THE WEIGHT DISTRIBUTION OF $C_5(1,n)$

KWOK YAN LAM AND FRANCESCO SICA

ABSTRACT. In [2] the codes $C_q(r,n)$ over $\mathbb{F}_q$ were introduced. These linear codes have parameters $[2^n, \sum_{i=0}^{r} \binom{n}{i}, 2^{n-r}]$, can be viewed as analogues of the binary Reed-Muller codes and share several features in common with them. In [2], the weight distribution of $C_3(1,n)$ is completely determined.

In this paper we compute the weight distribution of $C_5(1,n)$. To this end we transform a sum of a product of two binomial coefficients into an expression involving only exponentials and Lucas numbers. We prove an effective result on the set of Lucas numbers which are powers of two to arrive to the complete determination of the weight distribution of $C_5(1,n)$. The final result is stated as Theorem 2.

1. INTRODUCTION

We will recall later the definition of $C_q(r,n)$, where q is an odd prime power. These linear codes are defined in analogy with the binary Reed-Muller codes and have the same parameters [6]. Moreover, they are both generated by minimum weight codewords and the dual code $C_q(r,n)^{\perp}$ is

Date: August 13, 1999.

1991 *Mathematics Subject Classification.* Primary: 94B40; Secondary: 11B39.

Key words and phrases. Weight distribution, Lucas numbers.

Research of the second author supported by grant number RP 960668/M.

equivalent to $C_q(n-r-1,n)$, which is the analogue of the equality $R(r,n)^\perp = R(n-r-1,n)$.

In [2] the weight distribution of $C_3(1,n)$ is completely determined, but the method does not extend to $C_q(1,n)$ for $q \geqslant 5$. In this paper we determine completely the weight distribution of $C_5(1,n)$. The main result is summarised in Theorem 2. The method seems difficult to generalise to higher values of q.

The exposition is as follows. First we recall the definition of $C_q(r,n)$ and the general lemma of Ding, Kohel and Ling for the computation of the weight of codewords of $C_q(1,n)$. We then compute the weight function $\mathrm{wt}(\mathbf{u})$ and finally we prove its quasi-injectivity.

2. The code $C_q(r,n)$

Denote $(\mathbb{Z}/2)^n = \mathbb{F}_2^n$ the additive abelian group of exponent 2 and order $N = 2^n$. From now on we assume that $n \geqslant 2$ and that q is an odd prime power. Let M denote the multiplicative group of characters from $(\mathbb{Z}/2)^n$ to $\mathbb{F}_q^*$. The group M is isomorphic non-canonically to $(\mathbb{Z}/2)^n$ [7, Chapter VI]. In particular we have $|M| = |(\mathbb{Z}/2)^n| = N = 2^n$.

The set $(\mathbb{Z}/2)^n$ may be identified with the set of integers $\{i \ : \ 0 \leqslant i \leqslant 2^n - 1\}$: the element $(i_0, i_1, \ldots, i_{n-1})$ of $(\mathbb{Z}/2)^n$ 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

$$f_i(y) = (-1)^{i_0y_0+i_1y_1+\cdots+i_{n-1}y_{n-1}}, \tag{1}$$

where $y = (y_0, y_1, \ldots, y_{n-1}) \in (\mathbb{Z}/2)^n$, 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 $0 \leqslant i \leqslant 2^n - 1$, this gives all the 2^n characters from $(\mathbb{Z}/2)^n$ to $\mathbb{F}_q^*$ 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 representations, we have $f_i(y) = f_y(i)$. For any subset X of $(\mathbb{Z}/2)^n$, the group character code C_X over $\mathbb{F}_q$ described by Ding, Kohel and Ling [2] is:

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

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

Proposition 1. [2] *Let X be as above. For $0 \leqslant i \leqslant N-1$, 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,

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

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

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

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

Let $\{e_1, \ldots, e_n\}$ be a basis of $(\mathbb{Z}/2)^n$.

Definition 1. The Hamming weight $\|a\|$ of an element $a = \sum_{l=1}^{n} a_l e_l$ is defined to be the number of nonzero a_l.

Similarly, for a word $\mathbf{c} = (c_0, \ldots, c_{2^n-1})$ in $\mathbb{F}_q^{2^n}$, the Hamming weight of $\mathbf{c}$, denoted $\mathrm{wt}(\mathbf{c})$ is the number of nonzero c_i.

Definition 2. For $-1 \leqslant r \leqslant n$, let

$$X(r, n) = \{\, a \in (\mathbb{Z}/2)^n \colon \|a\| > r \,\}.$$

We define $C_q(r, n)$ to be the code $C_{X(r,n)}$ over $\mathbb{F}_q$.

The main properties of $C_q(r, n)$ are listed in the abstract and the introduction. For their proof, see [2].

We now move to the more specific problem of computing the weight distribution of these codes.

2.1. **The code $C_q(1,n)$.** In general, it is not an easy matter to determine the weight distribution of $C_q(r,n)$. However, when $r=1$, a partial result was found by Ding, Kohel and Ling. Notations as above, define for $1 \leqslant i \leqslant n$, x_i to be e_i and $x_0 = \mathbf{0}$. This implies that $\mathbf{v}_0$ is the vector $(1,\ldots,1)$ and $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a basis for the code $C_q(1,n)$.

From now on we assume $q=5$. Let $V = \mathbb{F}_5^n$. For $\mathbf{a} = (a_1,\ldots,a_n) \in V$, we let m be the Hamming weight of $\mathbf{a}$. Define

$$\mathbf{u}_0 \stackrel{\text{def}}{=} \sum_{l=1}^{n} a_l \mathbf{v}_l$$

and

$$\mathbf{u} \stackrel{\text{def}}{=} a_0\mathbf{v}_0 + \sum_{l=1}^{n} a_l \mathbf{v}_l$$

where $a_0 \in \mathbb{F}_5$. Then $\mathbf{u}$ is a typical codeword of $C_5(1,n)$ and $\mathbf{u}_0$ is a codeword with $a_0 = 0$.

Define also, for $i = 1, 2$

$$n_i(\mathbf{a}) = \Big|\{\, k\colon 1 \leqslant k \leqslant n \text{ and } a_k = \pm i \,\}\Big|.$$

Note that $n_1 + n_2 = m$. The result of Ding, Kohel and Ling is that $\mathrm{wt}(\mathbf{u}_0)$ and $\mathrm{wt}(\mathbf{u})$ depend only on n_1 and n_2, and of course n. This is a more complex situation than the case $q=3$ when the weight depends only on m. Their result can be summarised as follows.

Proposition 2. *Define* $\mathfrak{w}_0(n_1,n_2)=\mathfrak{w}_0(n_1,n_2,n)$ *to be the number of solutions to the equation in* $\mathbb{F}_5$

$$\sum_{l=1}^{n} a_l x_l = 0, \quad x_l = \pm 1$$

and respectively $\mathfrak{w}(n_1,n_2)$ *for the equation*

$$\sum_{l=1}^{n} a_l x_l = -a_0, \quad x_l = \pm 1, \quad a_0 \neq 0.$$

Then $\mathrm{wt}(\mathbf{u}_0)=2^n-\mathfrak{w}_0(n_1,n_2)$ *and* $\mathrm{wt}(\mathbf{u})=2^n-\mathfrak{w}(n_1,n_2)$. *Furthermore*

$$\mathfrak{w}_0(n_1,n_2)=2^{n-m}\sum_{\substack{0\leqslant u_1\leqslant n_1\\ 0\leqslant u_2\leqslant n_2\\ u_1+2u_2\equiv n_2+3n_1 \,(\mathrm{mod}\,5)}}\binom{n_1}{u_1}\binom{n_2}{u_2} \tag{2}$$

and, if $a_0=\pm 1$,

$$\mathfrak{w}(n_1,n_2)=2^{n-m}\sum_{\substack{0\leqslant u_1\leqslant n_1\\ 0\leqslant u_2\leqslant n_2\\ u_1+2u_2\equiv n_2+3n_1-3 \,(\mathrm{mod}\,5)}}\binom{n_1}{u_1}\binom{n_2}{u_2}$$

Remarks. (1) Notice that

$$\mathfrak{w}_0(n_1,n_2)=\mathfrak{w}_0(n_2,n_1). \tag{3}$$

This because $n_2(2\mathbf{a})=n_1(\mathbf{a})$ and $n_1(2\mathbf{a})=n_2(\mathbf{a})$, but the equations remain the same, being just multiplied by 2.

(2) $\mathfrak{w}$ and $\mathfrak{w}_0$ are related by the formula

$$\mathfrak{w}(n_1,n_2,n)=\begin{cases}\mathfrak{w}_0(n_1,n_2+1,n+1)/2, & \text{if } a_0=\pm 2,\\ \mathfrak{w}_0(n_1+1,n_2,n+1)/2, & \text{if } a_0=\pm 1.\end{cases} \tag{4}$$

Indeed it suffices to note that the equation $\sum_{l=0}^{n} a_l x_l = 0,\ x_l = \pm 1$ has an even number of solutions, half of them having $x_0 = 1$ and the other half being their opposites with $x_0 = -1$.

The remark shows that we need only focus our attention on the computation of $\mathfrak{w}_0(n_1, n_2, n)$ for all possible values of n_1, n_2, n.

3. Another expression for $\mathfrak{w}_0(n_1, n_2)$

Our goal in this section is to give a closed form for the sum in (2). By defining $\binom{n}{u} = 0$ when $u \notin [0, n]$ we can drop the limitations on the range of the u_i. Also we have the well-known formula of Pascal:

$$\binom{n}{u} + \binom{n}{u+1} = \binom{n+1}{u+1}, \tag{5}$$

valid for all integral values of n and u. We define

$$\mathcal{B}_k(n_1, n_2) = \sum_{i+2j \equiv k \,(\bmod 5)} \binom{n_1}{i}\binom{n_2}{j}$$

and

$$B_k(n) = \sum_{j \equiv k \,(\bmod 5)} \binom{n}{j}.$$

Lemma 1. *We have*

$$\sum_{j=0}^{n}\binom{n}{j}=2^n,$$

$$B_k(n)+B_{k+1}(n)=B_{k+1}(n+1),$$

$$\sum_{k=0}^{4}\mathcal{B}_k(n_1,n_2)=2^{n_1+n_2},$$

$$\sum_{k=0}^{4}B_k(n)=2^n.$$

Proof. The first equality is well-known and is proved by setting $x=1$ in the Leibniz expansion of $(1+x)^n$. The second is an easy consequence of (5). The third and the fourth follow formally from the first by noting that summing over k gets rid of the congruence condition of both summations. □

We now transform (2). Remark that

$$\mathfrak{w}_0(n_1,n_2)=2^{n-m}\mathcal{B}_{3n_1+n_2}(n_1,n_2).$$

Without loss of generality in view of (3), we may suppose that $n_1\geqslant n_2$. Let $\zeta\neq 1$ be a fifth root of unity. We have

$$(\zeta+1)^{n_1}(\zeta^2+1)^{n_2}=\sum_i\zeta^i\binom{n_1}{i}\ \sum_j\zeta^{2j}\binom{n_2}{j}=\sum_{i,j}\zeta^{i+2j}\binom{n_1}{i}\binom{n_2}{j}.$$

On the other hand

$$\begin{aligned}(\zeta+1)^{n_1}(\zeta^2+1)^{n_2} &= \left((\zeta+1)(\zeta^2+1)\right)^{n_2}(\zeta+1)^{n_1-n_2}\\ &= (1+\zeta+\zeta^2+\zeta^3)^{n_2}\sum_j \zeta^j\binom{n_1-n_2}{j}\\ &= (-\zeta^4)^{n_2}\sum_j \zeta^j\binom{n_1-n_2}{j}.\end{aligned}$$

Hence we have

$$\begin{aligned}&\sum_{i,j}\zeta^{i+2j}\binom{n_1}{i}\binom{n_2}{j} = (-1)^{n_2}\zeta^{-n_2}\sum_j\zeta^j\binom{n_1-n_2}{j}\\ \iff &\sum_{i,j}\zeta^{i+2j+n_2}\binom{n_1}{i}\binom{n_2}{j} + (-1)^{n_2-1}\sum_j\zeta^j\binom{n_1-n_2}{j} = 0\\ \iff &\sum_{l=0}^{4}\zeta^l\left(\mathcal{B}_{l-n_2}(n_1,n_2) + (-1)^{n_2-1}B_l(n_1-n_2)\right) = 0\end{aligned}$$

Since ζ is a fifth root of unity, this implies that the coefficients of ζ^l do not depend on l. Their sum is

$$\sum_{l=0}^{4}\left\{\mathcal{B}_{l-n_2}(n_1,n_2) + (-1)^{n_2-1}B_l(n_1-n_2)\right\} = 2^{n_1+n_2} - (-1)^{n_2}2^{n_1-n_2}$$

by Lemma 1, hence we get the formula

$$\mathcal{B}_{l-n_2}(n_1,n_2) = \frac{2^{n_1+n_2}-(-1)^{n_2}2^{n_1-n_2}}{5} + (-1)^{n_2}B_l(n_1-n_2),\ l=0,\dots,4.$$

By setting $l = 3n_1+2n_2 = 3(n_1-n_2)$, we obtain

(6)

$$\mathfrak{w}_0(n_1,n_2) = 2^{n-m}\left\{\frac{2^{n_1+n_2}-(-1)^{n_2}2^{n_1-n_2}}{5} + (-1)^{n_2}B_{3(n_1-n_2)}(n_1-n_2)\right\}.$$

It remains to find an explicit expression for $B_{3(n_1-n_2)}(n_1-n_2)$. We thus define the sequence $\mathfrak{B}_n \overset{\text{def}}{=} B_{3n}(n)$. A fundamental result here is the following.

Lemma 2. *We have, for $n \geqslant 0$*

$$\mathfrak{B}_n = \frac{2^n + (-1)^n 2L_n}{5},$$

where L_n is the n-th Lucas number defined by $L_0 = 2$, $L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ for $n \geqslant 0$.

Proof. This is a special case of the Ramus formula [4, p. 70]. However, a shorter proof can be achieved using induction. □

We combine the results of proposition 2, (6) and Lemma 2 into a theorem.

Theorem 1. *We have*

$$\mathfrak{w}_0(n_1, n_2) = \frac{2^n + 2^{n-m+1}(-1)^{n_1} L_{n_1-n_2}}{5},$$

provided $n_1 \geqslant n_2$ *(otherwise interchange* n_1 *and* n_2*). Hence the weight of* $\mathbf{u}_0$ *and* $\mathbf{u}$ *are*

(7)

$$\mathrm{wt}(\mathbf{u}_0) = \frac{2^{n+2} - 2^{n-m+1}(-1)^{n_1} L_{n_1-n_2}}{5} \quad \textit{if } n_1 \geqslant n_2,$$

(8)

$$\mathrm{wt}(\mathbf{u}) = \begin{cases} \left[2^{n+2} + 2^{n-m}(-1)^{n_1} L_{n_1+1-n_2}\right]/5 & \textit{if } n_1 + 1 \geqslant n_2 \textit{ and } a_0 = \pm 1 \\ \left[2^{n+2} - 2^{n-m}(-1)^{n_1} L_{n_1-n_2-1}\right]/5 & \textit{if } n_1 > n_2 \textit{ and } a_0 = \pm 2. \end{cases}$$

Here again the restriction on n_1 *and* n_2 *is not necessary provided one makes the necessary changes in the formulas.*

4. The quasi-injectivity of the weight function

The results of the last section equip us with the knowledge of the powers in the weight enumerator polynomial of $C_5(1,n)$. For some applications however, it is useful to know also the coefficients of the weight enumerator, that is the number of codewords of a given weight.

This is why a careful analysis of the distribution of the values of $\mathfrak{w}_0(n_1,n_2)$ as n_1 and n_2 vary is needed. The main result of this section is the following

Lemma 3. *The equation in nonnegative integers* n, m, k

$$\frac{L_n}{L_m} = 2^k$$

has the following solutions (n, m, k)*:*

$$(n, n, 0) \qquad (3, 0, 1)$$

$$(0, 1, 1) \qquad (3, 1, 2)$$

Assuming this theorem for the moment, we show how to compute the number of codewords of a given weight. Since $\mathbf{u}$ and $c\mathbf{u}$ have same weight when $c \neq 0$, we can assume without loss of generality that $a_0 = 1$ for $\mathbf{u}$ (and $n_1 \geqslant n_2$ for $\mathbf{u}_0$ until the next lemma). We then examine the occurrences of the equalities

$$\mathrm{wt}(\mathbf{u}) = \mathrm{wt}(\mathbf{u}') \tag{9a}$$

$$\mathrm{wt}(\mathbf{u}) = \mathrm{wt}(\mathbf{u}_0) \tag{9b}$$

$$\mathrm{wt}(\mathbf{u}_0) = \mathrm{wt}(\mathbf{u}_0') \tag{9c}$$

for differents codewords $\mathbf{u}, \mathbf{u}', \mathbf{u}_0, \mathbf{u}_0'$ normalised as described. Using (7), equation (9c) then reads as

$$(-1)^{n_1} \frac{L_{n_1 - n_2}}{2^m} = (-1)^{n_1'} \frac{L_{n_1' - n_2'}}{2^{m'}}.$$

Using Lemma 3, it is easy to determine that the only solutions to this equation (remember that $n_1 + n_2 = m$ and similarly for $\mathbf{u}'_0$) are

$$n_1 = n'_1,\ n_2 = n'_2$$

$$n_1 = n_2 \quad \text{and} \quad n'_1 = n_1 + 2,\ n'_2 = n_2 - 1$$

$$n_1 = n_2 \quad \text{and} \quad n'_1 = n_1,\ n'_2 = n_2 - 1$$

$$n_1 = n_2 + 1 \quad \text{and} \quad n'_1 = n_1 + 2,\ n'_2 = n_2.$$

We have then proved the following result

Lemma 4. *The equation*

$$\mathfrak{w}_0(n_1, n_2, n) = \mathfrak{w}_0(n'_1, n'_2, n)$$

has only the eight following possible solutions

$$n_1 = n'_1,\ n_2 = n'_2$$

$$n_1 = n_2 \quad \textit{and} \quad n'_1 = n_1 + 2,\ n'_2 = n_2 - 1$$

$$n_1 = n_2 \quad \textit{and} \quad n'_1 = n_1,\ n'_2 = n_2 - 1$$

$$n_1 = n_2 + 1 \quad \textit{and} \quad n'_1 = n_1 + 2,\ n'_2 = n_2$$

together with the other four solutions obtained by applying the transformation

$$n_1 = n'_2,\ n_2 = n'_1.$$

We can use this result to solve all equations (9) simultaneously. Indeed

$$\mathfrak{w}_0(n_1, n_2, n+1) = 2\mathfrak{w}_0(n_1, n_2, n)$$

hence by (4) we get that equations (9) are equivalent to

$$\mathfrak{w}_0(\nu_1, n_2, n+1) = \mathfrak{w}_0(\nu_1', n_2', n+1),$$

where $\nu_1 = n_1$ or $n_1 + 1$ according to whether the vector is $\mathbf{u}_0$ or $\mathbf{u}$, and similarly with ν_1'.

Then Lemma 4, together with this observation, allows us to construct the following maximal table of equalities, thus solving (9).

$$\begin{array}{ccccc} & & \mathfrak{w}_0(n_1+2, n_1-1) & = & \mathfrak{w}_0(n_1, n_1-1) \\ & & \| & & \| \\ \mathfrak{w}_0(n_1, n_1) & = & \mathfrak{w}_0(n_1-1, n_1+2) & = & \mathfrak{w}_0(n_1-1, n_1) \\ \| & & & & \\ \mathfrak{w}(n_1-1, n_1) & = & \mathfrak{w}(n_1+1, n_1-1) & = & \mathfrak{w}(n_1-1, n_1-1) \\ & & \| & & \| \\ & & \mathfrak{w}(n_1-2, n_1+2) & = & \mathfrak{w}(n_1-2, n_1) \end{array} \tag{10}$$

We wrote maximal because some of these values may not make sense for some values of n_1. Indeed the sum of the two arguments in $\mathfrak{w}$ and $\mathfrak{w}_0$ must be less or equal to n. For example in the top part of the equalities (with $\mathfrak{w}_0$), in the first column we must insure that $2n_1 \leqslant n$, in the second that $2n_1 + 1 \leqslant n$ and in the third that $2n_1 - 1 \leqslant n$.

Notice that the number of vectors $(a_0, \mathbf{a})$ with prescribed a_0, n_1 and n_2 is

$$\binom{n}{n_1\,;\,n_2} = 2^m \binom{n}{n_1}\binom{n-n_1}{n_2} = 2^m \,\frac{n!}{n_1!\,n_2!\,(n-m)!},$$

where we define $\binom{n}{n_1;n_2} = 0$ whenever $n_1 + n_2 > n$.

Let $n_1 \geqslant n_2$ with $n_2 \neq n_1, n_1 - 1, n_1 - 3$. Then the number of codewords of weight

$$\frac{2^{n+2} - 2^{n-m+1}(-1)^{n_1} L_{n_1-n_2}}{5}$$

is exactly

$$\begin{aligned} 2\binom{n}{n_1\,;\,n_2} + 4\binom{n}{n_1-1\,;\,n_2} + 4\binom{n}{n_2-1\,;\,n_1} &= 2^{m+1}\,\frac{(n+1)!}{n_1!\,n_2!\,(n+1-m)!} \\ &= 2\binom{n+1}{n_1\,;\,n_2}. \end{aligned}$$

On the other hand, by (10), the number of codewords of weight

$$\frac{2^{n+2} - 2^{n-2n_1+2}(-1)^{n_1}}{5}$$

is exactly

$$\begin{aligned} &\binom{n}{n_1\,;\,n_1} + 2\binom{n}{n_1+2\,;\,n_1-1} + 2\binom{n}{n_1\,;\,n_1-1} + 4\binom{n}{n_1-1\,;\,n_1} \\ &+4\binom{n}{n_1+1\,;\,n_1-1} + 4\binom{n}{n_1-2\,;\,n_1+2} + 4\binom{n}{n_1-1\,;\,n_1-1} \\ &+4\binom{n}{n_1-2\,;\,n_1} = \binom{n+1}{n_1\,;\,n_1} + 2\binom{n+1}{n_1+2\,;\,n_1-1} + 2\binom{n+1}{n_1-1\,;\,n_1}. \end{aligned}$$

We put this together in a theorem.

Theorem 2. *Let L_k denote the k-th Lucas number, defined in Lemma 2. Let $n_1 \geqslant n_2 \geqslant 0$ be integers. Then the number of codewords of $C_5(1,n)$ of weight*

$$w(n_1,n_2) = \frac{2^{n+2} - 2^{n-n_1-n_2+1}(-1)^{n_1} L_{n_1-n_2}}{5}$$

is exactly

$$2\binom{n+1}{n_1\,;\,n_2} = 2^{m+1}\,\frac{(n+1)!}{n_1!\,n_2!\,(n+1-m)!},$$

provided $n_2 \neq n_1, n_1-1, n_1-3$.

In the exceptional cases, we have that the number of codewords of $C_5(1,n)$ of weight

$$w(n_1,n_1) = \frac{2^{n+2} - 2^{n-2n_1+2}(-1)^{n_1}}{5}$$

is precisely

$$\binom{n+1}{n_1\,;\,n_1} + 2\binom{n+1}{n_1+2\,;\,n_1-1} + 2\binom{n+1}{n_1-1\,;\,n_1}.$$

This concludes the analysis of the weight distribution of $C_5(1,n)$. In passing, our method yields the following corollary.

Corollary 1. *The minimum weight of $C_5(1,n)$ is 2^{n-1}. The minimum weight codewords are all words of the form*

$$a_i\mathbf{v}_i + a_j\mathbf{v}_j, \quad 0 \leqslant i < j \leqslant n \quad \textit{and} \quad a_i = \pm a_j \neq 0.$$

Proof. We use the fact that

$$L_n < L_{n+1} < 2L_n \quad \text{for } n \geqslant 1 \text{ and } n \geqslant 2 \text{ respectively.} \tag{11}$$

Indeed $L_n > 0$, hence $L_{n+1} = L_n + L_{n-1} > L_n$ for $n \geqslant 1$. The same recurrence equation also implies that $L_{n+2} = L_{n+1} + L_n < 2L_{n+1}$ for $n \geqslant 1$, hence the claim.

This fact implies that $w(n_1, n_2) \geqslant \min\big(w(2,0), w(2,2)\big)$ when n_1 and n_2 are not both zero. Since

$$2^{n-1} = w(2,0) < w(2,2) = 2^{n-1} + 2^{n-2},$$

the minimum distance of $C_5(1,n)$ is 2^{n-1}.

Also, the proof of Theorem 2 shows that the codewords of weight $w(2,0)$ are precisely the $8n(n+1)/2$ listed above. □

5. Proof of Lemma 3

It remains to prove Lemma 3. Note that the sequence $L_n \bmod 8$ is clearly periodic with period 12. It is

$$2\ 1\ 3\ 4\ 7\ 3\ 2\ 5\ 7\ 4\ 3\ 7\ 2\ 1\ldots$$

In particular, we see that L_n is never divisible by 8. Hence $k \leqslant 2$.

By (11) we have that $L_n = L_m \Rightarrow n = m$. This accounts for all solutions $(n, n, 0)$. The recursion relation implies that $L_{n+2} > 2L_n$ when $n \geqslant 1$. This and (11) imply that when $k = 1$ the only possibilities for (n, m) are

$$(1,0), (2,0), (3,0), (0,1), (2,1)$$

and only $(3,0), (0,1)$ actually yield solutions for $k = 1$.

For $k = 2$, the previous relations imply that $L_{n+3} = 3L_n + 2L_{n-1} > 4L_n$ except for $n = 2$ and that $L_{n+2} < 4L_n$ except for $n = 1$. Thus the only solution in this case is $(3, 1)$ and this concludes the proof.

6. Conclusion

We have found the weight distribution of $C_5(1, n)$. Unfortunately, the methods of our proof are too specialised for an immediate generalisation, say to $C_7(1, n)$, although this task may not prove impossible. There are a number of questions which might prove more tractable, though. For example, is it always true that the minimum weight codewords of $C_q(1, n)$ are scalar multiples of $\mathbf{v}_i \pm \mathbf{v}_j$?

It is an interesting problem to combine these techniques together with the methods in [1] to extend the results of that paper to respective codes over $\mathbb{F}_5$.

Another interesting path would lead to the weight distribution of $C_3(2, n)$.

Acknowledgement: We are most grateful to the referees for their comments on the presentation of this paper. In particular, I owe this elegant proof of Lemma 3 to one of them.

References

[1] C. Ding, T. Kløve and F. Sica, *Two Classes of Ternary Codes and their Weight Distribution*, Discrete Appl. Math. 111 (2001) 37–53.

[2] C. Ding, D. Kohel and S. Ling, *Elementary 2-Group Character Codes*, IEEE Trans. on Infom. Theory 46 (2000), n°1, 280–284.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Oxford University Press (1989).

[4] D. E. Knuth, *The Art of Computer Programming*, Vol. 1, Second edition, Addison-Wesley (1973).

[5] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics 110, Springer-Verlag (1986).

[6] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1977).

[7] J.-P. Serre, *Cours d'arithmétique*, Presses Universitaires de France (1988).

School of Computing, National University of Singapore, Lower Kent Ridge Road, Singapore 119260

E-mail address: lamky@comp.nus.edu.sg

E-mail address: sica@comp.nus.edu.sg