Polynomial Functions on Finite Galois Rings*

[1]Zong-duo Dai, [2]Guang Gong and [1]Ding-feng Ye

[1]*State Key Laboratory of Information Security*
Graduate School (Beijing)
University of Science and Technology of China
100039-08, Beijing, CHINA
[2]*Department of Electrical and Computer Engineering*
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA

E-mail: yangdai@mimi.cnc.ac.cn, ggong@calliope.uwaterloo.ca

In this paper, the polynomial functions on R are determined, and some special polynomial functions such as those which factor through the natural map: $R \to R/(p)$ and those which take the values in any given sub-Galois ring of R including $Z/(p^e)$ are determined separately.

Key Words: Galois ring, sub-Galois ring, polynomial function on Galois ring

1. INTRODUCTION

Let $R = GR(p^e, n)$ be a finite Galois ring, which is a Galois extension of degree n over Z_{p^e}. Any polynomial $f(X)$ with coefficients in R gives a function from R to R: $x \mapsto f(x)\ \forall x \in R$, which is called a *polynomial function* on R. Let $R[X]$ be a polynomial ring over R. Let

$$\mathcal{K} = \{\ f(X) \in R[X] \mid f(x) = 0\ \forall x \in R\ \},$$

which is an idea of the ring $R[X]$. Then the set of all polynomial functions on R can be identified to the residue ring $R[X]/\mathcal{K}$. Polynomial functions on R have important applications in coding theory and cryptography [3, 4]. It is known that all functions from R to R are polynomial functions when R is a field, *i.e.,* when $e = 1$. However, it is not necessary that any function from R to R is a polynomial function on R when $e > 1$. In this paper, we will determine polynomial functions on R, and determine some special classes of the polynomial functions on R such as those which factor through the natural map: $R \to R/(p)$, or those which take the values in any given sub-Galois ring of R.

2. PRELIMINARIES

In the following, we will list some basic properties that will be used throughout this paper whose proof can be found in [1, 2]. For any given prime p and integers e and n, there exists one and only one Galois ring[1, 2] up to isomorphism, written as $GR(p^e, n)$. In this paper, we fix the prime p and the integers e and n, and denote $R = GR(p^e, n)$. Let $q = p^n$ and $\mathcal{T} = \{x \mid x \in R,\ x^q = x\ \}$. It is known that $\mathcal{T} = \{\ \beta^i \mid 1 \leq i < q\} \cup \{0\}$, where β is an invertible element of order $q-1$ in R.

1. Any element x in R has a unique p-adic expansion of the form

$$x = \sum_{i=0}^{e-1} w_i p^i,\ \ w_i \in \mathcal{T}\ \forall i. \tag{1}$$

Furthermore, x is invertible if and only if $w_0 \neq 0$, or equivalently, if and only if $x \not\equiv 0 \pmod p$. Thus, if $x \neq 0$, then x can be written in the form $p^j w(1+pz)$ with $0 \neq w \in \mathcal{T}$ and $z \in R$, where w and $z \pmod{p^{e-j-1}}$ are uniquely determined by x separately; and x is invertible if and only if $j = 0$. The order of w, $0 \neq w \in \mathcal{T}$, is a factor of $q-1$ and the order of $1+pz$, $z \in R$, is a factor of p^{e-1}, hence the order of $x = w(1+pz)$ is a factor of $(q-1)p^{e-1}$.

2. The quotient ring $GR(p^e, n)/(p^c)$ is isomorphic to the Galois ring $GR(p^c, n)$. In particular, $GR(p^e, n)/(p)$ is isomorphic to $GR(p, n) = F_{p^n}$, which is the finite field of p^n elements. The set $\mathcal{T}$ is mapped onto $GR(p^e, n)/(p) = F_{p^n}$ under the natural homomorphism from $GR(p^e, n)$ to $GR(p^e, n)/(p) = F_{p^n}$.

3. The function

$$\sigma(x) = \sum_{i=0}^{e-1} w_i^p p^i, \forall x = \sum_{i=0}^{e-1} w_i p^i, w_i \in \mathcal{T}$$

is an isomorphism of R, called as Frobenius automorphism. Sometimes it is also denoted as $\sigma(x) = x^\sigma$. For any $x \in R$, it is known that $\sigma(x) = x$ if and only if $x \in Z/(p^e)$.

4. For any factor d of n, there exists a unique sub-Galois ring K which is isomorphic to $GR(p^e, d)$, and the Galois group of R over K is a cyclic group generated by σ^d, where σ is the Frobenius automorphism of R.

5. Let d be a factor of n, and $K = GR(p^e, d)$. The trace function from R to K is defined as: $Tr_K^R(x) = \sum_{0 \leq i < n/d} x^{\sigma^{di}}$, where σ is the Frobenius

automorphism of R. If x is written as $x=\sum_{i=0}^{e-1} w_i p^i,\ w_i \in \mathcal{T}$, then

$$Tr_K^R(\sum_{i=0}^{e-1} w_i p^i) = \sum_{i=0}^{e-1} \sum_{0 \le j < n/d} w_i^{p^{dj}} p^i.$$

It is known that $Tr_K^R(x) \in K \forall x \in R$.

3. POLYNOMIAL FUNCTIONS FROM R TO R

Notations 1 In this paper, we always let x be a variable taking values in R. It is known that the variable x can be written as $x = y + pz$, where y and z are variables taking values in $\mathcal{T}$ and in R, respectively. It is clear that both $z \pmod{p^{e-1}}$ and y are uniquely determined by x.

LEMMA 3.1. *Let λ be the smallest positive integer such that $n\lambda \ge e-1$, define*

$$\begin{aligned} f_y(X) &= X^{q^\lambda} \in R[X], & (2)\\ f_{pz}(X) &= X - f_y(X) \in R[X], & (3)\\ f_a(X) &= 1-(X-a)^{p^{e-1}(q-1)} \in R[X],\ a \in \mathcal{T}. & (4) \end{aligned}$$

Then

1. $f_y(y+pz) = y\ \forall x = y+pz \in R$.

2. $f_{pz}(y+pz) = pz\ \forall x = y+pz \in R$.

3.$f_a(y+pz) = \delta_{y,a}\ \forall y+pz \in R$, *where* $\delta_{y,a} = \begin{cases} 1, & y=a,\\ 0, & a \ne y \in \mathcal{T}. \end{cases}$

Proof. By the assumption that $n\lambda \ge e-1$, we can see that p^{e-1} is a factor of q^λ and $q^\lambda \ge e$. We have

$$f_y(y+pz) = (y+pz)^{q^\lambda} = \begin{cases} [y(1+py^{-1}z)]^{q^\lambda} = y & if\ y \ne 0\\ (pz)^{q^\lambda} = 0 = y & if\ y = 0. \end{cases}$$

This establishes the assertion 1. According to (3), We have

$$f_{pz}(y+pz) = (y+pz) - f_y(y+pz) = (y+pz) - y = pz,$$

which gives the assertion 2. Note that

$$(y+pz-a)^{p^{e-1}(q-1)} = \begin{cases} [w(1+pu)]^{p^{e-1}(q-1)} = 1 & if\ y \ne a\\ (pz)^{p^{e-1}(q-1)} = 0 & if\ y = a \end{cases}$$

where $w \in \mathcal{T}$, $w \equiv y - a \not\equiv 0 \pmod p$ and $u \in R$. Therefore

$$f_a(y+pz) = 1 - (y-a)^{p^{e-1}(q-1)} = \begin{cases} 1-1=0 & if\ y \neq a \\ 1-0=1 & if\ y = a. \end{cases}$$

Hence the assertion 3 follows. ▌

Notation 2 In the following, we denote by Y the polynomial $f_y(X)$, and by Z the polynomial $f_{pz}(X)$.

LEMMA 3.2. *Let $B_{q,q} = (a_i^j)_{0\le i<q, 0\le j<q}$ be a $q\times q$ matrix over R, where $a_0 = 0$ and $a_j = \beta^j, 1 \le j < q$, more precisely:*

$$B_{q,q} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 1 & \beta & \beta^2 & \cdots & \beta^j & \cdots & \beta^{q-1} \\ & & & & & \cdots & \\ 1 & \beta^i & (\beta^i)^2 & \cdots & (\beta^i)^j & \cdots & (\beta^i)^{q-1} \\ & & & & & \cdots & \\ 1 & \beta^{q-1} & (\beta^{q-1})^2 & \cdots & (\beta^{q-1})^j & \cdots & (\beta^{q-1})^{q-1} \end{pmatrix}. \tag{5}$$

If $s \le q$, then the matrix $B_{s,s}$ is invertible, where $B_{s,s}$ is the sub-matrix of $B_{q,q}$ which is made of the first s rows and the first s columns of $B_{q,q}$.

Proof. Note that $det(B_{s,s}) = \pm\prod_{0\le i<j\le s}(a_i - a_j) \not\equiv 0 \pmod p$. Thus $det(B_{s,s})$ is an invertible element in R. Therefore $B_{s,s}$ is invertible. ▌

LEMMA 3.3. *Let $\mathcal{J}$ be an ideal generated by $e+1$ elements: $Y^q - Y$ and $p^{e-j}Z^j$, $0 \le j < e$. For any $f(X) \in R[X]$, then*

1.

$$f(X) \equiv \sum_{0\le i<q, 0\le j<e} u_{i,j}(f) Y^i Z^j \pmod{\mathcal{J}}, \tag{6}$$

for some $u_{i,j}(f) \in R$. Furthermore, the above equation can be written in terms of the matrices as follows:

$$f(X) \equiv (1, Y, Y^2, \cdots, Y^{q-1}) U(f) (1, Z, Z^2, \cdots, Z^{e-1})^\tau \pmod{\mathcal{J}} \tag{7}$$

where τ means the transpose and

$$U(f)=\begin{pmatrix} u_{00}(f) & u_{01}(f) & u_{02}(f) & \cdots & u_{0\ e-1}(f) \\ u_{10}(f) & u_{11}(f) & u_{12}(f) & \cdots & u_{1\ e-1}(f) \\ u_{20}(f) & u_{21}(f) & u_{22}(f) & \cdots & u_{2e-1}(f) \\ & & & \cdots & \\ u_{q-1\ 0}(f) & u_{q-1\ 1}(f) & u_{q-1\ 2}(f) & \cdots & u_{q-1\ e-1}(f) \end{pmatrix} \tag{8}$$

2.Keep the notations in item 1. Assume that $e \le q$. Then $f(X) \in \mathcal{K}$ if and only if $u_{i,j}(f) \equiv 0 \pmod{p^{e-j}}\ \forall i, j$.
3.Assume that $e \le q$. Then $\mathcal{K} = \mathcal{J}$.

Proof. Note that $Y^q - Y \in \mathcal{J}$, $Z^e \in \mathcal{J}$ and

$$X^k = (Y+Z)^k = \sum_{0\le i\le k} \binom{k}{i} Y^i (Z)^{k-i},$$

we have

$$\begin{aligned} f(X) &= \sum_{0\le k\le N} a_k X^k = \sum_{0\le k\le N} a_k (Y+Z)^k = \sum_{0\le i+j\le N} a_{i,j} Y^i Z^j \\ &\equiv \sum_{0\le i<q, 0\le j<e} u_{i,j} Y^i Z^j \pmod{\mathcal{J}} \end{aligned}$$

for some $a_{i,j} \in R$ and $u_{i,j} \in R$. Hence we get (6). The matrix expression (7) follows immediately from the definition.

According to Lemma 3.1, we have

$$\begin{aligned} f_y(x)^q - f_y(x) &= y^q - y = 0, \\ p^{e-j} f_{pz}(x) &= p^{e-j}(pz)^j = 0 \end{aligned}$$

for all $x = y + pz \in R$ where $y \in \mathcal{T}$ and $z \in R$. Thus

$$\begin{aligned} Y^q - Y &= f_y(X)^q - f_y(X) \in \mathcal{K} \\ p^{e-j} Z^j &= p^{e-j} f_{pz}(X)^j \in \mathcal{K}\ \forall 0 \le j < e, \end{aligned}$$

Therefore, $\mathcal{J} \subseteq \mathcal{K}$. Let

$$F(f) = \begin{pmatrix} f(0) & f(p\beta) & \cdots & f(p\beta^j) & \cdots & f(p\beta^{q-1}) \\ f(\beta) & f(\beta + p\beta) & \cdots & f(\beta + p\beta^j) & \cdots & f(\beta + p\beta^{q-1}) \\ & & & & \cdots & \\ f(\beta^i) & f(\beta^i + p\beta) & \cdots & f(\beta^i + p\beta^j) & \cdots & f(\beta^i + p\beta^{q-1}) \\ & & & & \cdots & \\ f(\beta^{q-1}) & f(\beta^{q-1} + p\beta) & \cdots & f(\beta^{q-1} + p\beta^j) & \cdots & f(\beta^{q-1} + p\beta^{q-1}) \end{pmatrix} \tag{9}$$

It is easy to check that

$$\begin{aligned} F(f) &= \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & \beta & \cdots & \beta^{q-1} \\ 1 & \beta^2 & \cdots & (\beta^2)^{q-1} \\ & & \cdots & \\ 1 & \beta^i & \cdots & (\beta^i)^{q-1} \\ & & \cdots & \\ 1 & \beta^{q-1} & \cdots & (\beta^{q-1})^{q-1} \end{pmatrix} U(f) \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & p\beta & \cdots & p\beta^{q-1} \\ 0 & (p\beta)^2 & \cdots & (p\beta^{q-1})^2 \\ & & \cdots & \\ 0 & (p\beta)^i & \cdots & (p\beta^{q-1})^i \\ & & \cdots & \\ 0 & (p\beta)^{e-1} & \cdots & (p\beta^{q-1})^{e-1} \end{pmatrix} \\ &= B_{q,q} U(f) C B_{q,e}^{\tau} \end{aligned}$$

where $C = diag(1,\ p\ p^2,\ \cdots, p^{e-1})$ is a $e \times e$ diagonal matrix, and $B_{q,e}$ is the sub-matrix of $B_{q,q}$ which is made of the first e columns of $B_{q,q}$, and $B_{q,q}$ is defined as in (5). We now have the following reasoning processes

$$\begin{aligned} & f(X) \in \mathcal{K} \\ \Longrightarrow\ & F(f) = 0 \\ \Longrightarrow\ & B_{q,q} U(f) C B_{q,e}^{\tau} = 0 \\ \Longrightarrow\ & B_{q,q} U(f) C B_{e,e}^{\tau} = 0 \\ \Longrightarrow\ & U(f) C = 0 \ (\ By\ e \leq q\ and\ Lemma\ 3.2\ ) \\ \Longrightarrow\ & u_{i,j}(f) p^j = 0 \forall i, j \\ \Longrightarrow\ & u_{i,j}(f) \equiv 0 \pmod{p^{e-j}} \forall i, j \\ \Longrightarrow\ & u_{i,j}(f) Z^j \in \mathcal{J} \forall i, j \\ \Longrightarrow\ & f(X) \in \mathcal{J}, \end{aligned}$$

which means $\mathcal{K} \subseteq \mathcal{J}$, which together with $\mathcal{J} \subseteq \mathcal{K}$ shows $\mathcal{K} = \mathcal{J}$. Therefore, $f(X) \in \mathcal{K}$ if and only if $u_{i,j} \equiv 0 \pmod{p^{e-j}}$, $\forall i, j$. ▮

THEOREM 3.1. *(Basis and Size of $R[X]/\mathcal{K}$)*

1.The set $\{\ Y^i Z^j \mid 0 \leq i < q, 0 \leq j < e\ \}$ is a basis for $R[X]/\mathcal{K}$ in the sense that each polynomial function f on R, considered as an element in

$R[X]/\mathcal{K}$, can be represented by a polynomial of the form:

$$f(X) = \sum_{0 \le i < q, 0 \le j < e} u_{i,j}(f) Y^i Z^j, \ u_{i,j}(f) \in R. \tag{10}$$

Moreover, in the case $e \le q$, the coefficient $u_{i,j}(f)$ modulo p^{e-j} is uniquely determined by the element f.

2. $|R[X]/\mathcal{K}| = q^{\frac{e(e+1)q}{2}}$.

Proof.

1. It is a simple consequence of Lemma 3.3.

2. When $e \le q$, let $\mathcal{U}$ be the set consisting of all $q \times e$ matrices $U = (u_{i,j})$, where $u_{i,j} \in R/(p^{e-j})$. From item 1 we see there is a one to one correspondence between $R[X]/\mathcal{K}$ and $\mathcal{U}$. So we have

$$\begin{aligned} |R[X]/\mathcal{K}| &= |\mathcal{U}| = \prod_{0 \le i < q, 0 \le j < e} [\sum_{u_{i,j} \in R/(p^{e-j})} 1] \\ &= \prod_{0 \le i < q, 0 \le j < e} q^{e-j} = \prod_{0 \le j < e} q^{(e-j)q} = q^{\frac{e(e+1)q}{2}}. \end{aligned}$$

∎

LEMMA 3.4. *We have*

$$f_y(X)^i \equiv \sum_{a \in \mathcal{T}} a^i f_a(X) \pmod{\mathcal{K}} \ \ \forall 0 \le i < q,$$

which can be rewritten by means of matrices as follows:

$$(1, Y, Y^2, \cdots, Y^{q-1}) \equiv (f_0(X), f_\beta(X), f_{\beta^2}(X), \cdots, f_{\beta^{q-1}}(X)) B_{q,q} \pmod{\mathcal{K}}, \tag{11}$$

where $B_{q,q}$ is the matrix defined in (5).

Proof. By Lemma 3.1 we have

$$f_y(x)^i = y^i \forall x = y + pz \in R, y \in \mathcal{T}, z \in R. \tag{12}$$

Note that $\sum_{a \in \mathcal{T}} f_a(b + pz) a^j = b^j$ for any $b \in \mathcal{T}$ and $z \in R$, we have

$$\sum_{a \in \mathcal{T}} f_a(x) a^j = y^j \ \forall x = y + pz \in R, y \in \mathcal{T}, z \in R. \tag{13}$$

From (12) and (13) we get $f_y(X)^i \equiv \sum_{a\in\mathcal{T}} a^i f_a(X) \pmod{\mathcal{K}}$, which is equivalent to the matrix equation (11). ▮

THEOREM 3.2. *The set* $\{ f_a(X)Z^j \mid a \in \mathcal{T}, 0 \le j < e \}$ *is a basis of* $R[X]/\mathcal{K}$ *in the sense that each polynomial function* f *on* R*, considered as an element in* $R[X]/\mathcal{K}$*, can be represented by a polynomial of the form:*

$$f(X) = \sum_{a\in\mathcal{T},0\le j<e} v_{a,j}(f) f_a(X)Z^j,\ v_{a,j}(f) \in R. \tag{14}$$

Moreover, in the case $e \le q$*, the coefficient* $v_{a,j}(f)$ *modulo* p^{e-j} *is uniquely determined by the function* f*.*

Proof. By Lemma 3.3 and 3.4 we see

$$\begin{aligned} & f(X) \\ \equiv\ & (1, Y, \cdots, Y^{q-1})U(f)(1, Z, \cdots, Z^{e-1})^\tau \\ \equiv\ & (f_0(X), f_\beta(X), \cdots, f_{\beta^{q-1}}(X))B_{q,q}U(f)(1, Z, \cdots, Z^{e-1})^\tau \pmod{\mathcal{K}}, \end{aligned}$$

where $B_{q,q}$ and $U(f)$ are defined as in (5) and (8) respectively. Write $B_{q,q}U(f) = (\ v_{a_i,j}(f)\ )$. Then we have

$$\begin{aligned} f(X) &\equiv \sum_{0\le i<q,0\le j<e} v_{a_i,j}(f) f_{a_i}(X)Z^j \\ &\equiv \sum_{a\in\mathcal{T},0\le j<e} v_{a,j}(f) f_a(X)Z^j \pmod{\mathcal{K}}. \end{aligned}$$

The rest of the results can be obtained from Theorem 3.1 directly. ▮

4. POLYNOMIAL FUNCTIONS FACTORED THROUGH THE NATURAL MAP: $R \to R/(P)$

We say a function f from R to R factorized through the natural homomorphism φ: $R \to R/(p)$, if there exists a map f^*: $R/(p) \to R$ such that $f = f^* \circ \varphi$. Denote by $\mathcal{P}^*(R)$ the set of the polynomial functions which factor through φ. For any function f from R to R, it is known that

$$f \in \mathcal{P}^*(R) \Longleftrightarrow f(y + pZ) = f(y)\ \forall y \in \mathcal{T}, z \in R. \tag{15}$$

We keep the notations in the previous sections.

THEOREM 4.1.

1.

$$\begin{aligned}\mathcal{P}^*(R) &= \{ \sum_{0\le i<q} u_i f_y(X)^i \mid u_i \in R \} \\ &= \{ \sum_{a\in\mathcal{T}} v_a f_a(X) \mid v_a \in R \},\end{aligned}$$

here we use the polynomials over R as the functions which they give.

2. $|\mathcal{P}^*(R)| = |R|^q = p^{nep^n}$.

Proof. Let f be a polynomial function on R, and represented by $f(X) \in R[X]$. From Theorems 3.1 and 3.2 we may assume

$$f(X) \equiv \sum_{0\le i<q, 0\le j<e} u_{i,j} Y^i Z^j \pmod{\mathcal{K}}$$

for some $u_{i,j} \in R$, and

$$f(X) \equiv \sum_{a\in\mathcal{T}, 0\le j<e} v_{a,j} f_a(X) Z^j \pmod{\mathcal{K}}$$

for some $v_{a,j} \in R$. For any $y \in \mathcal{T}$ and any $z \in R$, we have the following four equations:

$$\begin{aligned}f(y+pz) &= \sum_{0\le i<q,0\le j<e} u_{i,j} f_y(y+pz)^i f_{pz}(y+pz)^j &(16)\\ f(y) &= \sum_{0\le i<q} u_{i,0} f_y(y+pz)^i &(17)\\ f(y+pz) &= \sum_{a\in\mathcal{T},0\le j<e} v_{a,j} f_a(y+pz) f_{pz}(y+pz)^j &(18)\\ f(y) &= \sum_{a\in\mathcal{T}} v_{a,0} f_a(y+pz). &(19)\end{aligned}$$

Then we obtain the following equivalent conditions:

$$\begin{aligned}& u_{i,j} \equiv 0 \pmod{p^{e-j}}\ \forall j>0 &(20)\\ \iff\ & \sum_{0\le i<q,0\le j<e} u_{i,j} f_y(X)^i f_{pz}(X)^j \equiv \sum_{0\le i<q} u_{i,0} f_y(X)^i \pmod{\mathcal{K}} \\ & (By\ Theorem\ 3.1) \\ \iff\ & f(y+pz) = f(y)\ \forall y\in\mathcal{T}, z\in R &(21)\end{aligned}$$

$$
\begin{aligned}
& (By\ (16)\ and (17)\ ) \\
\iff & \sum_{a \in \mathcal{T}, 0 \le j < e} v_{a,j} f_a(X) f_{pz}(X)^j \equiv \sum_{a \in \mathcal{T}} v_{a,0} f_a(X) \pmod{\mathcal{K}} \\
& (By\ (18)\ and (19)\ ) \\
\iff & v_{a,j} \equiv 0 \pmod{p^{e-j}}\ \forall j > 0 \qquad (22) \\
& (\ By\ Theorem\ 3.2\ )
\end{aligned}
$$

From (15), (21) and (20) we get

$$f \in \mathcal{P}^*(R) \iff f(X) \equiv \sum_{0 \le i < q} u_{i,0} Y^i \pmod{\mathcal{K}}$$

. From (15), (21) and (22) we get

$$f \in \mathcal{P}^*(R) \iff f(X) \equiv \sum_{a \in \mathcal{T}} v_{a,0} f_a(X) \pmod{\mathcal{K}}.$$

These establish the assertion 1. The assertion 2 is a easy consequence of the assertion 1. ▌

5. POLYNOMIAL FUNCTIONS FROM *R* TO SUB-GALOIS RING *K*

Let K be a sub-Galois ring of R, and let $\mathcal{P}(R, K)$ be the set of the polynomial functions from R to K. We keep the notation in the previous sections.

THEOREM 5.1. *Assume $K = R(p^e, d)$ and $q > p^d(e-1)$. Then*

1.For any $f(X) \in R[X]$, the following conditions are equivalent:

(i)$f(X)$ represents an element in $\mathcal{P}(R, K)$,

(ii)$f(X) \equiv \sum_{a \in \mathcal{T}} v_a f_a(X) \pmod{\mathcal{K}}$ for some $v_a \in K$,

(iii)$f(X) \equiv \sum_{i \in \Gamma} \sum_{0 \le j < n_i} u_i^{\sigma^{dj}} f_y(X)^{ip^{dj}} \pmod{\mathcal{K}}$ for some $u_i \in R$, where Γ is a system of complete representatives of the distinct sets among the following sets: $\{ip^{dj} \pmod q \mid 0 \le j < n/d\}, 1 \le i < q$, n_i is the size of the set $\{ip^{dj} \pmod q \mid 0 \le j < n/d\}$, and σ is the Frobenius automorphism of R.

(iv)$f(x) = \sum_{i \in \Gamma} Tr_K^R(u_i f_y(x)^i)\ \forall x \in R$ for some $u_i \in R$, where Γ is defined in (iii).

2.$|P(R, K)| = p^{edq}$. In particular, $|P(R, Z/(p^e))| = p^{eq}$.

Proof. Note that the assertion 2 is an easy consequence of the assertion 1. So it is enough to prove the assertion 1. It is clear that (ii) implies (i), and (iii) implies (i). Note that $\sum_{0\le j<n_i} u_i^{\sigma^{dj}} f_y(X)^{ip^{dj}} = Tr_K^R(u_i f_y(X)^i)$. Thus (iii) is equivalent to (iv). Therefore, it is enough to prove "(i) $\to$ (ii)" and "(i) $\to$ (iii)".

(i) $\to$ (ii): We may assume

$$f(X) \equiv \sum_{a\in\mathcal{T},0\le<e} v_{a,j} f_a(X) f_{pz}(X)^j \pmod{\mathcal{K}}$$

for some $v_{a,j} \in R$. For any $b \in \mathcal{T}$ we have

$$f(b) = \sum_{a\in\mathcal{T},0\le j<e} v_{a,j} f_a(b) f_{pz}(b)^j = v_{b,0}$$

. Hence $v_{b,0} \in K$ by the assumption. Without loss of generality, we may assume $v_{a,0} = 0$ for all $a \in \mathcal{T}$. For any $b \in \mathcal{T}$ and $z \in R$, we have

$$\begin{aligned} f(b+pz) &= \sum_{a\in\mathcal{T},1\le j<q} v_{a,j} f_a(b+pz) f_{pz}(b+pz)^j \\ &= \sum_{1\le j<q} v_{b,j} f_{pz}(b+pz)^j \\ &= \sum_{1\le j<q} p^j v_{b,j} z^j. \end{aligned}$$

We may write $p^j v_{b,j} = p^{j+k_j} v_j^*$ where $0 \le j+k_j \le e$ and $v_j^* \not\equiv 0 \pmod p$. Let

$$k = \min\{j + k_j \mid 1 \le j < e\}.$$

If there exists a j such that $v_{b,j} \not\equiv 0 \pmod{p^{e-j}}$, then $k < e$. Thus we have

$$f(b+pz) = p^k \sum_{1\le j<e} p^{j+k_j-k} v_j^*(f) z^j = p^k g(z) \in K, \ \ \forall z \in R$$

where $g(X) = \sum_{1\le j<e} p^{j+k_j-k} v_j^* X^j \not\equiv 0 \pmod p$. For any $z \in R$, it is easy to see that there exists an element $g^*(z) \in K$ such that $g(z) \equiv g^*(z) \pmod{p^{e-k}}$ because $p^k g(z) \in K$. Denote by $\overline{z}$ the corresponding element of z in F_q under the natural homomorphism from R to $R/(p)(= F_q)$. Let

$\overline{g}(X) = \sum_{1 \leq j < e} \overline{p^{j+k_j-k} v_j^*} X^j$. Since $g^*(z) \in K \forall z \in R$, then $\overline{g}(\overline{z}) = \overline{g^*}(\overline{z}) = \overline{g^*(z)} \in F_{p^d} (= K/(p))$ for all $\overline{z} \in F_q (= R/(p))$. Therefore, each element in F_q is a root of some polynomial $\overline{g}(X) - \alpha$ where $\alpha \in F_{p^d}$. So

$$q \leq \sum_{\alpha \in F_{p^d}} deg(\overline{g}(X) - \alpha) \leq p^d(e-1),$$

a contradiction.

(i) $\rightarrow$ (iii): Let

$$S_{(t)} = \{f(X) \pmod{\mathcal{K}} | f(X) \text{ satisfies the condition } (t) \}, t \in \{i, ii, iii\}.$$

It is not difficult to see that the $|S_{(iii)}| = |S_{(ii)}|$. From the above arguments we see that $S_{(iii)} \subseteq S_{(i)} = S_{(ii)}$. Hence we obtain that $S_{(iii)} = S_{(ii)} = S_{(i)}$, which establishes (iii) $\leftrightarrow$ (i). ▮

Acknowledgment This work is supported by the 973-Foundation of China (No. G1999035804) and the National Natural Science Foundation of China (No. 69773015).

REFERENCES

1. Bernard R. McDonald , *Finite rings with identity.* Series: Pure and applied mathematics, a series of monographs and textbooks ; 28, New York, M. Dekker, Inc., 1974.
2. Jean Pierre Serre, *Local fields*, Springer-Verlag, New York, 1979.
3. P. Vijay Kumar, T. Helleseth, A.R. Calderbank, and A.R. Hammons, Large families of quaternary sequences with low correlation, *IEEE Trans. on Inform. Theory*, vol. 42, No. 2, March 1996, pp. 579-592.
4. Claude Carlet, More correlation-immune and resilient functions over Galios fields and Galois rings, *Advances in Cryptology-EuorCrypto'97*, Lecture-Notes in Computer Science, Springer-Verlag, Berlin, 1997. pp. 422-433.