J. Algebra Comb. Discrete Appl.
2(2) • 75-84
Received: 29 October 2014; Accepted: 2 February 2015
DOI 10.13069/jacodesmath.17537

Journal of Algebra Combinatorics Discrete Structures and Applications

On a class of repeated-root monomial-like abelian codes

Research Article

Edgar Martínez-Moro[1*], **Hakan Özadam**[2,3**], **Ferruh Özbudak**[2§], **Steve Szabo**[3***]

1. Institute of Mathematics and Applied Mathematics Department University of Valladolid, Castilla, Spain

2. Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University İnönü Bulvarı, 06531, Ankara, Turkey

3. University of Massachusetts, Medical School Worcester, Massachusetts

4. Department of Mathematics and Statistics, Eastern Kentucky University Richmond, KY, USA

Abstract: In this paper we study polycyclic codes of length $p^{s_1} \times \cdots \times p^{s_n}$ over $\mathbb{F}_{p^a}$ generated by a single monomial. These codes form a special class of abelian codes. We show that these codes arise from the product of certain single variable codes and we determine their minimum Hamming distance. Finally we extend the results of Massey et. al. in [10] on the weight retaining property of monomials in one variable to the weight retaining property of monomials in several variables.

2010 MSC: 94B15,11T71,11T55

Keywords: Repeated-root Cyclic code, Abelian code, Weight-retaining property

1. Introduction

Cyclic codes are said to be repeated-root when the codeword length and the characteristic of the alphabet are not coprime. Despite that it has been proved that in general they are asymptotically bad in some cases repeated-root cyclic codes are optimal and they have interesting properties. Massey et. al. have shown in [10] that cyclic codes of length p over a finite field of characteristic p are optimal. There also exist infinite families of repeated-root cyclic codes in even characteristic according to the results of [14]. Also in [10] it has been pointed out that some repeated-root cyclic codes can be decoded using a very simple circuitry. Among other studies on repeated-root cyclic codes with several different settings are [1, 2, 7, 8, 11, 12, 14].

[*] *E-mail: edgar@maf.uva.es*
[**] *E-mail: ozhakan@metu.edu.tr*
[§] *E-mail: ozbudak@metu.edu.tr*
[***] *E-mail: steve.szabo@eku.edu*

Contrary to the simple-root case, there are repeated root cyclic codes of the form $\big(f(x)^i\big)$ where $i > 1$. Specifically, all cyclic codes of length p^s over a finite field of characteristic p are generated by a single "monomial" of the form $(x-1)^i$, where $0 \leq i \leq p^s$ (see [2, 11]). In this paper, as a generalisation of these codes to several variables, we study cyclic codes of the form

$$\mathcal{I}_{(i_1,\dots i_n)} = \big((x_1-1)^{i_1}\cdots(x_n-1)^{i_n}\big) \subset \mathcal{R} = \frac{\mathbb{F}_{p^a}[x_1,\dots,x_n]}{\Big(x_1^{p^{s_1}}-1,\dots,x_n^{p^{s_n}}-1\Big)}, \tag{1}$$

i.e. $\mathcal{I}_{(i_1,\dots i_n)}$ is the ideal of $\mathcal{R}$ generated by a single monomial of the form $(x_1-1)^{i_1}\cdots(x_n-1)^{i_n}$.

This paper is organised as follows. First we introduce some notation, give some definitions and prove some structural properties of the ambient space of a particular class of abelian codes in Section 2. In Section 3, we show thatmonomial like codes arise from product codes and we determine their Hamming distance. We describe their duals which yields a parity check matrix for these codes. In Section 4, we explain the relationship of the Hasse derivative with the dual of this type of codes. Finally in Section 5, we generalise the weight retaining property of monomials in single variable to the multivariable case.

2. The Ambient Space

Throughout the paper, we consider the finite ring

$$\mathcal{R} = \frac{\mathbb{F}_{p^a}[x_1,\dots,x_n]}{\Big(x_1^{p^{s_1}}-1,\dots,x_n^{p^{s_n}}-1\Big)} \tag{2}$$

as the ambient space of the codes to be studied unless otherwise stated. It is a well known fact that $\mathcal{R}$ is a local ring with maximal ideal $(x_1-1,\dots,x_n-1)$. We define

$$L = \{(\alpha_1,\alpha_2,\dots,\alpha_n) \mid 0 \leq \alpha_j < p^{s_j}, \quad \alpha_j \in \mathbb{Z} \quad \text{for all} \quad 1 \leq j \leq n\}. \tag{3}$$

The elements of $\mathcal{R}$ can be identified uniquely with the polynomials of the form

$$f(x_1,\dots,x_n) = \sum_{(\alpha_1,\alpha_2,\dots,\alpha_n)\in L} f_{(\alpha_1,\alpha_2,\dots,\alpha_n)} x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}, \tag{4}$$

so throughout the paper, we identify the equivalence class

$$f(x_1,\dots,x_n) + \Big(x_1^{p^{s_1}}-1, x_2^{p^{s_2}}-1,\dots,x_n^{p^{s_n}}-1\Big)$$

with the polynomial $f(x_1,\dots,x_n)$. We shall consider a repeated-root code as just an ideal $\mathcal{C}$ of $\mathcal{R}$. The length of the code is $p^{s_1}\times p^{s_2}\times\cdots\times p^{s_n}$ and the support of a codeword $f(x_1,\dots,x_n)\in\mathcal{C}$ is the set $\operatorname{supp}(f) = \{(\alpha_1,\alpha_2,\dots,\alpha_n)\in L \mid f_{(\alpha_1,\alpha_2,\dots,\alpha_n)} \neq 0\}$. The Hamming weight of $f(x_1,\dots,x_n)$ is defined as $\mathrm{w}(f(x_1,\dots,x_n)) = |\operatorname{supp}(f)|$, i.e. the number of nonzero coefficients of $f(x_1,\dots,x_n)$. The minimum Hamming distance of the code $\mathcal{C}$ is defined as

$$\mathrm{d}(\mathcal{C}) = \min\{\mathrm{w}(f(x_1,\dots,x_n)) \mid f(x_1,\dots,x_n)\in\mathcal{C}\setminus\{0\}\}.$$

3. Monomial-like codes

In this paper we shall study a particular class of the codes over $\mathcal{R}$ called *monomial-like codes* given by an ideal generated by a single monomial of the form

$$\mathcal{C}_{(i_1,\dots,i_n)} = \big((x_1-1)^{i_1}\cdot(x_2-1)^{i_2}\cdots(x_n-1)^{i_n}\big) \subset \mathcal{R}. \tag{5}$$

Note that not all the ideals in $\mathcal{R}$ can be generated by a single monomial of this form.

In one variable case, the minimum Hamming distance of C was computed in [11] and [2]. It turns out that, in multivariate case, $\mathcal{C}_{(i_1,\ldots,i_n)}$ can be considered as a product code of single variable codes. This decomposition allows us to express the minimum Hamming distance of $\mathcal{C}_{(i_1,\ldots,i_n)}$ in terms of the Hamming distances of cyclic codes of length p^{s_j}.

Definition 3.1. *The product of two linear codes C, C' over $\mathbb{F}_{p^a}$ is the linear code $C \otimes C'$ whose codewords are all the two dimensional arrays for which each row is a codeword in C and each column is a codeword in C'.*

The following are some well-known facts about the product codes.

1. If C and C' are $[n, k, d]$ and $[n', k', d']$ codes respectively, then $C \otimes C'$ is a $[nn', kk', dd']$ code.
2. If G and G' are generator matrices of C and C' respectively, then $G \otimes G'$ is a generator matrix of $C \otimes C'$, where $\otimes$ denotes the Kronecker product of matrices and the codewords of $C \otimes C'$ are seen as concatenations of the rows in arrays in $C \otimes C'$.

Theorem 3.2. *Let n_1, n_2 be positive integers and let*

$$\hat{\mathcal{R}} = \frac{\mathbb{F}_{p^a}[x,y]}{(x^{n_1}-1, y^{n_2}-1)}, \mathcal{R}_x = \frac{\mathbb{F}_{p^a}[x]}{(x^{n_1}-1)}, \quad \mathcal{R}_y = \frac{\mathbb{F}_{p^a}[y]}{(y^{n_2}-1)}.$$

Suppose that $(x-1)^{k_1} | x^{n_1}-1$ and $(y-1)^{k_2} | y^{n_2}-1$. The code

$$C = \left((x-1)^{k_1} \cdot (y-1)^{k_2}\right) \subset \hat{\mathcal{R}}$$

is the product of the codes $C_x = \left((x-1)^{k_1}\right) \subset \mathcal{R}_x$ and $C_y = \left((y-1)^{k_2}\right) \subset \mathcal{R}_y$, i.e., $C = C_x \otimes C_y$.

Proof. Let

$$g(x) = (x-1)^{k_1} = g_{k_1}x^{k_1} + \cdots + g_1 x + g_0, \; h(y) = (y-1)^{k_2} = h_{k_2}y^{k_2} + \cdots + h_1 y + h_0.$$

Then

$$G_x = \begin{bmatrix} 0 & \ldots & 0 & 0 & g_{k_1} & \ldots & g_1 & g_0 \\ 0 & \ldots & 0 & g_{k_1} & \ldots & g_1 & g_0 & 0 \\ \vdots & & & & & & & \vdots \\ g_{k_1} & \ldots & g_1 & g_0 & 0 & \ldots & 0 & 0 \end{bmatrix}, G_y = \begin{bmatrix} 0 & \ldots & 0 & 0 & h_{k_2} & \ldots & h_1 & h_0 \\ 0 & \ldots & 0 & h_{k_2} & \ldots & h_1 & h_0 & 0 \\ \vdots & & & & & & & \vdots \\ h_{k_2} & \ldots & h_1 & h_0 & 0 & \ldots & 0 & 0 \end{bmatrix}$$

are two generator matrices for C_x and C_y, respectively.

We identify the polynomial $f(x,y) = \sum_{0 \le i < n_1, 0 \le j < n_2} c_{ij} x^i y^j \in \mathbb{F}_{p^a}[x,y]$, with the codeword

$$(c_{n_1-1,n_2-2}, \ldots, c_{n_1-1,1}, c_{n_1-1,0}, \ldots, c_{1,n_2-1}, \ldots, c_{1,1}, c_{1,0}, c_{0,n_2-1}, \ldots, c_{0,1}, c_{0,0}).$$

The elements of $C = \left((x-1)^{k_1}(y-1)^{k_2}\right) \subset \hat{\mathcal{R}}$ are exactly all the $\mathbb{F}_{p^a}$-linear combinations of the elements of the set

$$\beta = \{x^i y^j (x-1)^{k_1}(y-1)^{k_2} : \quad 0 \le i < n - k_1, \quad 0 \le j < n - k_2\}$$

Now we consider $G = G_x \otimes G_y$. Using the above identification for the rows of G, we obtain a basis for $C_x \otimes C_y$ which is equal to β. Thus $C = C_x \otimes C_y$. □

Corollary 3.3. *Let $r_1, \dots, r_n, i_1, \dots, i_n$ be positive integers and let*

$$\mathcal{R}' = \frac{\mathbb{F}_{p^a}[x_1, \dots, x_n]}{(x_1^{r_1} - 1, \dots, x_n^{r_n} - 1)}, \quad \mathcal{R}_{x_j} = \frac{\mathbb{F}_{p^a}[x_j]}{(x_j^{r_j} - 1)}.$$

Suppose that $(x_j - 1)^{i_j} | x_j^{r_j} - 1$ for all $1 \leq j \leq n$. The code

$$\mathcal{C}_{(i_1,\dots,i_n)} = \left((x_1 - 1)^{i_1} \cdots (x_r - 1)^{i_r}\right)$$

is the product of the codes $C_{x_j} = \left((x_j - 1)^{i_j}\right) \subset \mathcal{R}_{x_j}$, i.e.,

$$\mathcal{C}_{(i_1,\dots,i_n)} = (\cdots((C_{x_1} \otimes C_{x_2}) \otimes C_{x_3}) \otimes \cdots) \otimes C_{x_n} = \bigotimes_{i=1}^{n} C_{x_i}. \tag{6}$$

Remark 3.4.

1. *Note that the tensor product is associative in the sense that there is a natural isomorphism $(C \otimes C') \otimes C'' \cong C \otimes (C' \otimes C'')$. Thus we can remove all the parenthesis in Equation 6.*
2. *The reader can identify in Theorem and Corollary 3.3 as a polynomial version of the the fact that for G a finite p-group such that $G = G_1 \times G_2 \times \cdots \times G_n$ and $\mathbb{K}$ a field then $\mathbb{K}G \cong \mathbb{K}G_1 \otimes \mathbb{K}G_2 \otimes \cdots \otimes \mathbb{K}G_n$ where $g = g_1 g_2 \dots g_n$ is mapped to $g_1 \otimes g_2 \otimes \cdots \otimes g_n$.*

The previous construction give us a straightforward result for the minimum distance of our codes as follows.

Corollary 3.5. *Let $\mathcal{C}_{(i_1,\dots,i_n)} \subset \mathcal{R}$ then*

$$\mathrm{d}(\mathcal{C}_{(i_1,\dots,i_n)}) = \prod_{j=1}^{n} \mathrm{d}(\mathcal{C}_{(i_j)}), \tag{7}$$

where $\mathrm{d}(\mathcal{C}_{(i_j)})$ is the minimum distance of the code $(x_i^{i_j} - 1)$ in $\mathbb{F}_{p^a}[x]/(x_i^{i_j} - 1)$.

Note that $\mathrm{d}(\mathcal{C}_{(i_j)})$ is explicitly given in [2, Theorem 6.4] and [11, Theorem 1] in terms of p, a and i_j.

3.1. Weight hierarchy of some two-variable cases

In some very special two-variable cases we can go slightly further and compute explicitly the whole weight hierarchy of the code. The r-th generalised Hamming weight $\mathrm{d}_r(\mathcal{C})$, $1 \leq r \leq k$, of a $\mathbb{F}_p$-linear code $\mathcal{C}$ of dimension k is defined as the minimum of the cardinalities of the supports of all the subcodes (linear subspaces) of dimension r of $\mathcal{C}$. We will define $\mathrm{d}_0(\mathcal{C}) = 0$. The sequence $\{\mathrm{d}_r(\mathcal{C})\}_{r=0}^{k}$ is called the Hamming weight hierarchy of $\mathcal{C}$.

Let $\mathcal{R}' = \frac{\mathbb{F}_{p^a}[x]}{(x^p - 1)}$ and $\mathcal{C}_{(i_1)} = \left((x-1)^{i_1}\right) \subset \mathcal{R}'$. It was shown in [10, Theorem 5] that $\mathcal{C}_{(i_1)}$ is a Maximum Distance Separable (MDS) code.The weight hierarchy of a MDS code $\mathcal{C}$ is completely determined by its length n and dimension k as $\mathrm{d}_r(\mathcal{C}) = n - k + r$ for $r = 1, 2, \dots, k$, see for example [6, Theorem 7.10.7].

Consider now $\mathcal{C}_{(i_2)} = \left((x_2 - 1)^{i_2}\right) \subset \frac{\mathbb{F}_{p^a}[x_2]}{(x_2^p - 1)}$ and let k_1, k_2 the dimension as $\mathbb{F}_{p^a}$-linear spaces of the codes $\mathcal{C}_{(i_1)}, \mathcal{C}_{(i_2)}$ respectively. Using [13, Theorem 1] and since $\mathcal{C}_{(i_1)} \otimes \mathcal{C}_{(i_2)} = \mathcal{C}_{(i_1,i_2)}$ we get

$$\begin{aligned}
&d_r(\mathcal{C}_{(i_1,i_2)}) \\
= \ & \min\{\sum_{i=1}^{s}(d_i(\mathcal{C}_{(i_1)}) - d_{i-1}(\mathcal{C}_{(i_1)}))d_{t_i}(\mathcal{C}_{(i_2)}), 1 \leq t_s \leq \cdots \leq t_1 \leq k_2, s \leq k_1, \sum_{i=1}^{s} t_i = r\} \\
= \ & \min\{d_1(\mathcal{C}_{(i_1)})(i_2 + t_1) + \sum_{i=2}^{s}(i_2 + t_i), 1 \leq t_s \leq \cdots \leq t_1 \leq k_2, s \leq k_1, \sum_{i=1}^{s} t_i = r\} \\
= \ & \min\{(d_1(\mathcal{C}_{(i_1)}) - 1)(i_2 + t_1) + r + si_2, 1 \leq t_s \leq \cdots \leq t_1 \leq k_2, s \leq k_1, \sum_{i=1}^{s} t_i = r\}.
\end{aligned}$$

Since $d_1(C_1) = i_1 + 1$ and the minimum value of t_1, subject to $1 \leq t_s \leq \cdots \leq t_1 \leq k_2$ and $\sum_{i=1}^{s} t_i = r$, is $\lceil \frac{r}{s} \rceil$, we obtain

$$d_r(C_{(i_1,i_2)}) = \min\{i_1(i_2 + \left\lceil \frac{r}{s} \right\rceil) + r + si_2, \quad s \leq k_1\}, \quad r = 1, 2, \ldots, k_1 \cdot k_2. \tag{8}$$

3.2. Dual codes

Note that the elements of the form $\prod_{k=1}^{n}(x_k - 1)^{\mathbf{j}_k}$ with $\mathbf{j} \in \mathbb{N}^n$ form a basis of $\mathbb{F}_{p^a}[x_1, \ldots, x_n]$ and the elements of this form with $\mathbf{j}_k \geq p^{s_k}$ for some k form a basis of $(\{x^{p^{s_k}} - 1\}_{k=1}^{n})$. Let us consider

$$0 \neq f(x_1, \ldots, x_n) = \sum_{\mathbf{j} \in L} c_{\mathbf{j}} \prod_{k=1}^{n}(x_k - 1)^{\mathbf{j}_k}.$$

Therefore $(x_1 - 1)^{i_1} \cdots (x_n - 1)^{i_n} f(x_1, \ldots, x_n) = 0$ in $\mathcal{R}$ if and only if for every $\mathbf{j} \in L$ with $c_{\mathbf{j}} \neq 0$ we have $p^{s_k} \leq \mathbf{j}_k + i_k$ for some k if and only if $f(x_1, \ldots, x_n) \in (\{(x-1)^{p^{s_k} - i_k}\}_{k=1}^{n})$. This proves that the annihilator of $\mathcal{C}_{(i_1,\ldots,i_n)}$ is $(\{(x-1)^{p^{s_k} - i_k}\}_{k=1}^{n})$ and the dual of an ideal of $\mathcal{R}$ is exactly its annihilator. Therefore we have proved the following statement.

Theorem 3.6.

$$C_{(i_1,\ldots,i_n)}^{\perp} = (\{(x-1)^{p^{s_k} - i_k}\}_{k=1}^{n}) \subset \mathcal{R}.$$

Remark 3.7. *Note that the above fact does not hold for arbitrary ideals of algebras of type*

$$\mathbb{F}[x_1, \ldots, x_n]/(\{x_i^{n_i} - 1\}_{i=1}^{n})$$

and it relies on the fact that the $n_i = p^{s_i}$.

Let us construct an $\mathbb{F}_{p^a}$-basis for $C^{\perp}$. This will provide us a generator matrix for $C^{\perp}$ and hence a parity check matrix for C.

Let $T_k = \{(a_1, \ldots, a_n) \in \mathbb{N}^n \mid p^{s_j} - i_j \leq a_j < p^{s_j}$ if $j = k$, $0 \leq a_j < p^{s_j}$ if $j \neq k\}$ and $T = T_1 \cup \cdots \cup T_n$. Let $s = s_1 + s_2 + \cdots + s_n$, it is clear that for $e_1, \ldots, e_r$ pairwise distinct

$$|T_{e_1} \cap \cdots \cap T_{e_r}| = i_{e_1} \cdots i_{e_r} \frac{p^s}{p^{s_{e_1}} \cdots p^{s_{e_r}}}.$$

Now applying the inclusion-exclusion principle we obtain

$$\begin{aligned}
|T| \ &= \ \sum_{j=1}^{n} i_j \frac{p^s}{p^{s_j}} - \sum_{j<k} i_j i_k \frac{p^s}{p^{s_j} p^{s_k}} - \cdots + (-1)^{n+1} i_1 \cdots i_n \\
&= \ p^s - (p^{s_1} - i_1) \cdots (p^{s_n} - i_n).
\end{aligned}$$

Let $B = \{(x_1-1)^{a_1}\cdots(x_n-1)^{a_n} \mid (a_1,\ldots,a_n) \in T\}$. Clearly the elements of B are $\mathbb{F}_{p^a}$–linearly independent and $|B| = |T|$. On the other hand, we know, from Theorem 3.2, that $\dim(\mathcal{C}_{(i_1,\ldots,i_n)}) = (p^{s_1}-i_1)\cdots(p^{s_n}-i_n)$. This implies that $\dim(\mathcal{C}^{\perp}_{(i_1,\ldots,i_n)}) = p^s - \dim(\mathcal{C}_{(i_1,\ldots,i_n)})$ which agree the cardinality of B, thus the set B is an $\mathbb{F}_q$-basis for $C^{\perp}$. I.e., if we consider the vector representations of the elements of B, we obtain a generator matrix for $C^{\perp}$ and a parity check matrix for C.

4. Duality and the Hasse derivative

In this subsection we will show the natural relation between the Hasse derivative and the dual of monomial-like of codes. We begin by recalling the Hasse derivative which is used in the repeated-root factor test. For a detailed treatment of the Hasse derivative, we refer to [4, Chapter 1] and [5, Chapter 5]. Note that the standard derivative for polynomials over a field of positive characteristic, say p, is inappropriate because from the p^{th} derivative on, the result is always zero. For this reason, it is more convenient to work with the Hasse derivative. Sometimes the Hasse derivative is also called the hyper derivative. Throughout this section, we will use the convention that $\binom{a}{b} = 0$ whenever $b > a$. Let $g(x_1,\ldots,x_n) = \sum g_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ be a polynomial in $\mathbb{F}_q[x_1,\ldots,x_n]$. The Hasse derivative of $g(x_1,\ldots,x_n)$ in the direction $\mathbf{a} = (a_1,\ldots,a_n)$ is defined as

$$D^{[\mathbf{a}]}(g(x_1,\ldots,x_n)) = \sum g_{\alpha_1,\ldots,\alpha_n}\binom{\alpha_1}{a_1}\cdots\binom{\alpha_n}{a_n} x_1^{\alpha_1-a_1}\cdots x_n^{\alpha_n-a_n}. \tag{9}$$

We denote the evaluation of $D^{[\mathbf{a}]}(g(x_1,\ldots,x_n))$ at the point $(\lambda_1,\ldots,\lambda_n) \in \mathbb{F}_{p^a}^n$ by $D^{[\mathbf{a}]}(g)(\lambda_1,\ldots,\lambda_n)$. We can express $g(x_1,\ldots,x_n)$ as

$$g(x_1,\ldots,x_n) = \sum_{(j_1,\ldots,j_n)\in S} c_{j_1,\ldots,j_n}(x_1-1)^{j_1}\cdots(x_n-1)^{j_n}$$

where S is a finite nonempty subset of $\mathbb{N}^n$. Let $S = U_\ell \sqcup P_\ell$ where

$$U_\ell = \{(j_1,\ldots,j_n) \in S \mid j_\ell \geq i_\ell\}, \quad P_\ell = \{(j_1,\ldots,j_n) \in S \mid j_\ell < i_\ell\}.$$

Therefore

$$\begin{aligned} g(x_1,\ldots,x_n) &= \sum_{(j_1,\ldots,j_n)\in U_\ell} c_{j_1,\ldots,j_n}(x_1-1)^{j_1}\cdots(x_n-1)^{j_n} \\ &\quad + \sum_{(j_1,\ldots,j_n)\in P_\ell} c_{j_1,\ldots,j_n}(x_1-1)^{j_1}\cdots(x_n-1)^{j_n}, \end{aligned}$$

and the term $(x_\ell-1)^{i_\ell}$ divides $g(x_1,\ldots,x_n)$ if and only if $c_{j_1,\ldots,j_n} = 0$ for all $(j_1,\ldots,j_n) \in P_\ell$. Now suppose that $(x_\ell-1)^{i_\ell} \nmid g(x_1,\ldots,x_n)$. Then there is a $(\hat{\ae}_1,\ldots,\hat{\ae}_n) \in P_\ell$ such that $c_{\hat{\ae}_1,\ldots,\hat{\ae}_n} \neq 0$. Hence

$$D^{[\hat{\ae}]}(g)(1,\ldots,1) = c_{\hat{\ae}_1,\ldots,\hat{\ae}_n}\binom{\hat{\ae}_1}{\hat{\ae}_1}\cdots\binom{\hat{\ae}_n}{\hat{\ae}_n} \neq 0.$$

Conversely, if $(x_\ell-1)^{i_\ell}$ divides $g(x_1,\ldots,x_n)$, then

$$g(x_1,\ldots,x_n) = \sum_{(j_1,\ldots,j_n)\in U_\ell} c_{j_1,\ldots,j_n}(x_1-1)^{j_1}\cdots(x_n-1)^{j_n}.$$

Therefore $D^{[\vec{a}]}(g)(1,\ldots,1) = 0$ for all $\vec{a} = (a_1,\ldots,a_n)$ with $0 \leq a_\ell < i_\ell$. This proves the following result.

Lemma 4.1. *Let $g(x_1,\ldots,x_n) \in \mathbb{F}_{p^a}[x_1,\ldots,x_n]$ and let $A_\ell = \{\vec{a} = (a_1,\ldots,a_n) \in \mathbb{N}^n \mid 0 \leq a_\ell < i_\ell\}$. Then $(x_\ell-1)^{i_\ell}$ divides $g(x_1,\ldots,x_n)$ if and only if $D^{[\vec{a}]}(g)(1,\ldots,1) = 0$ for all $\vec{a} \in A_\ell$.*

As an immediate consequence, we have the following theorem.

Theorem 4.2. *Let $A_\ell = \{\vec{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n \mid 0 \le a_\ell < i_\ell\}$ and $A = \cup_{\ell=1}^n A_\ell$. Let $g(x_1, \ldots, x_n) \in \mathbb{F}_{p^a}[x_1, \ldots, x_n]$. We have $(x_1 - 1)^{i_1} \cdots (x_n - 1)^{i_n}$ divides $g(x_1, \ldots, x_n)$ if and only if $D^{[\vec{a}]}(g)(1, \ldots, 1) = 0$ for all $\vec{a} \in A$.*

Let $\mathcal{R}$ be as in (2) and let our code be $\mathcal{C}_{(i_1,\ldots i_n)} \subset \mathcal{R}$. We know that the polynomial $g(x_1, \ldots, x_n)$ is in the code $\mathcal{C}_{(i_1,\ldots i_n)}$ if and only if $(x_1 - 1)^{i_1} \cdots (x_n - 1)^{i_n}$ divides $g(x_1, \ldots, x_n)$. Note that $D^{[a_1,\ldots,a_n]}(g)(1, \ldots, 1) = 0$ if $a_\ell \ge p^{s_\ell}$ for some $1 \le \ell \le n$. Together with this fact, Theorem 4.2 implies the following result.

Theorem 4.3. *Let $\mathcal{C}_{(i_1,\ldots i_n)} \subset \mathcal{R}$, and let us define*

$$Q = \bigcup_{\ell=1}^{n} \{\vec{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n \mid 0 \le a_\ell < i_\ell, 0 \le a_j < p^{s_j} \text{ for } j \ne \ell\}.$$

Then $g(x_1, \ldots, x_n) \in \mathcal{C}_{(i_1,\ldots i_n)}$ if and only if $D^{[\vec{a}]}(g)(1, \ldots, 1) = 0$ for all $\vec{a} \in Q$.

Now let us fix a monomial order so that $x_1 > \cdots > x_n$. Let $\vec{a} = (a_1, \ldots, a_n) \in Q$. Consider the vector

$$w_a = \left(\binom{p^{s_1} - 1}{a_1} \cdots \binom{p^{s_n} - 1}{a_n}, \binom{p^{s_1} - 1}{a_1} \cdots \binom{p^{s_{n-1}} - 1}{a_{n-1}} \binom{p^{s_n} - 1}{a_n}, \cdots \binom{0}{a_1}, \cdots \binom{0}{a_n} \right).$$

For $g(x_1, \ldots, x_n) \in \mathcal{R}$, let u_g be the vector representation of the polynomial with respect to the fixed ordering. Then the dot product of w_a and u_g gives us the evaluation of the Hasse derivative of $g(x_1, \ldots, x_n)$ at $(1, \ldots, 1)$ in the direction $\vec{a}$, i.e., $w_a \cdot u_g = D^{[\vec{a}]}(g)(1, \ldots, 1)$. If we construct the matrix H whose rows are the vectors w_a where $\vec{a} \in Q$ and Q is as in Theorem 4.3 then H is an alternative parity check matrix for the code $\mathcal{C}_{(i_1,\ldots i_n)}$ by Theorem 4.3.

5. A generalisation of the weight retaining property

In [10], the so-called weight retaining property of polynomials over finite fields was stated and proved. This property turned out to be very useful for determining the Hamming distance of cyclic codes.

In this section, we give a generalisation of the weight retaining property to multivariate polynomials. We prove that the Hamming weight of any $\mathbb{F}_{p^a}$-linear combination of the monomials $(x_1 - c_1)^{i_1} \cdots (x_n - c_n)^{i_n}$ is greater than or equal to the Hamming weight of the "minimal" nonzero term, where a "minimal" term is the one that is not divisible by the rest of the nonzero terms of the summation.

First, we consider the case in one variable which was studied in [10]. The weight retaining property of $(x - c)^i$ is given in the following two theorems.

Theorem 5.1. *[10, Theorem 1.1 and Theorem 6.1] Let L be any nonempty finite subset of non-negative integers with least integer $i_{\min}$ and let*

$$f(x) = \sum_{i \in L} b_i (x - c)^i$$

where c and each b_i are nonzero elements of $\mathbb{F}_{p^a}$. Then

$$\mathrm{w}(f(x)) \ge \mathrm{w}((x - c)^{i_{\min}}).$$

It is not hard to see that Theorem 5.1 is equivalent to the following theorem.

Theorem 5.2. *[10, Theorem 6.2] For any polynomial $Q(x)$ over $\mathbb{F}_{p^a}$ and $c \in \mathbb{F}_{p^a} \setminus \{0\}$, and any non-negative integer N,*

$$\mathrm{w}(Q(x)(x-c)^N) \geq \mathrm{w}((x-c)^N)\mathrm{w}(Q(c)).$$

The Hamming weight of the monomial $(x-c)^i$, which is used above, was also determined in [10].

Theorem 5.3. *[10, Lemma 1] Let $c \in \mathbb{F}_{p^a} \setminus \{0\}$ and let i be an integer with the p-adic expansion*

$$i = \iota_0 + \iota_1 p + \cdots \iota_{m-1} p^{m-1}$$

where $0 \leq \iota_\ell \leq p-1$ for all $0 \leq \ell \leq m-1$. Then

$$\mathrm{w}((x-c)^i) = P(i) = \prod_{j=0}^{m-1} (\iota_j + 1).$$

The following theorem is a generalisation of the Massey's weight retaining property to n variables. Its proof is very similar to the proof of [3, Proposition 1.2].

Theorem 5.4. *Let $\psi \subset \mathbb{N}^n$ be a finite set and let $(N_1, N_2, \ldots, N_n) \in \psi$. Let*

$$f(x_1, \ldots, x_n) = \sum_{\beta \in \psi} c_\beta (x_1 - c_1)^{\beta_1} (x_2 - c_2)^{\beta_2} \cdots (x_n - c_n)^{\beta_n} \in \mathbb{F}_{p^a}[x_1, \ldots, x_n],$$

where $c_\beta \in \mathbb{F}_{p^a} \setminus \{0\}$, $\beta = (\beta_1, \ldots, \beta_n)$ and $(x_1-c_1)^{N_1}(x_2-c_2)^{N_2} \cdots (x_n-c_n)^{N_n}$ divides $(x_1-c_1)^{\beta_1}(x_2-c_2)^{\beta_2} \cdots (x_n-c_n)^{\beta_n}$ for every $\beta \in \psi$. Then

$$\mathrm{w}(f(x_1, \ldots, x_n)) \geq \prod_{i=1}^{n} P(N_i).$$

Proof. The proof is via induction on n. For $n = 1$, the claim follows by Theorem 5.1. Now assume that the claim holds true for $n-1$. We can express $f(x_1, \ldots, x_n)$ as

$$\begin{aligned}
&(x_n - c_n)^{N_n} (\sum_{\beta \in \psi} c_\beta^{(0)} (x_1 - c_1)^{\beta_1} (x_2 - c_2)^{\beta_2} \cdots (x_{n-1} - c_{n-1})^{\beta_{n-1}} \\
&+ (x_n - c_n) \sum_{\beta \in \psi} c_\beta^{(1)} (x_1 - c_1)^{\beta_1} (x_2 - c_2)^{\beta_2} \cdots (x_{n-1} - c_{n-1})^{\beta_{n-1}} \\
&\vdots \\
&+ (x_n - c_n)^r \sum_{\beta \in \psi} c_\beta^{(r)} (x_1 - c_1)^{\beta_1} (x_2 - c_2)^{\beta_2} \cdots (x_{n-1} - c_{n-1})^{\beta_{n-1}})
\end{aligned}$$

for some non-negative integer r and $c_\beta^{(\ell)} \in \mathbb{F}_{p^a}$. By the induction step, we have

$$\mathrm{w}(\sum_{\beta \in \psi} c_\beta^{(0)} (x_1 - c_1)^{\beta_1} (x_2 - c_2)^{\beta_2} \cdots (x_{n-1} - c_{n-1})^{\beta_{n-1}}) \geq P(N_1) \cdots P(N_{n-1}).$$

If we express each summand $\sum_{\beta \in \psi} c_\beta^{(u)} (x_1 - c_1)^{\beta_1} (x_2 - c_2)^{\beta_2} \cdots (x_{n-1} - c_{n-1})^{\beta_{n-1}}$ in the form $\sum_{\beta \in \psi'} e_\beta^{(u)} x_1^{\beta_1} x_2^{\beta_2} \cdots x_{n-1}^{\beta_{n-1}}$, we get

$$\begin{aligned}
&(x_n - c_n)^{N_n} (\sum_{\beta \in \psi'} e_\beta^{(0)} x_1^{\beta_1} x_2^{\beta_2} \cdots x_{n-1}^{\beta_{n-1}} + (x_n - c_n) \sum_{\beta \in \psi'} e_\beta^{(1)} x_1^{\beta_1} x_2^{\beta_2} \cdots x_{n-1}^{\beta_{n-1}} \\
&\ldots + (x_n - c_n)^r \sum_{\beta \in \psi'} e_\beta^{(r)} x_1^{\beta_1} x_2^{\beta_2} \cdots x_{n-1}^{\beta_{n-1}}).
\end{aligned}$$

Note that we have just shown that there are at least $P(N_1)\cdots P(N_{n-1})$ many nonzero $e^{(0)}_\beta$'s. We define

$$h_\beta(x_n) = e^{(0)}_\beta + e^{(1)}_\beta(x_n - c_n) + \cdots + e^{(r)}_\beta(x_n - c_n)^r.$$

So

$$f(x_1, \ldots, x_n) = (x_n - c_n)^{N_n}(\sum_{\beta\in\psi} h_\beta(x_n)x_1^{\beta_1}\cdots x_{n-1}^{\beta_{n-1}}).$$

There are at least $P(N_1)\cdots P(N_{n-1})$ many β's such that $h_\beta(x_n) \neq 0$. For every such $\beta = (\beta_1, \ldots, \beta_n)$, we have

$$\mathrm{w}((x_n - c_n)^{N_n} h_\beta(x_n)x_1^{\beta_1}\cdots x_{n-1}^{\beta_{n-1}}) \geq P(N_n)$$

because $\mathrm{w}((x_n - c_n)^{N_n} h_\beta(x_n)) \geq P(N_n)$ as the claim holds for one variable. Hence $\mathrm{w}(f(x_1, \ldots, x_n)) \geq P(N_1)\cdots P(N_{n-1})P(N_n)$. □

Remark 5.5. *This result only applies for polynomials f of a special kind, namely those for which the set denoted ψ contains $(N_1, \ldots, N_n)$. For example, $\psi = \{(1, 2), (2, 1)\}$ does not have that property. Note that the condition $(N_1, N_2) \in \psi$ is necessary, consider the following example*

$$f(x_1, x_2) = (x_1 + 1)^4(x_2 + 1)^3 + (x_1 + 1)^3(x_2 + 1)^4$$

with coefficients in the field of 2 elements. It is easy to check that $\mathrm{w}(f(x_1, x_2)) = 14$ but $P(3) = 4$ where P is the polynomial of Theorem 5.3.

Using Theorem 5.4, we generalise Theorem 5.3 to n variables.

Corollary 5.6. *Let $Q(x_1, \ldots, x_n) \in \mathbb{F}_{p^a}[x_1, \ldots, x_n]$, $c_1, \ldots, c_n \in \mathbb{F}_{p^a}$ and $N_1, \ldots, N_n \in \mathbb{N}$. We have*

$$\begin{aligned}&\mathrm{w}[Q(x_1, \ldots, x_n)(x_1 - c_1)^{N_1}\cdots(x_n - c_n)^{N_n}]\\ &\quad\geq \mathrm{w}[(x_1 - c_1)^{N_1}\cdots(x_n - c_n)^{N_n}][Q(c_1, \ldots, c_n)]\\ &\quad= P(N_1)\cdots P(N_n)w_H[Q(c_1, \ldots, c_n)].\end{aligned}$$

Note that this property roughly states that the Hamming weight of a polynomial of a linear combination of polynomials of the form $(x_1 - 1)^{i_1}, \ldots (x_n - 1)^{i_n}$ is at least the Hamming weight of a minimal term (in the lexicographical order of exponents).

Acknowledgment: The research of the first author was partly supported by the Spanish grants MTM2007-64704 and MTM2010-21580-C02-02. He was also funded by the Vernon Wilson Endowed Chair at Eastern Kentucky University during his sabbatical leave.

References

[1] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, *On repeated-root cyclic codes*, IEEE Trans. Inform. Theory, 37(2), 337-342, 1991.

[2] H. Q. Dinh. *On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions*, Finite Fields Appl., 14(1), 22-40, 2008.

[3] V. Drensky and P. Lakatos, *Monomial ideals, group algebras and error correcting codes*, In Applied algebra, algebraic algorithms and error-correcting codes, (Rome, 1988), volume 357 of Lecture Notes in Comput. Sci., pages 181-188. Springer, Berlin, 1989.

[4] D. M. Goldschmidt, *Algebraic functions and projective curves*, volume 215, Graduate Texts in Mathematics, Springer-Verlag, New York, 2003.

[5] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[6] W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[7] S. R. López-Permouth, S. Szabo, *On the Hamming weight of repeated root cyclic and negacyclic codes over Galois rings*, Adv. Math. Commun., 3(4), 409-420, 2009.

[8] E. Martínez-Moro, I. F. Rúa, *On repeated-root multivariable codes over a finite chain ring*, Des. Codes Cryptogr., 45(2), 219-227, 2007.

[9] C. Martínez-Pérez, W. Willems, *On the weight hierarchy of product codes*, Designs, Codes and Cryptography. An International Journal, 33(2), 95-108, 2004.

[10] J. L. Massey, D. J. Costello, Jørn Justesen, *Polynomial weights and code constructions*, IEEE Trans. Information Theory, IT-19, 101-110, 1973.

[11] Hakan Özadam and Ferruh Özbudak, *A note on negacyclic and cyclic codes of length p^s over a finite field of characteristic p*, Adv. Math. Commun., 3(3), 265-271, 2009.

[12] S. R. López-Permouth, H. Özadam, F. Özbudak, S Szabo, *Polycyclic codes over Galois rings with applications to repeated-root constacyclic codes*, Finite Fields and Their Applications, 19(1), 16-38, 2013.

[13] H. G. Schaathun, *The weight hierarchy of product codes*, IEEE Trans. Inform. Theory, 46(7), 2648-2651, 2000.

[14] J. H. van Lint. *Repeated-root cyclic codes*, IEEE Trans. Inform. Theory, 37(2), 343-345, 1991.