Korean J. Math. **28** (2020), No. 2, pp. 241–255
http://dx.doi.org/10.11568/kjm.2020.28.2.241

GENERALIZED COHN FUNCTIONS ON GALOIS RINGS

Young Ho Jang

Abstract. Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements. A complex valued Cohn function defined on $\mathbb{F}_q$ is introduced in [1]. In this paper we define generalized Cohn functions on Galois rings and investigate their properties.

1. Introduction

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

In [1], a function $f : \mathbb{F}_q \to \mathbb{C}$ is said to be a Cohn function if $f(0) = 0$, $|f(x)| = 1$ for all $x \in \mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ and

$$\sum_{x\in\mathbb{F}_q} f(x)\overline{f(x+a)} = \begin{cases} -1 & \text{if } a \neq 0, \\ q-1 & \text{if } a = 0. \end{cases} \tag{1.1}$$

For example, if $f = \theta\chi$, where $\theta \in \mathbb{C}^1$ and χ is a nontrivial multiplicative character of $\mathbb{F}_q$ (with $\chi(0) := 0$), then f is a Cohn function. In this case the sum in (1.1) is a well known Jacobi sum.

In this paper we define generalized Cohn functions on Galois rings and investigate their properties.

Received August 19, 2019. Revised March 20, 2020. Accepted March 31, 2020.
2010 Mathematics Subject Classification: 11T24, 16L60, 42A38, 42B10.
Key words and phrases: Galois rings, Fourier transforms, Dedekind determinant.

We conclude this section by recalling some basic properties of Galois rings. These have been well documented in [4, 5, 9]. Galois rings constitute a very important family of finite chain rings. They can be defined as follows: If $\overline{f}(x)$ is a primitive irreducible polynomial of degree m over $\mathbb{F}_p$, then $\mathbb{F}_p[x]/\langle\overline{f}(x)\rangle$ is a finite field $\mathbb{F}_q$ of order $q = p^m$. Hensel's lemma states that there is a unique primitive irreducible polynomial $f(x)$ over $\mathbb{Z}_{p^n}$ so that $f(x) \equiv \overline{f}(x) \bmod p$ and with a root ξ of $f(x)$ satisfying $\xi^{q-1} = 1$. The quotient ring

$$\begin{aligned} \mathcal{R} &= GR(p^n, m) = \mathbb{Z}_{p^n}[x]/\langle f(x)\rangle \cong \mathbb{Z}_{p^n}[\xi] \\ &= \{z_0 + z_1\xi + \cdots + z_{m-1}\xi^{m-1} : z_i \in \mathbb{Z}_{p^n}\} \end{aligned} \tag{1.2}$$

is called a Galois ring of characteristic p^n and cardinality $p^{mn} = q^n$. The modulo p reduction mapping

$$\mu : \mathbb{Z}_{p^n} \longrightarrow \mathbb{F}_p, \quad a \ (\mathrm{mod}\ p^n) \longmapsto \overline{a} \equiv a \ (\mathrm{mod}\ p)$$

can be naturally extended the following homomorphism of rings

$$\mu : \mathcal{R} = GR(p^n, m) = \frac{\mathbb{Z}_{p^n}[x]}{\langle f(x)\rangle} \cong \mathbb{Z}_{p^n}[\xi] \longrightarrow \mathbb{F}_q = \frac{\mathbb{F}_p[x]}{\langle\overline{f}(x)\rangle} \cong \mathbb{F}_p[\overline{\xi}].$$

Some basic facts about Galois ring $\mathcal{R} = GR(p^n, m)$ are given as follows.

(Fact 1) $\mathcal{R}$ is a local commutative ring with the unique maximal ideal $\mathcal{M} = \ker\mu = p\mathcal{R}$, $|\mathcal{M}| = q^{n-1}$ and the residue class field $\mathcal{R}/\mathcal{M} \cong \mathbb{F}_q$. Also, $\mathcal{R}$ is a finite chain ring of length n, its ideals $p^i\mathcal{R}$ with q^{n-i} elements are linearly ordered by inclusion,

$$\{0\} = p^n\mathcal{R} \subset p^{n-1}\mathcal{R} \subset \cdots \subset \mathcal{M} = p\mathcal{R} \subset \mathcal{R}.$$

(Fact 2) The group $\mathcal{R}^* = \mathcal{R}\backslash\mathcal{M}$ of units has the direct decomposition (see [4, Theorem XVIII.2]):

$$\mathcal{R}^* = \mathcal{T}^* \times (1 + \mathcal{M}) \tag{1.3}$$

where $\mathcal{T}^* = \langle\xi\rangle$ is the cyclic group of order $q-1$ and $1+\mathcal{M}$ is the multiplicative p-group of order q^{n-1}. Define $\mathcal{T} = \mathcal{T}^* \cup \{0\} = \{0, 1, \xi, \cdots, \xi^{q-2}\}$, which is referred to as the Teichmüller set. Then $\overline{\mathcal{T}} = \mathbb{F}_q$ and every element $z \in \mathcal{R}$ has a unique p-adic representation

$$z = z_0 + z_1p + \cdots + z_{n-1}p^{n-1}, \ z_i \in \mathcal{T}. \tag{1.4}$$

Note that the p-adic representation is not preserved under addition. From (1.4), $z \in \mathcal{M}$ if and only if $z_0 = 0$ and $z \in \mathcal{R}^*$ if and only if

$z_0 \in \mathcal{T}^*$. An arbitrary element u of $\mathcal{R}^*$ is uniquely represented as

(1.5)
$$\begin{aligned} u &= u_c + u_m,\ u_c \in \mathcal{T}^*,\ u_m \in \mathcal{M} \\ &= \xi^k x = \xi^k(1+py),\ x \in 1+\mathcal{M},\ y \in GR(p^{n-1},m),\ 0 \le k \le q-2. \end{aligned}$$

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

(1.6) $z = p^l u = p^l \xi^k x,\ u \in \mathcal{R}^*,\ x \in 1{+}\mathcal{M},\ 0 \le l \le n{-}1,\ 0 \le k \le q{-}2.$

(Fact 3) $\mathcal{R}/\mathbb{Z}_{p^n}$ is a Galois extension of rings with Galois group $Gal(\mathcal{R}/\mathbb{Z}_{p^n}) = \langle\sigma\rangle$, where σ is the Frobenius map from $\mathcal{R}$ to $\mathcal{R}$ given by:

$\sigma : z = (z_0{+}pz_1{+}\cdots{+}p^{n-1}z_{n-1}) \longmapsto z_0^p{+}pz_1^p{+}\cdots{+}p^{n-1}z_{n-1}^p$, for $z_i \in \mathcal{T}$.

Define the additive trace from $\mathcal{R}$ to $\mathbb{Z}_{p^n}$ by:

(1.7)
$$\mathrm{Tr}\left(z = \sum_{i=0}^{n-1} z_i p^i\right) = z + z^\sigma + \cdots + z^{\sigma^{m-1}} = \sum_{i=0}^{n-1}(z_i + z_i^p + \cdots + z_i^{p^{m-1}})p^i.$$

Tr is an epimorphism of $\mathbb{Z}_{p^n}$-modules and Tr can be reduced by μ to the trace mapping $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ of finite fields. Then we have $\mu(\mathrm{Tr}_n(z)) = \mathrm{tr}(\mu(z))$ for all $z \in \mathcal{R}$.

2. Characters of Galois rings

In this section, we give a few basic facts on the additive and multiplicative characters of Galois rings. Also, we give some simple but useful propositions which we will use later.

An additive character of $\mathcal{R}$ is a homomorphism from the additive group of $\mathcal{R}$ to $\mathbb{C}^1$. Using (1.7), for any $x, y \in R$, the additive characters of $\mathcal{R}$ are given by

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

different x's affording different additive characters. In fact, $\{\psi_x\}_{x\in\mathcal{R}}$ consists of all additive characters of $\mathcal{R}$ in [7, Lemma 6]. ψ_0 is the trivial additive character of $\mathcal{R}$ and $\psi = \psi_1$ is called the generating additive character of $\mathcal{R}$. Let $\widehat{\mathcal{R}^+}$ denote the additive characters group.

Proposition 2.1 ([6, Lemma 2.1, 2.2, 2.3]). *For any $x \in \mathcal{R}$ we have*

$$\sum_{y\in\mathcal{R}} \psi_x(y) = \begin{cases} q^n & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases}; \tag{2.2}$$

$$\sum_{y\in\mathcal{M}} \psi_x(y) = \begin{cases} q^{n-1} & \text{if } x \in p^{n-1}\mathcal{R} \\ 0 & \text{if } x \in \mathcal{R}\backslash p^{n-1}\mathcal{R} \end{cases}; \tag{2.3}$$

$$\sum_{y\in\mathcal{R}^*} \psi_x(y) = \begin{cases} (q-1)q^{n-1} & \text{if } x = 0, \\ -q^{n-1} & \text{if } x \in p^{n-1}\mathcal{R}\backslash\{0\}, \\ 0 & \text{if } x \in \mathcal{R}\backslash p^{n-1}\mathcal{R}. \end{cases} \tag{2.4}$$

Proposition 2.2 ([7, Lemma 8]). *For any $x \in \mathcal{R}$ we have*

$$\sum_{y\in\mathcal{T}} \psi_x(p^{n-1}y) = \begin{cases} q & \text{if } x \in \mathcal{M}, \\ 0 & \text{if } x \in \mathcal{R}^*. \end{cases} \tag{2.5}$$

Proposition 2.3 ([2, Proposition 2.3, 2.4]). *(1) If $\psi_x \in \widehat{\mathcal{R}^+}$ is non-trivial on $\mathcal{M}$, then*

$$\sum_{y\in\mathcal{R}^*} \psi_x(y) = -\sum_{y\in\mathcal{M}} \psi_x(y) = 0. \tag{2.6}$$

(2) If $\psi \in \widehat{\mathcal{R}^+}$ is trivial on $\mathcal{M}$, then

$$\sum_{y\in\mathcal{R}^*} \psi_x(y) = \sum_{y\in\mathcal{R}^*} \psi(xy) = \begin{cases} -q^{n-1} & \text{if } x \in \mathcal{R}^*, \\ (q-1)q^{n-1} & \text{if } x \in \mathcal{M}. \end{cases} \tag{2.7}$$

A multiplicative character χ of $\mathcal{R}^*$ is defined by $\chi(xy) = \chi(x)\chi(y)$ for $x, y \in \mathcal{R}^*$, 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 $\chi(x) = 0$ for all $x \in \mathcal{M}$. We call this the multiplicative character of $\mathcal{R}$. The trivial character χ_0 of $\mathcal{R}$ is defined by $\chi_0(x) = 1$ for all $x \in \mathcal{R}^*$.

Since $\mathcal{R}^* = \mathcal{T}^* \times (1 + \mathcal{M})$, there are several types of multiplicative characters of $\mathcal{R}$ (cf. [2]). In this paper, we treat multiplicative characters χ of $\mathcal{R}$ that vanish on $1 + \mathcal{M}$ (i.e. $\chi(1 + x) = 1$ for all $x \in \mathcal{M}$), which are in one-to-one correspondence with multiplicative characters η_j of $\mathcal{T}^*$ defined by

$$\eta_j(\xi^k) = e^{2\pi i(jk)/q-1} \text{ for } 0 \leq j, k \leq q-2. \tag{2.8}$$

We have the following Proposition 2.4 known as the orthogonality relations for characters.

PROPOSITION 2.4. *For any j and k $(0 \leq j, k \leq q-2)$ we have*

$$\sum_{k=0}^{q-2} \eta_j(\xi^k) = \begin{cases} q-1 & \textit{if } j = 0, \\ 0 & \textit{if } j \neq 0. \end{cases} \tag{2.9}$$

3. The Fourier transform over Galois rings

In this section, using Fourier analysis on finite groups (see [8]), we give a few basic facts on the Fourier transform on functions with domain $\mathcal{R} = GR(p^n, m)$. Also, we give some simple but useful propositions which we will use later.

Denote by $\mathbb{C}^{\mathcal{R}}$ the vector space over $\mathbb{C}$ of all functions from the Galois ring $\mathcal{R}$ to $\mathbb{C}$. This is an inner product space with Hermitian inner product $\langle\ ,\ \rangle$ defined for $f, g \in \mathbb{C}^{\mathcal{R}}$ by

$$\langle f, g\rangle = \sum_{x \in \mathcal{R}} f(x)\overline{g(x)}.$$

The vector space $\mathbb{C}^{\mathcal{R}}$ has the additional structure of an algebra under either of the following two definitions of multiplication:

(a) the pointwise product $f \cdot g$ of $f, g \in \mathbb{C}^{\mathcal{R}}$, defined for $x \in \mathcal{R}$ by $f \cdot g(x) = f(x)g(x)$

(b) the convolution $f * g$ of $f, g \in \mathbb{C}^{\mathcal{R}}$, defined for $x \in \mathcal{R}$ by

$$f * g(x) = \sum_{y \in \mathcal{R}} f(y)g(x-y) \tag{3.1}$$

The set $\{1_x \mid x \in \mathcal{R}\}$ of indicator functions defined by

$$1_x(y) = \begin{cases} 1 & y = x, \\ 0 & y \neq x, \end{cases} \tag{3.2}$$

form an orthonormal basis for $\mathbb{C}^{\mathcal{R}}$, with $\langle 1_x, 1_y\rangle = 1_x(y)$. The additive characters ψ_x of $\mathcal{R}$ defined by (2.1) are also orthogonal in this inner product space,

(3.3)

$$\langle \psi_x, \psi_y\rangle = \sum_{s \in \mathcal{R}} \psi_x(s)\overline{\psi_y(s)} = \sum_{s \in \mathcal{R}} \psi_{x-y}(s) = \begin{cases} q^n & \text{if } x = y \\ 0 & \text{if } x \neq y \end{cases} \quad \text{(by (2.2))}$$

and form an orthogonal basis for $\mathbb{C}^{\mathcal{R}}$.

The Fourier transform on functions with domain $\mathcal{R}$ seeks to express them in terms of the additive characters of $\mathcal{R}$.

DEFINITION 3.1. For $f \in \mathbb{C}^{\mathcal{R}}$ the Fourier transform (the Walsh transform) $\widehat{f} \in \mathbb{C}^{\widehat{\mathcal{R}^+}}$ is defined for $y \in \mathcal{R}$ by

$$\widehat{f}(y) = \langle f, \psi_y \rangle = \sum_{x \in \mathcal{R}} f(x)\psi_y(-x). \tag{3.4}$$

The Fourier transform maps the basis of indicator functions to the basis of additive characters: $\widehat{1_y} = \psi_{-y}$. The Fourier inversion formula $\widehat{\widehat{f}}(x) = q^n f(-x)$, gives the inverse transform

$$f(x) = \frac{1}{q^n}\langle \widehat{f}, \psi_{-x} \rangle = \frac{1}{q^n}\sum_{y \in \mathcal{R}} \widehat{f}(y)\psi_x(y). \tag{3.5}$$

PROPOSITION 3.1. *For the trivial character χ_0 of $\mathcal{R}$, we have*
(1) $\widehat{\chi_0}(x) = \sum_{y \in \mathcal{R}} \chi_0(y)\psi_x(-y) = \sum_{y \in \mathcal{R}^*} \psi_x(-y)$
$$= \begin{cases} (q-1)q^{n-1} & \text{if } x = 0, \\ -q^{n-1} & \text{if } x \in p^{n-1}\mathcal{R}\backslash\{0\}, \\ 0 & \text{if } x \in \mathcal{R}\backslash p^{n-1}\mathcal{R}. \end{cases}$$
(2) if $\psi \in \widehat{\mathcal{R}^+}$ is trivial on $\mathcal{M}$, then

$$\widehat{\chi_0}(x) = \sum_{y \in \mathcal{R}} \chi_0(y)\psi_x(-y) = \sum_{y \in \mathcal{R}^*} \psi(-xy) = \begin{cases} -q^{n-1} & \text{if } x \in \mathcal{R}^*, \\ (q-1)q^{n-1} & \text{if } x \in \mathcal{M}. \end{cases}$$

Proof. By (2.4) in Proposition 2.1 and (2.7) in Proposition 2.3, it is trivial. □

Suppose g is a translation of f, i.e., $g(x) = f(x-z)$ for fixed z and all $x \in \mathcal{R}$. Then $\widehat{g}(x) = \widehat{f} \cdot \psi_{-z}(x)$ is a modulation of $\widehat{f}(x)$. Now suppose g is a dilation of f by an invertible element of $\mathcal{R}$, i.e., $g(x) = f(ux)$ for fixed unit $u \in \mathcal{R}^*$ and all $x \in \mathcal{R}$. Then $\widehat{g}(x) = \widehat{f}(u^{-1}x)$ is a dilation of $\widehat{f}$ by u^{-1}. The orthogonality of characters (3.3) yields Plancherel's identity $\langle f, g \rangle = \frac{1}{q^n}\langle \widehat{f}, \widehat{g} \rangle$.

The Fourier transform gives an isomorphism of the algebra $\mathbb{C}^{\mathcal{R}}$ with multiplication pointwise product with the algebra $\mathbb{C}^{\mathcal{R}}$ with multiplication convolution: for $y \in \mathcal{R}$ we have

$$\widehat{f * g}(y) = \widehat{f} \cdot \widehat{g}(y) \quad \text{and} \quad \widehat{f \cdot g}(y) = \frac{1}{q^n}\widehat{f} * \widehat{g}(y). \tag{3.6}$$

If f^τ is the function defined for $x \in \mathcal{R}$ by

$$f^\tau(x) = \overline{f(-x)}, \tag{3.7}$$

then

$$\widehat{f^\tau} = \overline{\widehat{f}}. \tag{3.8}$$

THEOREM 3.1. *For any function* $f \in \mathbb{C}^{\mathcal{R}}$,

$$f * f^\tau = \widehat{\chi_0} \text{ on } \mathcal{R}. \tag{3.9}$$

if and only if

$$|\widehat{f}|^2 = q^n \chi_0 \text{ on } \mathcal{R} \tag{3.10}$$

Proof. From (3.4), for any $x \in \mathcal{R}$, we have

$$\begin{aligned}
\widehat{\widehat{\chi_0}}(x) &= \sum_{y \in \mathcal{R}} \widehat{\chi_0}(y)\psi_x(-y) \\
&= (q-1)q^{n-1} - q^{n-1} \sum_{y \in p^{n-1}\mathcal{R}\backslash\{0\}} \psi_x(-y) \text{ (by Proposition 3.1(1))} \\
&= (q-1)q^{n-1} - q^{n-1} \sum_{a \in \mathcal{T}^*} \psi_x(p^{n-1}a) \\
&\quad \text{(since } y \in p^{n-1}\mathcal{R}\backslash\{0\} \text{ if and only if } y = p^{n-1}a,\ a \in \mathcal{T}^*) \\
&= \begin{cases} (q-1)q^{n-1} - q^{n-1}(0-1) = q^n & \text{if } x \in \mathcal{R}^* \\ (q-1)q^{n-1} - q^{n-1}(q-1) = 0 & \text{if } x \in \mathcal{M} \end{cases} \\
&\quad \text{(by (2.5) in Proposition 2.2).}
\end{aligned}$$

That is, $\widehat{\widehat{\chi_0}} = q^n \chi_0$ on $\mathcal{R}$. Also, from (3.8) and (3.6), we have for any $x \in \mathcal{R}$

$$|\widehat{f}(x)|^2 = \widehat{f}(x)\overline{\widehat{f}(x)} = \widehat{f}(x)\widehat{f^\tau}(x) = \widehat{f * f^\tau}(x).$$

Assume (3.9) holds for any function $f \in \mathbb{C}^{\mathcal{R}}$. Then for any $x \in \mathcal{R}$

$$|\widehat{f}(x)|^2 = \widehat{f * f^\tau}(x) = \widehat{\widehat{\chi_0}}(x) = q^n \chi_0(x).$$

So that (3.10) holds. Conversely, if (3.10) is true, then for any $x \in \mathcal{R}$

$$\widehat{f * f^\tau}(x) = |\widehat{f}(x)|^2 = q^n \chi_0(x) = \widehat{\widehat{\chi_0}}(x).$$

So that (3.9) holds. □

4. Dedekind determinant relation on Galois rings

In this section, we introduce Dedekind determinant relation (see [3, p. 89]) on Galois rings.

We consider the (q^n-1)-dimensional subspace V of $\mathbb{C}^{\mathcal{R}}$ defined by

$$V=\left\{f\in\mathbb{C}^{\mathcal{R}}\ :\ \sum_{x\in\mathcal{R}}f(x)=0\right\}.$$

Proposition 4.1. *The set $\{\psi_x \mid x\in\mathcal{R}\backslash\{0\}\}$ is a basis for V.*

Proof. First, $\{\psi_x \mid x\in\mathcal{R}\backslash\{0\}\}\subseteq V$ since $\sum_{y\in\mathcal{R}}\psi_x(y)=0$ for any $x\in\mathcal{R}\backslash\{0\}$ by (2.2). If $\sum_{x\in\mathcal{R}}c_x\psi_x(y)=0$, then $c_x=0$ for all $x\in\mathcal{R}$ since each value of $\psi_x(y)$ is the principal p^nth-root of the unity in $\mathbb{C}$ by (2.1). Moreover, the set $\{\psi_x \mid x\in\mathcal{R}\backslash\{0\}\}$ spans V because that for any $g\in V$ we have

$$\begin{aligned} g(y) &= \frac{1}{q^n}\sum_{x\in\mathcal{R}}\widehat{g}(x)\psi_x(y) \text{ (by the inverse transform (3.5))}\\ &= \frac{1}{q^n}\widehat{g}(0)+\frac{1}{q^n}\sum_{x\in\mathcal{R}\backslash\{0\}}\widehat{g}(x)\psi_x(y)=\frac{1}{q^n}\sum_{x\in\mathcal{R}\backslash\{0\}}\widehat{g}(x)\psi_x(y)\end{aligned}$$

since $\widehat{g}(0)=\sum_{x\in\mathcal{R}}g(x)\psi_0(-x)=\sum_{x\in\mathcal{R}}g(x)=0$. □

Proposition 4.2. *The set $\{1_x-q^{-n} \mid x\in\mathcal{R}\backslash\{0\}\}$ is a basis for V, where 1_x is an indicator function defined by* (3.2).

Proof. First, $\{1_x-q^{-n} \mid x\in\mathcal{R}\backslash\{0\}\}\subseteq V$ since $\sum_{y\in\mathcal{R}}(1_x-q^{-n})(y)=\sum_{y\in\mathcal{R}}1_x(y)-1=0$ for any $x\in\mathcal{R}\backslash\{0\}$. Also, if $\sum_{x\in\mathcal{R}\backslash\{0\}}c_x(1_x-q^{-n})(y)=0$, then $c_x=0$ for all $x\in\mathcal{R}\backslash\{0\}$ because that for $y=0$ we have

$$0=\sum_{x\in\mathcal{R}\backslash\{0\}}c_x(1_x-q^{-n})(0)=\sum_{x\in\mathcal{R}\backslash\{0\}}c_x1_x(0)-q^{-n}\sum_{x\in\mathcal{R}\backslash\{0\}}c_x=-q^{-n}\sum_{x\in\mathcal{R}\backslash\{0\}}c_x$$

and for $y\in\mathcal{R}\backslash\{0\}$ we have

$$0=\sum_{x\in\mathcal{R}\backslash\{0\}}c_x(1_x-q^{-n})(y)=\sum_{x\in\mathcal{R}\backslash\{0\}}c_x1_x(y)-q^{-n}\sum_{x\in\mathcal{R}\backslash\{0\}}c_x=c_y-q^{-n}\sum_{x\in\mathcal{R}\backslash\{0\}}c_x=c_y.$$

Moreover, the set $\{1_x - q^{-n} \mid x \in \mathcal{R}\backslash\{0\}\}$ spans V because that for any $g \in V$ we have

$$\begin{aligned} g(y) &= g(y) - q^{-n}\sum_{x\in\mathcal{R}} g(x) = \sum_{x\in\mathcal{R}} g(x)\left(1_x - q^{-n}\right)(y) \\ &= \sum_{x\in\mathcal{R}\backslash\{0\}} g(x)\left(1_x - q^{-n}\right)(y) + g(0)\left(1_0 - q^{-n}\right)(y), \end{aligned}$$

and, since for $y \in \mathcal{R}$

$$\sum_{x\in\mathcal{R}\backslash\{0\}} (1_x - q^{-n})(y) = \sum_{x\in\mathcal{R}} (1_x - q^{-n})(y) - (1_0 - q^{-n})(y) = -(1_0 - q^{-n})(y),$$

we have

$$g(y) = \sum_{x\in\mathcal{R}\backslash\{0\}} (g(x) - g(0))\left(1_x - q^{-n}\right)(y). \tag{4.1}$$

□

LEMMA 4.1. *Let $f \in V$. Then*

$$diag\{\widehat{f}(-x)\}_{x\in\mathcal{R}\backslash\{0\}} \sim [f(x-y) - f(x)]_{x,y\in\mathcal{R}\backslash\{0\}}, \tag{4.2}$$

and consequently

$$\prod_{x\in\mathcal{R}\backslash\{0\}} \widehat{f}(-x) = q^n \cdot \det[f(x-y)]_{x,y\in\mathcal{R}\backslash\{0\}}. \tag{4.3}$$

Proof. For $x \in \mathcal{R}$ let $T_x : V \to V$ be defined by $T_x f(y) = f(y+x)$ for $y \in \mathcal{R}$. For a fixed element $f \in V$, let

$$T_f = \sum_{x\in\mathcal{R}} f(x) T_x.$$

Then for any $g \in V$ we have

$$\sum_{y\in\mathcal{R}} T_f g(y) = \sum_{y\in\mathcal{R}}\sum_{x\in\mathcal{R}} f(x) T_x g(y) = \sum_{x\in\mathcal{R}} f(x) \sum_{y\in\mathcal{R}} g(y+x) = 0$$

since adding $x \in \mathcal{R}$ to all $y \in \mathcal{R}$ permutes $\mathcal{R}$. Thus the function T_f is a linear map on V. From Proposition 4.1 and Proposition 4.2, the space V has two bases $A = \{\psi_x \mid x \in \mathcal{R}\backslash\{0\}\}$ and $B = \{1_x - q^{-n} \mid x \in \mathcal{R}\backslash\{0\}\}$.

For $\psi_x \in A$ we have

$$\begin{aligned} T_f\psi_x(z) &= \sum_{y\in\mathcal{R}} f(y)T_y\psi_x(z) = \sum_{y\in\mathcal{R}} f(y)\psi_x(z+y) \\ &= \psi_x(z)\sum_{y\in\mathcal{R}} f(y)\psi_x(y) = \psi_x(z)\widehat{f}(-x), \end{aligned}$$

that is, $T_f\psi_x = \widehat{f}(-x)\psi_x$. This means that ψ_x is an eigenvector of T_f with eigenvalue $\widehat{f}(-x)$. Therefore, the matrix for T_f with respect to the basis A is the diagonal matrix $diag\{\widehat{f}(-x)\}_{x\in\mathcal{R}\setminus\{0\}}$. On the other hand, we look at the effect of T_f on the other basis B. Now, since $f \in V$ it follows that T_f applied to any constant function is just zero. Thus for any $x \in \mathcal{R}\setminus\{0\}$,

$$\begin{aligned} T_f(1_x - q^{-n})(z) &= T_f 1_x(z) = \sum_{y\in\mathcal{R}} f(y)T_y 1_x(z) = \sum_{y\in\mathcal{R}} f(y)1_x(z+y) \\ &= f(x-z) = \sum_{y\in\mathcal{R}\setminus\{0\}} (f(x-y)-f(x))(1_y - q^{-n})(z) \end{aligned}$$

by (4.1), and so the matrix for T_f with respect to the basis B is $[f(x-y)-f(x)]_{x,y\in\mathcal{R}\setminus\{0\}}$ (indexing the rows by y and the columns by x). We obtain the similarity relationship in (4.2). Next, we have

$$\sum_{y\in\mathcal{R}\setminus\{0\}} \{f(x-y)-f(x)\} = \sum_{y\in\mathcal{R}\setminus\{0\}} f(x-y)-(q^n-1)f(x) = \sum_{y\in\mathcal{R}} f(x-y)-q^n f(x),$$

and, since adding $x \in \mathcal{R}\setminus\{0\}$ to all $-y \in \mathcal{R}$ permutes $\mathcal{R}$ and $f \in V$, we have

$$0 = \sum_{y\in\mathcal{R}} f(x-y) = \sum_{y\in\mathcal{R}\setminus\{0\}} f(x-y) + f(x)$$

and so

$$\sum_{y\in\mathcal{R}\setminus\{0\}} \{f(x-y)-f(x)\} = q^n \sum_{y\in\mathcal{R}\setminus\{0\}} f(x-y).$$

From elementary row operations, we obtain

$$\det[f(x-y)-f(x)]_{x,y\in\mathcal{R}\setminus\{0\}} = q^n \cdot \det[f(x-y)]_{x,y\in\mathcal{R}\setminus\{0\}},$$

and so we have (4.3). $\square$

5. Generalized Cohn functions on Galois rings

In this section, we define generalized Cohn functions on Galois rings and investigate their properties.

DEFINITION 5.1. We say that a complex valued function f defined on the Galois ring $\mathcal{R} = GR(p^n, m)$ is a generalized Cohn function if $f(x) = 0$ for all $x \in \mathcal{M}$, $|f(x)| = 1$ for all $x \in \mathcal{R}^*$, and f satisfies either

$$\sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)} = \begin{cases} -q^{n-1} & \text{if } y \in \mathcal{R}^*, \\ (q-1)q^{n-1} & \text{if } y \in \mathcal{M}. \end{cases} \tag{5.1}$$

or

$$\sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)} = \begin{cases} (q-1)q^{n-1} & \text{if } x = 0, \\ -q^{n-1} & \text{if } x \in p^{n-1}\mathcal{R}\backslash\{0\}, \\ 0 & \text{if } x \in \mathcal{R}\backslash p^{n-1}\mathcal{R}. \end{cases} \tag{5.2}$$

In the case of $n = 1$, both (5.1) and (5.2) is just (1.1), that is, f is a Cohn function on the finite field $\mathbb{F}_q$.

PROPOSITION 5.1. *If $f \in \mathbb{C}^{\mathcal{R}}$ is a generalized Cohn function satisfying* (5.1) *(resp.,* (5.2)*), then* $\sum_{x\in\mathcal{R}} f(x) = 0$.

Proof. Since adding $x \in \mathcal{R}$ to all $y \in \mathcal{R}$ permutes $\mathcal{R}$, for any generalized Cohn function $f \in \mathbb{C}^{\mathcal{R}}$ satisfying (5.1), we have

$$\begin{aligned} &\left|\sum_{x\in\mathcal{R}} f(x)\right|^2 \\ &\quad= \sum_{x\in\mathcal{R}} f(x) \sum_{y\in\mathcal{R}} \overline{f(x+y)} = \sum_{y\in\mathcal{R}}\sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)} \\ &\quad= \sum_{y\in\mathcal{M}}\sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)} + \sum_{y\in\mathcal{R}^*}\sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)} \\ &\quad= q^{n-1}(q-1)q^{n-1} + (q-1)q^{n-1}(-q^{n-1}) = 0 \text{ (by (5.1))}, \end{aligned}$$

and for any generalized Cohn function $f \in \mathbb{C}^{\mathcal{R}}$ satisfying (5.2), we have

$$\begin{aligned}
&\left|\sum_{x\in\mathcal{R}} f(x)\right|^2 \\
&= \sum_{x\in\mathcal{R}} f(x) \sum_{y\in\mathcal{R}} \overline{f(x+y)} = \sum_{y\in\mathcal{R}}\sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)} \\
&= \sum_{x\in\mathcal{R}} f(x)\overline{f(x+0)} + \sum_{y\in p^{n-1}\mathcal{R}\backslash\{0\}} \sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)} \\
&\qquad + \sum_{y\in\ \mathcal{R}\backslash p^{n-1}\mathcal{R}} \sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)} \\
&= |\mathcal{R}^*| - q^{n-1}|p^{n-1}\mathcal{R}\backslash\{0\}| + 0|\mathcal{R}\backslash p^{n-1}\mathcal{R}| \text{ (by } f(\mathcal{M}) = 0 \text{ and (5.2))} \\
&= (q-1)q^{n-1} - q^{n-1}(q^{n-(n-1)} - 1) + 0 = 0.
\end{aligned}$$

Thus $\sum_{x\in\mathcal{R}} f(x) = 0$. □

Let $\Delta \in \mathbb{C}^{\mathcal{R}}$ be the function defined by

$$\Delta(y) = \begin{cases} 1-q & \text{if } y \in \mathcal{R}^*, \\ 1 & \text{if } y \in \mathcal{M}. \end{cases} \tag{5.3}$$

Proposition 5.2. *Let $f \in \mathbb{C}^{\mathcal{R}}$. If the autocorrelation condition*

$$\sum_{x\in\mathcal{R}} f(bx)\overline{f(x+y)} = \frac{1}{\Delta(y)} \sum_{x\in\mathcal{R}} f(bx)\overline{f(x)} \tag{5.4}$$

holds for all $b \in \mathcal{R}^*$ and for all $y \in \mathcal{R}$, then $\sum_{x\in\mathcal{R}} f(x) = 0$.

Proof. Assume that (5.4) holds for all $b \in \mathcal{R}^*$ and for all $y \in \mathcal{R}$. Since multiplying $b \in \mathcal{R}^*$ by all $x \in \mathcal{R}$ permutes $\mathcal{R}$ and adding $x \in \mathcal{R}$ to all $y \in \mathcal{R}$ permutes $\mathcal{R}$, we have

$$\begin{aligned}
\left|\sum_{x\in\mathcal{R}} f(x)\right|^2 &= \sum_{x\in\mathcal{R}} f(x) \sum_{x\in\mathcal{R}} \overline{f(x)} = \sum_{x\in\mathcal{R}} f(bx) \sum_{y\in\mathcal{R}} \overline{f(x+y)} \\
&= \sum_{y\in\mathcal{R}}\sum_{x\in\mathcal{R}} f(bx)\overline{f(x+y)} = \sum_{y\in\mathcal{R}} \frac{1}{\Delta(y)} \sum_{x\in\mathcal{R}} f(bx)\overline{f(x)} \text{ (by (5.4))} \\
&= 0
\end{aligned}$$

since

$$\sum_{y\in\mathcal{R}} \frac{1}{\Delta(y)} = \sum_{y\in\mathcal{M}} \frac{1}{\Delta(y)} + \sum_{y\in\mathcal{R}^*} \frac{1}{\Delta(y)} = q^{n-1} + \frac{1}{1-q}(q-1)q^{n-1} = 0,$$

and so $\sum_{x\in\mathcal{R}} f(x) = 0$. $\square$

Theorem 5.1. *Let* $f = \theta\chi$, *where* $\theta \in \mathbb{C}^1$ *and* χ *is a nontrivial multiplicative character of* $\mathcal{R}$ *that vanishes on* $1+\mathcal{M}$. *Then*

(i) f *is a generalized Cohn function satisfying* (5.1).

(ii) f *satisfies the autocorrelation condition* (5.4) *for all* $b \in \mathcal{R}^*$ *and for all* $y \in \mathcal{R}$.

Proof. (i) By definition of multiplicative character of $\mathcal{R}$, $\chi(x) = 0$ for all $x \in \mathcal{M}$ and so $f(x) = 0$ for all $x \in \mathcal{M}$. Since χ is a nontrivial multiplicative character of $\mathcal{R}$ that vanishes on $1+\mathcal{M}$, χ's are in one-to-one correspondence with multiplicative characters η_j of $\mathcal{T}^*$, which are defined by (2.8). Thus $|f(x)| = |\eta_j(\xi^k)| = 1$ for all $x = \xi^k(1+x) \in \mathcal{R}^* = \mathcal{T}^* \times (1+\mathcal{M})$ $(0 \le j,k \le q-2)$. We show that (5.1) holds. Let $F = \sum_{x\in\mathcal{R}} f(x)\overline{f(x+y)}$. Then

$$F = \sum_{x\in\mathcal{R}^*} \chi(x)\overline{\chi(x+y)} = \sum_{x\in\mathcal{R}^*} \overline{\chi(1+x^{-1}y)}.$$

If $y \in \mathcal{M}$, then $F = (q-1)q^{n-1}$ because that $x^{-1}y \in \mathcal{M}$ for all $x \in \mathcal{R}^*$ and $\chi(1+x^{-1}y) = 1$. Let $y \in \mathcal{R}^*$. Since multiplying y by x^{-1} for all $x \in \mathcal{R}^*$ permutes $\mathcal{R}^*$, by setting $u = x^{-1}y \in \mathcal{R}^*$ we have

$$\begin{aligned}
F &= \sum_{u\in\mathcal{R}^*} \overline{\chi(1+u)} = \sum_{u\in\mathcal{R}} \overline{\chi(1+u)} - \sum_{u\in\mathcal{M}} \overline{\chi(1+u)} \\
&= \sum_{u\in\mathcal{R}} \overline{\chi(1+u)} - q^{n-1} \text{ (by } \chi(1+\mathcal{M}) = 1) \\
&= \sum_{v\in\mathcal{R}^*} \overline{\chi(v)} - q^{n-1} \text{ (by setting } v = 1+u \text{ and } \chi(x) = 0 \text{ for all } x \in \mathcal{M}) \\
&= \sum_{k=0}^{q-2} \overline{\eta(\xi^k)} - q^{n-1} \text{ (by setting } v = \xi^k y, \text{ where } y \in 1+\mathcal{M} \text{ and } \chi(y) = 1) \\
&= -q^{n-1} \text{ (by (2.9))}.
\end{aligned}$$

Thus (5.1) holds, i.e., f is a generalized Cohn function satisfying (5.1).
(ii) Since $bx \in \mathcal{M}$ for all $b \in \mathcal{R}^*$ and for all $x \in \mathcal{M}$, we have $f(bx) =$

$\chi(bx) = 0$. Thus for all $b \in \mathcal{R}^*$ and for all $y \in \mathcal{R}$ we have

$$\begin{aligned}
&\text{RHS of (5.4)}\\
&= \frac{1}{\Delta(y)} \sum_{x \in \mathcal{R}^*} f(bx)\overline{f(x)} = \frac{1}{\Delta(y)}\chi(b) \sum_{x \in \mathcal{R}^*} 1\\
&= \frac{1}{\Delta(y)}\chi(b)(q-1)q^{n-1} = \begin{cases} -\chi(b)q^{n-1} & \text{if } y \in \mathcal{R}^* \\ \chi(b)(q-1)q^{n-1} & \text{if } y \in \mathcal{M} \end{cases} \quad \text{(by (5.3))}
\end{aligned}$$

and

$$\begin{aligned}
\text{LHS of (5.4)} &= \sum_{x \in \mathcal{R}^*} f(bx)\overline{f(x+y)} = \chi(b) \sum_{x \in \mathcal{R}^*} \chi(x)\overline{\chi(x+y)}\\
&= \begin{cases} -\chi(b)q^{n-1} & \text{if } y \in \mathcal{R}^* \\ \chi(b)(q-1)q^{n-1} & \text{if } y \in \mathcal{M} \end{cases}
\end{aligned}$$

by (5.1) (since $\chi \in \mathbb{C}^{\mathcal{R}}$ is a generalized Cohn function satisfying (5.1)). Thus the autocorrelation condition (5.4) holds for all $b \in \mathcal{R}^*$ and for all $y \in \mathcal{R}$. □

From Proposition 3.1, Theorem 3.2 and Lemma 4.1, the following corollaries are now immediate.

Corollary 5.1. *$f \in \mathbb{C}^{\mathcal{R}}$ is a generalized Cohn function satisfying (5.2) if and only if $|f| = \chi_0$ and $|\widehat{f}| = q^{\frac{n}{2}}\chi_0$.*

Corollary 5.2. *If $f \in \mathbb{C}^{\mathcal{R}}$ is a generalized Cohn function satisfying (5.2), then the matrix*

$$[f(x-y)]_{x,y \in \mathcal{R}\setminus\{0\}}$$

is nonsingular.

Theorem 5.2. *If $f \in \mathbb{C}^{\mathcal{R}}$ is a generalized Cohn function satisfying $|\widehat{f}(x)| \neq 0$ for all $x \in \mathcal{R}\setminus\{0\}$, then the matrix*

$$[f(x-y)]_{x,y \in \mathcal{R}\setminus\{0\}}$$

is nonsingular.

Proof. Since f is a generalized Cohn function satisfying either (5.1) or (5.2), by Proposition 5.1, $\sum_{x \in \mathcal{R}} f(x) = 0$, that is, $f \in V = \{f \in \mathbb{C}^{\mathcal{R}} | \sum_{x \in \mathcal{R}} f(x) = 0\}$. From (4.3), (3.10) and assumption $|\widehat{f}(x)| \neq 0$ for all $x \in \mathcal{R}\setminus\{0\}$, we have

$$\left|\det[f(x-y)]_{x,y \in \mathcal{R}\setminus\{0\}}\right| = q^{-n} \prod_{x \in \mathcal{R}\setminus\{0\}} \left|\widehat{f}(-x)\right| \neq 0.$$

Thus the matrix $[f(x-y)]_{x,y\in\mathcal{R}\setminus\{0\}}$ is nonsingular. $\square$

Question 1: Is there an example of generalized Cohn functions satisfying (5.2)?

Question 2: For $n = 1$, i.e., in the case of finite fields, the converse of the Proposition 5.2 holds. For $n \geq 2$, what are the conditions under which the converse of the Proposition 5.2 will be established?

References

[1] T. Cochrane, D. Garth and Z. Zheng, *On a Problem of H. Cohn for Character Sums*, Journal of Number Theory **81** (2000), 120–129.

[2] Y. H. Jang and S. P. Jun, *The Gauss sums over Galois ring and its absolute values*, Korean J. Math. **26** (3) (2018), 519–535.

[3] S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York, 1978.

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

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

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

[7] 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.

[8] A. Terras, *Fourier Analysis on Finite Groups and Application*, Cambridge University Press, 1999.

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

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