No. 148 (82-15)

A Method to Construct Primitive Orthogonal Idempotents by Eigen Polynomials — For Cyclic and Abelian Codes

by

Iwaro Takahashi

March 1982

§ Introduction

Theories on error correcting codes play important roles for space communications and design of computers and other information processors. This paper gives basic theories for error correcting codes, especially cyclic codes and Abelian codes.

§1 eigen polynomials on polynomial rings

Let GF(q)[x] be the totality of polynomials in x over GF(q), the finite field of size q, q being a prime power. We consider a polynomial $g(x) \in GF(q)[x]$ of degree n, and the ring R = GF(q)[x] mod g(x). We can represent elements of R by polynomials of degree n-1.

Let us assume that g(x) has no multiple factors, then it is well known that R is a semisimple ring [1]. We often encounter the case $g(x) = x^n-1$ in coding theories. In this case if n and q are relatively prime g(x) has no multiple factors. And ideals of R are cyclic codes.

Let $GF(q^m)$ be the splitting field of g(x), i.e. $GF(q^m)$ is the smallest extension field of GF(q) containing all roots of g(x) = 0. And consider $\overline{R} = GF(q^m)[x]$ mod g(x) which contains R.

If a non zero polynomial

$$(1.1) \qquad \rho(x) = \rho_0 + \rho_1 x + \dots + \rho_{n-1} x^{n-1} \in \overline{R}$$

satisfies the equation

$$(1.2) \qquad x\rho(x) = \lambda\rho(x), \qquad \lambda \in GF(q^m)$$

Then $\rho(x)$ is called an eigen polynomial of the transform x on $\overline{R}$ and λ is called its eigen value.

Theorem 1 The transform x on $\overline{R}$ has n distinct eigen values $\lambda_i \in GF(q^m)$ (i=1, ..., n) which are roots of g(x) = 0, and corresponding eigen polynomials $\theta_i(x)$ (i=1, ..., n) have the following properties,

$$(1.3) \qquad \theta_i(x)\,\theta_j(x) = \delta_{ij}\,\theta_i(x), \quad i, j=1, \dots, n \text{ (orthogonal idempotents)}$$

$$(1.4) \qquad \theta_i(\lambda_j) = \delta_{ij}$$

(1.5) $\theta_1(x) + \dots + \theta_n(x) = 1$ (summed up to unity)

where δ_{ij} is Kronecker's delta, i.e. $\delta_{ij} = 1$ if $i=j$ and $\delta_{ij} = 0$ if $i\neq j$.

Proof Let $g(x) = x^n - g_{n-1}x^{n-1} - \dots - g_1x - g_0$. Writing the condition (1.2) in the matrix form (for n=5, for simplicity) we have

$$(1.6)\qquad \begin{pmatrix} -\lambda & 0 & 0 & 0 & g_0 \\ 1 & -\lambda & 0 & 0 & g_1 \\ 0 & 1 & -\lambda & 0 & g_2 \\ 0 & 0 & 1 & -\lambda & g_3 \\ 0 & 0 & 0 & 1 & g_4-\lambda \end{pmatrix} \begin{pmatrix} \rho_0 \\ \rho_1 \\ \rho_2 \\ \rho_3 \\ \rho_4 \end{pmatrix} = 0$$

Clearly the determinant of the matrix in (1.6) is equal to $g(\lambda)$. So the proper equation $g(x) = 0$ has n distinct roots $\lambda_1, \dots, \lambda_n$ in $GF(q^m)$ because of $g(x)$ having no multiple factors.

Now multiplying by $\theta_j(x)$ both sides of $\lambda_i\theta_i(x) = x\,\theta_i(x)$ we have

$$\lambda_i\theta_j(x)\theta_i(x) = x\theta_j(x)\theta_i(x) = \lambda_j\theta_j(x)\theta_i(x),$$

$$(\lambda_j-\lambda_i)\theta_j(x)\theta_i(x) = 0$$

So $\theta_i(x)\theta_j(x)=0$ if $i\neq j$. Letting $\theta_i(x)$ be

(1.7) $\theta_i(x) = \theta_{i0} + \theta_{i1}x + \dots + \theta_{i,n-1}x^{n-1}, \quad \theta_{ij} \in GF(q^m)$

we have

$$(1.8)\qquad \theta_i^2(x) = \theta_{i0}\theta_i(x) + \theta_{i1}\,x\theta_i(x) + \dots + \theta_{i,n-1}x^{n-1}\theta_i(x)$$

$$= (\theta_{i0} + \theta_{i1}\lambda_i + \dots + \theta_{i,n-1}\lambda_i^{n-1})\ \theta_i(x) = \sigma\theta_i(x)$$

where $\sigma = \theta_{i0} + \theta_{i1}\lambda_i + \dots + \theta_{i,n-1}\lambda_i^{n-1} \in GF(q^m)$. The value of σ is not zero. Because; let $\sigma=0$ then $\theta_i^2(x) = 0$ from (1.8), so $g(x)$ must devide $\theta_i^2(x)$ in $GF(q^m)[x]$. But $g(x)$ has no multiple factors, so $g(x)$ must devide $\theta_i(x)$ too, but this is imposible for $\theta_i(x)$ is not zero and has a lower degree than $g(x)$.

Of course a scalor multiple of an eigen polynomial is agin an eigen polynomial, so if $\sigma \neq 1$ in (1.8) then $\sigma^{-1}\theta_i(x)$ is an idempotent. So we have (1.3).

Now from (1.3) we have $\theta_i(x)\ (\theta_i(x)-1) = 0$ which states that $\theta_i(x)$ takes values only zero or unity in $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$. And from $(x-\lambda_i)\theta_i(x) = 0$ we have $\theta_i(\lambda_j) = 0$ for $i \neq j$. But if $\theta_i(\lambda_i) = 0$ then $\lambda_i(x)$ takes zero at n points $\lambda_1, \ldots, \lambda_n$ in $GF(q^m)$ therefore $\theta_i(x)$ must vanish. So $\theta_i(\lambda_i)$ must be unity. This proves (1.4).

Next from (1.4) $\theta_1(x) + \theta_2(x) + \ldots + \theta_n(x)$ with degree n-1 in $GF(q^m)[x]$ takes unity at n points $\lambda_1, \ldots, \lambda_n \in GF(q^m)$, therefore it must be uniformly unity which proves (1.5). ————

Incidentally viewing $\overline{R}$ as a vector space on $GF(q^m)$ we can say that $\theta_1(x), \ldots, \theta_n(x)$ are linearly independent because of their orthogonality. So every $\rho(x) \in \overline{R}$ is expressed on the basis $\theta_1(x), \ldots, \theta_n(x)$ such that

$$(1.9) \qquad \rho(x) = \alpha_1\theta_1(x) + \alpha_2\theta_2(x) + \ldots + \alpha_n\theta_n(x), \quad \alpha_i \in GF(q^m)$$

Multiplying the both sides of (1.9) by $\theta_i(x)$ we have

$$(1.10) \qquad \alpha_i\theta_i(x) = \rho(x)\ \theta_i(x)$$

$$= \rho_0 + \rho_1\lambda_i + \rho_2\alpha_i^2 + \ldots + \rho_{n-1}\lambda_i^{n-1}\ \theta_i(x) = \rho(\lambda_i)\theta_i(x), \ i=1, \ldots, n$$

$$\alpha_j = \rho(\lambda_j)$$

The product of any two elements, say, $\rho(x) = \alpha_1\theta_1(x) + \alpha_2\theta_2(x) + \ldots + \alpha_n\theta_n(x)$ and $\eta(x) = \beta_1\theta_1(x) + \ldots + \beta_n\theta_n(x)$ must be

(1.11) $\rho(x)\eta(x) = \alpha_1\beta_1\theta_1(x) + \alpha_2\beta_2\theta_2(x) + \dots + \alpha_n\beta_n\theta_n(x)$

because $\theta_i(x)$'s are orthogonal idempotents. And of course we have

(1.12) $\rho(x) + \eta(x) = (\alpha_1+\beta_1)\theta_1(x) + (\alpha_2+\beta_2)\theta_2(x) + \dots + (\alpha_n+\beta_n)\theta_n(x).$

From these we can easily conclude that $\overline{R}$ is isomorphic to the n-ply direct product $GF(q^m)$ that is $\overline{R} \cong GF(q^m) \times \dots \times GF(q^m)$.

Further it is clear that $\theta_i(x)\ \overline{R}$ is a minimal ideal of $\overline{R}$ because every element of $\theta_i(x)\ \overline{R}$ is a scalor multiple of $\theta_i(x)$ so $\theta_i(x)\ \overline{R}$ is one-dimensional subspace of $\overline{R}$. So $\theta_1(x), \dots, \theta_n(x)$ are primitive orthogonal idempotents in $\overline{R}$. But our purpose is to find primitive orthogonal idempotents in R.

§2 Primitive orthogonal idempotents in mono-variate polynomial rings —— for cyclic codes

Let denote by Σ the set of all roots of $g(x) = 0$. Thus

(2.1) $\Sigma = \{\lambda_1, \dots, \lambda_n\} \subseteqq GF(q^m)$

Let us call the transform on $GF(q^m)$

(2.2) $\xi \to \xi^q$

Frobenius transform and the set $\{\xi, \xi^q, \xi^{q^2}, \dots, \xi^{q^k}\}$ ($\xi^{q^{k+1}} = \xi$ and $\xi^{q^i} \neq \xi$ for $i \leqq k$) a Frobenius cycle [4]. Incidentally we call the total of elements of the Frobenius cycle including α the trace of α, and denote it by $tr(\alpha)$, i.e.,

(2.3) $tr(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^k}$

Now let us factor $g(x)$ into irreducible polynomials $p_1(x)$, $p_2(x)$, ..., and $p_c(x)$ with degree n_1, n_2, ... and n_c respectively over GF(q), i.e.,

$$(2.4) \qquad g(x) = p_1(x)\ p_2(x)\ \dots\ p_c(x), \quad n = n_1+n_2+\dots+n_c$$

where $p_1(x)$, $p_2(x)$, ..., $p_c(x)$ are different from each other because $g(x)$ has no multiple factors.

It is well known that Σ is decomposed into c Frobenious cycles Σ_1, Σ_2, ..., Σ_c and Σ_i is composed of the all roots of $p_i(x) = 0$ and so $|\Sigma_i| = n_i$, $i=1, \dots, c$. Further for notational conveniences let $N_i = \{j \in \{1,2, \dots, n\} \,|\, \lambda_j \in \Sigma_i\}$, then we have the following theorem which is one of our main results.

<u>Theorem 2</u> Though $\theta_1(x)$, ..., $\theta_n(x)$ are in $\overline{R}$,

$$(2.5) \qquad e_i(x) = \sum_{j \in N_i} \theta_j(x), \quad i=1, \dots, c.$$

are polynomials in R, and are orthogonal idempotents and summed up to unity. Further

$$(2.6) \qquad \begin{aligned} e_i(\lambda_j) &= 1 \qquad \text{if} \quad \lambda_j \in \Sigma_i \\ &= 0 \qquad \text{if} \quad \lambda_j \notin \Sigma_i \end{aligned}$$

<u>proof</u> From (1.3), (1.5) it is clear that $e_1(x)$, ..., $e_c(x)$ are orthogonal idempotents and summed up to unity. Further from (1.4) and (2.5) we have (2.6).

The main difficulty is to show that $e_i(x) \in R$, that is, in the form

$$(2.7) \qquad e_i(x) = e_{i0} + e_{i1}x + \dots + e_{i,n-1}\, x^{n-1}, \quad i=1, \dots, c,$$

e_{ij} ($j=0, \ldots, n-1$, $i=1, \ldots, c$) are all in GF(q).

First let us note that for any $n \times n$ matrix $A = (\alpha_{ij})$ ($\alpha_{ij} \in GF(q^m)$) its determinant $|A|$ has the following property,

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{vmatrix}^q = \begin{vmatrix} \alpha_{11}^q & \alpha_{12}^q & \cdots & \alpha_{1n}^q \\ \alpha_{21}^q & \alpha_{22}^q & \cdots & \alpha_{2n}^q \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1}^q & \alpha_{n2}^q & \cdots & \alpha_{nn}^q \end{vmatrix} . \tag{2.8}$$

Let $|A| = \Sigma \, \varepsilon \, \alpha_{1i_1} \alpha_{2i_2} \cdots \alpha_{ni_n}$, where $\varepsilon = \pm 1$, and $|A|^q = \Sigma \varepsilon^q \alpha_{1i_1}^q \alpha_{2i_2}^q \cdots \alpha_{ni_n}^q$. If $q = p^s$ (p being prime) and p is odd then $\varepsilon^q = \varepsilon$, and if $p=2$ then $-1 = +1$. In any case $\varepsilon^q = \varepsilon$, so we have (2.8).

Let us assume that $\lambda_1, \ldots, \lambda_n$ are ordered and decomposed into $\Sigma_1, \Sigma_2, \ldots, \Sigma_c$ such that

$$\left\{ \begin{array}{ll} \Sigma_1 = \{\lambda_1, \lambda_2 = \lambda_1^q, \lambda_3 = \lambda_2^q, \ldots, \lambda_{n_1} = \lambda_{n_1-1}^q\} & (\lambda_1 = \lambda_{n_1}^q) \\ \Sigma_2 = \{\lambda_{n_1+1}, \lambda_{n_1+2} = \lambda_{n_1+1}^q, \ldots, \lambda_{n_1+n_2} = \lambda_{n_1+n_2-1}^q\} & (\lambda_{n_1+1} = \lambda_{n_1+n_2}^q) \\ \cdots\cdots\cdots\cdots & \\ \Sigma_c = \{\lambda_{N_c+1}, \lambda_{N_c+2} = \lambda_{N_c+1}^q, \ldots, \lambda_n = \lambda_{n-1}^q\} & (\lambda_{N_c+1} = \lambda_n^q) \end{array} \right. \tag{2.9}$$

where $N_c = n_1 + \ldots + n_{c-1}$.

Now for $i=1$ we write down (2.6) in the form of (2.7) and (2.9) then we have

$$
(2.10)\qquad
\left[\begin{array}{ccccc}
1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{n-1} \\
1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^{n-1} \\
\multicolumn{5}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\
1 & \lambda_{n_1} & \lambda_{n_1}^2 & \cdots & \lambda_{n_1}^{n-1} \\
\hline
1 & \lambda_{n_1} & \lambda_{n_1+1}^2 & \cdots & \lambda_{n_1+1}^{n-1} \\
1 & \lambda_{n_1+2} & \lambda_{n_1+2}^2 & \cdots & \lambda_{n_1+1}^{n-1} \\
\multicolumn{5}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\
1 & \lambda_{n_1+n_2} & \lambda_{n_1+n_2}^2 & \cdots & \lambda_{n_1+n_2}^{n-1} \\
\hline
\multicolumn{5}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\
\hline
1 & \lambda_{N_c+1} & \lambda_{N_c+1}^2 & \cdots & \lambda_{N_c+1}^{n-1} \\
1 & \lambda_{N_c+2} & \lambda_{N_c+1}^2 & \cdots & \lambda_{N_c+2}^{n-1} \\
\multicolumn{5}{c}{\cdots\cdots\cdots\cdots\cdots\cdots} \\
1 & \lambda_n & \lambda_n^2 & & \lambda_n^{n-1}
\end{array}\right]
\left[\begin{array}{c}
e_{10} \\ e_{11} \\ \vdots \\ \vdots \\ e_{1,n-1}
\end{array}\right]
=
\left[\begin{array}{c}
1 \\ 1 \\ \vdots \\ 1 \\ \hline 0 \\ 0 \\ \vdots \\ 0 \\ \hline \vdots \\ \hline 0 \\ 0 \\ \vdots \\ 0
\end{array}\right].
$$

Let denote by Δ the determinant of the matrix in the left hand side of (2.10), and by Δ_j the determinant obtained from Δ by changing the j-th column with the right hand side vector in (2.10). Then $e_{1j} = \Delta_j/\Delta$, so $e_{1j}^q = \Delta_j^q/\Delta^q$. From (2.8) and (2.9) we can state that Δ^q and Δ_j^q incur only the same permutations of rows. So we have

$$(2.11)\qquad e_{1j}^q = \Delta_j^q/\Delta^q = \Delta_j/\Delta = e_{1j}, \quad j=1, \ldots, n$$

which proves $e_{1j} \in GF(q)$ (see e.g. [4]).

We can prove that $e_{ij} \in GF(q)$, i=2, 3, ... with the same way.

Theorem 3 For each i=1, ..., c the ideal

$$(2.12) \qquad e_i(x)\ R = \{e_i(x)\ f(x) \mid f(x) \in R\}$$

coincides with the ideal $q_i(x)$ R, where $q_i(x) = g(x)/p_i(x)$, therefore it is a minimal ideal of R. Thus $e_1(x), \ldots, e_c(x)$ are primitive orthogonal idempotents.

proof For any root λ of $q_i(x) = p_1(x) \ldots p_{i-1}(x)\ p_{i+1}(x) \ldots p_c(x) = 0$ we have $e_i(\lambda) = 0$ from (2.6). So $q_i(x)$ divides $e_i(x)$, that is $e_i(x) \in q_i(x)$ R. But $q_i(x)$ R is a minimal, so $e_i(x)\ R = q_i(x)\ R$ ___ .

Thus the formula (2.5) in Theorem 2 gives us the simple algorithm to find orthogonal primitive idempotents of R.

Example 1 Let R = GF(3)[x] mod g(x), GF(3) = {0, 1, 2} mod 3, and $g(x) = x^6 + x^5 + 2x^4 + 2x^3 + x^2 + x + 2 = (x^3 + 2x + 1)(x^3 + x^2 + 2)$, where $p_1(x) = x^3 + 2x + 1$ and $p_2(x) = x^3 + x^2 + 2$ are irreducible over GF(3). The splitting field of g(x) is $GF(3^3)$. Let α be the primitive elment of $GF(3^3)$ satisfying $\alpha^3 = 2+\alpha$. Then

$\Sigma_1 = \{\lambda_1=\alpha,\ \lambda_2=\alpha^3,\ \lambda_3=\alpha^9\}$: the set of roots of $p_1(x) = 0$

$\Sigma_2 = \{\lambda_4=\alpha^4, \lambda_5=\alpha^{12},\ \lambda_6=\alpha^{10}\}$: the set of roots of $p_2(x) = 0$.

By (1.2) or (1.6) we can easily obtain the coefficients of the eigen polynomial $\theta_j(x)$ corresponding to λ_j, j=1, 2, ..., 6, which are shown in Table I, and using (2.5) we get $e_i(x)$ (i=1, 2) from $\theta_j(x)$ (j=1, ..., 6). The coffeicients of $e_i(x)$ are also shown in Table I.

Table I

	1	x	x^2	x^3	x^4	x^5	
$\lambda_1=\alpha$	α^6	α^{21}	α^2	α^{18}	α^{16}	α^7	$\theta_1(x)$
$\lambda_2=\alpha^3$	α^{18}	α^{11}	α^6	α^2	α^{22}	α^{21}	$\theta_2(x)$
$\lambda_3=\alpha^9$	α^2	α^7	α^{18}	α^6	α^{14}	α^{11}	$\theta_3(x)$
	2	2	2	2	0	2	$e_1(x)$
$\lambda_4=\alpha^4$	α^4	α^{20}	α^{25}	α^{24}	1	α^8	$\theta_4(x)$
$\lambda_5=\alpha^{12}$	α^{12}	α^8	α^{23}	α^{20}	1	α^{24}	$\theta_5(x)$
$\lambda_6=\alpha^{10}$	α^{10}	α^{24}	α^{17}	α^8	1	α^{20}	$\theta_6(x)$
	2	1	1	1	0	1	$e_2(x)$

Note that for each k the coefficients of x^k in $\theta_j(x)$ $(j \in N_i)$ constitute the Frobenius cycle, so the coefficients in $e_i(x)$ is the trace of the one in $\theta_j(x)$.

Example 2 Let $R = GF(2)[x] \bmod (x^{15}-1)$, $GF(2) = \{0, 1\} \bmod 2$, and $x^{15} - 1 = (x + 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)$, where

$$p_1(x) = x + 1, \quad p_2(x) = x^2 + x + 1,$$

$$p_3(x) = x^4 + x^3 + x + 1,$$

$$p_4(x) = x^4 + x + 1, \quad p_5(x) = x^4 + x^3 + 1$$

are irreducible over GF(2). The splitting field of $x^{15}-1$ is $GF(2^4)$.

Let α be the primitive element of $GF(2^4)$ satisfying $\alpha^4 = \alpha + 1$. Then

$$\Sigma_1 = \{\lambda_1 = \alpha^0 = 1\}$$

$$\Sigma_2 = \{\lambda_2 = \alpha^5,\ \lambda_3 = \alpha^{10}\}$$

$$\Sigma_3 = \{\lambda_4 = \alpha^3,\ \lambda_5 = \alpha^6,\ \lambda_6 = \alpha^{12},\ \lambda_7 = \alpha^9\}$$

$$\Sigma_4 = \{\lambda_8 = \alpha,\ \lambda_9 = \alpha^2,\ \lambda_{10} = \alpha^4,\ \lambda_{11} = \alpha^8\}$$

$$\Sigma_5 = \{\lambda_{12} = \alpha^7,\ \lambda_{13} = \alpha^{14},\ \lambda_{14} = \alpha^{13},\ \lambda_{15} = \alpha^{11}\}$$

As in Example 1 we get coefficient, of $\theta_j(x)$ ($j = 1 \sim 15$) and $e_i(x)$ ($i=1, \ldots, 6$) in Table II. These five primitive orthogonal idempotents are shown in the example (on page 54) of [5] which are constructed by step-by-step algorithms.

It is easily seen that in the case of $g(x) = x^n - 1$, i.e. the cyclic code case, the coefficient of x^{n-1} in $\theta_j(x)$ is always its eigen value θ_j and that of x^{n-k} is λ_j^k. So we have only to calculate the trace (or its scalor multiple) of λ_j, λ_j, λ_j^2, λ_j^3, ..., λ_j^{n-1} ($\lambda_j \in \Sigma_i$) in order to get the coefficients of x^{n-1}, x^{n-2}, ..., x and 1 in $e_i(x)$ respectively.

§3 primitive orthogonal idempotents in multivariate polynomial rings ——— for Abelian codes

Here we confine ourselves to consider the ring

(3.1) $R = GF(q)[x_1, x_2, \ldots, x_n] \bmod (g_1(x_1), g_2(x_2), \ldots, g_n(x_n))$

More generally we might consider the ring

Table II

	1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}	x^{14}	
$\lambda_1=\alpha^0$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	$e_1(x)=\theta_1(x)$
$\lambda_2=\alpha^5$	1	α^{10}	α^5	1	α^{10}	α^5	1	α^{10}	α^5	1	α^{10}	α^5	1	α^{10}	α^5	$\theta_2(x)$
$\lambda_3=\alpha^{10}$	1	α^5	α^{10}	1	α^5	α^{10}	1	α^5	α^{10}	1	α^5	α^{10}	1	α^5	α^{10}	$\theta_3(x)$
	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	$e_2(x)$
$\lambda_4=\alpha^3$	1	α^{12}	α^9	α^6	α^3	1	α^{12}	α^9	α^6	α^3	1	α^{12}	α^9	α^6	α^3	$\theta_4(x)$
$\lambda_5=\alpha^6$	1	α^9	α^3	α^{12}	α^6	1	α^9	α^3	α^{12}	α^6	1	α^9	α^3	α^{12}	α^6	$\theta_5(x)$
$\lambda_6=\alpha^{12}$	1	α^3	α^6	α^9	α^{12}	1	α^3	α^6	α^9	α^{12}	1	α^3	α^6	α^9	α^{12}	$\theta_6(x)$
$\lambda_7=\alpha^9$	1	α^6	α^{12}	α^3	α^9	1	α^6	α^{12}	α^3	α^9	1	α^6	α^{12}	α^3	α^9	$\theta_7(x)$
	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	$e_3(x)$
$\lambda_8=\alpha$	1	α^{14}	α^{13}	α^{12}	α^{11}	α^{10}	α^9	α^8	α^7	α^6	α^5	α^4	α^3	α^2	α	$\theta_8(x)$
$\lambda_9=\alpha^2$	1	α^{13}	α^{11}	α^9	α^7	α^5	α^3	α	α^{14}	α^{12}	α^{10}	α^8	α^6	α^4	α^2	$\theta_9(x)$
$\lambda_{10}=\alpha^4$	1	α^{11}	α^7	α^3	α^{14}	α^{10}	α^6	α^2	α^{13}	α^9	α^5	α	α^{12}	α^8	α^4	$\theta_{10}(x)$
$\lambda_{11}=\alpha^8$	1	α^7	α^{14}	α^6	α^{13}	α^5	α^{12}	α^4	α^{11}	α^3	α^{10}	α^2	α^9	α	α^8	$\theta_{11}(x)$
	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	$e_4(x)$
$\lambda_{12}=\alpha^7$	1	α^8	α	α^9	α^2	α^{10}	α^3	α^{11}	α^4	α^{12}	α^5	α^{13}	α^6	α^{14}	α^7	$\theta_{12}(x)$
$\lambda_{13}=\alpha^{14}$	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	$\theta_{13}(x)$
$\lambda_{14}=\alpha^{13}$	1	α^2	α^4	α^6	α^8	α^{10}	α^{12}	α^{14}	α	α^3	α^5	α^7	α^9	α^{11}	α^{13}	$\theta_{14}(x)$
$\lambda_{15}=\alpha^{11}$	1	α^4	α^8	α^{12}	α	α^5	α^9	α^{13}	α^2	α^6	α^{10}	α^{14}	α^3	α^7	α^{11}	$\theta_{15}(x)$
	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1	$e_5(x)$

$$GF(q)[x_1,x_2,\ldots,x_n] \bmod (g_1(x_1,\ldots,x_n),\ g_2(x_1,\ldots,x_n),\ldots,g_k(x_1,\ldots,x_n)),$$

but its structure is too complicated. The ring

$$GF(q)[x_1,x_2,\ldots,x_n] \bmod (x_1^{m_1}-1,\ x_2^{m_2}-1,\ \ldots,\ x_n^{m_n}-1)$$

is isomorphic to the group algebra $GF(q)\cdot A$ on an Abelian groop A which is the direct product of cyclic groups of order m_i ($i=1, \ldots, n$). An Abelian code is defined as a ideal of a $GR(q)\cdot A$. So it suffices to consider the ring R defined in (3.1) to analize Abelian codes.

Further here we consider 2-variable case for simplicity, and only a formal task suffices to generalize it to n-variable case. Thus let

(3.2) $$R = GF(q)[x,\ y] \bmod (g(x),\ h(y)).$$

And let $g(x)$ and $h(x)$ have no multiple factors as before, and have degrees m and n respectively. We can represent elements of R by 2-variate polynomials of degree m-1 in x and of n-1 in y.

In mono-variable case eigen polynomials played fundamental roles. Instead we consider,

(3.3) $$\theta_{ij}(x,\ y) = \tau_i(x)\ \sigma_j(y),\quad i=1,\ \ldots,\ m,\quad j=1,\ \ldots,\ n$$

in the ring

(3.4) $$\overline{R} = GF(q^t)[x,\ y] \bmod (g(x),\ h(y))$$

where

$GF(q^t)$: the minimal extension field containg $GF(q^r)$ and $GF(q^s)$

$GF(q^r)$: the splitting field of $g(x)$

$GF(q^s)$: the splitting field of $h(x)$

$\tau_i(x)$: the eigen polynomial with eigen value λ_i of the transform x on $GF(q^r)[x]$ mod $g(x)$

$\sigma_j(x)$: the eigen polynomial with eigen value μ_j of the transform x on $GF(q^s)[x]$ mod $h(x)$.

From Theorem 1 and (3.3) it is clear that $\theta_{ij}(x, y)$ $(i=1, \ldots, m, j=1, \ldots, n)$ are orthogonal idempotents and summed up to unity and

$$\theta_{ij}(\lambda_k, \mu_\ell) = 1 \quad \text{if } (k, \ell) = (i, j) \qquad (3.5)$$
$$= 0 \quad \text{if } (k, \ell) \neq (i, j)$$

Every polynomial $\rho(x, y) \in \overline{R}$ is expressed on the basis $\theta_{ij}(x, y)$ $(i=1, \ldots m, j=1, \ldots, n)$ such that

$$\rho(x, y) = \Sigma_{i=1}^{n}\Sigma_{j=1}^{n} \alpha_{ij}\, \theta_{ij}(x, y), \quad \alpha_{ij} \in GF(q^t) \qquad (3.6)$$

where

$$\alpha_{ij} = \rho(\lambda_i, \mu_j), \quad i=1, \ldots, m, \quad j=1, \ldots, n, \qquad (3.7)$$

And the product and sum of any two elements, say, $\rho(x, y)$ and $\eta(x, y) = \Sigma_i\Sigma_j\beta_{ij}\theta_{ij}(x, y)$ are

$$\rho(x, y)\eta(x, y) = \Sigma_i\Sigma_j\, \alpha_{ij}\beta_{ij}\theta_{ij}(x, y) \qquad (3.8)$$

$$\rho(x, y) + \eta(x, y) = \Sigma_i\Sigma_j(\alpha_{ij}+\beta_{ij})\theta_{ij}(x, y). \qquad (3.9)$$

So $\overline{R}$ is isomorphic to the mn-ply direct product of $GF(q^t)$. From this $\overline{R}$ is a semisimple ring and its subring R is also semisimple [1].

Let denote by Σ the set of all pairs (λ_i, μ_j) of eigen values λ_i and μ_j $(i=1, \ldots, m, j=1, \ldots, n)$. Thus

(3.10) $\Sigma = \{(\lambda_i, \mu_j) \mid i=1, \ldots, m, \ j=1, \ldots, n\} \subseteq GF(q^t)^2$.

Let us call the transform on $GF(q^t)^2$

(3.11) $(\xi, \eta) \rightarrow (\xi^q, \eta^q), \quad (\xi, \eta) \in GF(q^t)^2$

(2-dimensional) Frobenius transform, and the set

$\{(\alpha, \beta), (\alpha^q, \beta^q), (\alpha^{q^2}, \beta^{q^2}), \ldots, (\alpha^{q^k}, \beta^{q^k})\}((\alpha^{q^{k+1}}, \beta^{q^{k+1}}) = (\alpha, \beta),$

$(\alpha^{q^\ell}, \beta^{q^\ell}) \neq (\alpha, \beta)$ for $\ell \leqq k)$ a Frobenius cycle. Then it is clear that Σ is decomposed into Frobenius cycles $\Sigma_1, \Sigma_2, \ldots, \Sigma_c$. Further let $N_i = \{(k, \ell) \mid (\lambda_k, \mu_\ell) \in \Sigma_i\}$, $i=1, \ldots, c$, then the following is another main result.

<u>Theorem 4</u> Though $\theta_{ij}(x, y)$ are in $\overline{R}$

(3.12) $e_i(x, y) = \sum_{(k,\ell)\in N_i} \theta_{k,\ell}(x, y), \quad i=1, \ldots, c,$

are in R, and are orthogonal idempotents and summed up to unity. Further,

(3.13)
$$\begin{aligned} e_i(\lambda_k, \mu_\ell) &= 1 \quad \text{if} \quad (k, \ell) \in N_i \\ &= 0 \quad \text{if} \quad (k, \ell) \notin N_i \end{aligned}$$

<u>Proof</u> It is clear that $e_i(x, y)$, $i=1, \ldots, c$, are orthogonal idempotents and summed up to unity and (3.13) is valid.

To show that $e_i(x, y) \in R$, let

$$e_i(x, y) = \Sigma_{k=0}^{m-1} \Sigma_{\ell=0}^{n-1} e_{i,k} x^k y^\ell, \quad e_{i,k} \in GF(q^t)$$

Writing (3.5) in the form of mn linear equations in mn unknown values $e_{i,k\ell}$ like (2.10), we can easily prove that $e_{i,k} \in GF(q)$ by the same reasoning as the proof of Theorem 2.

Theorem 5 For each i=1, ..., c, $e_i(x, y)$ R is a minimal ideal of R. Thus $e_i(x, y)$, i=1, ..., c, are primitive orthogonal idempotents in R.

proof First note that for any nonzero polynomial $f(x) \in e_i(x, y)$ R, the right hand side of

$$(3.14) \qquad f(x, y) = \sum_{(k,\ell)\in N_i} f(\lambda_k, \mu_\ell)\theta_{k,\ell}(x, y) \qquad \text{(see (3.7))}$$

has not zero terms, i.e. $f(\lambda_k, \mu_\ell)$ $((k, \ell) \in N_i)$ are all nonzero. Because if one of $f(\lambda_k, \mu_\ell)$ $((k, \ell) \in N_i)$ is zero then $f(\lambda_k^q, \mu_\ell^q) = (f(\lambda_k,\mu_\ell))^q = 0$ (for $f(x, y) \in R$), so all $f(\lambda_k, \mu_\ell)((k, \ell) \in N_i)$ are zero and $f(x, y) = 0$ to contradict.

Now let $M \subseteq e_i(x, y)$ R be a minimal ideal of R the M has a generating idempotent, say, $d(x, y) \in M$, because R is a semisimple ring [1]. That is $d(x, y)^2 = d(x, y)$ and $M = d(x, y)$ R. Let

$$(3.15) \qquad d(x, y) = \sum_{(k,\ell)\in N_i} \varepsilon_{k\ell}\theta_{k\ell}(x, y), \qquad \varepsilon_{k\ell} \in GF(q^t)$$

then

$$d^2(x, y) = \sum_{(k,\ell)\in N_i} \varepsilon_{k\ell}^2\, \theta_{k\ell}(x, y)$$

From $d^2(x, y) = d(x, y)$ we have $\varepsilon_{k\ell}^2 = \varepsilon_{k\ell}$ so $\varepsilon_{k\ell} = 0$ or 1 $((k\ \ell) \in N_i)$. Every nonzero polynomial in $e_i(x, y)$ R has not zero coefficients in the form (3.14), therefore

$$d(x, y) = \sum_{(k,\ell)\in N_i} \theta_{k\ell}(x, y) = e_i(x, y)$$

which implies $M = e_i(x, y)$ R.

Example 3 Let $R = GF(2)[x, y] \bmod (x^3-1, y^3-1)$. And we can factor x^3-1 into irreducible polynomials $x-1$ and x^2+x+1, whose splitting field is the $GF(2^2)$. Let α be the primitive element of $GF(2^2)$ satisfying $\alpha^2 = 1+\alpha$.

The eigenvalues and eigen polynomials of the transform x on $GF(2)[x] \bmod (x^3-1)$ are

$$\lambda_1 = 1 \qquad \tau_1(x) = 1 + x + x^2 = \sigma_1(x),$$

$$\lambda_2 = \alpha \qquad \tau_2(x) = 1 + \alpha^2 + \alpha x^2 = \sigma_2(x),$$

$$\lambda_3 = \alpha^2 \qquad \tau_3(x) = 1 + \alpha x + \alpha^2 x^2 = \sigma_3(x).$$

Decomposing $\Sigma = \{(\alpha^i, \alpha^j) \mid i, j = 0, 1, 2\}$ into Frobenius cycles

$$\Sigma_1 = \{(1, 1)\}, \ \Sigma_2 = \{(\alpha, 1), (\alpha^2, 1)\}, \ \Sigma_3 = \{(1, \alpha), (1, \alpha^2)\}$$

$$\Sigma_4 = \{(\alpha, \alpha), (\alpha^2, \alpha^2)\}, \ \Sigma_5 = \{(\alpha, \alpha^2), (\alpha^2, \alpha)\},$$

we have

$$e_1(x, y) = \tau_1(x)\sigma_1(y) = (1 + x + x^2)(1 + y + y^2),$$

$$e_2(x, y) = \tau_2(x)\sigma_1(y) + \tau_3(x)\sigma_1(y) = (x + x^2)(1 + y + y^2),$$

$$e_3(x, y) = \tau_1(x)\sigma_2(y) + \tau_1(x)\sigma_3(y) = (1 + x + x^2)(y + y^2),$$

$$e_4(x, y) = \tau_2(x)\sigma_2(y) + \tau_3(x)\sigma_3(y) = x + y + x^2 + y^2 + xy + x^2y^2,$$

$$e_5(x, y) = \tau_2(x)\sigma_3(y) = \tau_3(x)\sigma_2(y) = x + y + x^2 + y^2 + xy^2 + x^2y.$$

These are shown in the example of [3], where MacWilliams constructed them by other algorithms.

References

[1] Blake, I. F. and Mullin, R. C. (1975), "The Mathematical Theory of Coding", Academic Press, New York/London.

[2] Claasen, H. L. (1978), "The Multiplications in GF(q)[x]/(a(x)) Considered as Linear Transformations", Linear Algebra and its Applications 22, 105   123.

[3] MacWilliams, F. J. (1970), "Binary Codes Which are Ideals in the Group Algebra of an Abelian Group", The Bell System Technical Journal, July-August 987   1010.

[4] Takahashi, I. (1981), "Switching Functions Constructed by Galois Extension Fields", Information and Control 48, 95   108.

[5] Van Lint, J. H. (1971), "Coding Theory", Lecture Notes in Math.. 201. Springer Verlag, Berlin/New York.