Korean J. Math. **26** (2018), No. 3, pp. 519–535
https://doi.org/10.11568/kjm.2018.26.3.519

THE GAUSS SUMS OVER GALOIS RINGS AND ITS ABSOLUTE VALUES

Young Ho Jang and Sang Pyo Jun†

Abstract. Let $\mathcal{R}$ denote the Galois ring of characteristic p^n, where p is a prime. In this paper, we investigate the elementary properties of Gauss sums over $\mathcal{R}$ in accordance with conditions of characters of Galois rings, and we restate results for Gauss sums in [1, 2, 3, 7, 12, 13]. Also, we compute the modulus of the Gauss sums.

1. Introduction

Throughout this paper, p will denote a prime number and n, m positive integers. We set $q = p^m$. Let $\mathbb{C}$, $\mathbb{C}^1$, $\mathbb{F}_q$, $\mathbb{Z}_{p^n}$ and $\overline{a}$ denote the field of complex numbers, the unit circle in the complex plane, the finite field of order q, the ring of integers modulo p^n and the complex conjugate of $a \in \mathbb{C}$, respectively.

Let χ be a multiplicative character of $\mathbb{F}_q$ such that $\chi(0) = 0$ and let $\lambda_x (x \in \mathbb{F}_q)$ be an additive character of $\mathbb{F}_q$. The Gauss sum related to the pair (χ, λ_x) is defined by

$$G(\chi, \lambda_x) = \sum_{y \in \mathbb{F}_q^\times} \chi(y)\lambda_x(y).$$

If both χ and $\lambda(= \lambda_1)$ are not trivial character χ_0 and λ_0, respectively, one uses the orthogonality relations of characters to establish

Received May 7, 2018. Revised September 1, 2018. Accepted September 10, 2018.
2010 Mathematics Subject Classification: 11T24, 16L60, 42A38, 42B10.
Key words and phrases: Galois ring, characters of Galois rings, Gauss sums over Galois rings.
† Funding for this paper was provided by Namseoul University.

that $G(\chi, \lambda)$ has absolute value $\sqrt{q}$ and that

$$G(\chi_0, \lambda_0) = q - 1, \; G(\chi, \lambda_0) = 0, \; G(\chi_0, \lambda) = -1.$$

For the Gauss sums over finite fields we refer to Lidl and Niederreiter's book [4].

Let $\mathcal{R}$ be the Galois ring of characteristic p^n. As in the case of fields, the Gauss sums over $\mathcal{R}$ considered here are of the form

$$G(\chi, \psi_x) = \sum_{y \in \mathcal{R}^\times} \chi(y)\psi_x(y), \tag{1.1}$$

where $\mathcal{R}^\times$ is the multiplicative group of invertible elements of $\mathcal{R}$, χ a multiplicative character of $\mathcal{R}^\times$, and $\psi_x (x \in \mathcal{R})$ an additive character of $\mathcal{R}$.

The calculation of Gauss sums over quasi-Frobenius rings (we see that $\mathbb{F}_q$, $\mathbb{Z}_{p^n}$ and $\mathcal{R}$ are quasi-Frobenius rings) is initiated by Langevin and Solé [3] in 1999. Using multiplicative characters defined differently on Galois rings, the Gauss sums over Galois rings has been computed in [1, 7, 12] for characteristic 2^2, in [13] for characteristic 2^n, in [2] for characteristic p^2, and its absolute values given in [2, 3, 7]. In this paper, we investigate the elementary properties of Gauss sums over $\mathcal{R}$ given by (1.1) in accordance with conditions of characters of Galois rings, and we restate results for Gauss sums in [1, 2, 3, 7, 12, 13]. Also, we compute the modulus of the Gauss sums.

2. Basic properties of Galois rings and its characters

In this section, we discuss the Galois ring $\mathcal{R}$ of characteristic p^n and its additive and multiplicative characters. Also, we give some simple but useful propositions which shall use later.

2.1. The Galois ring $\mathcal{R}$ of characteristic p^n. The finite field $\mathbb{F}_q$ of order $q = p^m$ is a simple algebraic extension over the prime field $\mathbb{F}_p$. That is, if $\overline{\xi}$ is a primitive element of $\mathbb{F}_q$, then

$$\mathbb{F}_q = \mathbb{F}_p[\overline{\xi}] \cong \mathbb{F}_p[x]/\langle \overline{f}(x) \rangle \tag{2.1}$$

where $\overline{f}(x)$ is a monic primitive polynomial in $\mathbb{F}_p[x]$ of degree m having $\overline{\xi}$ as a root. The ring $\mathbb{Z}_{p^n}$ is a finite commutative local ring with a unique maximal ideal $p\mathbb{Z}_{p^n}$. Let $\mu : \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}/p\mathbb{Z}_{p^n} \cong \mathbb{F}_p$ be the mod-p reduction map. We can extend μ to a map $\mathbb{Z}_{p^n}[x] \to \mathbb{F}_p[x]$ in the natural way. In (2.1), since $\overline{\xi}$ is a simple zero of $\overline{f}(x)$, if $f(x) \in \mathbb{Z}_{p^n}[x]$ is a preimage of $\overline{f}(x)$ under the homomorphism μ, then, by [5, Lemma (XV.1)], there is precisely one element ξ such that $\xi^{q-1} = 1$, $\mu(\xi) = \overline{\xi}$ and $f(\xi) = 0$. Such polynomial $f(x)$ is called a monic basic primitive polynomial of degree m. The Galois ring $GR(p^n, m)$ of characteristic p^n is defined by

$$\mathcal{R} = \mathcal{R}_{n,m} = GR(p^n, m) = \mathbb{Z}_{p^n}[\xi] \cong \mathbb{Z}_{p^n}[x]/\langle f(x)\rangle. \tag{2.2}$$

The simplest examples of Galois rings are $\mathcal{R}_{n,1} = GR(p^n, 1) = \mathbb{Z}_{p^n}$ and $\mathcal{R}_{1,m} = GR(p, m) = \mathbb{F}_q$. By definition (2.2) of Galois rings, every element $z \in \mathcal{R}$ has a unique additive representation

$$z = z_0 + z_1\xi + z_2\xi^2 + \cdots + z_{m-1}\xi^{m-1},\ z_i \in \mathbb{Z}_{p^n}, \tag{2.3}$$

so that $\mathcal{R}$ is a finitely generated free $\mathbb{Z}_{p^n}$-module and $|\mathcal{R}| = q^n (= p^{nm})$. Also, $\mathcal{R}$ is a local ring with a unique maximal ideal $\mathcal{M} = \mathcal{M}_{n,m} = p\mathcal{R}$ which consisted of 0 and all zero divisors in $\mathcal{R}$, and its residue field $\mathcal{R}/\mathcal{M}$ is isomorphic to $\mathbb{F}_q$. Clearly μ has a natural extension to $\mathcal{R}$ and therefore to $\mathcal{R}[x]$, and $\mu(\mathcal{R}) = \mathcal{R}/\mathcal{M} \cong \mathbb{F}_q$. For more knowledge on Galois rings we refer to [5, 6, 9, 11].

The group $\mathcal{R}^\times = \mathcal{R}\backslash\mathcal{M}$ of units has the direct decomposition (see [5, Theorem XVIII.2]):

$$\mathcal{R}^\times = \Gamma_m^\times \times (1 + \mathcal{M}) \tag{2.4}$$

where $\Gamma_m^\times = \langle\xi\rangle$ is the cyclic group of order $q-1$ and $1+\mathcal{M}$ is the multiplicative p-group of order q^{n-1}. Define $\Gamma_m = \Gamma_m^\times \cup \{0\} = \{0, 1, \xi, \cdots, \xi^{q-2}\}$. It can be shown that every element $z \in \mathcal{R}$ has a unique p-adic representation

$$z = z_0 + z_1 p + \cdots + z_{n-1}p^{n-1},\ z_i \in \Gamma_m. \tag{2.5}$$

From (2.5) we have $\mathcal{M} = p\mathcal{R}_{n-1,m}$, i.e., $z \in \mathcal{M}$ if and only if $z_0 = 0$ and $z \in \mathcal{R}^\times$ if and only if $z_0 \in \Gamma_m^\times$. An arbitrary element z of $\mathcal{R}^\times$ is uniquely represented as

$$\begin{aligned} z &= z_0 + \tilde{z},\ z_0 \in \Gamma_m^\times,\ \tilde{z} \in \mathcal{M} && (2.6)\\ &= \xi^k x = \xi^k(1 + py),\ x \in 1 + \mathcal{M},\ y \in \mathcal{R}_{n-1,m},\ 0 \le k \le q-2. && (2.7)\end{aligned}$$

Any element of $\mathcal{R}\backslash\{0\}$ is either a unit or a zero divisor. Since the zero divisors in $\mathcal{R}$ are those elements divisible by p, any element $z \in \mathcal{R}\backslash\{0\}$

can be written as
(2.8)
$z = p^k u = p^k \xi^l (1+px),\ u \in \mathcal{R}^\times,\ x \in \mathcal{R}_{n-1,m},\ 0 \le k \le n-1,\ 0 \le l \le q-2.$

2.2. Additive characters of $\mathcal{R}$. Let σ be the Frobenius map of $\mathcal{R}$ over $\mathbb{Z}_{p^n}$ given by

$$\sigma(z) = z_0^p + pz_1^p + \cdots + p^{n-1} z_{n-1}^p$$

for $z = \sum_{i=0}^{n-1} p^i z_i \in \mathcal{R}$, where $z_i \in \Gamma_m$. As we know, σ is the generator of the Galois group of $\mathcal{R}/\mathbb{Z}_{p^n}$ which is a cyclic group of order m. The trace mapping $\mathrm{Tr}_n : \mathcal{R} \to \mathbb{Z}_{p^n}$ is defined by

$$\mathrm{Tr}_n(z) = z + \sigma(z) + \cdots + \sigma^{m-1}(z) \text{ for } z \in \mathcal{R}$$

where $\sigma^j(z) = \sigma(\sigma^{j-1}(z))$. Tr_n is an epimorphism of $\mathbb{Z}_{p^n}$-modules and Tr_n can be reduced by μ to the trace mapping $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ of finite fields. Then we have the following commutative diagram:

$$\begin{array}{ccc} \mathcal{R} & \xrightarrow{\mu} & \mathbb{F}_q \\ \big\downarrow \mathrm{Tr}_n & & \big\downarrow \mathrm{tr} \\ \mathbb{Z}_{p^n} & \xrightarrow{\mu} & \mathbb{F}_p \end{array}$$

Namely, we have $\mu(\mathrm{Tr}_n(z)) = \mathrm{tr}(\mu(z))$ for all $z \in \mathcal{R}$.

An additive character of $\mathcal{R}$ is a homomorphism from the additive group of $\mathcal{R}$ to $\mathbb{C}^1$. For any $x, y \in R$, the additive characters of $\mathcal{R}$ are given by

$$\psi_x(y) = e^{2\pi i \mathrm{Tr}_n(xy)/p^n}, \tag{2.9}$$

different x's affording different additive characters. In fact, $\{\psi_x\}_{x\in\mathcal{R}}$ consists of all additive characters of $\mathcal{R}$ (see [10, Lemma 6]). ψ_0 is the trivial additive character of $\mathcal{R}$ and $\psi(= \psi_1)$ is called the canonical additive character of $\mathcal{R}$. Let $\widehat{\mathcal{R}^+}$ denote the additive characters group.

Remark 2.1 ([1, 7, 12]). In the case of $\mathcal{R} = GR(2^2, m)$,

$$\psi_x(y) = \sqrt{-1}^{\,\mathrm{Tr}_2(xy)}. \tag{2.10}$$

Proposition 2.1 ([8, Lemma 2.1, 2.2, 2.3]). *For any $x \in \mathcal{R}$ we have*

$$\sum_{y\in\mathcal{R}} \psi_x(y) = \begin{cases} q^n & \text{if } x = 0 \\ 0 & \text{if } x \ne 0 \end{cases}; \tag{2.11}$$

$$\sum_{y\in\mathcal{M}} \psi_x(y) = \begin{cases} q^{n-1} & \text{if } x \in p^{n-1}\mathcal{R} \\ 0 & \text{if } x \in \mathcal{R}\backslash p^{n-1}\mathcal{R} \end{cases}; \tag{2.12}$$

$$\sum_{y\in\mathcal{R}^\times} \psi_x(y) = \begin{cases} (q-1)q^{n-1} & \text{if } x = 0, \\ -q^{n-1} & \text{if } x \in p^{n-1}\mathcal{R}\backslash\{0\}, \\ 0 & \text{if } x \in \mathcal{R}\backslash p^{n-1}\mathcal{R}. \end{cases} \tag{2.13}$$

Proposition 2.2 ([10, Lemma 8]). *For any $x \in \mathcal{R}$ we have*

$$\sum_{y\in\Gamma_m} \psi_x(p^{n-1}y) = \begin{cases} q & \text{if } x \in \mathcal{M}, \\ 0 & \text{if } x \in \mathcal{R}^\times. \end{cases} \tag{2.14}$$

Proposition 2.3. *If $\psi_x \in \widehat{\mathcal{R}^+}$ is nontrivial on $\mathcal{M}$, then*

$$\sum_{y\in\mathcal{R}^\times} \psi_x(y) = -\sum_{y\in\mathcal{M}} \psi_x(y) = 0. \tag{2.15}$$

Proof. From the assumption, $\psi_x \in \widehat{\mathcal{R}^+}$ is nontrivial on $\mathcal{R}$ and so

$$\sum_{y\in\mathcal{R}^\times} \psi_x(y) = \sum_{y\in\mathcal{R}} \psi_x(y) - \sum_{y\in\mathcal{M}} \psi_x(y) = -\sum_{y\in\mathcal{M}} \psi_x(y)$$

by (2.11). Also, there exists $z \in \mathcal{M}$ such that $\psi_x(z) \neq 1$. Since adding all $y \in \mathcal{M}$ by $z \in \mathcal{M}$ permutes $\mathcal{M}$. we have

$$\sum_{y\in\mathcal{M}} \psi_x(y) = \sum_{y+z\in\mathcal{M}} \psi_x(y+z) = \psi_x(z) \sum_{y\in\mathcal{M}} \psi_x(y).$$

As $1 - \psi_x(z) \neq 0$, we get (2.15). □

Proposition 2.4. *If $\psi \in \widehat{\mathcal{R}^+}$ is trivial on $\mathcal{M}$, then*

$$\sum_{y\in\mathcal{R}^\times} \psi_x(y) = \sum_{y\in\mathcal{R}^\times} \psi(xy) = \begin{cases} -q^{n-1} & \text{if } x \in \mathcal{R}^\times, \\ (q-1)q^{n-1} & \text{if } x \in \mathcal{M}. \end{cases} \tag{2.16}$$

Proof. If $x \in \mathcal{R}^\times$, then multiplying all $y \in \mathcal{R}^\times$ by x permutes $\mathcal{R}^\times$, so that by setting $z = xy \in \mathcal{R}^\times$ we have

$$\sum_{y\in\mathcal{R}^\times} \psi_x(y) = \sum_{y\in\mathcal{R}^\times} \psi(xy) = \sum_{z\in\mathcal{R}^\times} \psi(z) = \sum_{z\in\mathcal{R}} \psi(z) - \sum_{z\in\mathcal{M}} \psi(z) = -\sum_{z\in\mathcal{M}} 1 = -q^{n-1}$$

by (2.11) and the assumption. If $x \in \mathcal{M}$, then $xy \in \mathcal{M}$ for all $y \in \mathcal{R}^\times$ and

$$\sum_{y\in\mathcal{R}^\times} \psi_x(y) = \sum_{y\in\mathcal{R}^\times} \psi(xy) = \sum_{y\in\mathcal{R}^\times} 1 = (q-1)q^{n-1}$$

by the assumption. □

In definition (2.2) of Galois rings $\mathcal{R} = \mathcal{R}_{n,m}$, for the monic basic primitive polynomial $f(x)$ in $\mathbb{Z}_{p^n}[x]$ of degree m, put $\varphi(x) \equiv f(x) \pmod{p^k}$, where $1 \le k \le n-1$. Then $\varphi(x)$ is a monic basic primitive polynomial in $\mathbb{Z}_{p^k}[x]$ of degree m. Let $\theta \in \mathcal{R}_{k,m}$ be a root of $\varphi(x)$. Using additive representation (2.3), we define the homomorphism τ_k as

$$\tau_k : \mathcal{R} \to \mathcal{R}_{k,m}, \ \tau_k\left(\sum_{i=0}^{m-1} z_i\xi^i\right) = \sum_{i=0}^{m-1} \tilde{z}_i\theta^i \tag{2.17}$$

where $\tilde{z}_i \equiv z_i \pmod{p^k}$, $z_i \in \mathbb{Z}_{p^n}$ and $\tilde{z}_i \in \mathbb{Z}_{p^k}$. Then we have the following commutative diagram:

$$\begin{array}{ccc} \mathcal{R} & \xrightarrow{\tau_k} & \mathcal{R}_{k,m} \\ \big\downarrow \mathrm{Tr}_n & & \big\downarrow \mathrm{Tr}_k \\ \mathbb{Z}_{p^n} & \xrightarrow{\tau_k} & \mathbb{Z}_{p^k} \end{array}$$

Namely, we have

$$\tau_k(\mathrm{Tr}_n(z)) = \mathrm{Tr}_k(\tau_k(z)) \text{ for } z \in \mathcal{R}. \tag{2.18}$$

In particular, for $k = 1$, we have $\mathcal{R}_{1,m} = \mathbb{F}_q$, $\mathbb{Z}_p = \mathbb{F}_p$, $\tau_1 = \mu$ and $\mathrm{Tr}_1 = tr$.

Proposition 2.5. *For any $x \in \mathcal{R}$ we have*

$$\sum_{y\in\mathcal{M}} \psi_x(y) = \begin{cases} q^{n-1} & \text{if } \tau_{n-1}(x) = 0, \\ 0 & \text{if } \tau_{n-1}(x) \neq 0, \end{cases} \tag{2.19}$$

where $\tau_{n-1} : \mathcal{R} \to \mathcal{R}_{n-1,m}$ is the homomorphism defined by (2.17).

Proof. The element $y \in \mathcal{M} = p\mathcal{R}_{n-1,m}$ is written as $y = pz,\ z \in \mathcal{R}_{n-1,m}$. We have

$$\begin{aligned}\sum_{y\in\mathcal{M}} \psi_x(y) &= \sum_{y\in\mathcal{M}} e^{2\pi i \mathrm{Tr}_n(xy)/p^n} = \sum_{z\in\mathcal{R}_{n-1,m}} e^{2\pi i \mathrm{Tr}_n(xpz)/p^n}\\ &= \sum_{z\in\mathcal{R}_{n-1,m}} e^{2\pi i \mathrm{Tr}_{n-1}(\tau_{n-1}(x)z)/p^{n-1}} \text{ (by (2.18))}\\ &= \sum_{z\in\mathcal{R}_{n-1,m}} \psi_{\tau_{n-1}(x)}(z) \text{ (by (2.9))}.\end{aligned}$$

Since $\psi_{\tau_{n-1}(x)}$ is an additive character of $\mathcal{R}_{n-1,m}$, from (2.11) we get (2.19). □

Proposition 2.6. *For any $x \in \mathcal{R}$ we have*

$$\sum_{y\in\mathcal{R}^\times} \psi_x(y) = \begin{cases} (q-1)q^{n-1} & \text{if } x = 0,\\ -q^{n-1} & \text{if } x \neq 0 \text{ and } \tau_{n-1}(x) = 0,\\ 0 & \text{if } \tau_{n-1}(x) \neq 0,\end{cases} \tag{2.20}$$

where $\tau_{n-1} : \mathcal{R} \to \mathcal{R}_{n-1,m}$ is the homomorphism defined by (2.17).

Proof. Since

$$\sum_{y\in\mathcal{R}^\times} \psi_x(y) = \sum_{y\in\mathcal{R}} \psi_x(y) - \sum_{y\in\mathcal{M}} \psi_x(y),$$

combining (2.11) and (2.19) we get (2.20). □

2.3. Multiplicative characters of $\mathcal{R}$. A multiplicative character χ of $\mathcal{R}^\times$ is defined by $\chi(xy) = \chi(x)\chi(y)$ for $x, y \in \mathcal{R}^\times$, and each value of $\chi(x)$ is a $(q-1)q^{n-1}$-th root of unity. We extend χ as the character of $\mathcal{R}$ by defining $\chi(\mathcal{M}) = 0$. We call this the multiplicative character of $\mathcal{R}$. Let χ_0 and $\widehat{\mathcal{R}^\times}$ denote the trivial multiplicative character of $\mathcal{R}$ and the multiplicative characters group, respectively.

Proposition 2.7. *For any character $\chi \in \widehat{\mathcal{R}^\times}$,*

$$\sum_{x\in\mathcal{R}} \chi(x) = \sum_{x\in\mathcal{R}^\times} \chi(x) = \begin{cases} (q-1)q^{n-1} & \text{if } \chi = \chi_0,\\ 0 & \text{if } \chi \neq \chi_0.\end{cases} \tag{2.21}$$

Proof. It is clear if $\chi = \chi_0$. If $\chi \neq \chi_0$, there exists $y \in \mathcal{R}^\times$ such that $\chi(y) \neq 1$. Since multiplying all $x \in \mathcal{R}^\times$ by $y \in \mathcal{R}^\times$ permutes $\mathcal{R}^\times$, we have

$$\sum_{x\in\mathcal{R}^\times}\chi(x)=\sum_{xy\in\mathcal{R}^\times}\chi(xy)=\chi(y)\sum_{x\in\mathcal{R}^\times}\chi(x).$$

As $1-\chi(y)\neq 0$, we get $\sum_{x\in\mathcal{R}^\times}\chi(x)=0$. $\square$

Remark 2.2. In [7], the authors extend χ as the character of $\mathcal{R}=GR(2^2,m)$ by defining $\chi(\mathcal{M})=1$ for $\chi=\chi_0$ and $\chi(\mathcal{M})=0$ for $\chi\neq\chi_0$, and so that

$$\sum_{x\in\mathcal{R}}\chi(x)=\begin{cases} q^n=(2^m)^2=4^m & \text{if } \chi=\chi_0,\\ 0 & \text{if } \chi\neq\chi_0,\end{cases}$$

which is a little different with (2.21).

Since $\mathcal{R}^\times=\Gamma_m^\times\times(1+\mathcal{M})$ (see (2.4)), there are few kinds type of multiplicative characters of $\mathcal{R}$:

(I) The multiplicative characters χ of $\mathcal{R}$ that vanish on $1+\mathcal{M}$ (i.e. $\chi(1+x)=1$ for $x\in\mathcal{M}$) are in one-to-one correspondence with the multiplicative characters η_j of $\Gamma_m^\times$ defined by

$$\eta_j(\xi^k)=e^{2\pi i(jk)/q-1} \text{ for } 0\le j,k\le q-2. \tag{2.22}$$

Then η_j's form a cyclic group with $q-1$ elements. It is familiar that the order of each character η_j is a divisor of $q-1$.

Remark 2.3 ([10, Theorem 13]). Let ψ_x be a nontrivial additive character of $\mathcal{R}$ given by (2.9) and χ a nontrivial multiplicative character of $\Gamma_m^\times$ given by (2.22). Then

$$\left|\sum_{y\in\Gamma_m^\times}\chi(y)\psi_x(y)\right|\le p^{n-1}q^{1/2}.$$

(II) The multiplicative characters χ of $\mathcal{R}$ that vanish on $\Gamma_m^\times$ (i.e. $\chi(x)=1$ for $x\in\Gamma_m^\times$) are in one-to-one correspondence with the multiplicative characters of the multiplicative p-group $1+\mathcal{M}$ of order q^{n-1}. In the case of $\mathcal{R}=GR(p^2,m)$, from the p-adic representation (2.5)

$$z=z_0+z_1p \ (z_0,z_1\in\Gamma_m),\ \mathcal{M}=p\Gamma_m,\ \mathcal{M}^2=0$$

and

$$(1+\mathcal{M},\cdot)=(1+p\Gamma_m,\cdot)\cong(\mathbb{F}_q,+),\ 1+py\longmapsto\overline{y}=y \bmod p \text{ for } y\in\Gamma_m.$$

Hence multiplicative characters of $\mathcal{R}$ that vanish on $\Gamma_m^\times$ are given by

$$\chi_x(1+py)=\varphi_{\overline{x}}(\overline{y})\ (x,y\in\Gamma_m,\ \overline{x},\overline{y}\in\mathbb{F}_q). \tag{2.23}$$

where $\varphi_{\overline{x}}$ is an additive character of $\mathbb{F}_q$ defined by

$$\varphi_{\overline{x}}(\overline{y}) = e^{2\pi i \mathrm{tr}(\overline{xy})/p} \text{ for all } \overline{x}, \overline{y} \in \mathbb{F}_q. \tag{2.24}$$

Remark 2.4 ([12, Theorem 1, Theorem 2]). Let ψ_y be an additive character of $\mathcal{R} = GR(2^2, m)$ given by (2.10) in Remark 2.1 and χ_x a multiplicative character of $\mathcal{R}$ given by (2.23) such that $\chi_x^2 = \chi_0$. Then explicit form of Gauss sums over $\mathcal{R}$ is given as follows:

$$G(\chi_x, \psi_y) = \begin{cases} \chi(y)G(\chi_x, \psi_1) & \text{when } y \in \mathcal{R}^\times, \\ \chi\left(\frac{y}{2}\right) G(\chi_x, \psi_2) & \text{when } y \in \mathcal{M}\backslash\{0\}, \\ q(q-1) = 2^m(2^m - 1) & \text{when } x = 0 \text{ and } y = 0, \\ 0 & \text{when } x \neq 0 \text{ and } y = 0, \end{cases}$$

and

$$G(\chi_x, \psi_y) = \begin{cases} 2^m \sqrt{-1}^{\mathrm{Tr}_2(z)} & \text{when } x \neq 0 \text{ and } y = 1, \\ & \qquad \text{where } z \equiv \overline{x} \pmod{\mathcal{M}},\ z \in \Gamma_m^\times, \\ 0 & \text{when } x = 0 \text{ and } y = 1, \\ 0 & \text{when } x \neq 0 \text{ and } y = 2, \\ -2^m & \text{when } x = 0 \text{ and } y = 2. \end{cases}$$

Remark 2.5 ([1], [2]). Let ψ_y be an additive character of $\mathcal{R} = GR(p^2, m)$ given by (2.9) and χ a multiplicative character defined by

$$\chi = \eta_j \chi_x \ (x \in \Gamma_m,\ 0 \leq j \leq q-2), \tag{2.25}$$

where η_j is a multiplicative character of $\Gamma_m^\times$ given by (2.22) and χ_x is a multiplicative character of $1 + \mathcal{M}$ given by (2.23). The values of Gauss sums over $\mathcal{R}$ have been calculated explicitly as follows:

$$G(\chi, \psi_y) = \begin{cases} q(q-1) & \text{for } \chi = \chi_0 \text{ and } y = 0, \\ 0 & \text{for } \chi \neq \chi_0 \text{ and } y = 0, \\ -q & \text{for } \chi = \chi_0 \text{ and } y \in \mathcal{M}\backslash\{0\}, \\ 0 & \text{for } \chi = \chi_0 \text{ and } y \in \mathcal{R}^\times. \end{cases}$$

$$G(\chi, \psi_y) = \begin{cases} \overline{\chi}(y)G(\chi, \psi) & \text{for } y \in \mathcal{R}^\times, \\ \overline{\chi}(y)G(\chi, \psi_p) & \text{for } y = pz\ (z \in \Gamma_m^\times). \end{cases}$$

$$G(\chi, \psi) = \begin{cases} 0 & \text{if } x = 0, \\ q\eta_j(x_1)e^{2\pi i \mathrm{Tr}_2(x_1)/p^2} & \text{if } x \in \Gamma_m^\times, \end{cases}$$

where $x_1 = x$ for $p = 2$ and $x_1 = -x$ for $p \geq 3$.

$$G(\chi, \psi_p) = \begin{cases} q \sum_{z \in \Gamma_m^\times} \eta_j(z) e^{2\pi i \mathrm{tr}(\bar{z})/p} & \text{if } x = 0, \\ 0 & \text{if } x \in \Gamma_m^\times. \end{cases}$$

3. The Gauss sums over $\mathcal{R}$ and its absolute values

In this section, we give explicit form of the Gauss sum $G(\chi, \psi_x)$ over $\mathcal{R}$ given by (1.1) in accordance with conditions of characters of Galois rings, and we compute the modulus of the Gauss sums.

Let $\mathcal{R} = \mathcal{R}_{n,m} = GR(p^n, m)$, $\mathcal{M} = p\mathcal{R}$, $\mathcal{R}^\times = \mathcal{R} \backslash \mathcal{M}$, Γ_m, $\Gamma_m^\times$, $\widehat{\mathcal{R}^+}$, $\widehat{\mathcal{R}^\times}$, and τ_k be as in Section 1 and Section 2. From (2.21), we have

$$G(\chi, \psi_0) = \begin{cases} (q-1)q^{n-1} & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases} \tag{3.1}$$

Proposition 3.1. *For $x \in \mathcal{R}$ we have*

$$G(\chi_0, \psi_x) = \begin{cases} (q-1)q^{n-1} & \text{if } x = 0, \\ -q^{n-1} & \text{if } (x \in p^{n-1}\mathcal{R} \backslash \{0\}) \text{ or } (x \neq 0 \text{ and } \tau_{n-1}(x) = 0), \\ 0 & \text{if } (x \notin p^{n-1}\mathcal{R}) \text{ or } (\tau_{n-1}(x) \neq 0), \end{cases}$$

where $\tau_{n-1} : \mathcal{R} \to \mathcal{R}_{n-1,m}$ is the homomorphism defined by (2.17).

Proof. See (2.13) and Proposition 2.6. □

Remark 3.1 ([3, Proposition 1]). Let $\psi \in \widehat{\mathcal{R}^+}$. If $\chi \in \widehat{\mathcal{R}^\times}$ is trivial on $1 + \mathcal{M}$ then

$$G(\chi, \psi) = \begin{cases} q^{n-1} G_{\Gamma_m^\times}(\chi, \psi) & \text{if } \psi \text{ is trivial on } \mathcal{M}, \\ 0 & \text{else.} \end{cases}$$

Proposition 3.2. *Let $x \in \mathcal{R} \backslash \{0\}$. If $\chi \in \widehat{\mathcal{R}^\times}$ is trivial on $1 + \mathcal{M}$, then*

$$G(\chi, \psi_x) = \begin{cases} q^{n-1} G_{\Gamma_m^\times}(\chi, \psi_x) & \text{if } (\psi_x \text{ is trivial on } \mathcal{M}) \text{ or } (x \in p^{n-1}\mathcal{R}) \\ & \quad \text{or } (\tau_{n-1}(x) = 0), \\ 0 & \text{if } (\psi_x \text{ is nontrivial on } \mathcal{M}) \text{ or } (x \notin p^{n-1}\mathcal{R}) \\ & \quad \text{or } (\tau_{n-1}(x) \neq 0), \end{cases}$$

where $\tau_{n-1} : \mathcal{R} \to \mathcal{R}_{n-1,m}$ is the homomorphism defined by (2.17).

Proof. Indeed,

$$\begin{aligned} G(\chi, \psi_x) &= \sum_{z \in \mathcal{R}^\times} \chi(z)\psi_x(z) \\ &= \sum_{t \in \Gamma_m^\times} \sum_{y \in \mathcal{M}} \chi(t+y)\psi_x(t+y) \text{ (by (2.6))} \\ &= \sum_{t \in \Gamma_m^\times} \sum_{y \in \mathcal{M}} \chi(t)\chi(1+t^{-1}y)\psi_x(t)\psi_x(y) \text{ (where } t^{-1}y \in \mathcal{M}) \\ &= \sum_{t \in \Gamma_m^\times} \chi(t)\psi_x(t) \sum_{y \in \mathcal{M}} \psi_x(y) \text{ (by assumption).} \end{aligned}$$

From (2.12), (2.15) and Proposition 2.5, we completes the proof of Proposition 3.2. □

PROPOSITION 3.3. *Let $u \in \mathcal{R}^\times$ and t a fixed integer with $0 \le t \le n-1$. Then*

$$G(\chi, \psi_{p^t u}) = \overline{\chi}(u) G(\chi, \psi_{p^t}).$$

Proof. Indeed,

$$G(\chi, \psi_{p^t u}) = \sum_{x \in \mathcal{R}^\times} \chi(x)\psi_{p^t u}(x) = \overline{\chi}(u) \sum_{x \in \mathcal{R}^\times} \chi(ux)\psi_{p^t}(ux) = \overline{\chi}(u) G(\chi, \psi_{p^t})$$

since multiplying all $x \in \mathcal{R}^\times$ by u permutes $\mathcal{R}^\times$. □

We introduce a new operation $*$ in $\mathcal{R}_{n,m}$, $n \ge 2$. For elements $x, y \in \mathcal{R}_{n,m}$, we let

$$x * y = x + y + pxy. \tag{3.2}$$

Then the elements of the ring $\mathcal{R}_{n,m}$ form an abelian group with respect to the new operation $*$, an identity element is 0 and inverse of an element x is given by $-x(1+px)^{-1}$.

Let χ be a multiplicative character of $\mathcal{R}_{n+1,m}^\times$ that vanish on $\Gamma_m^\times$ (i.e. $\chi_{n+1}(x) = 1$ for $x \in \Gamma_m^\times$). For $1+px, 1+py \in 1+\mathcal{M}_{n+1,m} = 1+p\mathcal{R}_{n,m}$ where $x, y \in \mathcal{R}_{n,m}$, we have

$$(1+px)\cdot(1+py) = 1+p(x+y)+p^2xy = 1+p(x+y+pxy) = 1+p(x*y).$$

Thus a multiplicative character χ of $\mathcal{R}_{n+1,m}^\times$ that vanish on $\Gamma_m^\times$ can be regarded as a multiplicative character χ^* of the group $\mathcal{R}_{n,m}$ with respect to the new operation $*$ that vanish on $\Gamma_m^\times$. We extend χ as the character of $\mathcal{R}_{n+1,m}$ by defining $\chi(\mathcal{M}_{n+1,m}) = 0$.

THEOREM 3.1 ([13, Lemma 6] for $p = 2$). *Let χ be a multiplicative character of $\mathcal{R}_{n+1,m}$ that vanish on $\Gamma_m^\times$ and ψ_x ($x \in \mathcal{R}_{n,m}$) an additive character of $\mathcal{R}_{n+1,m}$ given by* (2.9)*. Then for*

$$x = p^k\xi^l(1+py) \in \mathcal{R}_{n+1,m}\backslash\{0\},\ y \in \mathcal{R}_{n,m},\ 0 \le k \le n,\ 0 \le l \le q-2,$$

we have

$$G(\chi, \psi_x) = \overline{\chi}\left(\frac{x}{p^k}\right) G(\chi, \psi_{p^k}).$$

Proof. Indeed,

$$\begin{aligned}
&G(\chi, \psi_x)\\
= &\sum_{y\in\mathcal{R}_{n+1,m}^\times} \chi(y)\psi_x(y) \text{ (put } y = \xi^t(1+pz), 0 \le t \le q-2, z \in \mathcal{R}_{n,m})\\
= &\sum_{t=0}^{q-2}\sum_{z\in\mathcal{R}_{n,m}} \chi(\xi^t(1+pz))e^{2\pi i \mathrm{Tr}_{n+1}(\xi^t(1+pz)p^k\xi^l(1+py))/p^{n+1}}\\
= &\sum_{t=0}^{q-2}\sum_{z\in\mathcal{R}_{n,m}} \chi^*(z)e^{2\pi i p^k \mathrm{Tr}_{n+1}(\xi^t(1+p(y*z))/p^{n+1}}\\
&\text{(since } 0 * z = z \text{ and } (1+py)(1+pz) = 1+p(y*z))\\
= &\sum_{t=0}^{q-2}\sum_{z\in\mathcal{R}_{n,m}} \chi^*(y*z)\chi^*(y^{-1})e^{2\pi i p^k \mathrm{Tr}_{n+1}(\xi^t(1+p(y*z))/p^{n+1}} \text{ (put } y*z = \alpha)\\
= &\overline{\chi^*}(y)\sum_{t=0}^{q-2}\sum_{\alpha\in\mathcal{R}_{n,m}} \chi^*(\alpha)e^{2\pi i p^k \mathrm{Tr}_{n+1}(\xi^t(1+p\alpha)/p^{n+1}}\\
= &\overline{\chi}(\xi^l(1+py))\sum_{t=0}^{q-2}\sum_{\alpha\in\mathcal{R}_{n,m}} \chi(\xi^t(1+p\alpha))e^{2\pi i p^k \mathrm{Tr}_{n+1}(\xi^t(1+p\alpha)/p^{n+1}}\\
= &\overline{\chi}(x/p^k)\sum_{\beta\in\mathcal{R}_{n+1,m}^\times} \chi(\beta)\psi_{p^k}(\beta)\\
= &\overline{\chi}(x/p^k)G(\chi, \psi_{p^k}).
\end{aligned}$$

□

LEMMA 3.1. *Let $\chi \in \widehat{\mathcal{R}^\times}$ be a nontrivial character. Then we have*

$$G(\chi, \psi_x) = \begin{cases} \overline{\chi}(x)G(\chi, \psi) & \text{if } x \in \mathcal{R}^\times,\\ 0 & \text{if } x \in \mathcal{M} \text{ and } \psi \in \widehat{\mathcal{R}^+} \text{ is trivial on } \mathcal{M}.\end{cases}$$

Proof. If $x \in \mathcal{R}^\times$, then multiplying all $y \in \mathcal{R}^\times$ by x permutes $\mathcal{R}^\times$, so that by setting $z = xy \in \mathcal{R}^\times$ we have

$$\begin{aligned} G(\chi, \psi_x) &= \sum_{y \in \mathcal{R}^\times} \chi(y)\psi_x(y) = \sum_{y \in \mathcal{R}^\times} \chi(y)\psi(xy) \\ &= \sum_{z \in \mathcal{R}^\times} \chi(x^{-1}z)\psi(z) = \overline{\chi}(x) \sum_{z \in \mathcal{R}^\times} \chi(z)\psi(z) \\ &= \overline{\chi}(x)G(\chi, \psi). \end{aligned}$$

If $x \in \mathcal{M}$ and $\psi \in \widehat{\mathcal{R}^+}$ is trivial on $\mathcal{M}$, then $xy \in \mathcal{M}$ for all $y \in \mathcal{R}^\times$ and $\psi(xy) = 1$, so that we have

$$GR(\chi, \psi_x) = \sum_{y \in \mathcal{R}^\times} \chi(y)\psi_x(y) = \sum_{y \in \mathcal{R}^\times} \chi(y)\psi(xy) = \sum_{y \in \mathcal{R}^\times} \chi(y) = 0$$

by (2.21). □

The following result has been proved in [3, Proposition 3]. Here we reproduce the proof for reader's convenience.

Theorem 3.2. *The modulus of a Gauss sum is completely determined:*

$$|G(\chi, \psi)|^2 = \begin{cases} q^n & \text{if } \chi \text{ is nontrivial on } 1 + \mathrm{ann}(\mathcal{M}), \\ 0 & \text{if } \chi \text{ is trivial on } 1 + \mathrm{ann}(\mathcal{M}), \end{cases} \tag{3.3}$$

where $\mathrm{ann}(\mathcal{M}) = \{x \in R \mid xy = 0$ *for all* $y \in \mathcal{M}\}$.

Proof. Let $S = 1 + \mathrm{ann}(\mathcal{M})$. Then S is a subgroup of $\mathcal{R}^\times$ and $1 \in S$. Since multiplying all $x \in \mathcal{R}^\times$ by $y^{-1} \in \mathcal{R}^\times$ permutes $\mathcal{R}^\times$, so that by setting $z = xy^{-1} \in \mathcal{R}^\times$ we have

$$\begin{aligned}
&|G(\chi,\psi)|^2 \\
=\ & \sum_{x\in\mathcal{R}^\times}\sum_{y\in\mathcal{R}^\times}\chi(xy^{-1})\psi(x-y) \text{ (by (1.1))} \\
=\ & \sum_{z\in\mathcal{R}^\times}\chi(z)\sum_{y\in\mathcal{R}^\times}\psi((z-1)y) \\
=\ & \left\{\sum_{z\in S}\chi(z)+\sum_{z\in\mathcal{R}^\times\setminus S}\chi(z)\right\}\left\{\sum_{y\in\mathcal{R}}\psi((z-1)y)-\sum_{y\in\mathcal{M}}\psi((z-1)y)\right\} \\
=\ & \chi(1)\sum_{y\in\mathcal{R}}1-\sum_{z\in S}\chi(z)\sum_{y\in\mathcal{M}}1-\sum_{z\in\mathcal{R}^\times\setminus S}\chi(z)\sum_{y\in\mathcal{M}}\psi((z-1)y) \text{ (by (2.11))} \\
=\ & q^n-q^{n-1}\sum_{z\in S}\chi(z)-\sum_{z\in\mathcal{R}^\times\setminus S}\chi(z)\sum_{y\in\mathcal{M}}\psi_{z-1}(y).
\end{aligned}$$

Since $z-1 \notin p^{n-1}\mathcal{R}$, from (2.12) we have $\sum_{z\in\mathcal{R}^\times\setminus S}\chi(z)\sum_{y\in\mathcal{M}}\psi((z-1)y) = 0$. This completes the proof of (3.3). □

PROPOSITION 3.4. *If* $\tau_{n-1}(y) \neq 0$ *for all* $y \in \mathcal{R}\setminus\{0\}$, *where* $\tau_{n-1} : \mathcal{R} \to \mathcal{R}_{n-1,m}$ *is the homomorphism defined by* (2.17), *then we have*

$$|G(\chi,\psi)|^2 = (q-1)q^{n-1}.$$

Proof. Since multiplying all $x \in \mathcal{R}^\times$ by $y^{-1} \in \mathcal{R}^\times$ permutes $\mathcal{R}^\times$, so that by setting $z = xy^{-1} \in \mathcal{R}^\times$ we have

$$\begin{aligned}
|G(\chi,\psi)|^2 &= \sum_{x\in\mathcal{R}^\times}\sum_{y\in\mathcal{R}^\times}\chi(xy^{-1})\psi(x-y) \text{ (by (1.1))} \\
&= \sum_{z\in\mathcal{R}^\times}\chi(z)\sum_{y\in\mathcal{R}^\times}\psi((z-1)y) \\
&= (q-1)q^{n-1}+\sum_{z\in\mathcal{R}^\times\setminus\{1\}}\chi(z)\sum_{y\in\mathcal{R}^\times}\psi_{z-1}(y).
\end{aligned}$$

By the assumption, $\tau_{n-1}(z-1) \neq 0$ and from Proposition 2.6, we have

$$\sum_{z\in\mathcal{R}^\times\setminus\{1\}}\chi(z)\sum_{y\in\mathcal{R}^\times}\psi_{z-1}(y) = 0,$$

this completes the proof of Proposition 3.4. □

THEOREM 3.3. *Let* $\chi \in \widehat{\mathcal{R}^\times}$ *be a nontrivial character. If* $\psi \in \widehat{\mathcal{R}^+}$ *is trivial on* $\mathcal{M}$, *then*

$$|G(\chi, \psi_x)|^2 = \begin{cases} q^n & \text{if } x \in \mathcal{R}^\times, \\ 0 & \text{if } x \in \mathcal{M}. \end{cases} \tag{3.4}$$

Proof. It is clear if $x \in \mathcal{M}$ by Lemma 3.1. Let $x \in \mathcal{R}^\times$. The definition (1.1) of Gauss sums yields that

$$\begin{aligned}
\sum_{x\in\mathcal{R}} G(\chi,\psi_x)\overline{G(\chi,\psi_x)} &= \sum_{x\in\mathcal{R}}\sum_{y\in\mathcal{R}^\times}\chi(y)\psi_x(y)\sum_{z\in\mathcal{R}^\times}\overline{\chi(z)\psi_x(z)} \\
&= \sum_{y\in\mathcal{R}^\times}\sum_{z\in\mathcal{R}^\times}\chi(y)\overline{\chi(z)}\sum_{x\in\mathcal{R}}\psi_{y-z}(x) \\
&= \sum_{z\in\mathcal{R}^\times}1\sum_{x\in\mathcal{R}}1 + \sum_{\substack{y,z\in\mathcal{R}^\times \\ y-z\neq 0}}\chi(y)\overline{\chi(z)}\sum_{x\in\mathcal{R}}\psi_{y-z}(x) \\
&= (q-1)q^{n-1}q^n \text{ (by (2.11))}.
\end{aligned}$$

On the other hand, by Lemma 3.1 we have

$$\sum_{x\in R} G(\chi,\psi_x)\overline{G(\chi,\psi_x)} = G(\chi,\psi)\overline{G(\chi,\psi)}\sum_{x\in\mathcal{R}^\times}1 = (q-1)q^{n-1}|G(\chi,\psi)|^2.$$

By comparing above two formulas we have $|G(\chi,\psi)|^2 = q^n$. This completes the proof of Theorem 3.1. □

COROLLARY 3.1. *Let* $\mathcal{R} = GR(p^2, m)$. *If* $\chi \in \widehat{\mathcal{R}^\times}$ *is nontrivial on* $1+\mathcal{M}$, *then*

$$|G(\chi, \psi_x)|^2 = \begin{cases} q^2 & \text{if } x \in \mathcal{R}^\times, \\ 0 & \text{if } x \in \mathcal{M}. \end{cases} \tag{3.5}$$

Proof. From (2.4) and (2.25), we have $\chi = \eta_j\varphi_t$ where $\eta_j \in \widehat{\Gamma_m^\times}$ and $\varphi_t \in \widehat{\mathbb{F}_q}^+$ $(t \in \mathbb{F}_q)$ is a nontrivial on $\mathbb{F}_q$. Let $y = z(1+pw),\ z \in \Gamma_m^\times,\ w \in \Gamma_m$ with $\bar{w} \equiv w \pmod p$, $\bar{w} \in \mathbb{F}_q$. Then

$$\begin{aligned}
&G(\chi,\psi_x) \\
={}& \sum_{y\in\mathcal{R}^\times}\chi(y)\psi_x(y) = \sum_{z\in\Gamma_m^\times}\sum_{\bar{w}\in\mathbb{F}_q}\eta_j(z)\varphi_t(\bar{w})\psi_x(z(1+pw)) \\
={}& \sum_{z\in\Gamma_m^\times}\eta_j(z)\psi_x(z)\sum_{\bar{w}\in\mathbb{F}_q}\varphi_t(\bar{w})\psi_x(pzw) = \sum_{z\in\Gamma_m^\times}\eta_j(z)\psi_x(z)\sum_{\bar{w}\in\mathbb{F}_q}\varphi_t(\bar{w})\psi_z(pxw).
\end{aligned}$$

If $x \in \mathcal{M}$, then $xw \in \mathcal{M}$ for all $w \in \Gamma_m \subset \mathcal{R}^\times$ and so that $pxw = 0$, i.e., $\psi_z(pxw) = 1$. Thus

$$G(\chi, \psi_x) = \sum_{z \in \Gamma_m^\times} \eta_j(z)\psi_x(z) \sum_{\bar{w} \in \mathbb{F}_q} \varphi_t(\bar{w}) = 0$$

since $\sum_{\bar{w} \in \mathbb{F}_q} \varphi_t(\bar{w}) = 0$ for a nontrivial character φ_t. For $x \in \mathcal{R}^\times$, we have the same proof of Theorem 3.3. $\square$

References

[1] H. Ishibashi, *The Terwilliger algebras of certain association schemes over the Galois rings of characteristic 4,* Graphs and Combinatorics **12** (1) (1996), 39–54.

[2] L. Jin, Z. ShiXin and F. KeQin, *The Gauss sums and Jacobi sums over Galois ring $GR(p^2, r)$,* Science China **56** (2013), 1457–1465.

[3] P. Langevin and P. Solé, *Gauss sums over quasi-Frobenius rings,* Proceedings of The Fifth International Conference on Finite Fields and Applications Fq5, held at the University of Augsburg, Germany, August 2–6, 1999, pp. 329–340.

[4] R. Lidl and H. Niederreiter, *Finite fields,* Addison-Wesley, London, 1997.

[5] B. R. McDonald, *Finite Rings with Identity,* Marcel Dekker, 1974.

[6] A. A. Nechaev, *Kerdock code in a cyclic form,* Discrete Math. Appl. **1** (1991), 365–384.

[7] Y. Oh and H. J. Oh, *Gauss sums over Galois rings of characteristic 4,* Kangweon-Kyungki Math. Jour. **9** (1) (2001), 1–7.

[8] F. Ozbudak and Z. Saygi, *Some constructions of systematic authentication codes using Galois rings,* Des. Codes Cryptography **41** (3) (2006), 343–357.

[9] R. Raghavendran, *Finite associative rings,* Compositio Math. **21** (1969), 195–229.

[10] F. Shuqin and H. Wenbao, *Character sums over Galois rings and primitive polynomials over finite fields,* Finite Fields and Their Applications **10** (2004), 36–52.

[11] Z. X. Wan, *Lectures on Finite Fields and Galois Rings,* World Scientific, 2003.

[12] M. Yamada, *Distance-Regular Digraphs of Girth* 4 *Over an Extension Ring of* $\mathbb{Z}/4\mathbb{Z}$*,* Graphs and Combinatorics **6** (1990), 381–394.

[13] M. Yamada, *Difference sets over the Galois rings with odd extension degrees and characteristic an even power of* 2*,* Des. Codes Cryptogr. **67** (2013), 37–57.

Young Ho Jang
Department of Mathematics
Inha University
Incheon, 22212, Korea
E-mail: yjang6105@inha.ac.kr

Sang Pyo Jun
Information Communication
Namseoul University
Chun-An 31020, Korea
E-mail: spjun7129@naver.com