Korean J. Math. **17** (2009), No. 4, pp. 385–397

CODES OVER POLYNOMIAL RINGS AND THEIR PROJECTIONS

Young Ho Park

Abstract. We study codes over the polynomial ring $\mathbb{F}_q[D]$ and their projections to the finite rings $\mathbb{F}_q[D]/(D^m)$ and the weight enumerators of self-dual codes over these rings. We also give the formula for the number of codewords of minimum weight in the projections.

1. Codes over polynomial rings

A code of length n over a ring R (finite or infinite) is a subset of R^n. If the code is a R-submodule of R^n then it is a *linear* code. We will always assume that codes are linear. The *Hamming weight* $\mathrm{wt}(\mathbf{v})$ of a vector $\mathbf{v}$ is the number of non-zero coordinates. The *minimum distance* of a code $\mathcal{C}$, denoted by $d(\mathcal{C})$, is the smallest of all non-zero weights in the code. To the ambient space R^n we attach the inner product

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i, \tag{1}$$

where $\mathbf{v} = (v_i),\ \mathbf{w} = (w_i)$. We define the *dual* code of $\mathcal{C}$ to be

$$\mathcal{C}^\perp = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0 \text{ for all } \mathbf{w} \in \mathcal{C}\}. \tag{2}$$

A code $\mathcal{C}$ satisfying $\mathcal{C} = \mathcal{C}^\perp$ is called a *self-dual* code.

Let $\mathbb{F}_q$ be the field of q elements, and throughout this paper let

$$\mathsf{P} = \mathbb{F}_q[D]$$

denote the infinite ring of polynomials in one indeterminate D over $\mathbb{F}_q$. The elements of the finite ring

$$\mathsf{P}_m = \mathbb{F}_q[D]/(D^m)$$

Received September 12, 2008. Revised October 14, 2008.
2000 Mathematics Subject Classification: 94B10, 94B05.
Key words and phrases: self-dual codes, weight enumerators.

are identified with polynomials $a_0 + a_1 D + a_2 D^2 + \cdots + a_{m-1} D^{m-1}$ of degree less than m. This ring is a commutative ring with q^m elements. We sometimes view P_m as a subset of P_r for $r > m$, and of P by assuming all coefficients of D^i are 0 for $i > m$. The units of P are precisely the non-zero elements of degree 0, i.e., $\mathsf{P}^* = \mathbb{F}_q - \{0\}$, while the units of P_m are polynomials with a nonzero constant term.

Since P is a principal ideal domain, any code $\mathcal{C}$ of length n over P is a free module of rank $k \leq n$. In this case, we shall write $\operatorname{rank} \mathcal{C} = k$. If $\mathcal{C}_1 \subset \mathcal{C}_2$ are codes over P, then $\operatorname{rank} \mathcal{C}_1 \leq \operatorname{rank} \mathcal{C}_2$. A code $\mathcal{C}$ of length n and rank k is said to be an $[n, k]$-code, or $[n, k, d]$-code if the minimum distance of $\mathcal{C}$ is d. A $k \times n$ matrix whose rows form a basis of $[n, k]$-code $\mathcal{C}$ is called a *generator matrix* of $\mathcal{C}$. A generator matrix of $\mathcal{C}^\perp$ is called a *parity check matrix* of $\mathcal{C}$.

Lemma 1.1. *For a code $\mathcal{C}$ over P of length n, we have*

$$\operatorname{rank} \mathcal{C}^\perp + \operatorname{rank} \mathcal{C} = n.$$

From the lemma, we obtain

$$\operatorname{rank} \mathcal{C} = \operatorname{rank} (\mathcal{C}^\perp)^\perp. \tag{3}$$

Furthermore, if $\mathcal{C}$ is a self-dual $[n, k]$-code over P, then $n = 2k$.

For codes $\mathcal{C}$ over an *infinite* ring $\mathbb{F}_q[D]$, we do not always have $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. For example, let $\mathcal{C} = (D^m)$ be the code of length 1 generated by D^m. Then $\mathcal{C}^\perp = \{0\}$ and $(\mathcal{C}^\perp)^\perp = \mathsf{P}$, which is much larger than $\mathcal{C} = (D^m)$. Nevertheless, it is always true that

$$\mathcal{C} \subset (\mathcal{C}^\perp)^\perp. \tag{4}$$

Definition 1.2. A code $\mathcal{C}$ over P is said to be *basic* if $\mathcal{C} = (\mathcal{C}^\perp)^\perp$.

Lemma 1.3. *Let $\mathcal{C}_1 \subset \mathcal{C}_2$ be codes over P of the same rank. If $\mathbf{v} \in \mathcal{C}_2$, then $\alpha \mathbf{v} \in \mathcal{C}_1$ for some nonzero $\alpha \in \mathsf{P}$.*

Proof. Let $\operatorname{rank} \mathcal{C}_1 = k$ and $\{\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k\}$ be a basis for $\mathcal{C}_1$. Since

$$\operatorname{rank} \mathcal{C}_2 \geq \operatorname{rank} \langle \mathcal{C}_1, \mathbf{v} \rangle \geq \operatorname{rank} \mathcal{C}_1 = \operatorname{rank} \mathcal{C}_2,$$

we have $\operatorname{rank} \langle \mathcal{C}_1, \mathbf{v} \rangle = k$. Thus the $k+1$ vectors $\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k$ and $\mathbf{v}$ are linearly dependent over P. Hence there is a dependence relation $\alpha_1 \mathbf{w}_1 + \cdots + \alpha_k \mathbf{w}_k + \alpha \mathbf{v} = 0$, and thus $\alpha \mathbf{v} \in \mathcal{C}_1$. Finally, $\alpha \neq 0$ since if $\alpha = 0$ then $\alpha_i = 0$ for all i. $\square$

Theorem 1.4. *The following conditions are equivalent for a code $\mathcal{C}$ over P.*

i. $\mathcal{C}$ *is basic.*
ii. $\alpha\mathbf{v} \in \mathcal{C}$ *implies* $\mathbf{v} \in \mathcal{C}$ *for any nonzero* $\alpha \in \mathsf{P}$.

Proof. Suppose $\mathcal{C}$ is basic. If $\alpha\mathbf{v} \in \mathcal{C}$, then $[\alpha\mathbf{v}, \mathbf{w}] = 0$ for all $\mathbf{w} \in \mathcal{C}^{\perp}$, which implies $[\mathbf{v}, \mathbf{w}] = 0$ for all $\mathbf{w} \in \mathcal{C}^{\perp}$ since P is an integral domain, and thus $\mathbf{v} \in (\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$. The converse follows from the previous lemma, (3) and (4). $\square$

Remark. Theorem 1.4 is true for any code of finite rank over a principal ideal domain.

Corollary 1.5. *A code* $\mathcal{C}$ *over* P *is basic if and only if* $\mathcal{C}$ *is a dual code of some code over* P.

Proof. If $\mathcal{C} = \mathcal{C}_1^{\perp}$ and $\alpha\mathbf{v} \in \mathcal{C}$, then $\mathbf{0} = [\alpha\mathbf{v}, \mathbf{w}] = \alpha[\mathbf{v}, \mathbf{w}]$ for all $\mathbf{w} \in \mathcal{C}_1$ and hence $[\mathbf{v}, \mathbf{w}] = \mathbf{0}$ for all $\mathbf{w} \in \mathcal{C}_1$, which implies that $\mathbf{v} \in \mathcal{C}_1^{\perp} = \mathcal{C}$. The converse is clear. $\square$

This corollary provides us a way of constructing basic codes. Indeed, the basic codes of length n are exactly the codes defined by an $s \times n$ matrix H_0 as

$$\mathcal{C}(H_0) = \{\mathbf{v} \in \mathsf{P}^n \mid H_0\mathbf{v}^T = 0\},$$

i.e., the solutions sets to a family of linear equations. $\mathcal{C}(H_0)$ is then basic, since it is dual to the code generated by the rows of H_0. Note that H_0 is not necessarily a parity check matrix of $\mathcal{C}(H_0)$ even if the row vectors of H_0 are linearly independent.

We shall present another way of describing basic codes in terms of their generator matrices. For a vector $\mathbf{u} = (u_1, \ldots, u_r) \in \mathsf{P}^r$, we denote

$$c(\mathbf{u}) = \gcd\{u_1, \cdots, u_r\}.$$

It is clear that $c(\alpha\mathbf{u}) = \alpha c(\mathbf{u})$ for any $\alpha \in \mathsf{P}$, and $c(\mathbf{u}) \mid c(\mathbf{u}G)$ for any $r \times s$ matrix G over P, since the components of $\mathbf{u}G$ are linear combinations of the components of $\mathbf{u}$. In addition, we can write $\mathbf{u} = c(\mathbf{u})\mathbf{u}_0$, with $c(\mathbf{u}_0) = 1$.

Lemma 1.6. *Let* $\{\mathbf{g}_i\}$ *be the rows of the generator matrix* G *of a basic code* $\mathcal{C}$. *Then* $c(\mathbf{g}_i) = 1$ *for all* i.

Proof. Suppose $\mathbf{g}_{i_0} = \beta\mathbf{f}$ for some $\beta \in \mathsf{P} = \mathbb{F}_q[D]$. Since $\mathcal{C}$ is basic, we have $\mathbf{f} \in \mathcal{C}$. Write $\mathbf{f} = \sum_{i=1}^{k} \alpha_i \mathbf{g}_i$. We then have

$$\beta\alpha_1\mathbf{g}_1 + \cdots + (\beta\alpha_{i_0} - 1)\mathbf{g}_{i_0} + \cdots + \beta\alpha_k\mathbf{g}_k = 0,$$

which implies that $\beta\alpha_{i_0} - 1 = 0$. Thus $\beta \in \mathbb{F}_q^*$ and hence $c(\mathbf{g}_{i_0}) = 1$. $\square$

The converse of the above lemma is not true. For example, let $\mathcal{C}$ be the code with generator matrix $G = \left(\begin{smallmatrix} 1 & D \\ D & 1 \end{smallmatrix}\right)$. So $c(1,D) = c(D,1) = 1$. But $G' = \left(\begin{smallmatrix} 1 & D \\ D+1 & 1+D \end{smallmatrix}\right)$ is also a generator matrix with $c(D+1, D+1) = D+1 \neq 1$. Thus $\mathcal{C}$ is not basic. In fact, since $\operatorname{rank} \mathcal{C} = 2$, we have $\mathcal{C}^{\perp} = \{0\}$ and $(\mathcal{C}^{\perp})^{\perp} = \mathsf{P}^2 \neq \mathcal{C}$.

THEOREM 1.7. *Let G be a generator matrix of an $[n,k]$-code $\mathcal{C}$ over P. Then $\mathcal{C}$ is basic if and only if one of the following is satisfied.*

i. $c(\mathbf{u}) = 1 \Rightarrow c(\mathbf{u}G) = 1$ *for all* $\mathbf{u} \in \mathsf{P}^k$.
ii. $c(\mathbf{u}) = c(\mathbf{u}G)$ *for all* $\mathbf{u} \in \mathsf{P}^k$.

Proof. (basic) $\Longleftrightarrow$ (i). First note that $\mathbf{u}G \in \mathcal{C}$ for all $\mathbf{u}$, and if $\mathbf{u}_1 G = \mathbf{u}_2 G$ then $\mathbf{u}_1 = \mathbf{u}_2$. Assume that $\mathcal{C}$ is basic and $c(\mathbf{u}) = 1$. Let $\mathbf{u}G = \alpha\mathbf{v}$ for some $\alpha \in \mathsf{P}$. Since $\mathcal{C}$ is basic, we have $\mathbf{v} \in \mathcal{C}$ so that $\mathbf{v} = \mathbf{w}G$ for some $\mathbf{w}$. Thus $\mathbf{u}G = \alpha\mathbf{v} = \alpha\mathbf{w}G$, which implies $\mathbf{u} = \alpha\mathbf{w}$. Since $c(\mathbf{u}) = 1$, we have $\alpha \in \mathbb{F}_q$ and hence $c(\mathbf{u}G) = 1$. Conversely, suppose $\alpha\mathbf{v} \in \mathcal{C}$. There exists some $\mathbf{u}$ such that $\alpha\mathbf{v} = \mathbf{u}G$. Write $\mathbf{u} = c(\mathbf{u})\mathbf{u}_0$ with $c(\mathbf{u}_0) = 1$. Since $c(\mathbf{u}_0 G) = 1$ by (i) and $\alpha\mathbf{v} = c(\mathbf{u})\mathbf{u}_0 G$, we have $c(\alpha\mathbf{v}) = c(\mathbf{u})$. Hence $\alpha\mathbf{v} = c(\mathbf{u})\mathbf{u}_0 G = c(\alpha\mathbf{v})\mathbf{u}_0 G = \alpha c(\mathbf{v})\mathbf{u}_0 G$. Consequently, $\mathbf{v} = c(\mathbf{v})\mathbf{u}_0 G \in \mathcal{C}$.

(i) $\Longleftrightarrow$ (ii). Write $\mathbf{u} = c(\mathbf{u})\mathbf{u}_0$ with $c(\mathbf{u}_0) = 1$. Then $c(\mathbf{u}G) = c(\mathbf{u})c(\mathbf{u}_0 G)$. Thus the proof follows from the fact that $c(\mathbf{u}_0 G) = 1$ iff $c(\mathbf{u}) = c(\mathbf{u}G)$. □

We now recall the definitions and facts about basic matrices over P.

DEFINITION 1.8. A $k \times n$ matrix G over P is said to be *basic* if G has a (polynomial) right inverse, that is, if there exists an $n \times k$ matrix M over P such that $GM = I_k$.

There are other characterizations of basic matrices as follows [2].

THEOREM 1.9. *A $k \times n$ matrix $G = G(D)$ over $\mathbb{F}_q[D]$ is basic iff one of the following conditions is satisfied.*

i. *The invariant factors of G are all* 1.
ii. *The* gcd *of the $k \times k$ minors of G is* 1.
iii. *$G(\alpha)$ has rank k for any α in the algebraic closure of $\mathbb{F}_q$.*
iv. *If $\mathbf{u}G \in \mathbb{F}_q[D]^n$ for $\mathbf{u} \in \mathbb{F}_q(D)^k$, then $\mathbf{u} \in \mathbb{F}_q[D]^k$.*
v. *There exists an $(n-k) \times n$ matrix L such that* $\det \begin{pmatrix} G \\ L \end{pmatrix}$ *is a nonzero element of $\mathbb{F}_q$.*

It turns out that basic codes are exactly those generated by basic matrices.

THEOREM 1.10. *Let G be a generator matrix of a code $\mathcal{C}$ over P. Then $\mathcal{C}$ is basic if and only if G is basic.*

Proof. Assume that the $k \times n$ matrix G generates a basic code. Suppose $\mathbf{u}G \in \mathsf{P}^n$ for $\mathbf{u} \in \mathbb{F}_q(x)^k$. There exists $\alpha \in \mathsf{P}$ such that $\mathbf{v} = \alpha\mathbf{u} \in \mathsf{P}^k$. Write $\mathbf{v} = c(\mathbf{v})\mathbf{v}_0$ for some $\mathbf{v}_0 \in \mathsf{P}^k$. Now Theorem 1.7 implies

$$\alpha c(\mathbf{u}G) = c(\alpha\mathbf{u}G) = c(\mathbf{v}G) = c(\mathbf{v}).$$

Thus $\alpha \mid c(\mathbf{v})$ and then $\mathbf{u} = \frac{1}{\alpha}\mathbf{v} = \frac{c(\mathbf{v})}{\alpha}\mathbf{v}_0 \in \mathsf{P}^k$. Therefore, G is basic by Theorem 1.9(iv). Conversely, suppose that G is basic so that there is a matrix M such that $GM = I_k$. Let $\alpha\mathbf{v} \in \mathcal{C}$. Then $\alpha\mathbf{v} = \mathbf{u}G$ for some $\mathbf{u}$, and $\alpha\mathbf{v}M = \mathbf{u}GM = \mathbf{u}$. Thus $\alpha\mathbf{v} = \mathbf{u}G = (\alpha\mathbf{v}M)G = \alpha(\mathbf{v}MG)$, which implies that $\mathbf{v} = (\mathbf{v}M)G \in \mathcal{C}$. □

COROLLARY 1.11. *If $\mathcal{C}_1$ is basic and $\mathcal{C}_2$ is equivalent to $\mathcal{C}_1$, then $\mathcal{C}_2$ is also basic.*

Proof. Let G_i be generator matrices for $\mathcal{C}_i$. The theorem follows from Theorem 1.9(ii) and the fact that the minors for G_1 and G_2 are the same up to ± 1. □

THEOREM 1.12. i. *Self-dual codes are basic.*
ii. *If $\mathcal{C}$ is a basic self-orthogonal $[2k, k]$-code, then $\mathcal{C}$ is self-dual.*

Proof. (i) If $\mathcal{C}^\perp = \mathcal{C}$, then $(\mathcal{C}^\perp)^\perp = \mathcal{C}^\perp = \mathcal{C}$.

(ii) Suppose that $\mathbf{v} \in \mathcal{C}^\perp$. Since $\mathcal{C} \subset \mathcal{C}^\perp$ and $\operatorname{rank}\mathcal{C}^\perp = 2k - k = k = \operatorname{rank}\mathcal{C}$, it follows from Lemma 1.3 that $\alpha\mathbf{v} \in \mathcal{C}$ for some $\alpha \in \mathsf{P}$. As $\mathcal{C}$ is basic, we have $\mathbf{v} \in \mathcal{C}$. □

2. Codes over $\mathbb{F}_q[D]/(D^m)$

We recall some of the basic facts about the codes over $\mathsf{P}_m = \mathbb{F}_q[D]/(D^m)$. Let M be a $k \times n$ matrix over P_m. Then by performing operations of the type

(R1) Permutation of the rows,
(R2) Multiplication of a row by a unit of P_m,
(R3) Addition of a scalar multiple of one row to another,
(C1) Permutation of the columns,

M can be transformed to the *standard form*

(5)

$$M' = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} & \dots & A_{0,m-1} & A_{0m} \\ 0 & DI_{k_1} & DA_{12} & DA_{13} & \dots & DA_{1,m-1} & DA_{1m} \\ 0 & 0 & D^2 I_{k_2} & D^2 A_{23} & \dots & D^2 A_{2,m-1} & D^2 A_{2m} \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \dots & D^{m-1} I_{k_{m-1}} & D^{m-1} A_{m-1,m} \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 I_{k_m} \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

where the columns are grouped into square blocks of sizes $k_0, k_1, \dots, k_{m-1}$, k_m and the k_i are nonnegative integers adding to n. A matrix with standard form as in (5) is said to have *type*

$$(1)^{k_0}(D)^{k_1}(D^2)^{k_2}\cdots(D^{m-1})^{k_{m-1}}0^{k_m}, \tag{6}$$

omitting terms with zero exponents, if any. Often the 0^{k_m} is left off the type, but we retain it since we use k_m later. Any $[n,k]$-code C over P_m is equivalent to a code with a generator matrix of the form as above with no zero rows. Such a code C is said to have *type*

$$1^{k_0}(D)^{k_1}(D^2)^{k_2}\cdots(D^{m-1})^{k_{m-1}}.$$

We have that $k = \sum_{i=0}^{m-1} k_i$, $k_m = n-k$ and $|C| = \prod_{j=0}^{m-1}(q^{m-j})^{k_j}$. The dual code $C^\perp$ has type $1^{k_m}(D)^{k_{m-1}}(D^2)^{k_{m-2}}\cdots(D^{m-1})^{k_1}$. Since P_m is finite, $(C^\perp)^\perp = C$ and $|C||C^\perp| = |\mathsf{P}_m^n| = q^{mn}$.

3. Weight enumerators and invariants

Throughout this section let $q = p^e$. For a code C over $\mathsf{P}_m = \mathbb{F}_q[D]/(D^m)$ of length n, define the *Hamming weight enumerator*

$$W_C(x,y) = \sum_{\mathbf{v}\in C} x^{n-wt(\mathbf{v})} y^{wt(\mathbf{v})}. \tag{7}$$

Fix an isomorphism ψ between the additive group $\mathbb{F}_q$ and $\mathbb{F}_p^e$ and define a map $\phi : \mathbb{F}_q \to \mathbb{F}_p$ by $\phi(a) = \sum_{i=1}^{e} a_i$, where $\psi(a) = (a_1, a_2, \dots, a_e)$. We now define an additive character χ_1 on P_m by

$$\chi_1(f) = \exp\left(\frac{2\pi\sqrt{-1}}{p}\sum_{i=0}^{m-1}\phi(a_i)\right),$$

where $f = a_0 + a_1 D + a_2 D^2 + \cdots + a_{m-1} D^{m-1} \in \mathsf{P}_m$. For any $g \in \mathsf{P}_m$, define $\chi_f(g) = \chi_1(fg)$.

THEOREM 3.1. P_m *is a Frobenius ring for every* m.

Proof. By the results in [4], it suffices to show that χ_1 is a generating character, i.e., every character of P_m has the form χ_g for some $g \in \mathsf{P}_m$. Since there are exactly $|\mathsf{P}_m|$ characters, it is enough to show that $\chi_g = \chi_h$ implies $g = h$. Suppose $\chi_g(f) = \chi_h(f)$ for all $f \in \mathsf{P}_m$. Then $\chi_1((g-h)f) = 1$ for all f. This means that the additive subgroup $\ker \chi_1$ contains the ideal $(g-h)$ of the ring P_m. Now note that either $(g-h) = \{0\}$ or $(g-h) = (D^{i_0})$ for some $i_0 \geq 0$. However, if we choose any $b \in \mathbb{F}_q$ such that $\phi(b) \neq 0$, then

$$\chi_1(bD^i) = \exp\left(\frac{2\pi\sqrt{-1}}{p}\phi(b)\right) \neq 1$$

and hence $bD^i \notin \ker \chi_1$ for any $i \geq 0$. Therefore $(g-h) = \{0\}$ and the theorem is proved. $\square$

By the results in [4] we have the following corollary.

COROLLARY 3.2 (MacWilliams relations). *Let* C *be a linear code over* P_m. *Then*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x + (q^m - 1)y, x - y). \tag{8}$$

4. Projections

Define the map $\Psi_m : \mathsf{P} \to \mathsf{P}_m$ by

$$\Psi_m(a_0 + a_1 D + \cdots + a_{r-1} D^{r-1}) = a_0 + a_1 D + \cdots + a_{m-1} D^{m-1}. \tag{9}$$

The maps is extended coordinatewise to make a map $\Psi_m : \mathsf{P}^n \to (\mathsf{P}_m)^n$. We define the similar map $\Psi_r^m : \mathsf{P}_r \to \mathsf{P}_m$ for $r > m$ by

$$\Psi_m^r(a_0 + a_1 D + \cdots + a_{r-1} D^{r-1}) = a_0 + a_1 D + \cdots + a_{m-1} D^{m-1}. \tag{10}$$

Again this map is applied coordinatewise to make a map $\Psi_m^r : (\mathsf{P}_r)^n \to (\mathsf{P}_m)^n$. The following lemma follows from a straightforward computation.

LEMMA 4.1. *The maps* Ψ_m *and* Ψ_m^r *are linear.*

Let $\mathcal{C}$ be a basic $[n,k]$-code over P. For every integer $m>0$, define a code $\mathcal{C}_m$ over P_m as

$$\mathcal{C}_m = \Psi_m(\mathcal{C}) = \{\Psi_m(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}\}.$$

Let G be a generator matrix of $\mathcal{C}$ and H its parity check matrix. Let

$$G_m = \Psi_m(G),\ H_m = \Psi_m(H).$$

For any integer $s \geq 0$, we have

$$(11)\quad \Psi_m^{m+s}(\mathcal{C}_{m+s}) = \mathcal{C}_m,\ \Psi_m^{m+s}(G_{m+s}) = G_m,\ \text{and } \Psi_m^{m+s}(H_{m+s}) = H_m.$$

THEOREM 4.2. *Let $\mathcal{C}$ be a basic $[n,k]$-code over P. Then we have*

i. $\operatorname{rank}\mathcal{C}_m = \operatorname{rank}\mathcal{C}$ *and each* $\mathcal{C}_m$ *has type* 1^k *for every* m. *In particular,* $|\mathcal{C}_m| = q^{mk}$.
ii. G_m *is a generator matrix of* $\mathcal{C}_m$.
iii. $\Psi_m(\mathcal{C}^\perp) = \Psi_m(\mathcal{C})^\perp$ *and hence* H_m *is a parity check matrix of* $\mathcal{C}_m$.

Proof. (i) Let $G = (g_{ij})$ and write $g_{ij} = a_{ij} + Df_{ij}$, $a_{ij} \in \mathbb{F}_q$, $f_{ij} \in \mathsf{P}$. Then the rows of $G_1 = (a_{ij})$ generates $\mathcal{C}_1$. We first show that $\operatorname{rank}\mathcal{C}_1 = \operatorname{rank}\mathcal{C} = k$. Suppose to the contrary that $\operatorname{rank}\mathcal{C}_1 < \operatorname{rank}\mathcal{C} = k$. By performing a sequence of operations of types (R1), (R2), (R3) and (C1), G_1 can be transformed into its standard form G_1' which must have a zero row. Note that the units of $\mathbb{F}_q$ are precisely the units of P. Thus we can apply the same sequence of operations to G and obtain a matrix of the form $G' = G_1' + DF'$. Undo the operations of type (C1), if any, applied to G in the reverse order. It is clear that the resulting matrix G'' is again a generator matrix of C. But now G'' contains a row which is a multiple of D. This contradicts Lemma 1.6. Therefore $\operatorname{rank}\mathcal{C}_1 = k$ and $\mathcal{C}_1$ has type 1^k. Since $\Psi_1^m(G_m) = G_1$ and $\Psi_1(D^j) = 0$, it is now clear that G_m has rank k and type 1^k.

(ii) This follows from (i).

(iii) Let $\{\mathbf{g}_i\}$ be the rows of G. Let $\mathbf{v}_m \in \Psi_m(\mathcal{C}^\perp)$. Then $\mathbf{v}_m = \Psi_m(\mathbf{v})$ for some $\mathbf{v} \in \mathcal{C}^\perp$, i.e., for some $\mathbf{v}$ with $[\mathbf{v}, \mathbf{g}_i] = 0$ for all i. Thus $[\mathbf{v}_m, \Psi_m(\mathbf{g}_i)] = \Psi_m([\mathbf{v}, \mathbf{g}_i]) = 0$ for all i, and hence $\mathbf{v}_m \in \Psi_m(\mathcal{C})^\perp$. Therefore $\Psi_m(\mathcal{C}^\perp) \subset \Psi_m(\mathcal{C})^\perp$. By (i), $\Psi_m(\mathcal{C}^\perp)$ has type 1^{n-k} since $\operatorname{rank}\mathcal{C}^\perp = n-k$, and $\Psi_m(\mathcal{C})^\perp$ has type 1^{n-k} since it is dual to $\Psi_m(\mathcal{C})$ which has type 1^k. Now they have the same type and hence have the same number of codewords. Thus $\Psi_m(\mathcal{C}^\perp) = \Psi_m(\mathcal{C})^\perp$. Finally, H_m is a generator matrix of $\Psi_m(\mathcal{C}^\perp) = \Psi_m(\mathcal{C})^\perp$ by (ii). Thus H_m is a parity check matrix of $\mathcal{C}_m = \Psi_m(\mathcal{C})$. $\square$

Corollary 4.3. *If $\mathcal{C}$ is self-dual, then $\mathcal{C}_m$ is self-dual for every m.*

Proof. It follows from Theorem 4.2(iii) that $(\mathcal{C}_m)^\perp = \Psi_m(\mathcal{C})^\perp = \Psi_m(\mathcal{C}^\perp) = \Psi_m(\mathcal{C}) = \mathcal{C}_m$. □

Theorem 4.4. *Self-dual codes of length n exist over $\mathbb{F}_q[D]$ if and only if self-dual codes of length n exist over $\mathbb{F}_q$.*

Proof. If a matrix G over $\mathbb{F}_q$ generates a self-dual code over $\mathbb{F}_q$, then it generates a self-dual code over $\mathbb{F}_q[D]$ by Theorem 1.12(ii). Conversely, if $\mathcal{C}$ is a self-dual $[n, k]$-code over $\mathbb{F}_q[D]$, then $n = 2k$ and $\Psi_1(\mathcal{C}) = \mathcal{C}_1$ is a self-orthogonal $[n, k]$-code over $\mathbb{F}_q$. The code $\mathcal{C}_1$ has type $1^k = 1^{n/2}$ by Theorem 4.2, and thus $\mathcal{C}_1$ is self-dual. □

For a matrix G over $\mathsf{P} = \mathbb{F}_q[D]$, the projections $\Psi_m(G)$ of G may be viewed as matrices over P. The property of being basic is not preserved by the projections.

Next, we shall show that the minimum distances of projections $\mathcal{C}_m$ are all the same.

Lemma 4.5. *Let $\mathcal{C}$ be a basic code over P. If $\mathbf{v}_m \in \mathcal{C}_m$ then $D^s\mathbf{v}_m \in \mathcal{C}_{m+s}$ for any $s \geq 0$.*

Proof. Let $\mathbf{v}_m \in \mathcal{C}_m$. If $\mathbf{v} \in \mathcal{C}$ is the codeword with $\Psi_m(\mathbf{v}) = \mathbf{v}_m$ then $D^s\Psi_{m+s}(\mathbf{v}) \in \mathcal{C}_{m+s}$ since D^s is in the ring. Then we notice that $\Psi_{m+s}(\mathbf{v}) - \Psi_m(\mathbf{v})$ is a multiple of D^m and hence $D^s\Psi_{m+s}(\mathbf{v}) = D^s\mathbf{v}_m$ in P^n_{m+s} which gives the result. □

If $\mathbf{v}_m = (v_1, \cdots, v_n) \in \mathcal{C}_m$, then $\deg v_i \leq m - 1$ for all i, and thus $D^s\mathbf{v}_m \in \mathcal{C}_{m+s}$ has the same weight as $\mathbf{v}_m \in \mathcal{C}_m$. Therefore, it follows that for any $s \geq 0$

$$d(\mathcal{C}_{m+s}) \leq d(\mathcal{C}_m). \tag{12}$$

Lemma 4.6. *Let $\mathcal{C}$ be a basic code over P. Then we have*

$$\{\mathbf{v} \in \mathcal{C}_{m+s} \mid \Psi_s^{m+s}(\mathbf{v}) = 0\} = D^s\mathcal{C}_m.$$

Proof. View $\Psi_s^{m+s} : \mathcal{C}_{m+s} \to \mathcal{C}_s$ as a map from $\mathcal{C}_{m+s}$ to $\mathcal{C}_s$. We know that Ψ_s^{m+s} is linear and that $\Psi_s^{m+s}(\mathcal{C}) = \mathcal{C}_s$. If $\mathbf{v}_m \in \mathcal{C}_m$ then $D^s\mathbf{v}_m \in \mathcal{C}_{m+s}$ by Lemma 4.5. Since $\Psi_s^{m+s}(D^s\mathbf{v}_m) = 0$, we have $D^s\mathcal{C}_m \subseteq \ker(\Psi_s^{m+s})$. Furthermore, since $\mathcal{C}_s$ has type 1^k for any s, we have $|\mathcal{C}_s| = (q^s)^k$. Thus we have

$$|\ker(\Psi_s^{m+s})| = \frac{|\mathcal{C}_{m+s}|}{|\mathcal{C}_s|} = \frac{q^{(m+s)k}}{q^{sk}} = q^{mk} = |\mathcal{C}_m| = |D^s\mathcal{C}_m|,$$

which gives the result. $\square$

THEOREM 4.7. *Let $\mathcal{C}$ be a basic code over P. Then we have*
i. $d(\mathcal{C}_m) = d(\mathcal{C}_1)$ *for all* m.
ii. $d(\mathcal{C}) \geq d(\mathcal{C}_m)$.

Proof. (i) We use induction on m, so assume that $d(\mathcal{C}_m) = d(\mathcal{C}_1)$. We shall prove that $d(\mathcal{C}_{m+1}) = d(\mathcal{C}_1)$. Taking into account (12), it suffices to show that $d(\mathcal{C}_{m+1}) \geq d(\mathcal{C}_1)$. Suppose, to the contrary, that there exists some nonzero $\mathbf{v} \in \mathcal{C}_{m+1}$ with $\mathrm{wt}(\mathbf{v}) < d(\mathcal{C}_1)$. Then $\mathrm{wt}(\Psi_1^{m+1}(\mathbf{v})) \leq \mathrm{wt}(\mathbf{v}) < d(\mathcal{C}_1)$, which implies $\Psi_1^{m+1}(\mathbf{v}) = 0$. By Lemma 4.6, we can find some nonzero $\mathbf{v}_m \in \mathcal{C}_m$ such that $\mathbf{v} = D\mathbf{v}_m$. Then $0 < \mathrm{wt}(\mathbf{v}_m) = \mathrm{wt}(\mathbf{v}) < d(\mathcal{C}_1) = d(\mathcal{C}_m)$, which is a contradiction.
(ii) If $\mathbf{v} \in \mathcal{C}$, then $\Psi_m(\mathbf{v}) = \mathbf{v}$ for some m. $\square$

There exist codes $\mathcal{C}$ such that $d(\mathcal{C}) > d(\mathcal{C}_1)$. As an example, take the $[n, 1]$-code $\mathcal{C}$ generated by the vector $(1, D, D, \cdots, D)$ over P of length n. Clearly G is basic and $d(\mathcal{C}) = n$. On the other hand, $D^{m-1}(1, D, \cdots, D) = (D^{m-1}, 0, \cdots, 0) \in \mathcal{C}_m$ has the weight 1, and thus $d(\mathcal{C}_m) = 1$ for all m.

5. Number of codewords of minimum weight

LEMMA 5.1. *Let k, n be any positive integers and let M be a $k \times n$ matrix over $\mathsf{P}_m = \mathbb{F}_q[D]/(D^m)$ whose standard form has type*

$$(1)^{k_0}(D)^{k_1}(D^2)^{k_2} \cdots (D^{m-1})^{k_{m-1}}.$$

Then $\ker M = \{\mathbf{v} \in \mathsf{P}_m^n \mid M\mathbf{v}^T = \mathbf{0}\}$ *has cardinality*

$$|\ker M| = (1)^{k_0}(q)^{k_1}(q^2)^{k_2} \cdots (q^{m-1})^{k_{m-1}}(q^m)^{k_m}. \tag{13}$$

Proof. We may assume that M is in standard form as in (5). Then $\mathbf{v} = (\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_m) \in \mathsf{P}_m^n$, where $\mathbf{v}_i \in \mathsf{P}_m^{k_i}$, is in $\ker M$ iff

$$I_{k_0}\mathbf{v}_0^T + A_{01}\mathbf{v}_1^T + \cdots + A_{0,m-1}\mathbf{v}_{m-1}^T + A_{0m}\mathbf{v}_m^T \equiv 0 \pmod{D^m} \tag{14}$$

$$I_{k_1}\mathbf{v}_1^T + \cdots + A_{1,m-1}\mathbf{v}_{m-1}^T + A_{1m}\mathbf{v}_m^T \equiv 0 \pmod{D^{m-1}} \tag{15}$$

$$\vdots$$

$$I_{k_{m-2}}\mathbf{v}_{m-2}^T + A_{m-2,m-1}\mathbf{v}_{m-1}^T + A_{m-2,m}\mathbf{v}_m^T \equiv 0 \pmod{D^2} \tag{16}$$

$$I_{k_{m-1}}\mathbf{v}_{m-1}^T + A_{m-1,m}\mathbf{v}_m^T \equiv 0 \pmod{D}. \tag{17}$$

From these equations, we can see that $\mathbf{v}_m \in \mathsf{P}_m^{k_m}$ can be set to be an arbitrary vector, and then (17) determines $\mathbf{v}_{m-1} \pmod{D}$ in a unique way, and then (16) determines $\mathbf{v}_{m-2} \pmod{D^2}$ in a unique way, and so on. Therefore,

$$|\ker M| = (q^m)^{k_m} \times (q^{m-1})^{k_{m-1}} \times \cdots \times (q^1)^{k_1} \times (q^0)^{k_0},$$

which gives the result. □

Let $\mathcal{C}$ be a basic $[n, k, d_\infty]$ code over P. Fix a parity check matrix H of the code $\mathcal{C}$ over P. We now introduce some notations. If $S = \{i_1, \cdots, i_s\}$ is a subset of $\{1, 2, \cdots, n\}$ and $\mathbf{v}$ is a vector of length n, then $\mathbf{v}_S$ denotes the vector of length s obtained from $\mathbf{v}$ by puncturing components outside S. For a given S as above and a vector $\mathbf{y} = (y_1, \cdots, y_s)$ of length s, $\mathbf{y}^S$ denotes the vector of length n obtained by adjoining 0's outside S, i.e., $\mathbf{y}^S = (x_1, x_2, \cdots, x_n)$ where $x_i = 0$ if $i \notin S$, and $x_{i_j} = y_j$ if $i_j \in S$. For a matrix $M = (\mathbf{m}_i)$, where $\mathbf{m}_i$ denotes the i-th column of M, let $M[S] = (\mathbf{m}_i)_{i \in S}$ be the matrix whose columns are the i-th columns of M for $i \in S$.

Let d be the minimum distance of $\mathcal{C}_1$. For each subset $S \subset \{1, 2, \cdots, n\}$ of d elements, let $H_m[S]'$ denote the standard form of $H_m[S]$. Since $\Psi_m^r(\mathsf{P}_r^*) = \mathsf{P}_m^*$ for $r > m$, we have that

$$\Psi_m^r(H_r[S]') = H_m[S]' \tag{18}$$

for all $r > m$. Since any $d-1$ columns of H_1 are independent over $\mathbb{F}_q$, any matrix consisting of $d-1$ columns of H_m has type 1^{d-1}. Thus $H_m[S]$ will have type $1^{d-1}(0)^1$ or $1^{d-1}(D^j)^1$ for some $j \geq 0$. We divide the subsets S into two classes:

(I) For any m, $H_m[S]$ has type $1^{d-1}0^1$.
(II) For some $m = m(S)$, $H_m[S]$ has type $1^{d-1}(D^j)^1$ for some $0 \leq j < m$.

If S is of class (II) so that $H_m[S]$ has type $1^{d-1}(D^j)^1$, then $H_r[S]$ has the same type $1^{d-1}(D^j)^1$ for all $r > j$, while $H_r[S]$ has type $1^{d-1}0^1$ for all $r \leq j$.

Theorem 5.2. *$H_m[S]$ has type $1^{d-1}0^1$ for all m iff $d \times d$ minors of $H[S]$ are all zero.*

Proof. Suppose S is of class (I). Then the $d \times d$ minors of $H_m[S]$ are all zero, since the property that determinant being zero is invariant under the operations (R1), (R2), (R3) and (C1). The minors of $H_m[S]$ are images of minors of $H[S]$ under Ψ_m. For any matrix M with entries in

P, $\det M \equiv 0 \pmod{D^m}$ for all m implies that $\det M = 0$. Thus all $d \times d$ minors of $H[S]$ are zero. The converse is clear. $\square$

Let

$$\mu_{-\infty} = |\{S \mid S \text{ is of class (I)}\}|. \tag{19}$$

Let N be the maximum of $m(S)$'s for S of class (II) and then let for $j \geq 0$

$$\mu_j = |\{S \mid H_N[S] \text{ has type } 1^{d-1}(D^j)^1\}| \tag{20}$$

THEOREM 5.3. *The number $A_{m,d}$ of codewords of weight d in $\mathcal{C}_m$ is given as follows.*

$$A_{m,d} = \left(\mu_{-\infty} + \sum_{j \geq m} \mu_j\right)(q^m - 1) + \sum_{j=1}^{m-1} \mu_j (q^j - 1). \tag{21}$$

Proof. Let D be the set of all codewords of weight d in $\mathcal{C}_m$, and

$$E_S = \{\mathbf{y}^S \mid 0 \neq y \in \ker H_m[S]\}$$

for the subsets S of d elements. Here $\ker H_m[S] = \{\mathbf{v} \in (\mathsf{P}_m)^{|S|} \mid H_m[S]\mathbf{v}^T = 0\}$. Clearly $(\mathbf{v}_S)^S = \mathbf{v}$ for any codeword $\mathbf{v}$, where $S = \operatorname{supp}(\mathbf{v})$. Thus D is a subset of $\cup_S E_S$. Since $\operatorname{wt}(\mathbf{y}^S) = \operatorname{wt}(\mathbf{y})$ and d is the minimum distance of $\mathcal{C}_m$, we have $\operatorname{wt}(\mathbf{y}) = \operatorname{wt}(\mathbf{y}^S) = d$ whenever $0 \neq \mathbf{y} \in \ker(H_e[S])$. Thus $D = \cup_S E_S$. Furthermore, if $\operatorname{wt}(\mathbf{y}_1) = \operatorname{wt}(\mathbf{y}_2) = d$, then it is clear that $\mathbf{y}_1^{S_1} = \mathbf{y}_2^{S_2}$ iff $\mathbf{y}_1 = \mathbf{y}_2$ and $S_1 = S_2$. Therefore $\cup_S E_S$ is a disjoint union and $|E_S| = |\ker H_m[S]|$.

If S is of class (II) and $H_N[S]$ has type $1^{d-1}(D^j)^1$ with $1 \leq j \leq m-1$ then $|\ker H_m[S]| = q^j$ by Lemma 5.1. On the other hand, and if S is of class (I) or if S is of class (II) such that $H_N[S]$ has type $1^{d-1}(D^j)^1$ with $j \geq m$, then $H_m[S]$ has type $1^{d-1}0^1$ and $|\ker H_m[S]| = q^m$. Finally, if S is of class (II) such that $H_N[S]$ has type 1^d, then $H_m[S]$ has type 1^d and $|\ker H_m[S]| = 1$. The theorem is proved. $\square$

COROLLARY 5.4. *For $m > N$, $A_{m,d} = aq^m + b$, where a, b are independent of m. In other words, $A_{m,d}$ is a linear polynomial in $Q = q^m$, independent of m.*

Proof. Simply let $a = \mu_{-\infty}$, and $b = \sum_{j=1}^{N} \mu_j (q^j - 1) - \mu_{-\infty}$. $\square$

It is easy to check that

$$A_{m+1,d} - A_{m,d} = (q^{m+1} - q^m)\left(\mu_{-\infty} + \sum_{j \geq m+1} \mu_j\right). \tag{22}$$

From this equation, we obtain the following corollaries.

Corollary 5.5. *If $A_{m,d} = A_{m+1,d}$ for some m, then $A_{m+s,d} = A_{m,d}$ for all $s \geq 0$.*

Corollary 5.6. *Suppose $\mu_{-\infty} = 0$. Then $A_{m,d} = A_{N,d}$ for all $m \geq N$. In particular, every codeword of weight d in $\mathcal{C}_m$ has the form $D^{m-N}\mathbf{v}_0$ for some codeword $\mathbf{v}_0$ of weight d in $\mathcal{C}_N$.*

Similar results and examples for the p-adic codes can be found in [1].

References

[1] S. T. Dougherty, S. Y. Kim, and Y. H. Park, *Lifted Codes and their Weight Enumerators*, submitted, 2004.

[2] R. J. McEliece, *The algebraic theory of convolutional codes*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Elsevier, Amsterdam, 1998, 1165–1138.

[3] E. Rains and N. J. A. Sloane, *Self-dual codes*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Elsevier, Amsterdam, 1998, 177–294.

[4] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math **121**, 1999, 555–575

Department of Mathematics
Kangwon National University
Chuncheon, Korea 200-701
E-mail: yhpark@kangwon.ac.kr