The weight distributions of some binary cyclic codes

Anuradha Sharma[*]
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi-110016, India

Suman Bala
Department of Mathematics
Panjab University
Chandigarh-160014, India

Abstract

Let p be an odd prime and n be a positive integer. For any positive integer $d \leq n$, let $g_1(x) = 1 + x^{p^{n-d}} + x^{2p^{n-d}} + \cdots + x^{(p-1)p^{n-d}}$ and $g_2(x) = 1 + x^{p^{n-d+1}} + x^{2p^{n-d+1}} + \cdots + x^{(p^{d-1}-1)p^{n-d+1}}$. In this paper, we provide a method to determine the weight distributions of binary cyclic codes of length p^n generated by the polynomials $g_1(x)$ and $g_1(x)g_2(x)$, which is effective for small values of p and d.

Keywords : cyclic codes, Hamming weight, weight spectrum.

2000 Mathematics Subject Classification : 94B15.

1 Introduction

Let $\mathbb{F}_q$ be the finite field of order q and n be a positive integer coprime to q. A cyclic code C of length n over $\mathbb{F}_q$ is a linear subspace of

[*] Corresponding Author, Email: anuradha@maths.iitd.ac.in

$\mathbb{F}_q^n$ with the property that if $(a_0, a_1, \cdots, a_{n-1}) \in C$, then the cyclic shift $(a_{n-1}, a_0, a_1, \cdots, a_{n-2})$ is also in C.

The Hamming weight of a vector $v \in \mathbb{F}_q^n$, denoted by $w(v)$, is the number of non-zero coordinates in v. For a code C of length n over $\mathbb{F}_q$, let $A_i^{(n)}$ denote the number of codewords of Hamming weight i in C. Then the list $A_0^{(n)}, A_1^{(n)}, \cdots, A_n^{(n)}$ is called the Hamming weight distribution (or weight spectrum) of C. Knowing the Hamming weight distribution of a code, one can calculate the probability of undetected errors when the code is used purely for error detection. The least positive integer i for which $A_i^{(n)}$ is non-zero, is called the minimum Hamming weight of C, which is a measure of error-correcting properties of the code. Thus the problem of determination of the weight distribution of a code is of great interest.

The cyclic code C can also be regarded as an ideal in the principal ideal ring $\mathbb{R}_n = \mathbb{F}_q[x]/ < x^n - 1 >$ under the vector space isomorphism from $\mathbb{F}_q^n \mapsto \mathbb{R}_n$ given by $(a_0, a_1, \cdots, a_{n-1}) \mapsto a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$. As an ideal in $\mathbb{R}_n$, the code C is generated by a unique monic polynomial $g(x)$, which is a divisor of $x^n - 1$, called the generator polynomial of C. The code C is called irreducible if the polynomial $\frac{x^n-1}{g(x)}$ is an irreducible polynomial over $\mathbb{F}_q$; otherwise C is called reducible.

Since the ring $\mathbb{R}_n$ is semi-simple, so every reducible cyclic code is a direct sum of certain irreducible cyclic codes. However, there is no relation known between the weight distributions of reducible and those of irreducible cyclic codes. Moreover, the weight distributions of irreducible cyclic codes are known only in some special cases.

MacWilliams & Seery [8] gave a procedure, involving generation of a pseudo-random sequence, to obtain the weight distributions of binary irreducible cyclic codes, which can be implemented only on a powerful computer. van der Vlugt [13] related the problem of computing weight distributions to the evaluation of certain sums involving Gauss sums, which are generally hard to determine explicitly. To evaluate these sums in some special cases, certain algorithms were given by Baumert & McEliece [3], Moisio & Väänänen [9], Fitzgerald & Yucas [6], etc., using various techniques. Segal & Ward [10] also computed the weight distributions of some binary irreducible cyclic codes by using the theory developed by Baumert & McEliece [3].

Aubry & Langevin [1] studied the divisibility of weights in binary irreducible cyclic codes. Zanotti [15] also studied the weight behavior of irreducible cyclic balanced weight codes, (i.e., the codes in which there are the same number of codewords for each non-zero weight). Augot [2] used the theory of Grobner basis for a certain system of algebraic equations to give information about the minimum weight codewords.

Sharma, Bakshi & Raka [12] determined the weight distribution of all the q-ary irreducible cyclic codes of length 2^m. Recently, Ding [4] computed the weight distribution of q-ary irreducible cyclic codes of length n provided $2 \leq \frac{q^{O_n(q)}-1}{n} \leq 4$, where $O_n(q)$ denotes the multiplicative order of q modulo n. He also pointed out that the weight formulas become quite messy if $\frac{q^{O_n(q)}-1}{n} \geq 5$ and therefore finding the weight distribution of q-ary irreducible cyclic codes is a notoriously difficult problem. In a recent work, Sharma & Bakshi [11] obtained the weight distributions of some q-ary irreducible cyclic codes of odd prime power lengths directly from their generating polynomials.

Very few results are known on the weight distributions of reducible cyclic codes.

Wang, Tang, Qi, Yang & Xu [14] determined the weight distributions of dual codes of cyclic codes with two zeros and for a few more cases, using the theory of elliptic curves. They also remarked that the weight distributions of cyclic codes are difficult to determine.

Feng & Luo [5] computed the weight distributions of a special class of linear codes by computing the values and multiplicities of certain special exponential sums involving Dembowski-Ostrom polynomial. Extending this result, Luo & Feng [7] determined the weight distributions of two special classes of cyclic codes by determining the values distribution of a certain exponential sum using the theory of quadratic forms.

Zeng, Hu, Jiang, Yue & Cao [16] obtained the weight distribution of a p-ary cyclic code C over $\mathbb{F}_p$ with non-zeros α^{-1}, $\alpha^{-(p^k+1)}$ and $\alpha^{-(p^{3k}+1)}$, α being a primitive element of $\mathbb{F}_{p^n}$, where p is an odd prime and $n \geq 3$, k are positive integers such that $\frac{n}{\gcd(n,k)}$ is odd. Zeng, Shan & Hu [17] determined the minimum distance of a binary cyclic code with three zeros α, α^3 and α^{13} of length $2^m - 1$ and studied the weight divisibility of its dual code, where $m \geq 5$ is odd and α is a primitive element of the finite field $\mathbb{F}_{2^m}$.

The aim of this paper is to provide a method to determine the weight distributions of some binary cyclic codes of odd prime power lengths directly from their generating polynomials, by extending the technique developed in [11].

Throughout this paper, we let p be an odd prime and $n \geq 1$ be an integer. For $1 \leq d \leq n$, we consider the following factorization of $x^{p^n} - 1$ over $\mathbb{F}_2$:

$$x^{p^n} - 1 = g_1(x)g_2(x)g_3(x),$$

where $g_1(x) = 1 + x^{p^{n-d}} + x^{2p^{n-d}} + \cdots + x^{(p-1)p^{n-d}}$, $g_2(x) = 1 + x^{p^{n-d+1}} + x^{2p^{n-d+1}} + \cdots + x^{(p^{d-1}-1)p^{n-d+1}}$ and $g_3(x) = x^{p^{n-d}} - 1$.

In Section 2, we determine the weight distribution of the binary code generated by $g_1(x)$. In Section 3, we determine the weight distribution of the binary code generated by $g_1(x)g_2(x)$.

In a subsequent work, we compute the weight distributions of q-ary (reducible) cyclic codes generated by the polynomials $g_2(x), g_3(x), g_1(x)g_3(x)$ and $g_2(x)g_3(x)$, where q is any prime power.

2 The weight distribution of $< g_1(x) >$

First we fix some notations. Given positive integers t and ν, let $P_t(\nu)$ denote the set of all tuples $(\nu_1, \nu_2, \cdots, \nu_t)$ of positive integers ν_i's$(1 \leq i \leq t)$ with $\sum_{i=1}^{t} \nu_i = \nu$. Further for any $(\nu_1, \nu_2, \cdots, \nu_t) \in P_t(\nu)$, let $L(\nu_1, \nu_2, \cdots, \nu_t)$ be the set of all tuples $(\ell_1, \ell_2, \cdots, \ell_t)$ of non-negative integers ℓ_j's satisfying $\sum_{j=1}^{t} \ell_j \leq p^d - pt$. And for any $(\ell_1, \ell_2, \cdots, \ell_t) \in L(\nu_1, \nu_2, \cdots, \nu_t)$, set

$$a(\ell_1, \ell_2, \ldots, \ell_t) = \sum_{m_1=0}^{p^d - \sum_{i=1}^{t} \ell_i - pt} \ \sum_{m_2=m_1+\ell_1+p}^{p^d - \sum_{i=2}^{t} \ell_i - p(t-1)} \cdots \sum_{m_t=m_{t-1}+\ell_{t-1}+p}^{p^d-\ell_t-p} 1. \quad (1)$$

We are now ready to state

Theorem 1 *Let p be an odd prime and $n \geq 1$ be an integer. Let $g_1(x) = 1 + x^{p^{n-d}} + x^{2p^{n-d}} + \cdots + x^{(p-1)p^{n-d}}$, where d is an integer satisfying $1 \leq d \leq n$. Then the weight distribution $A_0^{(p^n)}, A_1^{(p^n)}, \cdots, A_{p^n}^{(p^n)}$ of the binary cyclic code C_1, generated by $g_1(x)$, is given by*

$$A_w^{(p^n)} = \sum N(w_1)N(w_2)\cdots N(w_{p^{n-d}})$$

for each $w \geq 0$, where the summation runs over all tuples $(w_1, w_2, \cdots, w_{p^{n-d}})$ of non-negative integers w_i's satisfying $\sum_{i=1}^{p^{n-d}} w_i = w$; and for any $\nu \geq 0$, $N(\nu)$ equals
(i) 1 if $\nu = 0$;
(ii) 0 if $\nu \geq p^d + 1$;

$$(iii) \quad \sum_{t\geq 1} \sum_{(\nu_1,\nu_2,\cdots,\nu_t)\in P_t(\nu)} \sum_{(\ell_1,\ell_2,\cdots,\ell_t)\in L(\nu_1,\nu_2,\cdots,\nu_t)} a(\ell_1, \ell_2, \cdots, \ell_t) \prod_{i=1}^{t} n(\nu_i; \ell_i)$$

if $1 \leq \nu \leq p^d$; where $a(\ell_1, \ell_2, \cdots, \ell_t)$ is as defined by (1) and $n(\nu_r, \ell_r)$ $(1 \leq r \leq t)$ is as given by Lemma 9.

We need some preparation to prove this theorem.

As a vector subspace of R_{p^n}, the code C_1 is spanned by $g_1(x), xg_1(x), x^2g_1(x), \cdots, x^{p^{n-d}(p^d-p+1)-1}g_1(x)$. Therefore, under the standard isomorphism from R_{p^n} to $\mathbb{F}_2^{p^n}$, the code C_1 has the following $p^{n-d}(p^d-p+1)$ vectors as its basis, where each vector R_{i+1} corresponds to $x^ig_1(x)$:

$$R_1 \;=\; (1,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1,\cdots,1,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1,\ \underbrace{0,0,\cdots,0,0}_{(p^d-p+1)p^{n-d}-1}\ ),$$

$$R_2 \;=\; (0,1,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1,\cdots,1,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1,\ \underbrace{0,0,\cdots,0,0}_{(p^d-p+1)p^{n-d}-2}\ ),$$

$$\cdots \qquad\qquad \cdots\quad \cdots\quad \cdots\quad \cdots\quad \cdots$$

$$R_{(p^d-p+1)p^{n-d}} \;=\; (\ \underbrace{0,0,\cdots,0,0,}_{(p^d-p+1)p^{n-d}-1}\ 1,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1,\cdots,1,$$

$$\underbrace{0,\cdots,0,}_{p^{n-d}-1}\ 1).$$

(Note that the weight of each R_i is p.)

Let V_i $(1 \leq i \leq p^{n-d})$ be the subspace of $\mathbb{F}_2^{p^n}$ generated by $R_i, R_{i+p^{n-d}}, R_{i+2p^{n-d}}, \cdots, R_{i+(p^d-p)p^{n-d}}$. For any integer $\nu \geq 0$, let $N_i(\nu)$ denote the number of codewords in V_i of weight ν.

Proposition 1 *Let $w \geq 0$ and $A_w^{(p^n)}$ be the number of codewords in C_1 having weight w. Then*

$$A_w^{(p^n)} = \sum N_1(w_1)N_2(w_2)\cdots N_{p^{n-d}}(w_{p^{n-d}}),$$

where the summation runs over all tuples $(w_1, w_2, \cdots, w_{p^{n-d}})$ of non-negative integers w_i's satisfying $\sum_{i=1}^{p^{n-d}} w_i = w$.

Proof. It is clear that C_1 is a direct sum of the subspaces $V_1, V_2, \cdots, V_{p^{n-d}}$. Therefore any $v \in C_1$ can be uniquely written as $v = v_1 + v_2 + \cdots + v_{p^{n-d}}$, where $v_i \in V_i(1 \leq i \leq p^{n-d})$. Each $v_i \in V_i$ is of the form

$$(\underbrace{0,\cdots,0,}_{i-1}\ *,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ *,\ \underbrace{0,\cdots,0,}_{p^{n-d}-1}\ *,\cdots,*,\ \underbrace{0,\cdots,0}_{p^{n-d}-i}\ ),$$

where the non-zero entries can occur only at the places marked $*$.

Further note that for $i \neq j$, the non-zero entries of V_i and V_j occur at disjoint places, which gives

$$w(v) = w(v_1) + w(v_2) + \cdots + w(v_{p^{n-d}}).$$

For any tuple $(w_1, w_2, \cdots, w_{p^{n-d}})$ of non-negative integers w_i's satisfying $\sum_{i=1}^{p^{n-d}} w_i = w$, we define

$$S(w_1, w_2, \cdots, w_{p^{n-d}}) = \{v \in C_1 : v = \sum_{i=1}^{p^{n-d}} v_i, w(v_i) = w_i(1 \leq i \leq p^{n-d})\}.$$

Clearly $\cup S(w_1, w_2, \cdots, w_{p^{n-d}})$ is precisely the set of all codewords of C_1 having weight w, where the union runs over all tuples $(w_1, w_2, \cdots, w_{p^{n-d}})$ of non-negative integers w_i's satisfying $\sum_{i=1}^{p^{n-d}} w_i = w$. Therefore

$$A_w^{(p^n)} = |\cup S(w_1, w_2, \cdots, w_{p^{n-d}})|.$$

Also for any two distinct tuples $(w_1, w_2, \cdots, w_{p^{n-d}})$ and $(w'_1, w'_2, \cdots, w'_{p^{n-d}})$, the sets $S(w_1, w_2, \cdots, w_{p^{n-d}})$ and $S(w'_1, w'_2, \cdots, w'_{p^{n-d}})$ are disjoint. Therefore we get

$$|\cup S(w_1, w_2, \cdots, w_{p^{n-d}})| = \sum |S(w_1, w_2, \cdots, w_{p^{n-d}})|.$$

Since we have $|S(w_1, w_2, \cdots, w_{p^{n-d}})| = N_1(w_1)N_2(w_2)\cdots N_{p^{n-d}}(w_{p^{n-d}})$, the desired result follows. □

In order to calculate $N_i(\nu)$ for any $\nu \geq 0$ and for any i, $1 \leq i \leq p^{n-d}$, we prove the following proposition:

Proposition 2 *For any i $(1 \leq i \leq p^{n-d})$ and any $\nu \geq 0$, $N_i(\nu)$ equals* *(i)* 1 if $\nu = 0$;

(ii) 0 if $\nu \geq p^d + 1$;

$$(iii) \sum_{t \geq 1} \sum_{(\nu_1,\nu_2,\cdots,\nu_t) \in P_t(\nu)} \sum_{(\ell_1,\ell_2,\cdots,\ell_t) \in L(\nu_1,\nu_2,\cdots,\nu_t)} a(\ell_1,\ell_2,\cdots,\ell_t) \prod_{i=1}^{t} n(\nu_i;\ell_i)$$

if $1 \leq \nu \leq p^d$; *where* $a(\ell_1, \ell_2, \cdots, \ell_t)$ *is as defined by (1) and* $n(\nu_r, \ell_r)$ $(1 \leq r \leq t)$ *are as given by Lemma 9.*

Note that the value of $N_i(\nu)$ *is independent of* i.

To prove this proposition, we proceed as follows:

Lemma 1 *Let* $1 \leq i \leq p^{n-d}$ *be fixed. Let* $v \in V_i$ *be written as* $v = \alpha_0 R_i + \alpha_1 R_{i+p^{n-d}} + \alpha_2 R_{i+2p^{n-d}} + \cdots + \alpha_{p^d-p} R_{i+(p^d-p)p^{n-d}}$ *for some* $\alpha_0, \alpha_1, \cdots, \alpha_{p^d-p} \in \mathbb{F}_2$. *Let* $v[k]$ $(1 \leq k \leq p^n)$ *denote the kth component of* v. *Then*

(a) for all integers $k \equiv i (\text{mod } p^{n-d})$, $v[k]$ *is given by*

$$v[k] = \begin{cases} \alpha_0 + \alpha_1 + \cdots + \alpha_s & \text{if } 0 \leq s \leq p-1; \\ \alpha_{s+1-p} + \alpha_{s+2-p} + \alpha_\theta & \text{if } p \leq s \leq p^d - 1, \end{cases}$$

where $s = \frac{k-i}{p^{n-d}}$ *and* $\theta = \min(s, p^d - p)$.

(b) for all integers $k \not\equiv i (\text{mod } p^{n-d})$, *we have* $v[k] = 0$.

Proof. Since $v = \alpha_0 R_i + \alpha_1 R_{i+p^{n-d}} + \alpha_2 R_{i+2p^{n-d}} + \cdots + \alpha_{p^d-p} R_{i+(p^d-p)p^{n-d}}$, so v can be written as

$$\begin{aligned} v \;=\; (& \underbrace{0,\cdots,0,}_{i-1} \alpha_0, \underbrace{0,\cdots,0,}_{p^{n-d}-1} \alpha_0+\alpha_1, \underbrace{0,\cdots,0,}_{p^{n-d}-1} \alpha_0+\alpha_1+\alpha_2, \underbrace{0,\cdots,0,}_{p^{n-d}-1} \\ & \cdots, \alpha_0+\alpha_1+\cdots+\alpha_{p-1}, \underbrace{0,\cdots,0,}_{p^{n-d}-1} \alpha_1+\alpha_2+\cdots+\alpha_p, \underbrace{0,\cdots,0,}_{p^{n-d}-1} \\ & \alpha_2+\alpha_3+\cdots+\alpha_{p+1}, \underbrace{0,\cdots,0,}_{p^{n-d}-1} \alpha_{p^d-2p+1}+\alpha_{p^d-2p+2}+\cdots+\alpha_{p^d-p}, \\ & \underbrace{0,\cdots,0,}_{p^{n-d}-1} \alpha_{p^d-2p+3}+\cdots+\alpha_{p^d-p}, \underbrace{0,\cdots,0,}_{p^{n-d}-1} \alpha_{p^d-p-1}+\alpha_{p^d-p}, \underbrace{0,\cdots,}_{p^{n-d}-} \\ & \alpha_{p^d-p}, \underbrace{0,\cdots,0}_{p^{n-d}-i}), \end{aligned} \qquad (2)$$

from which the lemma follows. □

Remark 1 *From Lemma 1, we note that the scalars α_r and α_s appear as summands of the same component of $v \in V_i$ if and only if their subscripts r and s satisfy $|r-s| \le p-1$.*

Definition 1 *Let $\ell \ge 0$ be an integer. Let $0 \le j_0 < j_1 < j_2 < \cdots < j_\ell \le p^d - p$ be the integers satisfying $j_u - j_{u-1} \le p-1$ for $1 \le u \le \ell$. For a fixed i $(1 \le i \le p^{n-d})$, we say that a vector $v \in V_i$ is a nice vector of the type $(j_0, j_1, j_2, \cdots, j_\ell)$ if $v = R_{i+j_0p^{n-d}} + R_{i+j_1p^{n-d}} + \cdots + R_{i+j_\ell p^{n-d}}$. The integer j_0 is called the initial point of v, denoted by $I(v)$. The integer j_ℓ is called the end point of v, denoted by $E(v)$. And the integer $j_\ell - j_0$ is called the length of v, denoted by $L(v)$. The integer ℓ is called the size of v. We denote the weight of a nice vector $v \in V_i$ of the type $(j_0, j_1, j_2, \cdots, j_\ell)$ as $w_i(j_0, j_1, j_2, \cdots, j_\ell)$.*

Remark 2 *Note that a nice vector $v \in V_i$ of the type $(j_0, j_1, \cdots, j_\ell)$ can be obtained by putting $\alpha_{j_0} = \alpha_{j_1} = \cdots = \alpha_{j_\ell} = 1$ and the remaining scalars equal to 0 in the vector given by (2).*

Lemma 2 *Let $1 \le i \le p^{n-d}$ be fixed. Let $v \in V_i$ be a nice vector of the type $(j_0, j_1, \cdots, j_\ell)$. Then $v[i+sp^{n-d}] = 0$ for all s satisfying $0 \le s \le j_0 - 1$ and $j_\ell + p \le s \le p^d - 1$.*

Proof. Let $0 \le s \le j_0 - 1$. Then by Lemma 1(a), we have

$$v[i+sp^{n-d}] = \begin{cases} \alpha_0 + \alpha_1 + \cdots + \alpha_s & \text{if } 0 \le s \le p-1; \\ \alpha_{s+1-p} + \alpha_{s+2-p} + \cdots + \alpha_\theta & \text{if } p \le s \le p^d - 1, \end{cases}$$

where $\theta = \min(s, p^d - p)$. Since $0 \le s < j_0$, by Remark 2, we have $\alpha_0 = \alpha_1 = \cdots = \alpha_s = 0$, which gives $v[i+sp^{n-d}] = 0$ if $s \le p-1$. Now let $p \le s \le p^d - 1$. Since $s+1-p \le p^d - p$ and $s+1-p \le s$, so we get $s+1-p \le \min(s, p^d - p) = \theta$. This gives $s+1-p \le \theta \le s < j_0$, which, by Remark 2, implies that $\alpha_{s+1-p} = \alpha_{s+2-p} = \cdots = \alpha_\theta = 0$. This implies that $v[i + sp^{n-d}] = 0$ if $s \geq p$. Hence $v[i + sp^{n-d}] = 0$ for $0 \leq s \leq j_0 - 1$. Now let $j_\ell + p \leq s \leq p^d - 1$. As $s \geq j_\ell + p > p$, by Lemma 1(a), we have $v[i + sp^{n-d}] = \alpha_{s+1-p} + \alpha_{s+2-p} + \cdots + \alpha_\theta$. Since $s \geq j_\ell + p$ implies that $s + 1 - p > j_\ell$, which by Remark 2, gives $\alpha_{s+1-p} = \alpha_{s+2-p} = \cdots = \alpha_\theta = 0$. Hence $v[i + sp^{n-d}] = 0$ for $j_\ell + p \leq s \leq p^d - 1$. □

Lemma 3 *Let $v \in V_i$ $(1 \leq i \leq p^{n-d})$ be a nice vector of the type $(j_0, j_1, j_2, \cdots, j_\ell)$. Then*
(i) $\ell \leq L(v) \leq p^d - p$,
(ii) $I(v) \geq 0$ *and* $E(v) \leq p^d - p$,
(iii) $E(v) = I(v) + L(v)$.

Proof. From the definition of nice vector, we have $j_\ell \leq p^d - p$, which gives $L(v) = j_\ell - j_0 \leq j_\ell \leq p^d - p$. Also $j_{u+1} - j_u \geq 1$ for each u, $0 \leq u \leq \ell - 1$, implies that $L(v) = j_\ell - j_0 \geq \ell$. This proves (i). The part (ii) follows from the definition of nice vector. And the part (iii) follows immediately from the fact that $L(v) = j_\ell - j_0 = E(v) - I(v)$. □

Definition 2 *Let $1 \leq i \leq p^{n-d}$ be fixed. Let v_1 and v_2 be nice vectors in V_i. Then we say that v_2 is a right neighbour of v_1 if $I(v_2) \geq E(v_1) + p$.*

Remark 3 *Given any non-zero vector $v \in V_i$, we observe that v can be written as $v = v_1 + v_2 + \cdots + v_t$, $t \geq 1$, where each v_r $(1 \leq r \leq t)$ is a nice vector in V_i and each v_r $(2 \leq r \leq t)$ is a right neighbour of v_{r-1}.*

Lemma 4 *Let $1 \leq i \leq p^{n-d}$ be fixed. Let $v_1, v_2, \cdots, v_t \in V_i$ be nice vectors such that each v_r $(2 \leq r \leq t)$ is a right neighbour of v_{r-1}. Then $w(v_1 + v_2 + \cdots + v_t) = w(v_1) + w(v_2) + \cdots + w(v_t)$.*

Proof. On writing each v_r, $1 \leq r \leq t$, as an element of $\mathbb{F}_2^{p^n}$, we see that the non-zero entries of $v_1, v_2, \cdots, v_t$ occur at disjoint places. Therefore the result follows. □

In view of Remark 3 and Lemma 4, we see that in order to determine the weight of a non-zero vector $v \in V_i$, one needs to determine the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of nice vector of the type $(j_0, j_1, \cdots, j_\ell)$ for each integer $\ell \geq 0$.

2.1 Determination of the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of a nice vector of the type $(j_0, j_1, \cdots, j_\ell)$

Next we proceed to determine the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of a nice vector $v \in V_i$ of the type $(j_0, j_1, j_2, \cdots, j_\ell)$ with $I(v) = j_0$, $E(v) = j_\ell$ and $L(v) = j_\ell - j_0$.

Note that $w_i(j_0) = w(R_{i+j_0p^{n-d}}) = p$. So we take $\ell \geq 1$ from now onwards. For a nice vector v of the type $(j_0, j_1, \cdots, j_\ell)$, $\ell \geq 1$, we first define $L_e(v; m)$ and $L_o(v; m)$ $(1 \leq m \leq \ell)$ as follows:

$$L_e(v;m) = \begin{cases} \sum\limits_{k=1}^{m-1} (-1)^k j_k & \text{if } m \text{ is odd;} \\ \sum\limits_{k=1}^{m} (-1)^k j_k & \text{if } m \text{ is even.} \end{cases}$$

$$L_o(v;m) = \begin{cases} \sum\limits_{k=0}^{m} (-1)^{k-1} j_k & \text{if } m \text{ is odd;} \\ \sum\limits_{k=0}^{m-1} (-1)^{k-1} j_k & \text{if } m \text{ is even.} \end{cases}$$

Now we consider the two cases, $L(v) \leq p-1$ and $L(v) \geq p$, in the Propositions 3 and 4 respectively.

Proposition 3 *Let $\ell \geq 1$ be an integer. Let v be a nice vector of the type $(j_0, j_1, \cdots, j_\ell)$ with $L(v) = j_\ell - j_0 \leq p-1$. Then the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of v is given by*

$$w_i(j_0, j_1, \cdots, j_\ell) = \begin{cases} 2L_o(v;\ell) & \text{if } \ell \text{ is odd;} \\ p & \text{if } \ell \text{ is even.} \end{cases}$$

Proof. Here we have $0 \leq j_0 < j_1 < \cdots < j_\ell \leq p^d - p$ with $j_u - j_{u-1} \leq p-1$ for $1 \leq u \leq \ell$ and $j_\ell - j_0 \leq p-1$. In order to compute the number $w_i(j_0, j_1, \cdots, j_\ell)$, we need to compute the number of non-zero components of v. By Lemma 1(b), we have $v[k] = 0$ if $k \not\equiv i (\text{mod } p^{n-d})$. So we focus our attention on the components $v[k]$ with $k \equiv i(\text{mod } p^{n-d})$. In view of Lemma 2, we see that it is enough to study the components $v[k]$, where $k = i + sp^{n-d}$ with $j_0 \leq s \leq j_\ell + p - 1$, and we make the following observations :

(i) For $0 \leq u \leq \ell - 1$, as $j_u - j_0 < j_\ell - j_0 \leq p - 1$, so by Remark 1, there exists a component of v, which is equal to the sum $\alpha_{j_0} + \alpha_{j_1} + \cdots + \alpha_{j_u}$. Further we see that there are a total of $j_{u+1} - j_u$ such components, viz. $v[i + j_u p^{n-d}] = v[i + (j_u + 1)p^{n-d}] = \cdots = v[i + (j_{u+1} - 1)p^{n-d}] = \alpha_{j_0} + \alpha_{j_1} + \cdots + \alpha_{j_u} = \begin{cases} 1 & \text{if } u \text{ is even;} \\ 0 & \text{if } u \text{ is odd.} \end{cases}$

This is because, for $j_u \leq s \leq j_{u+1} - 1$, we have, by Lemma 1(a), $v[i + sp^{n-d}] = \alpha_0 + \alpha_1 + \cdots + \alpha_s$ if $s \leq p - 1$, which, by Remark 2, equals $\alpha_{j_0} + \alpha_{j_1} + \cdots + \alpha_{j_u}$, as $0 \leq j_0 < j_u \leq s$. If $p \leq s \leq p^d - 1$, then by Lemma 1(a), we have $v[i + sp^{n-d}] = \alpha_{s+1-p} + \alpha_{s+2-p} + \cdots + \alpha_\theta$ with $\theta = \min(s, p^d - p)$, which, again by Remark 2, equals $\alpha_{j_0} + \alpha_{j_1} + \cdots + \alpha_{j_u}$, as $s + 1 - p \leq j_{u+1} - p \leq j_\ell - p < j_0 < j_u \leq \min(s, p^d - p) = \theta$ in this case.

(ii) As $j_\ell - j_0 = L(v) \leq p - 1$, again by Remark 1, there exists a component of v which is equal to the sum $\alpha_{j_0} + \alpha_{j_1} + \cdots + \alpha_{j_\ell}$. We see that there are a total of $p - (j_\ell - j_0) = p - L(v)$ such components, viz. $v[i + j_\ell p^{n-d}] = v[i + (j_\ell + 1)p^{n-d}] = \cdots = v[i + (j_0 + p - 1)p^{n-d}] = \alpha_{j_0} + \alpha_{j_1} + \cdots + \alpha_{j_\ell} = \begin{cases} 1 & \text{if } \ell \text{ is even;} \\ 0 & \text{if } \ell \text{ is odd.} \end{cases}$

This is because, when $j_\ell \leq s \leq j_0 + p - 1$, we have $v[i + sp^{n-d}] = \alpha_0 + \alpha_1 + \cdots + \alpha_s$ for $s \leq p-1$ by Lemma 1(a), which, by Remark 2, equals $\alpha_{j_0} + \alpha_{j_1} + \cdots + \alpha_{j_\ell}$, as $0 \leq j_0 < j_\ell \leq s$. And for $s \geq p$, by Lemma 1(a), we have $v[i + sp^{n-d}] = \alpha_{s+1-p} + \alpha_{s+2-p} + \cdots + \alpha_\theta$, which, again by Remark 2, equals $\alpha_{j_0} + \alpha_{j_1} + \cdots + \alpha_{j_\ell}$, as $s + 1 - p \leq j_0 < j_\ell \leq \min(s, p^d - p) = \theta$.

(iii) For $1 \leq u \leq \ell$, as $j_\ell - j_u \leq j_\ell - j_0 \leq p-1$, by Remark 1, there exists a component of v which is equal to $\alpha_{j_u} + \alpha_{j_{u+1}} + \cdots + \alpha_{j_\ell}$. And we note that there are a total of $j_u - j_{u-1}$ such components of v, viz. $v[i+(j_{u-1}+p)p^{n-d}] = v[i+(j_{u-1}+p+1)p^{n-d}] = \cdots = v[i+(j_u+p-1)p^{n-d}] = \alpha_{j_u} + \alpha_{j_{u+1}} + \cdots + \alpha_{j_\ell} = \begin{cases} 1 & \text{if } \ell - u \text{ is even;} \\ 0 & \text{if } \ell - u \text{ is odd.} \end{cases}$

This is because, when $j_{u-1} + p \leq s \leq j_u + p - 1$, we have $s \geq p$. Therefore by Lemma 1(a), $v[i+sp^{n-d}] = \alpha_{s+1-p} + \alpha_{s+2-p} + \cdots + \alpha_\theta$ with $\theta = \min(s, p^d - p)$. Note that $j_\ell - j_{u-1} \leq j_\ell - j_0 \leq p-1$ for each u. This, together with $j_{u-1} + p \leq s \leq j_u + p - 1$, implies that $j_{u-1} + 1 \leq s + 1 - p \leq j_u < j_\ell \leq j_{u-1} + p - 1 < s$, which gives $s + 1 - p \leq j_u < j_\ell \leq \min(s, p^d - p) = \theta$. Therefore by Remark 2, we have $v[i+sp^{n-d}] = \alpha_{j_u} + \alpha_{j_{u+1}} + \cdots + \alpha_{j_\ell}$.

For ℓ odd, we see, from the above discussion, that the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of v is given by

$$w_i(j_0, j_1, \cdots, j_\ell) = j_1 - j_0 + \sum_{\substack{m=1 \\ m \text{ even}}}^{\ell-1} (j_{m+1} - j_m) + \sum_{\substack{u=1 \\ u \text{ odd}}}^{\ell} (j_u - j_{u-1}) = 2L_o(v; \ell).$$

And for ℓ even, it is clear from the above discussion that the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of v is given by

$$j_1 - j_0 + \sum_{\substack{m=1 \\ m \text{ even}}}^{\ell-1} (j_{m+1} - j_m) + (p - j_\ell + j_0) + \sum_{\substack{u=1 \\ u \text{ even}}}^{\ell} (j_u - j_{u-1}) = p.$$

This proves the proposition. □

Let us now consider the case $L(v) \geq p$. Here we must have $\ell \geq 2$, and the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of a nice vector v of the type $(j_0, j_1, \cdots, j_\ell)$ is given by the following proposition:

Proposition 4 *Let $\ell \geq 2$ be an integer. Let v be a nice vector of the type $(j_0, j_1, \cdots, j_\ell)$ with $L(v) = j_\ell - j_0 \geq p$. Then the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of v satisfies the following recurrence relation:*

$$w_i(j_0, j_1, \cdots, j_\ell) = w_i(j_0, j_1, \cdots, j_{\ell-1}) + w_i(j_1, j_2, \cdots, j_\ell) - w_i(j_1, j_2, \cdots, j_{\ell-1}),$$

where $w_i(j_0, j_1, \cdots, j_{\ell-1})$, $w_i(j_1, j_2, \cdots, j_\ell)$ and $w_i(j_1, j_2, \cdots, j_{\ell-1})$ denote the weights of nice vectors in V_i of the type $(j_0, j_1, \cdots, j_{\ell-1})$, $(j_1, j_2, \cdots, j_\ell)$ and $(j_1, j_2, \cdots, j_{\ell-1})$ respectively and can be calculated using the recurrence formula and Proposition 3.

Proof. Let v_1, v_2 and v_3 be nice vectors of the type $(j_0, j_1, \cdots, j_{\ell-1})$, $(j_1, j_2, \cdots, j_\ell)$ and $(j_1, j_2, \cdots, j_{\ell-1})$ respectively.

Since $w(v) = w_i(j_0, j_1, \cdots, j_\ell)$, $w(v_1) = w_i(j_0, j_1, \cdots, j_{\ell-1})$, $w(v_2) = w_i(j_1, j_2, \cdots, j_\ell)$ and $w(v_3) = w_i(j_1, j_2, \cdots, j_{\ell-1})$, so to prove the proposition, it is enough to prove that $w(v) = w(v_1) + w(v_2) - w(v_3)$.

For this, we assert the following:

(i) $v = v_1 + v_2 + v_3$. As a consequence, we have $v[k] = v_1[k] + v_2[k] + v_3[k]$ for $1 \leq k \leq p^n$.

(ii) For $0 \leq s \leq j_\ell - 1$, we have $v[i + sp^{n-d}] = v_1[i + sp^{n-d}]$ and $v_2[i + sp^{n-d}] = v_3[i + sp^{n-d}]$.

(iii) For $j_\ell \leq s \leq p^d - 1$, we have $v[i + sp^{n-d}] = v_2[i + sp^{n-d}]$ and $v_1[i + sp^{n-d}] = v_3[i + sp^{n-d}]$.

On writing $v = \alpha_{j_0} R_{i+j_0 p^{n-d}} + \alpha_{j_1} R_{i+j_1 p^{n-d}} + \cdots + \alpha_{j_\ell} R_{i+j_\ell p^{n-d}}$, $v_1 = \alpha_{j_0} R_{i+j_0 p^{n-d}} + \alpha_{j_1} R_{i+j_1 p^{n-d}} + \cdots + \alpha_{j_{\ell-1}} R_{i+j_{\ell-1} p^{n-d}}$, $v_2 = \alpha_{j_1} R_{i+j_1 p^{n-d}} + \alpha_{j_2} R_{i+j_2 p^{n-d}} + \cdots + \alpha_{j_\ell} R_{i+j_\ell p^{n-d}}$, $v_3 = \alpha_{j_1} R_{i+j_1 p^{n-d}} + \alpha_{j_2} R_{i+j_2 p^{n-d}} + \cdots + \alpha_{j_{\ell-1}} R_{i+j_{\ell-1} p^{n-d}}$, the assertion (i) follows.

Let $0 \leq s \leq j_\ell - 1$. Note that the vector v_1 can be obtained from v by putting $\alpha_{j_\ell} = 0$. Therefore the component of v which does not contain the scalar α_{j_ℓ} as its summand, must be equal to the same corresponding component of v_1. By Lemma 1 and Remark 2, we see that for $0 \leq s \leq j_\ell - 1$, the $(i + sp^{n-d})$th component of v does not involve the scalar α_{j_ℓ} as its summand. Therefore we must have $v[i + sp^{n-d}] = v_1[i + sp^{n-d}]$ for $0 \leq s \leq j_\ell - 1$. From assertion (i), we get $v_2[i + sp^{n-d}] = v_3[i + sp^{n-d}]$. This proves assertion (ii).

Let $j_\ell \leq s \leq p^d - 1$. Since the vector v_2 can be obtained from v by putting $\alpha_{j_0} = 0$, so the component of v which does not involve the scalar α_{j_0} as a summand, must be equal to the same corresponding component of v_2. By Lemma 1(a), note that for $s \geq j_\ell$, the $(i + sp^{n-d})$th component of v contains α_{j_ℓ} as its summand. Since $j_\ell - j_0 \geq p$, so by Remark 1, the $(i + sp^{n-d})$th component of v for all $s \geq j_\ell$, does not contain α_{j_0} as its summand. This gives $v[i + sp^{n-d}] = v_2[i + sp^{n-d}]$ for $s \geq j_\ell$. And $v_1[i+sp^{n-d}] = v_3[i+sp^{n-d}]$ follows from assertion (i). This proves assertion (iii).

Now consider

$$\begin{aligned} w(v) &= |\{s : 0 \leq s \leq p^d - 1, v[i + sp^{n-d}] = 1\}| \\ &= |\{s : 0 \leq s \leq j_\ell - 1, v[i + sp^{n-d}] = 1\}| \\ &\quad +|\{s : j_\ell \leq s \leq p^d - 1, v[i + sp^{n-d}] = 1\}| \end{aligned}$$

(Here $|A|$ denotes cardinality of the set A.)

From the assertions (ii) and (iii), we have $v[i + sp^{n-d}] = v_1[i + sp^{n-d}]$ for $0 \leq s \leq j_\ell - 1$, and $v[i + sp^{n-d}] = v_2[i + sp^{n-d}]$ for $j_\ell \leq s \leq p^d - 1$. This gives

$$\begin{aligned} w(v) &= |\{s : 0 \leq s \leq j_\ell - 1, v_1[i + sp^{n-d}] = 1\}| \\ &\quad +|\{s : j_\ell \leq s \leq p^d - 1, v_2[i + sp^{n-d}] = 1\}| \\ &= w(v_1) - |\{s : j_\ell \leq s \leq p^d - 1, v_1[i + sp^{n-d}] = 1\}| + \\ &\quad +w(v_2) - |\{s : 0 \leq s \leq j_\ell - 1, v_2[i + sp^{n-d}] = 1\}|. \end{aligned}$$

Again using assertions (ii) and (iii), we have $v_2[i+sp^{n-d}] = v_3[i+sp^{n-d}]$ for $0 \leq s \leq j_\ell - 1$, and for $j_\ell \leq s \leq p^d - 1$, we have $v_1[i+sp^{n-d}] = v_3[i+sp^{n-d}]$. This gives

$$\begin{aligned} w(v) &= w(v_1) + w(v_2) - |\{s : 0 \leq s \leq p^d - 1, v_3[i + sp^{n-d}] = 1\}| \\ &= w(v_1) + w(v_2) - w(v_3). \end{aligned}$$

This completes the proof of the proposition. □

Remark 4 *From Propositions 3 & 4, we note that the weight $w_i(j_0, j_1, \cdots, j_\ell)$ of a nice vector is independent of i. So we drop the subscript i from now onwards.*

2.2 Proof of Theorem 1

To prove Theorem 1, we need to prove the following results:

Lemma 5 *Let ν and $\ell \leq p^d - p$ be non-negative integers. Let $n_i(\nu;\ell)$ denote the number of nice vectors in V_i having weight ν and size ℓ. Then*

$$n_i(\nu;\ell) = \sum_{\substack{(j_0,j_1,\cdots,j_\ell) \\ w(j_0,j_1,\cdots,j_\ell)=\nu}} 1,$$

where the summation runs over all $(\ell+1)$-tuples $(j_0, j_1, \cdots, j_\ell)$ satisfying $0 \leq j_0 < j_1 < \cdots < j_\ell \leq p^d - p$, $j_u - j_{u-1} \leq p-1$ for $1 \leq u \leq \ell$, and $w(j_0, j_1, \cdots, j_\ell) = \nu$, (note that $w(j_0, j_1, \cdots, j_\ell)$ is obtained in Subsection 2.1).

By Remark 5, as the value of $w(j_0, j_1, \cdots, j_\ell)$ is independent of i, the value of $n_i(\nu;\ell)$ is also independent of i. So we drop the subscript i from now onwards.

Clearly $n(\nu;\ell) = 0$ if there does not exist any nice vector of weight ν and size ℓ.

Proof. Proof is trivial. □

The following algorithm computes the number $n(\nu;\ell)$ $(\nu \geq 0)$ for a fixed ℓ, $0 \leq \ell \leq p^d - p$:

An algorithm to compute the number $n(\nu;\ell)$

Step I: List all $(\ell+1)$-tuples $(j_0, j_1, \cdots, j_\ell)$ satisfying $0 \leq j_0 < j_1 < \cdots < j_\ell \leq p^d - p$ and $j_u - j_{u-1} \leq p-1$ for $1 \leq u \leq \ell$.

Step II: Compute the weights $w(j_0, j_1, \cdots, j_\ell)$ for each $(\ell+1)$-tuple listed in Step I, using Propositions 3 and 4.

Step III: Count the number of tuples $(j_0, j_1, \cdots, j_\ell)$ for which $w(j_0, j_1, \cdots, j_\ell)$ $= \nu$. This number equals $n(\nu;\ell)$.

Remark 5 *For a fixed ℓ $(0 \leq \ell \leq p^d - p)$, it is manually hard to list all $(\ell+1)$-tuples $(j_0, j_1, \cdots, j_\ell)$ satisfying $0 \leq j_0 < j_1 < \cdots < j_\ell \leq p^d - p$ and*

$j_u - j_{u-1} \le p-1$ for $1 \le u \le \ell - 1$, and compute the corresponding weights $w(j_0, j_1, \cdots, j_\ell)$ using Propositions 3 and 4. However, for small values of p and d, a simple computer program in Maple or Magma effectively lists all such $(\ell+1)$-tuples and computes the weights of all the nice vectors of length ℓ, and hence counts the numbers $n(\nu;\ell)$ of nice vectors having weight ν and size ℓ.

Proposition 5 *Let $1 \le i \le p^{n-d}$ be fixed. For any $\nu \ge 0$ and $(\nu_1, \nu_2, \cdots, \nu_t)$ in $P_t(\nu)$, let*

$$V_i(\nu_1, \nu_2, \cdots, \nu_t) = \left\{ \sum_{r=1}^{t} v_r \; : \; \begin{array}{l} v_r (1 \le r \le t) \text{ is a nice vector in } V_i \\ \text{having weight } \nu_r \text{ and each } v_r (2 \le \\ r \le t) \text{ is a right neighbour of } v_{r-1} \end{array} \right\}.$$

Then $\bigcup\limits_{t\ge 1} \bigcup\limits_{(\nu_1,\nu_2,\cdots,\nu_t)\in P_t(\nu)} V_i(\nu_1, \nu_2, \cdots, \nu_t)$ is the set of all vectors in V_i having weight ν. Moreover, this union is disjoint.

Proof. Let S_ν be the set of all vectors in V_i having weight ν. We assert that

$$S_\nu = \bigcup_{t\ge 1} \bigcup_{(\nu_1,\nu_2,\cdots,\nu_t)\in P_t(\nu)} V_i(\nu_1, \nu_2, \cdots, \nu_t). \tag{3}$$

Let $v \in S_\nu$, i.e., v is a vector in V_i having weight ν. Then by Remark 3, each $v \in V_i$ can be written as a sum of nice vectors v_r's such that each v_r is a right neighbour of v_{r-1} so that $v = v_1 + v_2 + \cdots + v_m$ for some integer $m \ge 1$. Let $w(v_r) = \nu_r$ for $1 \le r \le m$. Also by Lemma 4, we have $w(v) = w(v_1) + w(v_2) + \cdots + w(v_m) = \nu_1 + \nu_2 + \cdots + \nu_m$. This gives $(\nu_1, \nu_2, \cdots, \nu_m) \in P_m(\nu)$ and consequently, $v \in V_i(\nu_1, \nu_2, \cdots, \nu_m)$. Therefore we get

$$S_\nu \subseteq \bigcup_{t\ge 1} \bigcup_{(\nu_1,\nu_2,\cdots,\nu_t)\in P_t(\nu)} V_i(\nu_1, \nu_2, \cdots, \nu_t). \tag{4}$$

On the other hand, let $t \ge 1$ and $(\nu_1, \nu_2, \cdots, \nu_t) \in P_t(\nu)$. Let $v \in V_i(\nu_1, \nu_2, \cdots, \nu_t)$. Then $v = v_1 + v_2 + \cdots + v_t$, where each v_r $(1 \le r \le t)$ is a nice vector in V_i such that $w(v_r) = \nu_r$ and each v_r $(2 \leq r \leq t)$ is a right neighbour of v_{r-1}. By Lemma 4, we have $w(v) = w(v_1)+w(v_2)+\cdots+w(v_t)$, which gives $\nu = \nu_1 + \nu_2 + \cdots + \nu_t$. This shows that $v \in S_\nu$. Thus

$$\bigcup_{t\geq 1} \bigcup_{(\nu_1,\nu_2,\cdots,\nu_t)\in P_t(\nu)} V_i(\nu_1,\nu_2,\cdots,\nu_t) \subseteq S_\nu. \tag{5}$$

On combining (4) and (5), we get (3). Further it is easy to see that the union on the right hand side of (3) is disjoint, which completes the proof. □

Proposition 6 *Let $1 \leq i \leq p^{n-d}$ be fixed. Let $(\nu_1,\nu_2,\cdots,\nu_t) \in P_t(\nu)$ and $(\ell_1,\ell_2,\cdots,\ell_t) \in L(\nu_1,\nu_2,\cdots,\nu_t)$. Let*

$$V_i(\nu_1,\nu_2,\cdots,\nu_t;\ell_1,\ell_2,\cdots,\ell_t) = \left\{ \sum_{r=1}^{t} v_r : \begin{array}{l} v_r\ (1 \leq r \leq t) \textit{ is a nice vector} \\ \textit{in } V_i \text{ of size } \ell_r \textit{ and weight} \\ \nu_r, \textit{ and each } v_r\ (2 \leq r \leq t) \textit{ is} \\ \textit{a right neighbour of } v_{r-1}. \end{array} \right\}$$

Then

$$(i) \quad \bigcup_{(\ell_1,\ell_2,\cdots,\ell_t)\in L(\nu_1,\nu_2,\cdots,\nu_t)} V_i(\nu_1,\nu_2,\cdots,\nu_t;\ell_1,\ell_2,\cdots,\ell_t) = V_i(\nu_1,\nu_2,\cdots,\nu_t). \tag{6}$$

Moreover this union is disjoint.
(ii) $|V_i(\nu_1,\nu_2,\cdots,\nu_t;\ell_1,\ell_2,\cdots,\ell_t)|$ equals $a(\ell_1,\ell_2,\cdots,\ell_t)\prod_{r=1}^{t} n(\nu_r;\ell_r)$, where the numbers $n(\nu_r;\ell_r)$'s are as given by Lemma 9.

Proof. (i) It is clear that $V_i(\nu_1,\nu_2,\cdots,\nu_t;\ell_1,\ell_2,\cdots,\ell_t) \subseteq V_i(\nu_1,\nu_2,\cdots,\nu_t)$ for any $(\ell_1,\ell_2,\cdots,\ell_t) \in L(\nu_1,\nu_2,\cdots,\nu_t)$. Therefore

$$\bigcup_{(\ell_1,\ell_2,\cdots,\ell_t)\in L(\nu_1,\nu_2,\cdots,\nu_t)} V_i(\nu_1,\nu_2,\cdots,\nu_t;\ell_1,\ell_2,\cdots,\ell_t) \subseteq V_i(\nu_1,\nu_2,\cdots,\nu_t). \tag{7}$$

Conversely, let $v \in V_i(\nu_1,\nu_2,\cdots,\nu_t)$. Then $v = v_1 + v_2 + \cdots + v_t$, where each v_r $(1 \leq r \leq t)$ is a nice vector in V_i of weight ν_r, and each

v_r $(2 \le r \le t)$ is a right neighbour of v_{r-1}. Let ℓ_r be the size of v_r for $1 \le r \le t$. By Lemma 3, we have $L(v_r) \ge \ell_r$ and $E(v_r) = I(v_r) + L(v_r)$ for $1 \le r \le t$. This gives

$$\begin{aligned}
\sum_{r=1}^{t} \ell_r \le \sum_{r=1}^{t} L(v_r) &= \sum_{r=1}^{t} (E(v_r) - I(v_r)) \\
&= \sum_{r=2}^{t} (E(v_{r-1}) - I(v_r)) + E(v_t) - I(v_1) \\
&\le \sum_{r=2}^{t} (E(v_{r-1}) - I(v_r)) + E(v_t) \quad (\because I(v_1) \ge 0) \\
&\le -p(t-1) + E(v_t) \\
&\qquad (\because I(v_r) - E(v_{r-1}) \ge p \ (2 \le r \le t)) \\
&\le -p(t-1) + p^d - p = p^d - pt \ \text{(by Lemma 3 (ii))}.
\end{aligned}$$

This shows that $(\ell_1, \ell_2, \cdots, \ell_t) \in L(\nu_1, \nu_2, \cdots, \nu_t)$, and hence $v \in V_i(\nu_1, \nu_2, \cdots, \nu_t; \ell_1, \ell_2, \cdots, \ell_t)$, which gives

$$V_i(\nu_1, \nu_2, \cdots, \nu_t) \subseteq \bigcup_{(\ell_1, \ell_2, \cdots, \ell_t) \in L(\nu_1, \nu_2, \cdots, \nu_t)} V_i(\nu_1, \nu_2, \cdots, \nu_t; \ell_1, \ell_2, \cdots, \ell_t). \tag{8}$$

On combining (7) and (8), we get (6). Also it can be easily seen that the union on the right hand side of (6) is disjoint, which completes the proof of part (i).

(ii) We have $v \in V_i(\nu_1, \nu_2, \cdots, \nu_t; \ell_1, \ell_2, \cdots, \ell_t)$ if and only if $v = v_1 + v_2 + \cdots + v_t$, where each v_r $(1 \le r \le t)$ is a nice vector in V_i of size ℓ_r and weight ν_r, and each v_r $(2 \le r \le t)$ is a right neighbour of v_{r-1}. par By Lemma 9, the number of nice vectors having weight ν_r and size ℓ_r is $n(\nu_r; \ell_r)$ for each r, $1 \le r \le t$. Thus the number of vectors in $V_i(\nu_1, \nu_2, \cdots, \nu_t; \ell_1, \ell_2, \cdots, \ell_t)$ is equal to $n(\nu_1; \ell_1) n(\nu_2; \ell_2) \cdots n(\nu_t; \ell_t)$ times the total number of choices for the initial points of the nice vectors $v_1, v_2, \cdots, v_r \in V_i$ having sizes $\ell_1, \ell_2, \cdots, \ell_r$ and weights $\nu_1, \nu_2, \cdots, \nu_r$ respectively, such that each v_r is a right neighbour of v_{r-1}. Note that the number of choices for initial points of such nice vectors v_r's depends only upon the sizes $\ell_1, \ell_2, \cdots, \ell_r$ and is independent of their weights ν_r's. Now to calculate the number, let $I(v_r) = j_r$ for $1 \leq r \leq t$. Then by Lemma 3, we have $j_1 \geq 0$, $E(v_r) = I(v_r) + L(v_r)$ $(1 \leq r \leq t)$, $j_{r-1} + \ell_{r-1} + p \leq j_r$ for each r, $2 \leq r \leq t$ and $j_t + \ell_t \leq p^d - p$, which gives

$$\begin{aligned}
&0 \leq j_1 \leq p^d - \sum_{r=1}^{t} \ell_r - pt, \\
&j_1 + \ell_1 + p \leq j_2 \leq p^d - \sum_{r=2}^{t} \ell_r - p(t-1), \\
&j_2 + \ell_2 + p \leq j_3 \leq p^d - \sum_{r=3}^{t} \ell_r - p(t-2), \\
&\cdots\cdots\cdots\cdots\cdots \\
&j_{t-1} + \ell_{t-1} + p \leq j_t \leq p^d - \ell_t - p.
\end{aligned}$$

Therefore the total number of choices for the initial points j_r's of the nice vectors v_r's of size ℓ_r such that each v_r is a right neighbour of v_{r-1}, is given by the sum

$$\sum_{m_1=0}^{p^d - \sum_{i=1}^{t} \ell_i - pt} \quad \sum_{m_2=m_1+\ell_1+p}^{p^d - \sum_{i=2}^{t} \ell_i - p(t-1)} \cdots \sum_{m_t=m_{t-1}+\ell_{t-1}+p}^{p^d - \ell_t - p} 1,$$

which, by (1), is equal to $a(\ell_1, \ell_2, \cdots, \ell_t)$.

Consequently, the total number of vectors in $V_i(\nu_1, \nu_2, \cdots, \nu_t; \ell_1, \ell_2, \cdots, \ell_t)$ is given by

$$a(\ell_1, \ell_2, \cdots, \ell_t) n(\nu_1; \ell_1) n(\nu_2; \ell_2) \cdots n(\nu_t; \ell_t),$$

which proves (ii). □

Proof of Proposition 2. Proposition 2 follows from Propositions 5 & 6. □

Proof of Theorem 1. Theorem 1 follows from Propositions 1 & 2. □

3 The weight distribution of $< g_1(x)g_2(x) >$

To compute the weight distribution of $C_2 =< g_1(x)g_2(x) >$, we observe the following:

Lemma 6 *Let C and $\mathcal{D}$ be cyclic codes of length m and ℓ generated by the polynomials $g(x)$ and $h(x)$ respectively. If $g(x) = h(x)(1 + x^{\ell} + x^{2\ell} + \cdots + x^{\ell(k-1)})$, then*
(a) C is a repetition code of $\mathcal{D}$, repeated k times.
(b) the weight distribution $A_0^{(m)}, A_1^{(m)}, \cdots, A_m^{(m)}$ of C and the weight distribution $B_0^{(\ell)}, B_1^{(\ell)}, \cdots, B_\ell^{(\ell)}$ of $\mathcal{D}$ are related by

$$A_w^{(m)} = \begin{cases} 0 & if k \nmid w; \\ B_{w'}^{(\ell)} & if w = kw',\ 0 \leq w' \leq \ell \end{cases}$$

for $0 \leq w \leq m$.

Proof. Proof is trivial.

Theorem 2 *Let p be an odd prime and $n \geq 1$ be an integer. Let $g_1(x) = 1 + x^{p^{n-d}} + x^{2p^{n-d}} + \cdots + x^{(p-1)p^{n-d}}$ and $g_2(x) = 1 + x^{p^{n-d+1}} + x^{2p^{n-d+1}} + \cdots + x^{(p^{d-1}-1)p^{n-d+1}}$, where d is an integer satisfying $1 \leq d \leq n$. The code C_2 generated by $g_1(x)g_2(x)$ of length p^n is the repetition code of the code $C_1 =< g_1(x) >$ of length p^{n-d+1}, repeated p^{d-1} times. Hence the weight distribution $B_0^{(p^n)}, B_1^{(p^n)}, \cdots, B_{p^n}^{(p^n)}$ of C_2 is given by*

$$B_w^{(p^n)} = \begin{cases} 0 & if p^{d-1} \nmid w; \\ A_{w'}^{(p^{n-d+1})} & if w = p^{d-1}w',\ 0 \leq w' \leq p^{n-d+1} \end{cases}$$

for $0 \leq w \leq p^n$, where the numbers $A_{w'}^{(p^{n-d+1})}$'s can be computed from Theorem 1 on replacing n by $n - d + 1$.

Proof. Proof follows from Lemma 10.

Acknowledgements

The authors are grateful to the anonymous referee for his comments and suggestions which helped us to write the paper in the present form.

References

[1] Y. Aubry & P. Langevin, "On the weights of binary irreducible cyclic codes", Proc. Workshop on Coding and Cryptography, Bergen, Norway, pp. 161169, 2005.

[2] D. Augot, "Description of minimum weight codewords of cyclic codes by algebraic systems", *Finite Fields Appl.* 2, no. 2, 138-152, 1996.

[3] L. D. Baumert & R. J. McEliece, "Weights of irreducible cyclic codes", *Information and Control* 20, pp. 158-175, 1972.

[4] C. Ding, "The weight distributions of some irreducible cyclic codes", *IEEE Trans. Inform. Theory* 55, no. 3, pp. 955-960, 2009.

[5] K. Feng & J. Luo, "Weight distributions of some reducible cyclic codes", *Finite Fields Appl.* 14, Issue 2, pp. 390-409, April 2008.

[6] R. W. Fitzgerald & J. L. Yucas, "Sums of Gauss sums and weights of irreducible codes", *Finite Fields Appl.* 11, no. 1, 89–110, 2005.

[7] J. Luo & K. Feng, "On the weight distributions of two classes of cyclic codes", *IEEE Trans. Inform Theory* 54, Issue 12, pp. 5332-5344, Dec. 2008.

[8] F. J. MacWilliams & J. Seery, "The weight distributions of some minimal cyclic codes", *IEEE Trans. Inform. Theory* 27, no. 6, pp. 796-806, 1981.

[9] M. J. Moisio & K. O. V *äänänen*, "Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes", *IEEE Trans. Inform. Theory* 45, no. 4, 1244-1249, 1999.

[10] R. Segal & R. L. Ward, "Weight distributions of some irreducible cyclic codes", *Math. Comp.* 46, no. 173, pp. 341-354, 1986.

[11] A. Sharma & G. K. Bakshi, "The weight distributions of some irreducible cyclic codes", *Finite Fields Appl.*, doi:10.1016/j.ffa.2011.07.002, 2011.

[12] A. Sharma, G. K. Bakshi & M. Raka, "The weight distributions of irreducible cyclic codes of length 2^m", *Finite Fields Appl.* 13, no. 4, pp. 1086-1095, 2007.

[13] M. van der Vlugt, "Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes", *J. Number Theory* 55, no. 2, pp. 145-159, 1995.

[14] B. Wang, C. Tang, Y. Qi, Y. Yang & M. Xu, "The Weight Distributions of Cyclic Codes and Elliptic Curves", arXiv:1109.0628v1.

[15] J. P. Zanotti, "Weight behavior of irreducible cyclic BWD-codes", *Finite Fields Appl.* 2, no. 2, pp. 192-203, 1996.

[16] X. Zeng, L. Hu, W. Jiang, Q. Yue & X. Cao, "The weight distributions of a class of *p*-ary cyclic codes", *Finite Fields Appl.* 16, Issue 1, pp. 56-73, January 2010.

[17] X. Zeng, J. Shan & L. Hu, "A triple-error-correcting cyclic code from the Gold and Kasami-Welch APN power functions", *Finite Fields Appl.*, doi:10.1016/j.ffa.2011.06.005, 2011.