathbf{v}_l + a\mathbf{v}_{2^n-1},$$

where $a_l \neq 0$ and $a \neq 0$. If $m - 2 < n$, with an argument similar to Subcase I.1 of Section 3, we can prove that $\mathrm{wt}(\mathbf{u}) = w(m)$. If $m - 2 = n$, similarly we can prove the following:

(1) If n is even, $\mathrm{wt}(\mathbf{u})$ takes on $\frac{2^{n+2}-1+3(-3)^{n/2}}{6}$ and $\frac{2^{n+2}-1-3(-3)^{n/2}}{6}$ respectively for 2^{n+1} codewords $\mathbf{u}$.

(2) If n is odd, $\mathrm{wt}(\mathbf{u})$ takes on $\frac{2^{n+2}+1+(-3)^{(n+1)/2}}{6}$ and $\frac{2^{n+2}+1-(-3)^{(n+1)/2}}{6}$ respectively for 2^{n+1} codewords $\mathbf{u}$.

Combining these two conclusions and Propositions 5 and 9 proves this proposition. □

Remarks: 1. Combining Proposition 13 and MacWilliams identity we get that the code $(T_{0,1,2,\cdots,n,2^n-1})^{\perp}$ has minimum weight 4 and

$$A_4((T_{0,1,2,\cdots,n,2^n-1})^{\perp}) = \begin{cases} (3\cdot 6^n - 8\cdot 4^n + 5\cdot 2^n)/16 & \text{if } n \text{ is even,} \\ (3\cdot 6^n - 8\cdot 4^n + 7\cdot 2^n)/16 & \text{if } n \text{ is odd.} \end{cases}$$

2. By Lemma 10, if $n \geq 8$ and n is even or if $n \geq 13$ and n is odd, $T_{0,1,2,\cdots,n,2^n-1}$ has minimum distance $d = 2^{n-1}$. Thus the code $T_{0,1,2,\cdots,n,2^n-1}$ is better than $T_{1,2,\cdots,n,2^n-1}$ and $T_{0,1,2,\cdots,n}$ except for a few n's.

Proposition 14 *If $n \geq 8$ is even or if $n \geq 13$ is odd, then the minimum weight codewords of $T_{0,1,2,\cdots,n,2^n-1}$ generate this code.*

Proof: The proof of Proposition 11 applies here. □

Proposition 15 *The set of supports of the minimum nonzero weight codewords of $T_{0,1,2,\cdots,n,2^n-1}$ is a 1-$(2^n, 2^{n-1}, (n+2)(n+1)/2)$ design when $n \geq 8$ is even or $n \geq 13$ is odd.*

Proof: Note that all the minimum weight codewords of $T_{0,1,2,\cdots,n,2^n-1}$ must be of the form $a\mathbf{v}_i + b\mathbf{v}_j$, where $i \neq j$, $a \neq 0$, and $b \neq 0$, when $n \geq 8$ is even or $n \geq 13$ is odd. Then this proposition can be proved similarly as Corollary 17 in [3]. □

5 Using the codes for error detection

Let C be a ternary $[N, K, d]$ code. The probability of undetected error when the code is used purely for error detection on a ternary symmetric channel is given by

$$P_{\mathrm{ue}}(C, p) = \sum_{i=d}^{N} A_i(C)\Big(\frac{p}{2}\Big)^i (1-p)^{N-i},$$

where p is the symbol error probability, see e.g. Kløve and Korzhik [9]. In particular,

$$P_{\rm ue}(C, 2/3) = (3^K - 1)(1/3)^N < 3^{K-N}. \tag{8}$$

The error probability threshold of C, introduced in Kløve [8], is defined by

$$\theta(C) = \max\left\{p' \in [0, 2/3] \;\mid\; P_{ud}(C, p) \le P_{ud}(C, 2/3) \text{ for all } p \in [0, p']\right\}.$$

A code C is called good for error detection (in the technical sense) if and only if $\theta(C) = 2/3$. However, for practical applications the important things are that $P_{\rm ue}(C, 2/3)$ is small (that is, $N - K$ is large) and that $\theta(C)$ is above the range of actual values of p. It is therefore of interest to estimate $\theta(C)$. It turns out that the performances on error detection of the codes described in this paper are very similar. Therefore, we will only discuss $C = C_3(1, n)$ in detail. For this code we have $N = 2^n$, $K = n + 1$ and $d = 2^{n-1}$.

Proposition 16 *For all $n \ge 2$ we have*

$$\frac{1}{3} < \theta(C_3(1, n)) < \frac{1}{3} + \frac{n}{2^{n-2}}.$$

Proof: First we note that for fixed $p \in (0, 2/3)$, the expression $(\frac{p}{2(1-p)})^i$ decreases with increasing i. Hence

$$\begin{aligned} P_{\rm ue}(C, p) &= (1-p)^N \sum_{i=d}^{N} A_i(C) \Big(\frac{p}{2(1-p)}\Big)^i \\ &< (1-p)^N \sum_{i=d}^{N} A_i(C) \Big(\frac{p}{2(1-p)}\Big)^d \\ &= \Big(\frac{p(1-p)}{2}\Big)^{N/2} (3^K - 1). \end{aligned}$$

Further, we note that $p(1-p)$ is increasing on the interval $(0, 1/2)$. Hence, if $p \le 1/3$, then

$$P_{\rm ue}(C, p) \le P_{\rm ue}\Big(C, \frac{1}{3}\Big) < \Big(\frac{1}{9}\Big)^{N/2} (3^K - 1) = \Big(\frac{1}{3}\Big)^N (3^K - 1) = P_{\rm ue}\Big(C, \frac{2}{3}\Big).$$

Hence

$$\theta(C) > \frac{1}{3}.$$

A direct calculation of $\theta(C)$ for $n \le 9$ gives the following values:

n	$2, 3, 4, 5$	6	7	8	9
$\theta(C)$	$2/3$	0.4369	0.3852	0.3619	0.3427
$1/3 + n/2^{n-3}$	$> 2/3$	1.0833	0.7708	0.5833	0.3759

In particular, the upper bound is true for $n \leq 9$. To prove the upper bound for $n \geq 10$, we first note that $A_d(C) \geq 3$. Let p be the root in the interval $(0, 1/2)$ of the equation

$$\left(\frac{p(1-p)}{2}\right)^{2^{n-1}} = \frac{3^n}{3^{2^n}},$$

that is

$$p = \frac{3 - \sqrt{9 - 8 \cdot 3^{n/2^{n-1}}}}{6}.$$

Then

$$\begin{aligned} P_{\mathrm{ue}}(C, p) &\geq A_d\Big(\frac{p}{2}\Big)^{2^{n-1}} (1-p)^{2^{n-1}} \\ &> 3\left(\frac{p(1-p)}{2}\right)^{2^{n-1}} \\ &= \frac{3^{n+1}}{3^{2^n}} > P_{\mathrm{ue}}(C, 2/3). \end{aligned}$$

Hence

$$\theta(C) < p.$$

Simple calculus shows that

$$\frac{3 - \sqrt{9 - 8x}}{6} < \frac{1}{3} + 4\log_3(x)$$

for $1 < x < 1.12$. Hence

$$p < \frac{1}{3} + \frac{n}{2^{n-3}}$$

for $n \geq 10$. □

Proposition 16 shows that $C_3(1, n)$ is good for practical error detection (even if it is not "good" in the technical sense). A similar proof shows that also the other codes have a threshold close to $1/3$ (for most n).

Now, consider the dual codes.

Proposition 17 *For all $n \geq 13$ we have*

$$\theta(C_3(1, n)^{\perp}) < \frac{6}{18^{n/4}}.$$

Proof: We have

$$P_{\mathrm{ue}}(C^{\perp}, 2/3) = \frac{3^{2^n - n - 1} - 1}{3^{2^n}} < \frac{1}{3^{n+1}}.$$

Let

$$p = \frac{6}{18^{n/4}}.$$

We have $p < 2/3$ for $n \geq 4$. By (4) we have

$$\begin{aligned} \frac{P_{\rm ue}(C^\perp, p)}{P_{\rm ue}(C^\perp, 2/3)} &> A_4(C^\perp)\Big(\frac{p}{2}\Big)^4 (1-p)^{2^n-4} \cdot 3^{n+1} \\ &= \frac{243}{16}\Big(1 - 2\Big(\frac{2}{3}\Big)^n + \Big(\frac{1}{3}\Big)\Big)\Big(1 - \frac{6}{18^{n/4}}\Big)^{2^n-4} > 1 \end{aligned}$$

for all $n \geq 13$. □

Proposition 17 shows that $C_3(1,n)^\perp$ is not very useful for error detection except possibly for some very moderate values of n. The upper bound on $\theta(C_3(1,n)^\perp)$ can be improved by some factor by the same method, e.g.

$$\theta(C_3(1,n)^\perp) < \frac{3}{18^{n/4}} \text{ for } n \geq 28.$$

However, it is of less interest to determine precise bounds on $\theta(C_3(1,n)^\perp)$ since it is very small in any case.

6 Concluding remarks

The code $T_{1,2,\cdots,n,2^n-1}$ can not be equivalent to $T_{0,1,\cdots,n}$ when n is odd. This is because $T_{1,2,\cdots,n,2^n-1}$ has only even weights when n is odd, while $T_{0,1,\cdots,n}$ has always one odd weight $w(n+1)$. The class of codes $T_{1,2,\cdots,n,2^n-1}$ described here have the same codeword length, dimension and minimum weight as the first-order binary Reed-Muller codes [1], [8], if and only if n is even. However, their weight distributions are quite different. The first-order Reed-Muller codes are two-weight codes, while $T_{1,2,\cdots,n,2^n-1}$ has many weights $w(m)$. When $n \geq 13$, the minimum weight of $T_{1,2,\cdots,n,2^n-1}$ is still 2^{n-1}.

When $n \geq 8$ is even or $n \geq 13$ is odd, the ternary code $T_{0,1,2,\cdots,n,2^n-1}$ has length 2^n and minimum weight 2^{n-1}. But its dimension is $n+2$. So $T_{0,1,2,\cdots,n,2^n-1}$ is better than the first-order binary Reed-Muller code as the former has one more dimension while they have the same codeword length and minimum weight.

References

[1] I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding.* New York: Academic Press, 1975.

[2] G. T. Bogdanova and I. G. Boukliev, "New linear codes of dimension 5 over $GF(3)$," in *Proc. 4th Int. Workshop on Algebraic and Combinatorial Coding Theory,* 1994, pp. 41–43.

[3] C. Ding, D. R. Kohel and S. Ling, "Elementary 2-group character codes," Preprint.

[4] C. Ding, D. R. Kohel and S. Ling, "Secret sharing with a class of ternary codes," submitted manuscript, May 1999.

[5] N. Hamada, T. Helleseth and Ø. Ytrehus, "The nonexistence of $[51, 5, 33; 3]$-codes," *Ars Combinatoria,* Vol. 25, pp. 25–32, 1993.

[6] R. Hill and D. E. Newton, "Some optimal ternary linear codes," *Ars Combinatoria,* Vol. 25-A, pp. 61–72, 1988.

[7] R. Hill and D. E. Newton, "Optimal ternary linear codes," *Designs, Codes, and Cryptography,* Vol. 2, pp. 137–157, 1992.

[8] T. Kløve, "Reed-Muller codes for error detection, the good, the bad, and the ugly," *IEEE Trans. Inform. Theory,* Vol. 42, pp. 2265–2272, 1996.

[9] T. Kløve and V. Korzhik, *Error Detecting Codes, General Theory and their Application in Feedback Communication Systems.* Boston: Kluwer Acad. Publ., 1995.

[10] D. E. Knuth, *The Art of Computer Programming,* Vol. 1, Second ed. Reading: Addison-Wesley, 1973.

[11] V. S. Pless and W. C. Huffman, *Handbook of Coding Theory,* Vol. 1. Amsterdam: North-Holland, 1998.

[12] J.-P. Serre, *A Course in Arithmetic,* Graduate Texts in Mathematics 7. New York: Springer, 1973.

[13] M. van Eupen, "Five new optimal ternary linear codes," *IEEE Trans. Inform. Theory,* Vol. 40, No. 1, p. 193, 1993.

[14] M. van Eupen, "Four nonexistence results for ternary linear codes," *IEEE Trans. Inform. Theory,* Vol. 41, No. 3, pp. 800–805, 1995.

[15] M. van Eupen, "Some new results for ternary linear codes of dimension 5 and 6," *IEEE Trans. Inform. Theory,* Vol. 41, No. 6, pp. 2048–2051, 1995.

[16] M. van Eupen and J. H. van Lint, "On the minimum distance of ternary cyclic codes," *IEEE Trans. Inform. Theory,* Vol. 39, No. 2, pp. 409–422, 1993.

List of Tables

1 Weight distribution in $T_{1,2,\cdots,n,2^n-1}$ when n is even. 7
2 Weight distribution in $T_{1,2,\cdots,n,2^n-1}$ when n is odd. 8
3 Distribution of elements of $GF(3)$ in $\mathbf{u}$, where $g := (m-1-2w) \bmod 3$. 10
4 The frequency distribution of the elements of $GF(3)$ in $\mathbf{u}$ 10
5 The weight of $\mathbf{u}$ in Subcase I.2 11
6 Weight distribution in $T_{0,1,2,\cdots,n,2^n-1}$ when n is even, where all a_i and a are nonzero. 13
7 Weight distribution in $T_{0,1,2,\cdots,n,2^n-1}$ when n is odd, where all a_l and a are nonzero. 13