Kangweon-Kyungki Math. Jour. **15** (2007), No. 1, pp. 79–85

BASIC CODES OVER POLYNOMIAL RINGS

Young Ho Park

Abstract. We study codes over the polynomial ring $\mathbb{F}_q[D]$ and introduce the notion of basic codes which play a fundamental role in the theory.

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 submodule of the ambient space 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 in that vector. 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. See [2] for general theory on codes and [3] on self-dual codes.

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 June 04, 2007.
2000 Mathematics Subject Classification: 94B10, 94B05.
Key words and phrases: linear codes, codes over polynomial rings.

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, i.e., $\mathsf{P}_m^* = \{a_0 + a_1 D + a_2 D^2 + \cdots + a_{m-1} D^{m-1} \mid a_0 \neq 0\}$. 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 $\mathcal{C}$ of length over P, we have*

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

Proof. Let $\mathbf{g}_1, \cdots, \mathbf{g}_k$ be the rows of a generator matrix of $\mathcal{C}$, and let $\hat{\mathcal{C}} = \mathcal{C} \otimes_{\mathbb{F}_q[D]} \mathbb{F}_q(D)$ be the code generated by $\{\mathbf{g}_i\}$ over the quotient field $\mathbb{F}_q(D)$ of $\mathsf{P} = \mathbb{F}_q[D]$. Thus $\operatorname{rank} \hat{\mathcal{C}} = \dim_{\mathbb{F}_q(D)} \hat{\mathcal{C}} = k$. Since $\hat{\mathcal{C}}$ is a code over a field, we know that $\dim_{\mathbb{F}_q(D)} \hat{\mathcal{C}}^\perp = n - k$, where

$$\hat{\mathcal{C}}^\perp = \{\mathbf{v} \in \mathbb{F}_q(D)^n \mid [\mathbf{v}, \mathbf{g}_i] = 0 \text{ for all } i\}.$$

It is easy to check that the "integral" vectors $\mathbf{f}_1, \cdots, \mathbf{f}_k \in \mathsf{P}^n$ are linearly independent over $\mathbb{F}_q(D)$ iff they are linearly independent over P. Note that $\hat{\mathcal{C}}^\perp \cap \mathsf{P}^n \subset \mathcal{C}^\perp$. Let $\hat{\mathbf{h}}_1, \cdots, \hat{\mathbf{h}}_{n-k} \in \mathbb{F}_q(D)^n$ be a basis for $\hat{\mathcal{C}}^\perp$. There are elements $\beta_i \in \mathsf{P}$ such that $\beta_i \hat{\mathbf{h}}_i \in \mathsf{P}^n$. Thus the $\beta_i \hat{\mathbf{h}}_i$ are in $\mathcal{C}^\perp$ and they are linearly independent over P as well as over $\mathbb{F}_q(D)$. Hence $n - k \leq \operatorname{rank} \mathcal{C}^\perp$. Conversely, if $\mathbf{h}_1, \cdots, \mathbf{h}_s$ is a basis for $\mathcal{C}^\perp$, then they are in $\hat{\mathcal{C}}^\perp$ and linearly independent over $\mathbb{F}_q(D)$. Thus $\operatorname{rank} \mathcal{C}^\perp \leq n - k$. The lemma is proved. □

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 $n = 2k$.

2. Basic codes

For codes $\mathcal{C}$ over P, which are codes 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 2.1. A code $\mathcal{C}$ over P is said to be *basic* if $\mathcal{C} = (\mathcal{C}^\perp)^\perp$.

LEMMA 2.2. *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. □

THEOREM 2.3. *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). □

REMARK. Theorem 2.3 is true for any code of finite rank over a principal ideal domain.

COROLLARY 2.4. *A code $\mathcal{C}$ over P is basic iff $\mathcal{C}$ 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. □

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. For example, take

$$H_0 = \begin{pmatrix} 1 & D & 1 \\ D & 1 & 1 \end{pmatrix}.$$

The rank of the code $\mathcal{C}_1$ generated by H_0 is 2, and thus $\mathcal{C}(H_0) = {\mathcal{C}_1}^\perp$ will have rank $3-2=1$. A straightforward computation yields $\mathcal{C}(H_0) = \langle(1, 1, -(D+1))\rangle$ and

$$\mathcal{C}(H_0)^\perp = \{((D+1)\gamma - \beta, \beta, \gamma) \mid \beta, \gamma \in \mathsf{P}\}.$$

Therefore we see that H_0 is not a parity check matrix of $\mathcal{C}(H_0)$ since it does not generate the codeword $(-1, 1, 0) \in \mathcal{C}(H_0)^\perp$, for example. A parity check matrix of $\mathcal{C}(H_0)$ can be given by

$$\begin{pmatrix} -1 & 1 & 0 \\ D+1 & 0 & 1 \end{pmatrix}, \text{ or } \begin{pmatrix} -1 & 1 & 0 \\ D & 1 & 1 \end{pmatrix}.$$

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

$$\mathbf{u} = c(\mathbf{u})\mathbf{u}_0, \text{ with } c(\mathbf{u}_0) = 1.$$

Lemma 2.5. *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 $c(\mathbf{g}_{i_0}) = 1$. □

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 2.6. *Let G be a generator matrix of an $[n, k]$-code $\mathcal{C}$ over P. Then $\mathcal{C}$ is basic iff one of the following conditions 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) $\iff$ (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) $\iff$ (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 $c(\mathbf{u}) = c(\mathbf{u}G)$. □

3. Characterizations of basic codes

We now recall the definitions and facts about basic matrices over P, which play important roles in the theory of convolutional codes.

DEFINITION 3.1. 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 [1].

Theorem 3.2. *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 3.3. *Let G be a generator matrix of a convolutional code $\mathcal{C}$. Then $\mathcal{C}$ is basic iff 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 2.6 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 3.2(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 3.4. *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 3.2(ii) and the fact that the minors for G_1 and G_2 are the same up to ± 1. □

Example 3.5. The matrices in this example are taken from [1]. Let

$$G_4 = \begin{pmatrix} 1 & D & 1+D & 1 \\ 0 & 1+D & D & 0 \end{pmatrix}$$

be a matrix over $\mathbb{F}_2[D]$. The matrix G_4 is basic since G has $1 = \det I_2$ as a 2×2 minor. By Theorem 3.3, G_4 generates a basic code $\mathcal{C}$. Let

$$G_5 = \begin{pmatrix} 1+D & 0 & 1 & D \\ D & 1+D+D^2 & D^2 & 1 \end{pmatrix}.$$

For $\mathbf{u} = (1 + D, 1)$, $\mathbf{u}G_5 = (1 + D + D^2)(1, 1, 1, 1)$. Thus the code generated by G_5 is not basic by Theorem 2.6. Nevertheless, we note that the matrices G_4 and G_5 generate the same code over $\mathbb{F}_2(D)$, the quotient field of $\mathbb{F}_2[D]$.

THEOREM 3.6. 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 2.2 that $\alpha\mathbf{v} \in \mathcal{C}$ for some $\alpha \in \mathsf{P}$. As $\mathcal{C}$ is basic, we have $\mathbf{v} \in \mathcal{C}$. □

References

[1] 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.
[2] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
[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.

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