Peer-reviewed version available at *Symmetry* **2018**, *10*, 702; doi:10.3390/sym10120702

Article

Normal Bases on Galois Ring Extensions

Zhang Aixian [1,*] and Feng Keqin [2]

[1] Department of Mathematical Sciences, Xi'an University of Technology; zhangaixian1008@126.com
[2] Department of Mathematical Sciences, Tsinghua University; kfeng@math.tsinghua.edu.cn
* Correspondence: zhangaixian1008@126.com; Tel.: +86-29-89667695

Version September 27, 2018 submitted to Journal Not Specified

Abstract: In this paper we study the normal bases for Galois ring extension $\mathbf{R}/\mathrm{Z}_{p^r}$ where $\mathbf{R} = \mathrm{GR}(p^r, n)$. We present a criterion on normal basis for $\mathbf{R}/\mathrm{Z}_{p^r}$ and reduce this problem to one of finite field extension $\overline{\mathbf{R}}/\overline{\mathrm{Z}}_{p^r} = \mathbb{F}_q/\mathbb{F}_p$ $(q = p^n)$ by Theorem 1. We determine all optimal normal bases for Galois ring extension.

Keywords: Galois ring; optimal normal basis; multiplicative complexity; finite field

1. Introduction

The theory of finite fields is one of the fundamental mathematical tools in computer science and communication engineering since 1950's when digit communications and computations were rapidly developed. For it to be useful in practice, a lot of study have focused for decades on the complexity of operations, particularly the multiplicative operation, and with this respect, many useful bases for $\mathbb{F}_{q^n}/\mathbb{F}_q$ with low complexity have been found ([2]-[9],[13]-[15]).

In the past two decades, Galois rings have been used successfully in many aspects of combinatorics to construct different kinds of combinatorial designs, and in communication theory to construct error-correcting codes, sequences with good correlation properties, secret sharing schemes, hash functions and so on ([17],[18],[10],[4],[11]). However, comparing to the case of finite field extensions, the complexity problem of operations in Galois ring has not attracted much attention from scholars except Abrahamsson who considered the complexity of bases and carefully discussed architectures for multiplication in Galois rings (for $p = 2$) in his thesis [1], 2004. Therefore, the operations, particularly for the multiplication, on the Galois rings become one of the interesting problems to be considered. So many works remain to be done to extend various methods and results in finite fields on constructing bases with low complexity to Galois rings.

In this paper we will study one aspect of the complexity problem of operations in Galois rings. More precisely, we will focus on normal bases for Galois ring extensions in this paper. This paper is organised as follows. In Section 2 we introduce some basic facts on Galois rings. We present some results on normal bases and some basic properties on multiplicative complexity of normal bases for Galois ring extension $\mathrm{GR}(p^r, n)/\mathrm{Z}_{p^r}$ in Section 3. Then we determine all optimal normal bases for these Galois ring extensions in Section 4.

2. Basic Facts on Galois Rings

In this section we introduce several basic facts on Galois rings. For more informations, the reader is referred to [19].

Let p be a prime number and $r \geq 2$, $\mathrm{Z}_{p^r} = \mathbb{Z}/p^r\mathbb{Z}$. We have the *modulo p* reduction mapping

$$\varphi : \mathrm{Z}_{p^r} \longrightarrow \mathbb{F}_p, \quad a \pmod{p^r} \longmapsto \bar{a} = a \pmod{p},$$

Peer-reviewed version available at Symmetry 2018, 10, 702; doi:10.3390/sym10120702

which induces the following modulo p reduction mapping between polynomial rings:

$$\varphi : \mathbb{Z}_{p^r}[x] \longrightarrow \mathbb{F}_p[x], \quad f(x) = \sum c_i x^i \longmapsto \overline{f}(x) = \sum \bar{c}_i x^i.$$

$f(x)$ is said to be a monic basic irreducible (primitive) polynomial over $\mathbb{Z}_{p^r}$ if $\overline{f}(x)$ is a monic irreducible (primitive) polynomial over $\mathbb{F}_p$.

Let $f(x)$ be a basic primitive polynomial of degree n in $\mathbb{Z}_{p^r}[x]$. The quotient ring

$$\begin{aligned}\mathbf{R} &= \mathrm{GR}(p^r, n) = \frac{\mathbb{Z}_{p^r}[x]}{(f(x))} \cong \mathbb{Z}_{p^r}[\gamma] \\ &= \{c_0 + c_1\gamma + \cdots + c_{n-1}\gamma^{n-1} : c_i \in \mathbb{Z}_{p^r}\}, \end{aligned} \tag{1}$$

where γ is a root of $f(x)$ in $\mathbf{R}$ with order $p^n - 1$, $\mathbf{R}$ is called a Galois ring. And we note that $\overline{\gamma}$ is a primitive element of the finite field $\mathbb{F}_q$ where $q = p^n$. From now on, we take $f(x)$ to be a basic primitive polynomial. The modulo p reduction can be naturally extended to the following homomorphism of rings:

$$\varphi : \mathbf{R} = \mathrm{GR}(p^r, n) = \frac{\mathbb{Z}_{p^r}[x]}{(f(x))} \cong \mathbb{Z}_{p^r}[\gamma] \longrightarrow \mathbb{F}_q = \frac{\mathbb{F}_p[x]}{(\overline{f}(x))} \cong \mathbb{F}_p[\overline{\gamma}].$$

Some basic facts on Galois ring $\mathbf{R} = \mathrm{GR}(p^r, n)$ are given as follows.

(Fact 1) Let $\mathrm{T}^* = \langle \gamma \rangle$ be the cyclic multiplicative group of order $q - 1$ generated by γ, and $\mathrm{T} = \mathrm{T}^* \cup \{0\}$. Then $\overline{\mathrm{T}} = \mathbb{F}_q$ and

$$\mathbf{R} = \{x_0 + px_1 + p^2x_2 + \cdots + p^{r-1}x_{r-1} : x_i \in \mathrm{T}\}, \quad |\mathbf{R}| = |\mathrm{T}|^r = q^r = p^{nr}. \tag{2}$$

(Fact 2) $\mathbf{R}$ is a local commutative ring with the unique maximal ideal $\mathcal{M} = p\mathbf{R}$, $|\mathcal{M}| = q^{r-1}$ and the group of units is $\mathbf{R}^* = \mathbf{R} \backslash \mathcal{M} = \mathrm{T}^* \times (1 + \mathcal{M})$, $|\mathbf{R}^*| = q^r - q^{r-1}$.

(Fact 3) $\mathbf{R}/\mathbb{Z}_{p^r}$ is a Galois extension of rings with Galois group $Gal(\mathbf{R}/\mathbb{Z}_{p^r}) = \langle \sigma_p \rangle$, where σ_p is the automorphism of order n defined by

$$\sigma_p(\sum_{i=0}^{r-1} p^i x_i) = \sum_{i=0}^{r-1} p^i x_i^p \quad (x_i \in \mathrm{T}). \tag{3}$$

More generally, for each positive integer l, $\mathbf{R} = \mathrm{GR}(p^r, n)$ is a subring of $\mathbf{R}_{(l)} = \mathrm{GR}(p^r, nl)$ and $\mathbf{R}_{(l)}/\mathbf{R}$ is a Galois extension of rings with Galois group $Gal(\mathbf{R}_{(l)}/\mathbf{R}) = \langle \sigma_q \rangle$, where σ_q is the automorphism of $\mathbf{R}_{(l)}$ defined by

$$\sigma_q(\sum_{i=0}^{r-1} p^i x_i) = \sum_{i=0}^{r-1} p^i x_i^q \quad (x_i \in \mathrm{T}_{(l)}), \tag{4}$$

and $\mathbf{R}_{(l)} = \mathbb{Z}_{p^r}[\gamma_{(l)}] = \{\sum_{i=0}^{r-1} p^i x_i : x_i \in \mathrm{T}_{(l)}\}$, $\mathrm{T}_{(l)} = \mathrm{T}^*_{(l)} \cup \{0\}$, $\mathrm{T}^*_{(l)} = \langle \gamma_{(l)} \rangle$, $\gamma_{(l)}^{\frac{q^l-1}{q-1}} = \gamma$.

(Fact 4) We have the trace mapping

$$\mathrm{Tr}_n^{nl} : \mathbf{R}_{(l)} = \mathrm{GR}(p^r, nl) \longrightarrow \mathbf{R} = \mathrm{GR}(p^r, n),$$

defined by

$$\mathrm{Tr}_n^{nl}(\alpha) = \sum_{i=0}^{l-1} \sigma_q^i(\alpha) \quad (\alpha \in \mathbf{R}_{(l)}),$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 September 2018 doi:10.20944/preprints201809.0559.v1

Peer-reviewed version available at *Symmetry* **2018**, *10*, 702; doi:10.3390/sym10120702

which is an epimorphism of **R**-modules and we have the following commutative diagram:

$$\begin{array}{ccccc} \mathbf{R}_{(l)} = \mathrm{GR}(p^r, nl) & \xrightarrow{\mathrm{Tr}_n^{nl}} & \mathbf{R} = \mathrm{GR}(p^r, n) & \xrightarrow{\mathrm{Tr}_1^n} & \mathrm{Z}_{p^r} = \mathrm{GR}(p^r, 1) \\ \varphi \downarrow & & \varphi \downarrow & & \varphi \downarrow \\ \overline{\mathbf{R}}_{(l)} = \mathbb{F}_{p^{nl}} & \xrightarrow{\mathrm{tr}_n^{nl}} & \overline{\mathbf{R}} = \mathbb{F}_{p^n} & \xrightarrow{\mathrm{tr}_1^n} & \overline{\mathrm{Z}}_{p^r} = \mathbb{F}_p \end{array} \quad (5)$$

where tr_n^{nl} and tr_1^n are the trace mappings for finite field extensions.

On the other hand, for $r \geq 2$, the modulo p^{r-1} reduction gives the homomorphism of rings $\mathrm{GR}(p^r, n) \longrightarrow \mathrm{GR}(p^{r-1}, n)$ and we get the following commutative diagram:

$$\begin{array}{ccccccccc} \mathrm{GR}(p^r, n) & \xrightarrow{mod\ p^{r-1}} & \mathrm{GR}(p^{r-1}, n) & \longrightarrow & \cdots & \xrightarrow{mod\ p^2} & \mathrm{GR}(p^2, n) & \xrightarrow{mod\ p} & \mathrm{GR}(p, n) = \mathbb{F}_q \\ \sigma^{(r)} \downarrow & & \sigma^{(r-1)} \downarrow & & & & \sigma^{(2)} \downarrow & & \sigma^{(1)} \downarrow \\ \mathrm{GR}(p^r, n) & \xrightarrow{mod\ p^{r-1}} & \mathrm{GR}(p^{r-1}, n) & \longrightarrow & \cdots & \xrightarrow{mod\ p^2} & \mathrm{GR}(p^2, n) & \xrightarrow{mod\ p} & \mathbb{F}_q \end{array} \quad (6)$$

where $\sigma^{(\lambda)}$ is the automorphism of $\mathrm{GR}(p^\lambda, n)$ defined by

$$\sigma^{(\lambda)}\left(\sum_{i=0}^{\lambda-1} p^i x_i\right) = \sum_{i=0}^{\lambda-1} p^i x_i^p \quad (x_i \in \mathrm{T}).$$

Next we need some basic properties on the polynomial ring $\mathbf{R}[x]$. One of the most important properties on $\mathbf{R}[x]$ is the following Hensel's Lemma.

Two polynomials $f(x)$ and $g(x)$ in $\mathbf{R}[x]$ are called coprime if there exist $A(x)$ and $B(x)$ in $\mathbf{R}[x]$ such that $f(x)A(x) + g(x)B(x) = 1$.

Lemma 1. *([19], Lemma 14.20) Let* $\mathbf{R} = \mathrm{GR}(p^r, n)$ *and* $\overline{\mathbf{R}} = \mathbb{F}_q$ $(q = p^n)$*. Let* $f(x)$ *be a monic polynomial in* $\mathbf{R}[x]$ *and* $g_i(x)$ $(1 \leq i \leq s)$ *be pairwise coprime monic polynomials in* $\overline{\mathbf{R}}[x]$*. If* $\overline{f}(x) = g_1(x)g_2(x)\cdots g_s(x)$ *in* $\overline{\mathbf{R}}[x]$*, then there exist pairwise coprime polynomials* $f_i(x)$ $(1 \leq i \leq s)$ *in* $\mathbf{R}[x]$ *such that* $f(x) = f_1(x)f_2(x)\cdots f_s(x)$ *and* $\overline{f}_i(x) = g_i(x)$ $(1 \leq i \leq s)$*.*

The polynomial $f_i(x)$ is called the Hensel lift of $g_i(x)$. A monic polynomial $f(x)$ in $\mathbf{R}[x]$ is called primary if $\overline{f}(x)$ is a power of a monic irreducible polynomial in $\mathbb{F}_q[x]$. One can deduce the following result from the Hensel's Lemma .

Lemma 2. *([19], Theorem 14.21) Let* $f(x)$ *be a monic polynomial of* $\deg f \geq 1$ *in* $\mathbf{R}[x]$*. We have the following decomposition*

$$f(x) = f_1(x)f_2(x)\cdots f_r(x),$$

where $f_i(x)$ $(1 \leq i \leq r)$ *are pairwise coprime primary polynomials in* $\mathbf{R}[x]$ *and* $f_i(x)$ $(1 \leq i \leq r)$ *are uniquely determined up to their order. Particularly, if* $\overline{f}(x) = p_1(x)p_2(x)\cdots p_r(x)$ *where* $p_i(x)$ $(1 \leq i \leq r)$ *are distinct monic irreducible polynomials in* $\overline{\mathbf{R}}[x] = \mathbb{F}_q[x]$*, then* $f_i(x)$ $(1 \leq i \leq r)$ *are distinct monic irreducible polynomials in* $\mathbf{R}[x]$ *and* $\overline{f}_i(x) = p_i(x)$ $(1 \leq i \leq r)$*.*

3. Criteria on Normal bases for Galois Ring Extensions

From (1) we know that $\mathbf{R} = \mathrm{GR}(p^r, n)$ is a free Z_{p^r}-module of rank n and $\{1, \gamma, \cdots, \gamma^{n-1}\}$ is a basis for $\mathbf{R}/\mathrm{Z}_{p^r}$, where γ is an element of order $q - 1$ $(q = p^n)$ in $\mathbf{R}$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 September 2018 doi:10.20944/preprints201809.0559.v1

Peer-reviewed version available at Symmetry 2018, 10, 702; doi:10.3390/sym10120702

Definition 1. *An element $\alpha \in \mathbf{R}$ is called a normal basis generator (NBG) for extension $\mathbf{R}/Z_{p^r}$ if $\mathfrak{B} = \{\sigma^0(\alpha) = \alpha, \sigma(\alpha), \cdots, \sigma^{n-1}(\alpha)\}$ is a basis for $\mathbf{R}/Z_{p^r}$, where σ is the automorphism σ_p of $\mathbf{R}$ defined by (3). Such basis $\mathfrak{B}$ is called a normal basis for $\mathbf{R}/Z_{p^r}$.*

In this section we present several criteria on normal bases for Galois ring extension $\mathbf{R}/Z_{p^r}$, these criteria can be reduced to the ones of finite field extensions $\overline{\mathbf{R}}/\overline{Z}_{p^r} = \mathbb{F}_q/\mathbb{F}_p$ according to the following theorem. Recall that an element $a \in \mathbb{F}_q$ $(q = p^n)$ is a NBG for $\mathbb{F}_q/\mathbb{F}_p$ if $\mathfrak{B} = \{a, \bar{\sigma}(a), \cdots, \bar{\sigma}^{n-1}(a)\}$ is a normal basis for $\mathbb{F}_q/\mathbb{F}_p$, where $\bar{\sigma}$ is the Frobenius automorphism of $\mathbb{F}_q$ defined by $\bar{\sigma}(b) = b^p$ for $b \in \mathbb{F}_q$. From the definition of σ in (3), one has for $\alpha \in \mathbf{R}$, $\overline{\sigma(\alpha)} = \bar{\sigma}(\bar{\alpha})$.

Theorem 1. *For an element α in $\mathbf{R}$, α is a NBG for $\mathbf{R}/Z_{p^r}$ if and only if $\bar{\alpha}$ is a NBG for finite field extension $\overline{\mathbf{R}}/\overline{Z}_{p^r} = \mathbb{F}_q/\mathbb{F}_p$.*

Proof. Suppose that $\bar{\alpha}$ is not a NBG for $\mathbb{F}_q/\mathbb{F}_p$. Then there exist $a_i \in \mathbb{F}_p$ $(0 \le i \le n-1)$ such that

$$\sum_{i=0}^{n-1} a_i \bar{\sigma}^i(\bar{\alpha}) = 0 \tag{7}$$

and $a_j \neq 0$ for some j. Let $A_i \in \mathbf{R}$, $\overline{A_i} = a_i$ $(0 \le i \le n-1)$. The formula (7) implies that $\overline{\sum_{i=0}^{n-1} A_i \sigma^i(\alpha)} = \sum_{i=0}^{n-1} a_i \bar{\sigma}^i(\bar{\alpha}) = 0$ so that $\sum\limits_{i=0}^{n-1} A_i \sigma^i(\alpha) \in p\mathbf{R}$. Therefore $\sum\limits_{i=0}^{n-1} p^{r-1} A_i \sigma^i(\alpha) = 0$. From $a_j \in \mathbb{F}_p^{\times}$ we know that $A_j \in \mathbf{R}^*$ and $p^{r-1} A_j \neq 0$. Therefore α is not a NBG for $\mathbf{R}/Z_{p^r}$.

On the other hand, suppose that α is not a NBG for $\mathbf{R}/Z_{p^r}$. Then there exist $A_i \in \mathbf{R}$ $(0 \le i \le n-1)$ such that

$$\sum_{i=0}^{n-1} A_i \sigma^i(\alpha) = 0 \tag{8}$$

and $A_j \neq 0$ for some j. Let $A_i \in p^{d_i}\mathbf{R} \setminus p^{d_i+1}\mathbf{R}$ $(0 \le i \le n-1)$ and $d = \min\{d_i | 0 \le i \le n-1\}$. From $A_j \neq 0$, we get $0 \le d \le r-1$. Then $A_i = p^d a_i$ where $a_i \in \mathbf{R}$ $(0 \le i \le n-1)$ and $a_j \in \mathbf{R}^*$ by assuming $A_j \in p^d\mathbf{R} \backslash p^{d+1}\mathbf{R}$. The formula (8) implies that $p^d \sum\limits_{i=0}^{n-1} a_i \sigma^i(\alpha) = 0$ so that $\sum\limits_{i=0}^{n-1} a_i \sigma^i(\alpha) \in p^{r-d}\mathbf{R}$. Then from $r - d \ge 1$, we get $\sum\limits_{i=0}^{n-1} \bar{a}_i \bar{\sigma}^i(\bar{\alpha}) = 0$ where $\bar{a}_i \in \mathbb{F}_p$ $(0 \le i \le n-1)$ and $\bar{a}_j \neq 0$. Therefore $\bar{\alpha}$ is not a NBG for $\mathbb{F}_q/\mathbb{F}_p$. This completes the proof of Theorem 1. □

By Theorem 1, a series of criteria on normal bases for finite field extensions can be shifted to ones for Galois ring extensions.

Lemma 3. *([20]) Let $n = p^t l$, $(l, p) = 1$, $Q = p^n$ and $q = p^l$. Let tr_q^Q be the trace mapping for $\mathbb{F}_Q/\mathbb{F}_q$. Then for $a \in \mathbb{F}_Q$, a is a NBG for $\mathbb{F}_Q/\mathbb{F}_p$ if and only if $\mathrm{tr}_q^Q(a)$ is a NBG for $\mathbb{F}_q/\mathbb{F}_p$.*

From the diagram (5) we know that for $\alpha \in \mathbf{R}$, $\mathrm{tr}_l^n(\bar{\alpha}) = \overline{\mathrm{Tr}_l^n(\alpha)}$.

Corollary 1. *Let $n = p^t l$, $(l, p) = 1$. Let $\mathbf{R} = \mathrm{GR}(p^r, n)$, $\mathbf{R}' = \mathrm{GR}(p^r, l)$, and $\mathrm{Tr} : \mathbf{R} \to \mathbf{R}'$ be the trace mapping from $\mathbf{R}$ to $\mathbf{R}'$. Then for $\alpha \in \mathbf{R}$, α is a NBG for $\mathbf{R}/Z_{p^r}$ if and only if $\mathrm{Tr}(\alpha)$ is a NBG for $\mathbf{R}'/Z_{p^r}$.*

By Corollary 1, we assume $(n, p) = 1$ without loss of generality. In this case, $x^n - 1$ has the following decomposition in the polynomial ring $\mathbb{F}_p[x]$:

$$x^n - 1 = p_1(x) p_2(x) \cdots p_r(x), \tag{9}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 September 2018 doi:10.20944/preprints201809.0559.v1

Peer-reviewed version available at Symmetry 2018, 10, 702; doi:10.3390/sym10120702

where $p_1(x), p_2(x), \cdots, p_r(x)$ are distinct monic irreducible polynomials in $\mathbb{F}_p[x]$.

Let $\mathcal{F}_p[x]$ be the set of all p-polynomials $\sum_i c_i x^{p^i}$ $(c_i \in \mathbb{F}_p)$. Then $\mathcal{F}_p[x]$ is a ring with respect to the ordinary addition and the following multiplication defined by composition $\otimes$:

$$F(x) \otimes G(x) = F(G(x)), \quad \text{for } F(x), G(x) \in \mathcal{F}_p[x],$$

and the mapping

$$\mu : \mathbb{F}_p[x] \longrightarrow \mathcal{F}_p[x], \qquad \sum_i c_i x^i \longrightarrow \sum_i c_i x^{p^i}$$

is an isomorphism of rings. Corresponding to the decomposition (9) in $\mathbb{F}_p[x]$, we have the following decomposition of

$$x^{p^n} - x = P_1(x) \otimes P_2(x) \otimes \cdots \otimes P_r(x),$$

where $P_i(x) = \mu(p_i(x))$ $(1 \le i \le r)$ are distinct monic irreducible p-polynomials in $\mathcal{F}_p[x]$. Let $m_i(x) = \frac{x^n - 1}{p_i(x)}$ and $M_i(x) = \mu(m_i(x)) = \bigotimes_{\substack{\lambda=1 \\ \lambda \neq i}}^{r} P_\lambda(x) \in \mathcal{F}_p[x]$.

Lemma 4. *([19]) Let $q = p^n$ and $(n, p) = 1$. For $a \in \mathbb{F}_q$, a is a NBG for $\mathbb{F}_q/\mathbb{F}_p$ if and only if $M_i(a) \neq 0$ $(1 \le i \le r)$.*

As a direct consequence of Theorem 1 and Lemma 4. We have the following criterion.

Corollary 2. *Let $\mathbf{R} = \mathrm{GR}(p^r, n)$, where $(n, p) = 1$. Then for $\alpha \in \mathbf{R}$, α is a NBG for $\mathbf{R}/Z_{p^r}$ if and only if $M_i(\bar{\alpha}) \neq 0$ $(1 \le i \le r)$.*

By the decomposition (9) we have

$$\frac{\mathbb{F}_p[x]}{(x^n - 1)} = \bigoplus_{i=1}^{r} \frac{\mathbb{F}_p[x]}{(p_i(x))} \cong \bigoplus_{i=1}^{r} \mathbb{F}_{p^{d_i}},$$

where $d_i = \deg p_i(x)$. Then we have the orthogonal idempotents $e_i(x) \in \mathbb{F}_p[x], \deg e_i(x) \le n - 1$ $(1 \le i \le r)$ satisfying

$$e_i(x) \equiv \delta_{ij} (\mathrm{mod}\ p_j(x)) \ (1 \le i \le j \le r),$$

where δ_{ij} is the Kronecker symbol. These idempotents $e_i(x)$ $(1 \le i \le r)$ can be computed by using σ_p-class of the roots of $x^n - 1$ (see [20]).

In [20], we present a new criterion of NBG for $\mathbb{F}_q/\mathbb{F}_p$ $(q = p^n, (n, p) = 1)$ by using idempotents in the ring $\frac{\mathbb{F}_p[x]}{(x^n - 1)}$.

Lemma 5. *([20]) Let $E_i(x) = \mu(e_i(x)) \in \mathcal{F}_p[x]$ $(1 \le i \le r)$, $a \in \mathbb{F}_q$ $(q = p^n, (n, p) = 1)$, a is a NBG for $\mathbb{F}_q/\mathbb{F}_p$ if and only if $E_i(a) \neq 0$ $(1 \le i \le r)$.*

Corollary 3. *Let $\mathbf{R} = GR(p^r, n)$, where $(n, p) = 1$. Then for $\alpha \in \mathbf{R}$, α is a NBG for $\mathbf{R}/Z_{p^r}$ if and only if $E_i(\bar{\alpha}) \neq 0 \in \mathbb{F}_q$ $(1 \le i \le r)$.*

In [20] we present more explicit criteria on normal bases for $\mathbb{F}_q/\mathbb{F}_p$ for several specific cases where the decomposition (9) has a simpler form. By Corollary 3 we can give more explicit criteria on normal bases of Galois ring extension for such cases. For example, let p and n be prime numbers and $(\mathbb{Z}/n\mathbb{Z})^* = \langle p \rangle$. Then for $a \in \mathbb{F}_q$ $(q = p^n)$, a is a NBG for $\mathbb{F}_q/\mathbb{F}_p$ if and only if $a \notin \mathbb{F}_p$ and $\mathrm{tr}(a) \neq 0$, where $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace mapping. Let $\mathrm{Tr} : \mathbf{R} = \mathrm{GR}(p^r, n) \to \mathrm{Z}_{p^r}$ be the trace mapping. For $\alpha \in \mathbf{R}$,

$$\mathrm{tr}(\overline{\alpha}) \in \mathbb{F}_p \Leftrightarrow \mathrm{tr}(\overline{\alpha})^p - \mathrm{tr}(\overline{\alpha}) = 0 \Leftrightarrow \mathrm{Tr}(\alpha)^p - \mathrm{Tr}(\alpha) \in p\mathbf{R}$$

and

$$\mathrm{tr}(\bar{\alpha}) = 0 \Leftrightarrow \mathrm{Tr}(\alpha) \in p\mathbf{R}.$$

Corollary 4. *Let $\mathbf{R} = \mathrm{GR}(p^r, n)$, where p and n are distinct prime numbers and $(\mathbb{Z}/n\mathbb{Z})^* = \langle p \rangle$. Then for $\alpha \in \mathbf{R}$, α is a NBG for $\mathbf{R}/\mathrm{Z}_{p^r}$ if and only if both of $\mathrm{Tr}(\alpha)$ and $\mathrm{Tr}(\alpha)^p - \mathrm{Tr}(\alpha)$ belong to $\mathbf{R}^*$.*

We end this section by counting the number of NBG for $\mathbf{R}/\mathrm{Z}_{p^r}$ where $\mathbf{R} = \mathrm{GR}(p^r, n)$. It is well known ([19], Corollary 8.25) that the number of NBG's for $\mathbb{F}_q/\mathbb{F}_p$ $(q = p^n)$ is (let $n = p^e m$ and $(m, p) = 1$)

$$\psi_q(n) = p^n \prod_{d|m} (1 - p^{-\mathrm{ord}_d(p)})^{\phi(d)/\mathrm{ord}_d(p)},$$

where $\phi(d)$ is the Euler function and $\mathrm{ord}_d(p)$ is the order of p in $(\mathbb{Z}/d\mathbb{Z})^*$. Since the mapping $\varphi : \mathbf{R} = \mathrm{GR}(p^r, n) \to \overline{\mathbf{R}} = \mathbb{F}_q$ $(q = p^n)$ is surjective and $\mathbb{F}_p$-linear, we get that $|\mathrm{Ker}\ \varphi| = |\mathbf{R}|/|\overline{\mathbf{R}}| = p^{rn-n}$. As a direct consequence of Theorem 1, we can count the number of NBG's for $\mathbf{R}/\mathrm{Z}_{p^r}$.

Corollary 5. *Let p be a prime number and $n = p^e m$ be a positive integer with $(m, p) = 1$. For $\mathbf{R} = \mathrm{GR}(p^r, n)$, the number of NBG's for $\mathbf{R}/\mathrm{Z}_{p^r}$ is*

$$\psi = p^{rn} \prod_{d|m} (1 - p^{-\mathrm{ord}_d(p)})^{\phi(d)/\mathrm{ord}_d(p)}$$

and the number of normal bases for $\mathbf{R} = \mathrm{GR}(p^r, n)$ is ψ/n.

4. Multiplicative Complexity on Normal Bases

It is well known that normal bases on finite fields with low multiplication are useful in various applications including coding theory, cryptography, signal processing and so on. Similar to the case of finite fields, Abrahamsson discussed the multiplicative complexity on normal bases over Galois rings, and considered the architectures for multiplication in Galois rings (for $p = 2$) in his thesis. In this section we discuss the complexity of normal bases for extension $\mathbf{R}/\mathrm{Z}_{p^r}$, where $\mathbf{R} = \mathrm{GR}(p^r, n)$.

Definition 2. *Let α be a NBG for $\mathbf{R}/\mathrm{Z}_{p^r}$, so that $\mathfrak{B} = \{\alpha, \sigma(\alpha), \cdots, \sigma^{n-1}(\alpha)\}$ is a normal basis for $\mathbf{R}/\mathrm{Z}_{p^r}$, where σ is the automorphism of $\mathbf{R}$ defined by (3). Then*

$$\alpha\sigma^i(\alpha) = \sum_{j=0}^{n-1} c_{ij}\sigma^j(\alpha) \quad (0 \le i \le n-1, c_{ij} \in \mathrm{Z}_{p^r}). \tag{10}$$

The multiplicative complexity $\mathrm{M}(\mathfrak{B}(\alpha))$ of the normal basis $\mathfrak{B}$ is defined by the number of nonzero c_{ij}. Namely,

$$\mathrm{M}(\mathfrak{B}(\alpha)) = \sharp\{(i, j) : 0 \le i, j \le n-1, c_{ij} \ne 0\}.$$

For each λ $(1 \le \lambda \le r)$, $\alpha \in \mathbf{R}$, let $\alpha^{(\lambda)}$ denote the modulo p^λ reduction of α. The mapping

$$\mathbf{R} = \mathrm{GR}(p^r, n) \longrightarrow \mathbf{R}^{(\lambda)} = \mathrm{GR}(p^\lambda, n), \quad \alpha \mapsto \alpha^{(\lambda)}$$

is a homomorphism of rings and $\alpha^{(r)} = \alpha$, $\alpha^{(1)} = \bar{\alpha} \in \overline{\mathrm{GR}(p, n)} = \overline{\mathbf{R}^{(1)}} = \mathbb{F}_p$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 September 2018 doi:10.20944/preprints201809.0559.v1

Peer-reviewed version available at Symmetry 2018, 10, 702; doi:10.3390/sym10120702

For $\alpha \in \mathbf{R}(=\mathbf{R}^{(r)}), \alpha$ is a NBG for $\mathbf{R}/\mathrm{Z}_{p^r}$ if and only if $\bar{\alpha}$ is a NBG for $\mathbb{F}_q/\mathbb{F}_p$ by Theorem 1, then this is also equivalent to that $\alpha^{(\lambda)}$ is a NBG for $\mathbf{R}^{(\lambda)}/\mathrm{Z}_{p^r}$ for any $\lambda \geq 1$. Moreover, by the diagram (6) we get that for any λ, the equality (10) implies that

$$\alpha^{(\lambda)}\sigma^{(\lambda)i}(\alpha^{(\lambda)}) = \sum_{j=0}^{n-1} c_{ij}^{(\lambda)}\sigma^{(\lambda)j}(\alpha^{(\lambda)}) \quad (0 \leq i \leq n-1, c_{ij}^{(\lambda)} \in \mathrm{Z}_{p^\lambda}).$$

If $0 \neq c_{ij}^{(\lambda)} \in \mathrm{Z}_{p^\lambda}$, then $0 \neq c_{ij}^{(\mu)} \in \mathrm{Z}_{p^\mu}$ for all $\mu \geq \lambda$. Therefore we get the following simple and basic result.

Theorem 2. *Let $\mathbf{R} = \mathrm{GR}(p^r, n)$ and α be a NBG for $\mathbf{R}/\mathrm{Z}_{p^r}$. Then for each $1 \leq \lambda \leq r-1, \alpha^{(\lambda)}$ is a NBG for $\mathbf{R}^{(\lambda)}/\mathrm{Z}_{p^r}$, where $\mathbf{R}^{(\lambda)} = \mathrm{GR}(p^\lambda, n)$. Moreover, let $\mathfrak{B}^{(\lambda)} = \mathfrak{B}(\alpha^{(\lambda)}) = \{\sigma^{(\lambda)i}(\alpha^{(\lambda)}) : 0 \leq i \leq n-1\}$. Then*

$$\mathrm{M}(\mathfrak{B}^{(r)}) \geq \mathrm{M}(\mathfrak{B}^{(r-1)}) \geq \cdots \geq \mathrm{M}(\mathfrak{B}^{(1)}),$$

where $\mathfrak{B}^{(1)}$ is the normal basis $\overline{\mathfrak{B}} = \{\bar{\alpha}^{p^i} : 0 \leq i \leq n-1\}$ for $\mathrm{GR}(p,n)/\mathrm{Z}_p = \mathbb{F}_q/\mathbb{F}_p$.

It is well known that for any normal basis $\mathfrak{B}$ for finite field extension $\mathbb{F}_{q^n}/\mathbb{F}_q, \mathrm{M}(\mathfrak{B}) \geq 2n-1$. Hence, by Theorem 2, for any normal basis $\mathfrak{B}$ for Galois ring extension $\mathrm{GR}(p^r,n)/\mathrm{Z}_{p^r}, \mathrm{M}(\mathfrak{B}) \geq 2n-1$. The basis $\mathfrak{B}$ is called optimal if $\mathrm{M}(\mathfrak{B}) = 2n-1$. If $\mathfrak{B}$ is an optimal normal basis for $\mathbf{R}/\mathrm{Z}_{p^r}$, then by Theorem 2,

$$2n-1 = \mathrm{M}(\mathfrak{B}) \geq \mathrm{M}(\mathfrak{B}^{(r-1)}) \geq \cdots \geq \mathrm{M}(\mathfrak{B}^{(1)}) \geq 2n-1.$$

Therefore $\mathrm{M}(\mathfrak{B}^{(\lambda)}) = 2n-1$. Namely, $\mathfrak{B}^{(\lambda)}$ is an optimal normal basis for $\mathbf{R}^{(\lambda)}/\mathrm{Z}_{p^r}$ for all $1 \leq \lambda \leq r$. Particularly, $\mathfrak{B}^{(1)} = \overline{\mathfrak{B}}$ is an optimal normal basis for the finite field extension $\mathbf{R}^{(1)}/\mathrm{Z}_p = \mathbb{F}_q/\mathbb{F}_p$ $(q = p^n)$.

Definition 3. *Two elements $\alpha, \ \beta \in \mathbf{R}^* = \mathrm{GR}(p^r,n)^*$ equivalent to each other if $\alpha = \varepsilon\beta$ for some $\varepsilon \in \mathrm{Z}_{p^r}^*$, and denoted by $\alpha \sim \beta$.*

If α is a NBG for $\mathbf{R}/\mathrm{Z}_{p^r}$ and $\alpha \sim \beta, \beta = \varepsilon\alpha$ for some $\varepsilon \in \mathrm{Z}_{p^r}^*$. It is easy to see that β is also a NBG for $\mathbf{R}/\mathrm{Z}_{p^r}$. Moreover, let

$$\alpha\sigma^\lambda(\alpha) = \sum_{i=0}^{n-1} c_{\lambda i}\sigma^i(\alpha) \quad (c_{\lambda i} \in \mathrm{Z}_{p^r}, 0 \leq \lambda \leq n-1).$$

Then $\sigma^\lambda(\beta) = \varepsilon\sigma^\lambda(\alpha)$ and

$$\beta\sigma^\lambda(\beta) = \sum_{i=0}^{n-1} \varepsilon c_{\lambda i}\sigma^i(\beta) \quad (\varepsilon c_{\lambda i} \in \mathrm{Z}_{p^r}).$$

Since $c_{\lambda i} = 0$ if and only if $\varepsilon c_{\lambda i} = 0$, two normal bases $\mathfrak{B}(\alpha) = \{\sigma^\lambda(\alpha) : 0 \leq \lambda \leq n-1\}$ and $\mathfrak{B}(\beta) = \{\sigma^\lambda(\beta) : 0 \leq \lambda \leq n-1\}$ have the same complexity: $\mathrm{M}(\mathfrak{B}(\alpha)) = \mathrm{M}(\mathfrak{B}(\beta))$.

All optimal normal bases for finite field extension have been determined in [9].

Lemma 6. *(Gao and Lenstra, [9]) There are only two types of optimal normal bases $\mathfrak{B}$ for finite field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ as following.*

Type (I): *$n+1$ and p are distinct prime numbers, $\mathrm{Z}_{n+1}^* = \langle p \rangle$, and $\mathfrak{B}$ is equivalent to the following (optimal) normal bases for $\mathbb{F}_{p^n}/\mathbb{F}_p$,*

$$\mathfrak{B}(\xi) = \{\sigma_p^\lambda(\xi) = \xi^{p^\lambda} : 0 \leq \lambda \leq n-1\} = \{\xi^i : 1 \leq i \leq n\},$$

where ξ is an (n+1)-th primitive root of 1 in the algebraic closure of $\mathbb{F}_p$ so that $\mathbb{F}_p(\xi) = \mathbb{F}_{p^n}$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 September 2018 doi:10.20944/preprints201809.0559.v1

Peer-reviewed version available at *Symmetry* **2018**, *10*, 702; doi:10.3390/sym10120702

Type (II): *$p = 2$ and $2n+1$ is a prime number, $Z^*_{2n+1} = \langle -1, 2 \rangle$, and $\mathfrak{B}$ is equivalent to the following (optimal) normal bases for $\mathbb{F}_{2^n}/\mathbb{F}_2$*

$$\begin{aligned} \mathfrak{B}(\xi+\xi^{-1}) &= \{\sigma_2^{\lambda}(\xi+\xi^{-1}) = \xi^{2^\lambda} + \xi^{-2^\lambda} : 0 \le \lambda \le n-1\} \\ &= \{\xi^i + \xi^{-i} : 1 \le i \le n\}, \end{aligned}$$

where ξ is a $(2n+1)$-th root of 1 in the algebraic closure of $\mathbb{F}_2$, $\mathbb{F}_2(\xi+\xi^{-1}) = \mathbb{F}_{2^n}$.

Abrahamsson [1] presented the following optimal normal bases for Galois ring extension as a generalization of Type (I) optimal normal bases for finite field extension.

Lemma 7. *([1]) Let p and $n+1$ be distinct prime numbers such that $Z^*_{n+1} = \langle p \rangle$. Let ζ be an $(n+1)$-th root of 1 in $\mathbf{R} = \mathrm{GR}(p^r, n)$. Then*

$$\mathfrak{B}(\zeta) = \{\sigma^{\lambda}(\zeta) = \zeta^{p^\lambda} : 0 \le \lambda \le n-1\} = \{\zeta^i : 1 \le \lambda \le n\}$$

is an optimal normal basis for $\mathbf{R}/Z_{p^r}$.

In this section we determine all optimal normal bases for Galois ring extensions. If $\alpha \in \mathbf{R}^*$ and $\mathfrak{B}(\alpha)$ is an optimal normal bases for $\mathbf{R}/Z_{p^r}$ ($\mathbf{R} = \mathrm{GR}(p^r, n)$), then $\mathfrak{B}(\bar{\alpha})$ is an optimal normal basis for $\mathbb{F}_q/\mathbb{F}_p$ ($q = p^n$), and then $\mathfrak{B}(\bar{\alpha})$ is an optimal normal basis for Type (I) or Type (II) by Lemma 6. Now we consider these two cases separably.

Theorem 3. *Suppose that $n+1$ and p be distinct primes and $Z^*_{n+1} = \langle p \rangle, \mathbf{R} = \mathrm{GR}(p^r, n), n \ge 2$. Then any optimal normal basis for $\mathbf{R}/Z_{p^r}$ is equivalent to one given by Lemma 6.*

Proof. For $r = 1, \mathbf{R}/Z_{p^r} = \mathbb{F}_q/\mathbb{F}_p$ is the finite field extension case. For $r = 2$, we assume that $\mathfrak{B}(\alpha) = \{\sigma^{\lambda}(\alpha) : 0 \le \lambda \le n-1\}$ is an optimal normal basis for $\mathbf{R}/Z_{p^2}$, $\mathbf{R} = \mathrm{GR}(p^2, n)$. Then $\bar{\alpha} = \xi$ where ξ is an $(n+1)$-th primitive root of 1 in $\mathbb{F}_q$ ($q = p^n$). Let ζ be an $(n+1)$-th primitive root of 1 in $\mathbf{R}$ such that $\bar{\zeta} = \xi$. Then $\zeta \in \mathrm{T}^*$ by $(n+1)|(q-1)$, where T^* is the cyclic multiplicative group of $\mathbf{R}$, see Fact 3 in Section II, and

$$\alpha = \zeta + pa = \zeta + p\sum_{i=1}^{n} c_i\zeta^i \quad (a \in \mathbf{R}, c_i \in Z_{p^2}), \tag{11}$$

since $\{\zeta^i : 1 \le i \le n\} = \{\zeta^{p^\lambda} : 0 \le \lambda \le n-1\}$ is a (normal) basis for $\mathbf{R}/Z_{p^2}$. Therefore

$$\sigma^{\lambda}(\alpha) = \zeta^{p^\lambda} + p\sum_{i=1}^{n} c_i\zeta^{ip^\lambda} \text{ since } \sigma^{\lambda}(\zeta^i) = \zeta^{ip^\lambda},\ 0 \le \lambda \le n-1 \tag{12}$$

and for $0 \le \lambda \le n-1, \lambda \ne \frac{n}{2}$ (we can assume that $n+1$ is an odd prime number, so that n is even),

$$\begin{aligned} \alpha\sigma^{\lambda}(\alpha) &= (\zeta + p\sum_{i=1}^{n} c_i\zeta^i)(\zeta^{p^\lambda} + p\sum_{i=1}^{n} c_i\zeta^{ip^\lambda}) \\ &= \zeta^{1+p^\lambda} + p\sum_{i=1}^{n} c_i(\zeta^{i+p^\lambda} + \zeta^{1+ip^\lambda}) \text{ since } p^2 = 0. \end{aligned} \tag{13}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 September 2018 doi:10.20944/preprints201809.0559.v1

Peer-reviewed version available at Symmetry 2018, 10, 702; doi:10.3390/sym10120702

From $\lambda \neq \frac{n}{2}$ we know that $p^{\lambda} \not\equiv -1 (\text{mod } n+1)$ and $1 + p^{\lambda} \equiv p^{\mu} (\text{mod } n+1)$ for some $\mu, 0 \leq \mu \leq n-1$. Then by (13) we have

$$\begin{aligned} \alpha\sigma^{\lambda}(\alpha) &= \zeta^{p^{\mu}} + p \sum_{i=1}^{n} c_i (\zeta^{i+p^{\lambda}} + \zeta^{1+ip^{\lambda}}) \\ &= \sigma^{\mu}(\alpha) + p \sum_{i=1}^{n} c_i (\zeta^{i+p^{\lambda}} + \zeta^{1+ip^{\lambda}} - \zeta^{i(1+p^{\lambda})}) \text{ by } (12) \\ &= \sigma^{\mu}(\alpha) + p[\sum_{l=0}^{n-1} \zeta^{p^l} (c_{p^l - p^{\lambda}} + c_{(p^l-1)p^{-\lambda}} - c_{p^l(1+p^{\lambda})^{-1}}) + c_{-p^{\lambda}} + c_{-p^{-\lambda}}], \end{aligned}$$

where we consider $i \in \mathbb{Z}_{n+1}$ for c_i and assume $c_0 = 0$, so Equation (13) becomes to

$$\alpha\sigma^{\lambda}(\alpha) = \sigma^{\mu}(\alpha) + p(\sum_{l=0}^{n-1} \sigma^{l}(\alpha)(c_{p^l - p^{\lambda}} + c_{(p^l-1)p^{-\lambda}} - c_{p^l(1+p^{\lambda})^{-1}}) - (c_{-p^{\lambda}} + c_{-p^{-\lambda}}) \sum_{l=0}^{n-1} \sigma^{l}(\alpha)),$$

since $\sigma^{l}(\alpha) \equiv \sigma^{l}(\zeta) \equiv \zeta^{p^l} (\text{mod } p)$ and $\sum_{l=0}^{n-1} \sigma^{l}(\alpha) \equiv \sum_{l=0}^{n-1} \sigma^{l}(\zeta) = \sum_{l=0}^{n-1} \zeta^{p^l} = \sum_{j=1}^{n} \zeta^{j} = -1 (\text{mod } p)$.

Therefore for $0 \leq \lambda \leq n-1, \lambda \neq \frac{n}{2}$,

$$\alpha\sigma^{\lambda}(\alpha) = \sum_{l=0}^{n-1} b_{\lambda l} \sigma^{l}(\alpha) \quad (b_{\lambda l} \in \mathbb{Z}_{p^2}),$$

where

$$b_{\lambda l} = \begin{cases} p(c_{p^l - p^{\lambda}} + c_{(p^l-1)p^{-\lambda}} - c_{p^l(1+p^{\lambda})^{-1}} - c_{-p^{-\lambda}} - c_{-p^{\lambda}}), & \text{if } p^l \not\equiv p^{\mu} \equiv (1+p^{\lambda}) (\text{mod } n+1); \\ 1 + p(c_1 - c_{-p^{-\lambda}} - c_{-p^{\lambda}}), & \text{if } p^l \equiv 1 + p^{\lambda} (\text{mod } n+1). \end{cases} \tag{14}$$

And then the complexity $\mathrm{M}(\mathfrak{B}(\alpha)) = \sum_{\lambda=0}^{n-1} \mathrm{M}_{\lambda}$, where

$$\mathrm{M}_{\lambda} = \sharp\{l \mid 0 \leq l \leq n-1, b_{\lambda l} \neq 0 \in \mathbb{Z}_{p^2}\}.$$

For the case of $\lambda = \frac{n}{2}$,

$$\alpha\sigma^{\frac{n}{2}}(\alpha) \equiv \zeta^{p^{n/2}} \zeta = \zeta^{-1}\zeta = 1 = -\sum_{i=1}^{n} \zeta^{i} = -\sum_{\lambda=0}^{n-1} \zeta^{p^{\lambda}} \equiv -\sum_{\lambda=0}^{n-1} \sigma^{\lambda}(\alpha) (\text{mod } p).$$

We get $\mathrm{M}_{\frac{n}{2}} = n$. For $0 \leq \lambda \leq n-1, \lambda \neq \frac{n}{2}$, we have $\mathrm{M}_{\lambda} \geq 1$ since $b_{\lambda l} \equiv 1 (\text{mod } p)$ for l satisfying $p^l \equiv 1 + p^{\lambda} (\text{mod } n+1)$. Then we have

$$2n - 1 = \mathrm{M}(\mathfrak{B}(\alpha)) = \sum_{\lambda=0}^{n-1} \mathrm{M}_{\lambda} = n + \sum_{\substack{\lambda=0 \\ \lambda \neq \frac{n}{2}}}^{n-1} \mathrm{M}_{\lambda} \geq n + \sum_{\substack{\lambda=0 \\ \lambda \neq \frac{n}{2}}}^{n-1} 1 = 2n - 1,$$

which implies that $\mathrm{M}_{\lambda} = 1$ for all $0 \leq \lambda \leq n-1, \lambda \neq \frac{n}{2}$, which means that $b_{\lambda l} = 0$ for all $0 \leq \lambda, l \leq n-1, \lambda \neq \frac{n}{2}$ and $p^l \not\equiv p^{\lambda} + 1 (\text{mod } n+1)$. Let $s \equiv p^{\lambda}, t \equiv p^l (\text{mod } n+1)$. From (14), one gets $\mathfrak{B}(\alpha)$ is an optimal normal basis for $\mathrm{GR}(p^2, n)/\mathbb{Z}_{p^2}$ if and only if when $1 \leq t \leq n, 1 \leq s \leq n-1$ and $t \not\equiv 1 + s (\text{mod } n+1)$, we have

$$-c_{-s^{-1}} - c_{-s} + c_{t-s} + c_{(t-1)s^{-1}} - c_{t(1+s)^{-1}} = 0 \in \mathbb{Z}_p. \tag{15}$$

Peer-reviewed version available at Symmetry 2018, 10, 702; doi:10.3390/sym10120702

Particularly, for $s = 1$ we get

$$-2c_{-1} + 2c_{t-1} - c_{t/2} = 0, \text{ for } 1 \leq t \leq n, t \neq 2.$$

If $p = 2$, then $c_{t/2} = 0 \in \mathbb{F}_2$ for all $1 \leq t \leq n, t \neq 2$. By assumption $Z^*_{n+1} = \langle 2 \rangle$, this means that $c_j = 0$ for all $2 \leq j \leq n$ so that $\alpha = \zeta + pc_1\zeta = (1 + pc_1)\zeta$ by (11) and the basis $\mathfrak{B}(\alpha)$ is equivalent to one given by Lemma 6.

Now we assume that $p \geq 3$. For any fixed $s, 1 \leq s \leq n-1$, by (15), we get

$$\begin{aligned}
0 &= \sum_{\substack{t=1\\ t\neq 1+s}}^{n} (-c_{-s^{-1}} - c_{-s} + c_{t-s} + c_{(t-1)s^{-1}} - c_{t(1+s)^{-1}}) \\
&= (n-1)(-c_{-s^{-1}} - c_{-s}) + \sum_{\substack{l=0\\ l\neq 1,-s}}^{n} c_l + \sum_{\substack{l=0\\ l\neq -s^{-1},1}}^{n} c_l - \sum_{\substack{l=0\\ l\neq 0,1}}^{n} c_l \\
&= (1-n)(c_{-s^{-1}} + c_{-s}) + \sum_{l=1}^{n} c_l - c_1 - c_{-s} - c_{-s^{-1}} \\
&= -n(c_{-s^{-1}} + c_{-s}) + A
\end{aligned}$$

where $A = \sum_{l=2}^{n} c_l$. Therefore

$$n(c_{-s} + c_{-s^{-1}}) = A \tag{16}$$

for all $s, 1 \leq s \leq n-1$. If $3 \leq p \nmid n$, we get $c_{-s} + c_{-s^{-1}} = \frac{A}{n}$ for all $1 \leq s \leq n-1$. Particularly, for $s = 1$ we get $c_n = c_{-1} = \frac{A}{2n}$ and

$$A = c_n + \sum_{l=2}^{n-1} c_l = \frac{A}{2n} + \frac{n-2}{2}\frac{A}{n} = \frac{n-1}{2n}A.$$

Therefore $(n+1)A = 0$ and $A = 0 \in \mathbb{F}_p$, since $(p, n+1) = 1$. Then we have $c_n = 0$ and $c_{-s} + c_{-s^{-1}} = 0$ for $2 \leq s \leq n-1$. Taking $t = s$ in (15) and remark $c_0 = 0$, we get $c_{\frac{s-1}{s}} = c_{\frac{s}{s+1}}$ for $2 \leq s \leq n-1$. Namely,

$$c_{\frac{1}{2}} = c_{\frac{2}{3}} = \cdots = c_{\frac{n-1}{n}}.$$

Since for $1 \leq a, b \leq n-1$,

$$\frac{a}{a+1} \equiv \frac{b}{b+1} (\text{mod } n+1) \Longrightarrow a \equiv b (\text{mod } n+1) \Longrightarrow a = b,$$

we know that $\{\frac{s-1}{s} (\text{mod } n+1) : 2 \leq s \leq n\} = Z_{n+1} \backslash \{0, 1\}$. Therefore $c_2 = c_3 = \cdots = c_{n-1} = c_n = 0$, and $\alpha = (1 + pc_1)\zeta$. Therefore $\mathfrak{B}(\alpha)$ is equivalent to one given by Lemma 6. If $3 \leq p \mid n$, from (16) we have $A = 0$. In this case we fix t $(2 \leq t \leq n-1)$ and the condition (15) implies that

$$\begin{aligned}
0 &= \sum_{\substack{s=1\\ s\neq t-1}}^{n-1} (-c_{-s^{-1}} - c_{-s} + c_{t-s} + c_{(t-1)s^{-1}} - c_{t(1+s)^{-1}}) \\
&= -\sum_{\substack{l=2\\ l\neq -(t-1)^{-1}}}^{n} c_l - \sum_{\substack{l=2\\ l\neq 1-t}}^{n} c_l + \sum_{\substack{l=2\\ l\neq t,t+1}}^{n} c_l + \sum_{\substack{l=2\\ l\neq 1-t}}^{n} c_l - \sum_{\substack{l=2\\ l\neq t}}^{n} c_l \\
&= c_{-(t-1)^{-1}} + c_{1-t} - c_t - c_{t+1} - c_{1-t} + c_t = c_{-(t-1)^{-1}} - c_{t+1}.
\end{aligned}$$

Let $a = -(t-1)^{-1}$, we get

$$c_a = c_{2-a^{-1}} \ (2 \leq a \leq n). \tag{17}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 September 2018 doi:10.20944/preprints201809.0559.v1

Peer-reviewed version available at Symmetry 2018, 10, 702; doi:10.3390/sym10120702

Consider the fraction linear transformation

$$f : Z_{n+1} \cup \{\infty\} \to Z_{n+1} \cup \{\infty\}, f(x) = 2 - x^{-1} = \frac{2x-1}{x}$$

with matrix $M = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$. For any $m \geq 0, M^m = \begin{pmatrix} m+1 & -m \\ m & -(m-1) \end{pmatrix}$ so that

$$f^m(2) = \frac{2(m+1)-m}{2m-(m-1)} = 1 + \frac{1}{m+1} \in Z_{n+1} \backslash \{0,1\} \; (0 \leq m \leq n-2).$$

Therefore $\{f^m(2) : 0 \leq m \leq n-2\} = Z_{n+1} \backslash \{0,1\} = \{2,3,\cdots,n\}$. By (17) we get

$$c_2 = c_3 = \cdots = c_n = \frac{1}{n-1} A = 0.$$

Thus $\alpha = (1+pc_1)\zeta \sim \zeta$. This completes the proof of Theorem 3 for $r = 2$.

Now we assume that $r \geq 3$ and this theorem is true for $r-1$. Let $\alpha \in \mathbf{R} = \mathrm{GR}(p^r, n)$ and $\{\sigma^\lambda(\alpha) : 0 \leq \lambda \leq n-1\}$ is an optimal normal basis for $\mathbf{R}/Z_{p^r}$. By assumption we have, up to equivalence,

$$\alpha = \zeta + p^{r-1}a \; (a \in \mathbf{R}) = \zeta + p^{r-1} \sum_{i=1}^{n} c_i \zeta^i \; (c_i \in Z_{p^r}).$$

Then the same argument for $r = 2$ can be shifted to get $c_i = 0$ for all $2 \leq i \leq n$. Therefore $\alpha = (1+p^{r-1}c_1)\zeta \sim \zeta$. This completes the proof of Theorem 3 □

Remark 1. *Gao and Lenstra determined all optimal normal bases by using the Galois theory on finite fields [9], consequently confirmed a conjecture that was raised by Mullin et al. Here, we give a direct proof of the Theorem 3 by using the mathematical induction.*

Theorem 4. *Assume that $2n+1$ is an odd prime number and $Z^*_{2n+1} = \langle -1, 2 \rangle$. Let $\mathbf{R} = \mathrm{GR}(2^r, n)$ $(r, n \geq 2)$. Then*

(1) If $n \geq 3$, there is no optimal normal basis for $\mathbf{R}/Z_{2^r}$.

(2) If $n = 2$ and $\alpha \in \mathbf{R} = \mathrm{GR}(2^r, 2), \mathfrak{B}^{(\lambda)} = \{\alpha, \sigma(\alpha)\}$ is an optimal normal basis for $\mathbf{R}/Z_{2^r}$ if and only if α is equivalent to $\zeta + \zeta^{-1} + 2b(\zeta^2 + \zeta^{-2})$ where ζ is a 5-th primitive root of 1 in $\mathrm{GR}(2^r, 4)$ so that $\zeta + \zeta^{-1} \in \mathbf{R}$ and b is the unique element in $Z_{2^{r-1}}$ satisfying $1 - b + 4b^2 = 0$.

Proof. (1) First we consider $r = 2$. Suppose that $\alpha \in \mathbf{R} = \mathrm{GR}(4, n)$ and $\mathfrak{B}^{(\lambda)} = \{\sigma^\lambda(\alpha) : 0 \leq \lambda \leq n-1\}$ is an optimal normal basis for $\mathbf{R}/Z_4$. Then $\overline{\mathfrak{B}^{(\lambda)}} = \{\bar{\alpha}^{2^\lambda} : 0 \leq \lambda \leq n-1\}$ is an optimal normal basis for $\mathbb{F}_{2^n}/\mathbb{F}_2$. By Lemma 6, $\bar{\alpha}$ is equivalent to $\xi + \xi^{-1}$ where ξ is a $(2n+1)$-th primitive root of 1 in $\mathbb{F}_{q^2}$. Let ζ be the $(2n+1)$-th primitive root of 1 in $\mathrm{GR}(4, n)$ such that $\bar{\zeta} = \xi$. Then $\zeta + \zeta^{-1} \in \mathbf{R}$ and, up to equivalence

$$\alpha = \zeta + \zeta^{-1} + 2a \; (a \in \mathbf{R}).$$

Since $\{\zeta^{2^\lambda} + \zeta^{-2^\lambda} : 0 \leq \lambda \leq n-1\} = \{\zeta^i + \zeta^{-i} : 1 \leq i \leq n\}$ is a normal basis for $\mathbf{R}/Z_4$ by the assumption that $Z^*_{2n+1} = \langle -1, 2 \rangle$, also, tell me $a = \sum_{i=1}^{n} c_i(\zeta^i + \zeta^{-i})$. So we know that

$$\alpha = \zeta + \zeta^{-1} + 2\sum_{i=1}^{n} c_i(\zeta^i + \zeta^{-i}) \; (c_i \in Z_2), \tag{18}$$

and

$$\sigma^\lambda(\alpha) = \zeta^{2^\lambda} + \zeta^{-2^\lambda} + 2\sum_{i=1}^{n} c_i(\zeta^{i2^\lambda} + \zeta^{-i2^\lambda}) \; (0 \leq \lambda \leq n-1). \tag{19}$$

Let

$$\alpha\sigma^{\lambda}(\alpha) = \sum_{i=0}^{n-1} b_{\lambda i}\sigma^{i}(\alpha) \ (b_{\lambda i} \in \mathrm{Z}_4, 0 \le \lambda \le n-1).$$

We defined

$$\mathrm{M}_{\lambda} = \sharp\{0 \le i \le n-1 : b_{\lambda i} \ne 0\}.$$

Then $2n-1 = \mathrm{M}(\mathfrak{B}^{(\lambda)}) = \sum_{\lambda=0}^{n-1} \mathrm{M}_{\lambda}$. Since

$$\begin{aligned} \overline{\alpha\sigma^{\lambda}(\alpha)} &= (\xi+\xi^{-1})(\xi^{2^{\lambda}}+\xi^{-2^{\lambda}}) \\ &= \begin{cases} \xi^{2}+\xi^{-2}, & \text{for } \lambda = 0 \\ \xi^{2^{\lambda}+1}+\xi^{-(2^{\lambda}+1)}+\xi^{2^{\lambda}-1}+\xi^{-(2^{\lambda}-1)}, & \text{for } 1 \le \lambda \le n-1. \end{cases} \end{aligned}$$

We get $\mathrm{M}_0 \ge 1$ and $\mathrm{M}_{\lambda} \ge 2$ for $1 \le \lambda \le n-1$. Then from $\sum_{\lambda=0}^{n-1} \mathrm{M}_{\lambda} = 2n-1$ we know that $\mathrm{M}_0 = 1$ and $\mathrm{M}_{\lambda} = 2$ for $1 \le \lambda \le n-1$. But

$$\begin{aligned} \alpha\sigma^{0}(\alpha) &= \alpha^{2} = \zeta^{2}+\zeta^{-2}+2 \\ &= \sigma(\alpha) - 2\sum_{i=1}^{n} c_i(\zeta^{2i}+\zeta^{-2i}) - 2(\sum_{i=1}^{n}(\zeta^{2i}+\zeta^{-2i})) \ \text{(by (19))} \\ &= \sigma(\alpha) + 2\sum_{i=1}^{n}(c_i+1)(\zeta^{2i}+\zeta^{-2i}) \\ &= (1+2(c_1+1))\sigma(\alpha) + 2\sum_{i=2}^{n}(c_i+1)\sigma^{l_i}(\alpha), \end{aligned}$$

where l_i is an integer determined by $0 \le l_i \le n-1$ and $2^{l_i} \equiv 2i$ or $-2i (\mathrm{mod}\ 2n+1)$ so that $l_i \ne 1$. From $\mathrm{M}_0 = 1$ we get $c_i = 1 \in \mathrm{Z}_2$ for all $i, 2 \le i \le n$. By (18) we have

$$\begin{aligned} \alpha &= (1+2c_1)(\zeta+\zeta^{-1}) + 2 \ (c_1 \in \mathrm{Z}_2), \\ \zeta+\zeta^{-1} &= (\alpha+2)(1+2c_1) = (1+2c_1)\alpha + 2, \end{aligned}$$

and

$$\begin{aligned} \alpha\sigma(\alpha) &= [(1+2c_1)(\zeta+\zeta^{-1})+2][(1+2c_1)(\zeta^{2}+\zeta^{-2})+2] \\ &= \zeta+\zeta^{-1}+\zeta^{3}+\zeta^{-3}+2(\zeta+\zeta^{-1}+\zeta^{2}+\zeta^{-2}) \\ &= (3+2c_1)\alpha + (1+2c_1)\sigma^{\lambda}(\alpha) + 2\sigma(\alpha), \end{aligned}$$

where λ is determined by $2^{\lambda} \equiv \pm 3 (\mathrm{mod}\ 2n+1)$ and $0 \le \lambda \le n-1$. If $n \ge 3$, then $\lambda \ne 0, 1$. Therefore $\mathrm{M}_1 = 3 \ne 2$. So we proved that there is no optimal normal basis in the case $n \ge 3$.

(2) Let $\alpha \in \mathbf{R} = GR(2^r, 2)$ $(r \ge 2)$ and $\mathfrak{B}^{(\lambda)} = \{\alpha, \sigma(\alpha)\}$ is an optimal normal basis for $\mathbf{R}/\mathrm{Z}_{p^r}$. By Lemma 6, we get

$$\alpha = \zeta+\zeta^{-1}+2(c_1(\zeta+\zeta^{-1})+c_2(\zeta^{2}+\zeta^{-2})) = (1+2c_1)(\zeta+\zeta^{-1})+2c_2(\zeta^{2}+\zeta^{-2}),$$

where ζ is a 5-th primitive root of 1 in $GR(2^r, 4)$, so that $\zeta+\zeta^{-1} \in \mathbf{R}$ and $c_1, c_2 \in \mathrm{Z}_{2^{r-1}}$. Since $1+2c_1$ is invertible in Z_{2^r}, we can assume, up to equivalence,

$$\alpha = \zeta+\zeta^{-1}+2b(\zeta^{2}+\zeta^{-2}), \ \text{for } b \in \mathrm{Z}_{2^{r-1}}. \tag{20}$$

Then $\sigma(\alpha) = \zeta^2 + \zeta^{-2} + 2b(\zeta + \zeta^{-1})$ so that

$$\zeta + \zeta^{-1} = \frac{\begin{vmatrix} \alpha & 2b \\ \sigma(\alpha) & 1 \end{vmatrix}}{\begin{vmatrix} 1 & 2b \\ 2b & 1 \end{vmatrix}} = \frac{\alpha - 2b\sigma(\alpha)}{1-4b^2}, \zeta^2 + \zeta^{-2} = \frac{\begin{vmatrix} 1 & \alpha \\ 2b & \sigma(\alpha) \end{vmatrix}}{\begin{vmatrix} 1 & 2b \\ 2b & 1 \end{vmatrix}} = \frac{\sigma(\alpha) - 2b\alpha}{1-4b^2}$$

and by (20), we have

$$\begin{aligned} \alpha^2 &= \zeta^2 + \zeta^{-2} + 2 + 4b(\zeta + \zeta^{-1})(\zeta^2 + \zeta^{-2}) + 4b^2(\zeta + \zeta^{-1} + 2) \\ &= 2 - 4b + 8b^2 + 4b^2(\zeta + \zeta^{-1}) + \zeta^2 + \zeta^{-2} \\ &= (\zeta + \zeta^{-1})(-2 + 4b - 4b^2) + (\zeta^2 + \zeta^{-2})(-1 + 4b - 8b^2) \\ &= \frac{-2 + 4b - 4b^2}{1 - 4b^2}(\alpha - 2b\sigma(\alpha)) + \frac{-1 + 4b - 8b^2}{1 - 4b^2}(\sigma(\alpha) - 2b\alpha) \\ &= A\alpha + B\sigma(\alpha), \end{aligned}$$

where $(1 + 2b)A = -2(1 - b + 4b^2), (1 + 2b)B = -1 + 6b - 4b^2$. Therefore $\{\alpha, \sigma(\alpha)\}$ is an optimal basis for $\mathbf{R}/\mathrm{Z}_{2^r}$ if and only if $A = 0 \in \mathrm{Z}_{2^r}$, and then if and only if $b \in \mathrm{Z}_{2^{r-1}}$ satisfying $1 - b + 4b^2 \equiv 0(\bmod\ 2^{r-1})$.

Let $\mathbf{Z}_{(2)}$ be the ring of 2-adic integers. Consider $f(x) = 1 - x + 4x^2 \in \mathbf{Z}_{(2)}[x], f'(x) = -1 + 8x$. We have $\mathrm{v}_2(f(1)) = \mathrm{v}_2(4) = 2$ and $\mathrm{v}_2(f'(1)) = \mathrm{v}_2(7) = 0$ where v_2 is the 2-adic exponential valuation. From Hensel's Lemma and $\mathrm{v}_2(f(1)) > 2\mathrm{v}_2(f'(1))$ we know that there exists unique $b \in \mathrm{Z}_{2^{r-1}}$ such that $1 - b + 4b^2 = 0$ for any $r \geq 2$. This completes the proof of Theorem 4. □

Putting Theorem 3 together with Theorem 4, we can derive the following results.

Theorem 5. *Let* $\mathbf{R} = \mathrm{GR}(p^r, n), r, n \geq 2$. *Then*
(1) There exists optimal normal basis $\mathfrak{B}(\alpha) = \{\sigma^\lambda(\alpha) : 0 \leq \lambda \leq n-1\}$ *for* $\mathbf{R}/\mathrm{Z}_{p^r}$ *if and only if (A)* $n+1$ *and* p *are distinct prime numbers and* $\mathrm{Z}_{n+1}^* = \langle p \rangle$ *or; (B)* $p = n = 2$.
(2) For case (A), $\mathfrak{B}(\alpha)$ *is an optimal normal basis for* $\mathbf{R}/\mathrm{Z}_{p^r}$ *if and only if* α *is equivalent to an* $(n+1)$*-th primitive root* ζ *of 1. Namely,* $\alpha = a\zeta$ $(a \in \mathrm{Z}_{p^r}^*)$.
(3) For case (B), $\mathfrak{B}(\alpha)$ *is an optimal normal basis for* $\mathrm{GR}(2^r, 2)/\mathrm{Z}_{2^r}$ *if and only if* α *is equivalent to* $\zeta + \zeta^{-1} + 2b(\zeta^2 + \zeta^{-2})$ *where* ζ *is a 5-th primitive root of 1 in* $\mathrm{GR}(2^r, 4)$ *so that* $\zeta + \zeta^{-1}, \zeta^2 + \zeta^{-2} \in \mathrm{GR}(2^r, 2)$ *and* $b \in \mathrm{Z}_{2^{r-1}}$ *is the unique element satisfying* $1 - b + 4b^2 = 0$.

Author Contributions: Feng Keqin obtained the idea from Abrahamsson's thesis to research the normal bases on Galois ring extension, and then we wrote and revised the paper together.

Funding: This research was funded by the National Natural Science Foundation of China under Grants 11471178 and 11571107

Conflicts of Interest: The authors declare no conflict of interest..

References

1. Abrahamsson, B. Architectures for Multiplication in Galois Rings, thesis, Linköping, Sweden, http:// www. ep.liu.se/exjobb/isy/ex/3549/, 2004.
2. Ash, D.W.; Blake, I.F.; Vanstone,S.A. Low complexity normal bases, *Disc. Appl. Math.* **1989**, *25*, 191-210.
3. Ballet, S.; Chaumine,J.; Pieltant, J.; Rolland, R. On the tensor rank of multiplication in finite extensions of finite fields. *Jour. Number Theory* **2011**, *128(6)*, 1795-1806.
4. Boztas,S.; Hammons, R.; Kumar, P.Y. 4-phase sequences with near-optimum correlation properties. *IEEE Trans. Inf. Theory* **1992**, *38(3)*, 1101-1113.

5. Cascudo, I.; Cramer,R.; Xing,C.; Yang,A. Asymptotic bound for multiplication complexity in the extensio s of small finite fields. *IEEE Trans. Inf. Theory* **2012**, *58(7)*, 4930-4935.
6. Christopolou,M.; Garefalakis,T.; Panario,D.; Thomson,D. Gauss periods as constructions of low complexity normal bases. *Des. Codes and Cryptogr.,* **2012**, *62* , 43-62.
7. Gao,S. Normal Bases over Finite Fields, thesis, the university of Waterloo, Ontario, Canada, 1993.
8. Gao,S. Abelian groups, Gauss periods and normal bases. *Finite Fields Appl.* **2001**, *7*, 149-164.
9. Gao,S.; Lenstra,H.W. Optimal normal bases. *Des. Codes and Cryptogr.* **1992**,*2*, 315-323.
10. Hammons, A.R.; Kumar, Jr.P.V.; Calderbank, A.R. The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inf. Theory* **1994**, *40(2)*, 301-319.
11. Helleseth,T.; Johansson,T. Universal hash functions from exponential sums over finite fields and Galois rings *Advances in Cryptology-CRYPTO' 96*, Springer Berlin Heidelberg, **1996**, 31-44.
12. Irwansyal, I.M.A.; Barra,A.; Muchlis,A. Self-dual normal basis of a Galios ring. *Journal of Mathematics* 2014 ID:258187, (2014) Hindawi Publishing.
13. Liao,Q. The Gaussian normal basis and its trace basis over finite field. *Jour. Number Theory* **2012**, *132*, 1507-1518.
14. Liao,Q.; Feng, K. On the complexity of the normal bases via prime Gauss period over finite fields. *Jour. Syst. Sci. and Complexity* **2009**,*22*, 395-406.
15. Liao,Q.; You,L. Low complexity of a class of normal bases over finite fields. *Finite Fields Appl.* **2011**,*17*, 1-14.
16. Séguin, G. Low complexity normal bases for $\mathbb{F}_{2^{mn}}$, *Disc. Appl. Math.* **1990**,*28*, 309-312.
17. Yamada,M. Gifference sets over Galois rings with odd extension degrees and characteristic an even power of 2. *Des. Codes and Cryptogr.* **2013**, *67*, 37-57.
18. Yildiz, B. A combinatorial construction of the Gray map over Galois rings. *Disc. Math.* **2009**, *309*, 3408-3412.
19. Wan,Z.X. *Lecture Notes on Finite Fields and Galois Rings*, World Scientific, Singapore, 2003.
20. Zhang,A.; Feng,K. A new criterion on normal bases for finite field extensions. *Finite Fields Appl.* **2015**, *31*, 25-41.