# Difference sets over Galois rings obtained from the subgroup of a variation ring of a local field

Mieko Yamada
School of Arts and Sciences
Tokyo Woman's Christian University

## 1 Introduction

A difference set with the parameters $v = 2^{2n}, k = 2^{n-1}(2^n - 1), \lambda = 2^{n-1}(2^{n-1} - 1)$ is well known and has been studied over several kinds of algebraic structures, which is called Menon-Hadamard difference sets (see e.g. [2], [3]). We showed there exists a family of Menon-Hadamard difference sets over Galois rings of characteristic of an ever power of 2 and of an odd extension degree ([9], [10]). Though this family produce no new orders, it has an interesting property, an embedded structure. That is, the difference set over the Galois ring of characteristic $2^n$ is embedded in the ideal part of a difference set over the Galois ring of characteristic $2^{n+2}$.
The projective limit of Galois rings is a variation ring of a local field(see e.g. [4], [5]). Then the projective limit of these Menon-Hadamard difference sets is a non-empty subset of a variation ring of a local field. Thus we have a question: does there exist a subset of a local field whose image by the natural projection always gives a difference set over a Galois ring? We give an example answer to this question. A family of Menon-Hadamard difference sets is obtained from a subgroup of a variation ring of a local field by the natural projections. Furthermore this family also has an embedded structure. The formal group and the $p$-adic logarithm function serve an important role.
We knew $p$-adic codes were considered by Calderbank and Sloane first [1]. They generalized cyclic codes from $GF(p)$ to $\boldsymbol{Z}_{p^a}, 0 \leq a \leq \infty$, and to the $p$-adic numbers. They showed the examples of $p$-adic codes, 2-adic Hamming codes of length 7, 2-adic Golay codes of length 24, 3-adic Golay codes of length 12. From these examples, they define quadratic residue codes of prime length $n = 8m - 1$, over $\boldsymbol{Z}_{2^\infty}$ and proved the self-dual code by appending the first column of a quadratic residue code has minimum Hamming distance $(n + 3)/2$ and is MDS code. On the other hand, Lagorce defined codes over $p$-adic fields similarly to convolution codes over finite fields directly not by generalizing the codes over finite algebraic structures [6]. The author considered the basic strongly non-catastrophic encoder, and showed it can be encoded and decoded. The author noticed the Hamming distance cannot be introduced from Hamming weight of 2-adic codes in Remark.
It is difficult to define combinatorial concepts over infinite algebraic structures extending them defined over finite algebraic structure. We think the first step is to find some relations between combinatorial concepts and some concepts over infinite algebraic structures.

## 2 Galois Rings

Let $\boldsymbol{Z}$ be a rational integer ring and denote $\boldsymbol{Z}/2^n\boldsymbol{Z}$ by $\mathcal{A}_n$. Let $\varphi(x) \in \mathcal{A}_n[x]$ be a primitive basic irreducible polynomial of degree $s$ and denote the root of $\varphi(x)$ by $\xi$. Then $\mathcal{A}_n[x]/\varphi(x)$ is a Galois extension of $\mathcal{A}_n$ and is called a Galois ring of characteristic $2^n$ and of an extension degree $s$, denoted by $GR(2^n, s)$. The extension ring of $\mathcal{A}_n$ obtained by adjoining $\xi$ is isomorphic to $\mathcal{A}_n[x]/\varphi(x)$. For easy reference, we put $\mathcal{R}_n = GR(2^n, s)$. $\mathcal{R}_n$ is a local ring and has a unique maximal ideal $\mathfrak{p}_n = 2\mathcal{R}_n$. Every ideal of $\mathcal{R}_n$ is $\mathfrak{p}_n^l = 2^l\mathcal{R}_n, 1 \leq l \leq n-1$. The residue class field $\mathcal{R}_n/\mathfrak{p}_n$ is isomorphic to a finite field $GF(2^s)$. We take the Teichmüller system $\mathcal{T}_n = \{0, 1, \xi, \cdots, \xi^{2^s-2}\}$ as a set of complete representatives of $\mathcal{R}_n/\mathfrak{p}_n$. More details, we refer the reader to [7].

Any element $\alpha$ of the unit group $\mathcal{R}_n^\times$ is uniquely represented as

$$\alpha = \xi^t e = \xi^t(1 + 2a),\ a \in \mathcal{R}_{n-1}.$$

The ring automorphism $\mathfrak{f} : \mathcal{R}_n \longrightarrow \mathcal{R}_n$ as

$$\alpha^{\mathfrak{f}} = \alpha_0^2 + 2\alpha_1^2 + \cdots + 2^{n-1}\alpha_{n-1}^2.$$

is called a Frobenius automorphism. We define the relative trace $T_n$ from $\mathcal{R}_n$ to $\mathcal{A}_n$ as

$$T_n(\alpha) = \alpha + \alpha^{\mathfrak{f}} + \cdots + \alpha^{\mathfrak{f}^{s-1}}.$$

We define the homomorphism $\tau_{n-l} : \mathcal{R}_n \to \mathcal{R}_{n-l}$ as

$$\tau_{n-l}(\sum_{i=0}^{s-1} \tilde{\gamma}_i \xi^i) = \sum_{i=0}^{s-1} \gamma_i \xi^i$$

where $\gamma_i \equiv \tilde{\gamma}_i \pmod{2^{n-l}}$, $\tilde{\gamma}_i \in \mathcal{A}_n$ and $\gamma_i \in \mathcal{A}_{n-l}$. The commutative relation

$$\tau_{n-l}T_n = T_{n-l}\tau_{n-l}$$

holds.

**Lemma 1.** ([10]) *The additive characters of $\mathcal{R}_n$ are given by*

$$\psi_\beta(\alpha) = \zeta_{2^n}^{T_n(\beta\alpha)}$$

*where $\beta \in \mathcal{R}_n$ and $\zeta_{2^n}$ is a primitive $2^n$th root of unity.*

In what follows, we denote a primitive $2^n$th root of unity by $\zeta_{2^n}$. We let $\psi_1(\mathcal{R}_n^\times) = \sum_{\alpha\in\mathcal{R}_n^\times} \psi_1(\alpha)$ and $\psi_1(\mathfrak{p}_n) = \sum_{\alpha\in\mathfrak{p}_n} \psi_1(\alpha)$.

**Lemma 2.** ([10])*For a nontrivial additive character $\psi_1$, we have*

$$\psi_1(\mathcal{R}_n^\times) = 0 \quad \textit{and} \quad \psi_1(\mathfrak{p}_n) = 0.$$

## 3 A Necessary and Sufficient Condition

We define the elements

$$\mathcal{D}_{n+1} = \sum_{\alpha \in D_{n+1}} \alpha \quad \text{and} \quad \mathcal{D}_{n+1}^{-1} = \sum_{\alpha \in D_{n+1}} (-\alpha)$$

of the group ring $\boldsymbol{Z}\mathcal{R}_{n+1}$. The subset $D_{n+1}$ of $\mathcal{R}_{n+1}$ is a difference set with parameters

$$v = 2^{(n+1)s},\ k = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1),\ \lambda = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}-1} - 1)$$

if and only if $(n+1)s$ is even and

$$\mathcal{D}_{n+1}\mathcal{D}_{n+1}^{-1} = (k-\lambda)0 + \lambda \sum_{\alpha \in \mathcal{R}_{n+1}} \alpha.$$

It suffices to show that for every additive character $\psi_\beta$ of $\mathcal{R}_{n+1}$

$$\psi_\beta(\mathcal{D}_{n+1}\mathcal{D}_{n+1}^{-1}) = \begin{cases} k-\lambda, & \text{if } \beta \neq 0, \\ k-\lambda+\lambda v = k^2, & \text{if } \beta = 0 \end{cases}$$

holds. If $\beta = 0$, then $\psi_0(\mathcal{D}_{n+1})$ has to be $|D_{n+1}| = k$. For $\beta \neq 0$, $\psi_\beta(\mathcal{D}_{n+1})$ is an element of the integer ring of the cyclotomic field $\boldsymbol{Q}(\zeta_{2^{n+1}})$. Since the principal ideal $(\psi_\beta(\mathcal{D}_{n+1}))$ is equivalent to the principal ideal $(\overline{\psi_\beta(\mathcal{D}_{n+1})})$ and the ideal (2) is completely ramified in the integer ring of $\boldsymbol{Q}(\zeta_{2^{n+1}})$, the ideal $(\psi_\beta(\mathcal{D}_{n+1}))$ is equivalent to the ideal $(2^{\frac{(n+1)s}{2}-1})$, or

$$\psi_\beta(\mathcal{D}_{n+1}) = 2^{\frac{(n+1)s}{2}-1}u$$

where $u$ is a unit of $\boldsymbol{Q}(\zeta_{2^{n+1}})$.

## 4 Local Fields

Let $p$ be a prime number and denote the $p$-adic absolute value by $|\ |_p$. Let $\boldsymbol{Q}_p$ be the completion of rational field $\boldsymbol{Q}$ under the $p$-adic absolute value and $\boldsymbol{Z}_p$ be a variation ring of $\boldsymbol{Q}_p$. Let $f_Q(x)$ be a monic irreducible polynomial of degree $s$ over $\boldsymbol{Z}_p$ which divides $x^{p^s-1} - 1$. Assume that $f_G(x) \equiv f_Q(x) \pmod{p^n}$ be a basic primitive polynomial over $GR(p^n, s)$ and $f_F(x) \equiv f_Q(x) \pmod{p}$ be a primitive polynomial over $GF(p^s)$.

We consider the extension $K = \boldsymbol{Q}_p(\bar{\xi})$ by adjoining $\bar{\xi}$, a root of $f_Q(x)$. The extension $K$ is complete with respect to the unique extended absolute value $|\ |$ of the $p$-adic absolute value $|\ |_p$. As the $p$-adic field $\boldsymbol{Q}_p$ is a local field, the algebraic extension $K$ is also a local field and the splitting field of $f_Q(x)$. Then we note that the prime element of $K$ is $p$.

The Galois group of $K/\boldsymbol{Q}_p$ is isomorphic to the Galois group of $GF(p^s)/GF(p)$. Let $\langle\phi\rangle$ be the Galois group of $K$. We define the relative trace of $\alpha$ from $K$ to $\boldsymbol{Q}_p$ as

$$T_{K/\boldsymbol{Q}_p} = \alpha + \phi(\alpha) + \cdots + \phi^{s-1}(\alpha).$$

# 5 A $p$-adic Logarithm Function

$\mathcal{O}_K = \{x \in K : |x| \leq 1\}$ is the variation ring of $K$ and $\mathfrak{p}_K = \{x \in K : |x| < 1\}$ is the maximal ideal of $\mathcal{O}_K$. We define a $p$-adic logarithm function over $K$.

**Definition 1.** *Let $B = 1 + p\mathcal{O}_K$. We define a $p$-adic logarithm function $\log_p : B \longrightarrow p\mathcal{O}_K$ as*

$$\log_p(1+x) = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{x^j}{j}$$

*for $x \in p\mathcal{O}_K$.*

The $p$-adic logarithm function satisfies the following equation(see Proposition 4.5.3. in [4]),

$$\log_p(1+x)(1+y) = \log_p(1+x) + \log_p(1+y).$$

In what follows, we assume $p = 2$. We have the following lemma.

**Lemma 3.** *Let $\mathcal{O}_K$ be a variation ring of $K = Q_2(\bar{\xi})$.*

1. *The 2-adic logarithm function $\log_2$ from $1 + 2\mathcal{O}_K$ to $2\mathcal{O}_K$ is a homomorphism and the kernel of $\log_2$ is $\{1, -1\}$.*
2. *We restrict $\log_2$ to $1 + 2^2\mathcal{O}_K$. Then $\log_2$ is an isomorphism from $1 + 2^2\mathcal{O}_K$ to $2^2\mathcal{O}_K$.*

# 6 Formal Groups

Let $R$ be a commutative ring with an identity. We denote the set of formal power series $\sum_{n=0}^{\infty} a_n X^n$ by $R[[X]]$ and $\sum_{n,m=0}^{\infty} a_{n,m} X^n Y^m$ by $R[[X,Y]]$.

**Definition 2.** *A formal group over $R$ is a formal power series $F(X,Y)$ satisfies the following properties*

1. $F(X,Y) \equiv X + Y \pmod{\deg 2}$.
2. $F(X,Y) = F(Y,X)$.
3. $F(X,F(Y,Z)) = F(F(X,Y),Z)$.

**Lemma 4.** *Assume $p = 2$. A power series $H(X,Y) = X + Y + 2XY \in \mathcal{O}_K[[X,Y]]$ is a formal group over $\mathcal{O}_K$.*

*Proof.* We easily check the conditions in Definition 2. □

We introduce a homomorphism between two formal groups.

**Definition 3.** *A homomorphism $h : F \longrightarrow G$ between two formal groups is a power series $h(X) \in R[[X]]$ with $h(0) = 0$ such that*

$$h(F(X,Y)) = G(h(X), h(Y)).$$

We consider $\log_2(1+2x) = \sum_{j=1}^{\infty}(-1)^{j+1}\frac{(2x)^j}{j}$ as a formal power series.

**Lemma 5.** *Assume $p = 2$. Denote the additive formal group by $G_a(X,Y) = X + Y$. A homomorphism $h$ from $H(X,Y)$ to $G_a(X,Y)$ is given by*

$$h(x) = \frac{1}{2}\log_2(1+2x).$$

*Proof.* From $h(x+y+2xy) = \frac{1}{2}\log_2(1+2(x+y+2xy)) = \frac{1}{2}\log_2(1+2x)(1+2y)$, we have

$$h(x+y+2xy) = \frac{1}{2}\log_2(1+2x) + \frac{1}{2}\log_2(1+2y) = h(x) + h(y).$$

□

## 7 A New Operation

We see that $H(\alpha,\beta)$ converges in $\mathcal{O}_K$ for $\alpha,\beta \in \mathcal{O}_K$. Then we define a new operation of $\mathcal{O}_K$ by the formal group $H(X,Y)$ as follows:

$$\alpha * \beta = H(\alpha,\beta).$$

The operation defines a new abelian group structure on $\mathcal{O}_K$. We denote it by $\mathcal{O}_K^*$.

Let $\mu_n : \mathcal{O}_K^* \longrightarrow GR(2^n,s)$be the natural projection. For $\overline{\alpha},\overline{\beta} \in \mathcal{O}_K^*$, we define a new operation $*$ by

$$\mu_n(\overline{\alpha}) * \mu_n(\overline{\beta}) = \mu_n(\overline{\alpha} * \overline{\beta}).$$

Then the Galois ring $GR(2^n,s)$ forms an abelian group with respect to this operation. The additive formal group by $G_a(X,Y)$ introduces the ordinary additions of $\mathcal{O}_K$ and $GR(2^n,s)$.

## 8 A Family of Menon-Hadamard Difference Sets

We fix an integer $m \geq 0$ and assume $n$ is odd. Let $\mathcal{T}$ be a set of a complete representatives of $\mathcal{O}_K/\mathfrak{p}_K$. We define an additive subgroup of the ideal $\mathfrak{p}_K^m = 2^m\mathcal{O}_K^+$ as follows:

$$X(m) = \{2^m u \mid T_{K/\mathcal{O}_2}(u) \equiv 0 \pmod 2\}.$$

We define a subset $X_m(j)$ of $\mathfrak{p}_K^j$ by using $X(m)$, that is

$$X_m(j) = \bigcup_{\alpha_1\in\mathcal{T}}\bigcup_{\alpha_2\in\mathcal{T}}\cdots\bigcup_{\alpha_{m-j}\in\mathcal{T}}(X(m) + 2^{m-1}\alpha_1 + 2^{m-2}\alpha_2\cdots + 2^j\alpha_{m-j})$$

for $0 \leq j \leq m-1$. Furthermore put

$$Y_m(j) = h^{-1}(X_m(j)) \subset 2^j\mathcal{O}_K^*.$$

Let $m = n-2l-1$ and put

$$V(n-2l-1) = \mu_n(Y_{n-2l-1}(l)) \subset \mathcal{R}_{n-l}^*.$$

We define the subset $D_{\mathfrak{p}_{n+1}^l}$ of $\mathfrak{p}_{n+1}^l$ as

$$D_{\mathfrak{p}_{n+1}^l} = 2^l \bigcup_{l=0}^{2^s-1} \bigcup_{\alpha \in V(n-2l-1)} \xi^l(1+2\alpha)$$

**Theorem 1.** *Assume that $n$ is an odd positive integer. The subset*

$$D = \bigcup_{l=0}^{(n-1)/2} D_{\mathfrak{p}_{n+1}^l}$$

*is a Menon-Hadamard difference set with the parameters $v = 2^{(n+1)s}$, $k = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1)$, $\lambda = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}-1} - 1)$. This family of difference sets has an embedded structure.*

## 9 Gauss Sums

Let $\tilde{\chi}$ be a character of the ordinary multiplicative group $\mathcal{R}_{n+1}^{\times}$ of $\mathcal{R}_{n+1}$. We assume the order of $\tilde{\chi}$ is a power of 2. Then $\tilde{\chi}(\xi) = 1$ and

$$\tilde{\chi}(\xi^t(1+2\alpha)\cdot\xi^u(1+2\beta)) = \tilde{\chi}((1+2\alpha)(1+2\beta)) = \tilde{\chi}(1+2(\alpha*\beta))$$

for $\xi^t(1+2\alpha), \xi^u(1+2\beta) \in \mathcal{R}_{n+1}^{\times}$. Hence a multiplicative character $\tilde{\chi}$ of $\mathcal{R}_{n+1}^{\times}$ can be regarded as a multiplicative character $\chi$ of the group $\mathcal{R}_n^*$. We extend $\tilde{\chi}$ as the character of $\mathcal{R}_{n+1}$ by defining $\tilde{\chi}(\alpha) = 0$ for any element $\alpha \in \mathfrak{p}_{n+1}$. Denote the trivial character by $\tilde{\chi}^0$. For a multiplicative character $\tilde{\chi}$ and an additive character $\psi_\beta$ of $\mathcal{R}_{n+1}$, we define the Gauss sum over $\mathcal{R}_{n+1}$ by

$$G(\tilde{\chi}, \psi_\beta) = \sum_{\alpha \in \mathcal{R}_{n+1}} \tilde{\chi}(\alpha)\psi_\beta(\alpha).$$

Gauss sums has the following relation.

**Lemma 6.** ([10]) *For $\beta = 2^h(1+2\beta_0)\xi^u \in \mathcal{R}_{n+1}$, we have*

$$G(\tilde{\chi}, \psi_\beta) = \tilde{\chi}^{-1}(\frac{\beta}{2^h})G(\tilde{\chi}, \psi_{2^h}).$$

## 10 The determination of Gauss Sums

We define a multiplicative character $\eta$ of $\mathcal{R}_{n-l}^*$ as follows

$$\eta(\alpha_0) = \begin{cases} 1 & \text{if } \alpha_0 \in V(n-2l-1), \\ -1 & \text{if } \alpha_0 \notin V(n-2l-1) \end{cases}$$

for $\alpha_0 \in \mathcal{R}_{n-l}^*$ and define the multiplicative character $\tilde{\eta}$ of $\mathcal{R}_{n+1-l}^{\times}$ as follows

$$\tilde{\eta}(\alpha) = \tilde{\eta}(\xi^t(1+2\alpha_0)) = \eta(\alpha_0).$$

We extend $\tilde{\eta}$ as the character of $\mathcal{R}_{n+1-l}$ by defining $\tilde{\eta}(\alpha) = 0$ for any element $\alpha \in \mathfrak{p}_{n+1}$.

The characteristic function of $D_l$ is

$$\frac{1}{2}\sum_{j=0}^{1}\tilde{\eta}^j(\alpha)=\begin{cases}1, & \alpha\in D_l,\\ 0, & \alpha\notin D_l.\end{cases}$$

For an additive character $\psi_\beta$,

$$\psi_\beta(\mathcal{D}_{\mathfrak{p}_{n+1}^l})=\frac{1}{2}\sum_{j=0}^{1}\sum_{\alpha\in\mathcal{R}_{n+1-l}}\tilde{\eta}^j(\alpha)\psi_\beta(\alpha)=\frac{1}{2}\sum_{j=0}^{1}G(\tilde{\eta}^j,\psi_\beta).$$

In order to prove Theorem 1, we must determine the values of $G(\tilde{\eta}^j,\psi_\beta)$.

**Theorem 2.** *Put $\mathcal{R}=\mathcal{R}_{n+1}$ and $\mathfrak{p}=\mathfrak{p}_{n+1}$. $G(\tilde{\eta},\psi_\beta),G(\tilde{\eta}^0,\psi_\beta)$ have the following values.*

| $\beta$ | $G(\tilde{\eta},\psi_\beta)$ | $G(\tilde{\eta}^0,\psi_\beta)$ |
|---|---|---|
| $\mathcal{R}^\times-\mathfrak{p}^l$ | 0 | 0 |
| $\mathfrak{p}^l-\mathfrak{p}^{l+1}$ | $2^{\frac{n+1}{2}s}u$ | 0 |
| $\mathfrak{p}^{l+1}-\mathfrak{p}^{n-l}$ | 0 | 0 |
| $\mathfrak{p}^{n-l}-\mathfrak{p}^{n-l+1}$ | 0 | $-2^{(n-l)s}u$ |
| $\mathfrak{p}^{n-l+1}$ | 0 | $2^{n-l}(2^s-1)$ |

*where $u$ is a unit of $\boldsymbol{Q}(\zeta_{2^{n+1-l}})$.*

*Proof.* Put $M=n+1-l$.
(1) Assume $\beta\in\mathcal{R}_{n+1}^\times-\mathfrak{p}_{n+1}^l$ and put $\beta=2^h\xi^t(1+2\beta_0)$, $0\le h\le l$. From Lemma 6, it suffices to determine the values of $G(\tilde{\eta}^j,\psi_{2^h})$.

$$\begin{aligned}N_G &= |G(\tilde{\eta}^m,\psi_{2^u})|^2=\sum_{\gamma\in\mathcal{R}_M^\times}\tilde{\eta}^j(\gamma)\psi_1(\gamma)\sum_{\delta\in\mathcal{R}_M^\times}\tilde{\eta}^{-j}(\delta)\psi_1(-\delta)\\ &= \sum_{\delta\in R_M^\times}\tilde{\eta}^{-j}(\delta)\psi_1(-\delta)\sum_{\theta\in\mathcal{R}_M^\times}\tilde{\eta}^j(\delta\theta)\psi_1(\delta\theta)\\ &= \sum_{\theta\in\mathcal{R}_M^\times}\tilde{\eta}^j(\theta)\sum_{\delta\in R_M^\times}\psi_1((\theta-1)\delta).\end{aligned}$$

We calculate the inner sum $\sum_{\delta\in R_M}\psi_1((\theta-1)\delta)$. Assume that $\theta-1\notin\mathfrak{p}_M^{M-1-h}$. We put $\theta=1+2^u\theta_0, 0\le u\le M-1-h$, $\theta_0\in\mathcal{R}_{M-1-u}^\times$. From the commutability between the trace function and the homomorphism, $\tau_{M-u-1}T_M=T_{M-u}\tau_{M-u}$ mentioned in Section 2.

$$\sum_{\delta\in\mathcal{R}_M^\times}\psi_1((\theta-1)\delta)=\sum_{\delta\in\mathcal{R}_M^\times}\zeta_{2^M}^{2^uT_M(\theta_0\delta)}=\sum_{\bar{\delta}\in R_{M-u}^\times}\zeta_{2^{M-u}}^{T_{M-u}(\bar{\theta}_0\bar{\delta})}$$

where $\bar{\delta}=\tau_{M-u}(\delta),\bar{\theta}_0=\tau_{M-u}(\theta_0)$. Thus we obtain

$$\sum_{\delta\in R_M^\times}\psi_1((\theta-1)\delta)=0.$$

Next let $2^h(\theta-1)\in \mathfrak{p}_M^{M-1}-\mathfrak{p}_M^M$, we have

$$\sum_{\delta\in R_M^\times}\psi_1((\theta-1)\delta)=\sum_{\delta\in R_M^\times}\zeta_{2^M}^{2^hT_M((\theta-1)\delta)}=\frac{|\mathcal{R}_M^\times|}{|GF(2^s)^\times|}\sum_{\bar\delta\in GF(2^s)^\times}(-1)^{tr(\theta_0\bar\delta)}=-2^{(n-l)s}$$

where $tr$ is the absolute trace from $GF(2^s)$ to $GF(2)$. If $2^h(\theta-1)\in\mathfrak{p}_M^M$, then

$$\sum_{\delta\in R_M^\times}\psi_1((\theta-1)\delta)=|\mathcal{R}_M^\times|=2^{(n-l)s}(2^s-1).$$

Hence

$$\begin{aligned}\sum_{\delta\in\mathcal{R}_M^\times}\psi_1((\theta-1)\delta) &= \sum_{\delta\in\mathcal{R}_M^\times}\zeta_{2^M}^{2^hT_M((\theta-1)\delta)}\\ &= \begin{cases}0 & \text{if}\quad \theta-1\notin\mathfrak{p}_M^{M-h-1},\\ -2^{(n-l)s} & \text{if}\quad \theta-1\in\mathfrak{p}_M^{M-h-1}-\mathfrak{p}_M^{M-h},\\ 2^{(n-l)s}(2^s-1) & \text{if}\quad \theta-1\in\mathfrak{p}_M^{M-h}.\end{cases}\end{aligned}$$

Assume that $\theta-1=2^{M-h-1}\theta_0\in\mathfrak{p}_M^{M-h-1}-\mathfrak{p}_M^{M-h}$ with $\theta_0\in\mathfrak{p}_{h+1}^\times$. There exists an element $2^{M-h-2}\tilde\theta_0=2^{n-l-h-1}\tilde\theta_0\in 2^{n-l-h-1}\mathcal{O}_K^\times\subset 2^{n-2l-1}\mathcal{O}_K^\times$ such that $\mu_M(2^{n-l-h-1}\tilde\theta_0)=2^{n-l-h-1}\theta_0$. From $2^{n-l-h-1}\tilde\theta_0=2^{n-2l-1}(2^{l-h}\tilde\theta_0)$, $T_{K/\boldsymbol{Q}_2}(2^{l-h}\tilde\theta_0)\equiv 0\pmod 2$. Thus $2^{n-l-h-1}\tilde\theta_0\in W(n-2l-1)$, that is $2^{n-l-h-1}\theta_0\in V(n-2l-1)$.
Hence

$$\sum_{\theta-1\in\mathfrak{p}_M^{M-h-1}-\mathfrak{p}_M^{M-h}}\tilde\eta^j(\theta)=\sum_{\theta_0\in\mathcal{R}_{h+1}^\times}\eta^j(2^{n-l-h-1}\theta_0)=2^{hs}(2^s-1).$$

If $\theta-1\in 2^{M-h}\theta_0$ with $\theta_0\in\mathfrak{p}_h$, then from $T_{K/\boldsymbol{Q}_2}(2^{l-h-1}\tilde\theta_0)\equiv 0\pmod 2$,

$$\sum_{\theta-1\in\mathfrak{p}_M^{M-h}}\tilde\eta^j(\theta)=\sum_{\theta_0\in\mathcal{R}_h^\times}\eta^j(2^{n-l-h}\theta_0)=2^{hs}.$$

Thus we obtain

$$N_G=-2^{(n-l)s}2^{hs}(2^s-1)+2^{(n-l)s}(2^s-1)2^{hs}=0,$$

then it follows $G(\tilde\eta^j,\psi_{2^n})=0$ for $j=0,1$.
(2) Assume that $\beta=2^l\xi^t(1+2\beta_0)\in\mathfrak{p}_M^l-\mathfrak{p}_M^{l+1}$. It suffices to determine the value of $G(\tilde\eta_j,\psi_{2^l})$. Similarly to the case (1), we have

$$\sum_{\delta\in\mathcal{R}_M^\times}\zeta_{2^M}^{2^lT_M((\theta-1)\delta)} = \begin{cases}0 & \text{if}\quad \theta-1\notin\mathfrak{p}_M^{M-l-1},\\ -2^{(n-l)s} & \text{if}\quad \theta-1\in\mathfrak{p}_M^{M-l-1}-\mathfrak{p}_M^{M-l},\\ 2^{(n-l)s}(2^s-1) & \text{if}\quad \theta-1\in\mathfrak{p}_M^{M-l}.\end{cases}$$

If $\theta-1=2^{M-l-1}\theta_0\in\mathfrak{p}_M^{M-l-1}-\mathfrak{p}_M^{M-l}$, then

$$\sum_{\theta-1\in\mathfrak{p}_M^{M-l-1}-\mathfrak{p}_M^{M-l}}\tilde\eta^j(\theta)=\sum_{\theta_0\in\mathcal{R}_{l+1}^\times}\eta^j(2^{n-2l-1}\theta_0)=\sum_{\theta_0\in\mathcal{R}_{l+1}}\eta^j(2^{n-2l-1}\theta_0)-\sum_{\theta_0\in\mathfrak{p}_{l+1}}\eta^j(2^{n-2l-1}\theta_0).$$

Let $2^{n-2l-1}\tilde{\theta}_0 \in 2^{n-2l-1}\mathcal{O}_K$ such that $\mu_M(2^{n-2l-1}\tilde{\theta}_0) = 2^{n-2l-1}\theta_0$. If $\tilde{\theta}_0 \in \mathfrak{p}_K$, then $2^{n-2l-1}\tilde{\theta}_0 \in X(n-2l-1)$ and $2^{n-2l-1}\theta_0 \in V(n-2l-1)$. Thus

$$\sum_{\theta_0 \in \mathfrak{p}_{l+1}} \eta^j(2^{n-2l-1}\theta_0) = 2^{ls}.$$

If $\tilde{\theta}_0$ runs through $\mathcal{O}_K$, then $\theta_0 = \mu_M(\tilde{\theta}_0)$ runs through $\mathcal{R}_{l+1}$. Therefore

$$\sum_{\theta_0 \in \mathcal{R}_{l+1}} \eta^j(2^{n-2l-1}\theta_0) = \begin{cases} 2^{(l+1)s}, & \text{if } j = 0, \\ 0, & \text{if } j = 1, \end{cases}$$

Thus we have

$$\sum_{\theta-1 \in \mathfrak{p}_M^{M-l-1} - \mathfrak{p}_M^{M-l}} \tilde{\eta}^j(\theta) = \begin{cases} -2^{ls}, & \text{if } j = 0, \\ 2^{ls}(2^s - 1). & \text{if } j = 1. \end{cases}$$

Next we assume $\theta - 1 = 2^{M-l}\theta_0 \in \mathfrak{p}_M^{M-l}$. Similarly to the above,

$$\sum_{\theta-1 \in \mathfrak{p}_M^{M-l}} \tilde{\eta}^j(\theta) = 2^{ls}.$$

Consequently,

$$N_G = \begin{cases} -2^{(n-l)s} \cdot 2^{ls}(2^s - 1) + 2^{(n-l)s}(2^s - 1)2^{ls} = 0 & \text{if } j = 0, \\ -2^{(n-l)s}(-2^{ls}) + 2^{(n-l)s}(2^s - 1)2^{ls} = 2^{(n+1)s} & \text{if } j = 1. \end{cases}$$

Hence

$$G(\tilde{\eta}^0, \psi_{2^s}) = 0, \quad G(\tilde{\eta}, \psi_{2^s}) = 2^{\frac{n+1}{2}s}u$$

where $u$ is a unit of $\boldsymbol{Q}(\zeta_M)$. It follows $G(\tilde{\eta}, \psi_\beta) = 2^{\frac{n+1}{2}s}u'$ where $u'$ is a unit of $\boldsymbol{Q}(\zeta_M)$.

(3) Assume $\beta \in \mathfrak{p}_{n+1}^h$, $l+1 \le h < n-l$. Similarly to the case (2),

$$\sum_{\delta \in \mathfrak{p}_M^\times} \zeta_M^{2^h T_M((\theta-1)\delta)} = \begin{cases} 0 & \text{if } \theta - 1 \notin \mathfrak{p}_M^{M-h-1}, \\ -2^{(n-l)s} & \text{if } \theta - 1 \in \mathfrak{p}_M^{M-h-1} - \mathfrak{p}_M^{M-h}, \\ 2^{(n-l)s}(2^s - 1) & \text{if } \theta - 1 \in \mathfrak{p}_M^{M-h}. \end{cases}$$

Let $\theta - 1 \in \mathfrak{p}_M^{M-h-1} - \mathfrak{p}_M^{M-h}$.

$$\begin{aligned} \sum_{\theta-1 \in \mathfrak{p}_M^{M-h-1} - \mathfrak{p}_M^{M-h}} \tilde{\eta}^j(\theta) &= \sum_{\theta_0 \in \mathcal{R}_{h+1}^\times} \eta^j(2^{n-l-h-1}\theta_0) \\ &= \sum_{\theta_0 \in \mathcal{R}_{h+1}} \eta^j(2^{n-l-h-1}\theta_0) - \sum_{\theta_0 \in \mathfrak{p}_{h+1}} \eta^j(2^{n-l-h-1}\theta_0). \end{aligned}$$

Notice that $2^{n-l-h-1}\mathcal{O}_K \supset 2^{n-2l-1}\mathcal{O}_K$. If the element $\tilde{\theta}_0$ such that $\mu_M(\tilde{\theta}_0) = \theta_0$ runs through $\mathcal{O}_K$, then $\theta_0$ runs through $\mathcal{R}_{h+1}$. Therefore

$$\sum_{\theta_0 \in \mathcal{R}_{h+1}} \eta(2^{n-l-h-1}\theta_0) = 0$$

and also

$$\sum_{\theta_0 \in \mathfrak{p}_{h+1}} \eta(2^{n-l-h-1}\theta_0) = 0.$$

Then

$$\sum_{\theta-1 \in \mathfrak{p}_M^{M-h-1} - \mathfrak{p}_M^{M-h}} \tilde{\eta}(\theta) = 0, \quad \text{and} \quad \sum_{\theta-1 \in \mathfrak{p}_M^{M-h-1} - \mathfrak{p}_M^{M-h}} \tilde{\eta}^0(\theta) = 2^{hs}(2^s - 1).$$

If $\theta - 1 \in \mathfrak{p}_M^{M-h}$, then

$$\sum_{\theta-1 \in \mathfrak{p}_M^{M-h}} \tilde{\eta}^j(\theta) = \begin{cases} 2^{ls} & \text{if } j = 0, \\ 0 & \text{if } j = 1. \end{cases}$$

It follows $N_G = 0$, that is, $G(\tilde{\eta}^j, \psi_{2^n}) = G(\tilde{\eta}^j, \psi_\beta) = 0$. We assume $h = n - l$ and put $\beta = 2^{n-l}\xi^t(1 + 2\beta_0)$.

$$\begin{aligned} G(\tilde{\eta}^j, \psi_\beta) &= \sum_{\gamma \in \mathcal{R}_M^\times} \tilde{\eta}^j(\gamma)\zeta_{2^M}^{2^{n-l}T_M(\xi^t(1+2\beta_0)\gamma)} \\ &= \sum_{\gamma_0 \in \mathcal{R}_{M-1}} \eta(\gamma_0) \sum_{u=0}^{2^s-1} (-1)^{Tr(\xi^u(1+2\beta_0)(1+2\gamma_0))} \\ &= \begin{cases} 2^{n-l}(2^s - 1) & \text{if } j = 0, \\ 0 & \text{if } j = 1. \end{cases} \end{aligned}$$

If $h \geq M$, then

$$G(\tilde{\eta}^j, \psi_\beta) = \sum_{\gamma \in \mathcal{R}_M^\times} \tilde{\eta}^j(\gamma) = \begin{cases} 2^{n-l}(2^s - 1) & \text{if } j = 0, \\ 0 & \text{if } j = 1. \end{cases}$$

It completes the proof of the theorem. □

## 11 The Proof of the Main Theorem

As mentioned in Section 3, we verify $\psi_\beta(\mathcal{D}) = 2^{\frac{(n+1)s}{2}-1}u$ if $\beta \neq 0$ and $\psi_0(\mathcal{D}) = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1)$ if $\beta = 0$, where $u$ is a unit of $\boldsymbol{Q}(\zeta_{2^{n+1}})$. Since $X(m)$ is a subgroup of $2^m\mathcal{O}_K^+$ with index 2, $Y(j), 0 \leq j \leq m-1$ is a subgroup of $2^j\mathcal{O}_K^*$ with index 2. It leads $|V(n-2l-1)| = 2^{(n-l)s-1}$. Thus

$$\psi_0(\mathcal{D}) = \sum_{l=0}^{\frac{n-1}{2}} 2^{(n-l)s-1}(2^s - 1) = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1).$$

We denote the corresponding elements of $D_{\mathcal{R}_{n+1}^\times}$ and $D_{\mathfrak{p}_{n+1}^l}$ by $\mathcal{D}_{\mathcal{R}_{n+1}^\times}$ and $\mathcal{D}_{\mathfrak{p}_{n+1}^l}$. We display the values $\psi_\beta(\mathcal{D}_{\mathcal{R}_{n+1}^\times})$, $\psi_\beta(\mathcal{D}_{\mathfrak{p}_{n+1}^l})$ $1 \leq l \leq \frac{n-1}{2}$ from Theorem 2, which is a similar table as in the paper [10]. For convenience, we put $\mathcal{R}^\times = \mathcal{R}_{n-1}^\times$ and $\mathfrak{p}^l = \mathfrak{p}_{n+1}^l$. Notice that resultant difference sets and the constructions are different from them in the paper [10].

| $\beta$ | $\psi_\beta(\mathcal{D}_{R^\times})$ | $\psi_\beta(\mathcal{D}_{\mathfrak{p}})$ | $\psi_\beta(\mathcal{D}_{\mathfrak{p}^l})$ | $\psi_\beta(\mathcal{D}_{\mathfrak{p}^{\frac{n-3}{2}}})$ | $\psi_\beta(\mathcal{D}_{\mathfrak{p}^{\frac{n-1}{2}}})$ |
|---|---|---|---|---|---|
| $R^\times$ | $\pm 2^{\frac{n+1}{2}s-1}$ | $0$ | $0$ | $0$ | $0$ |
| $\mathfrak{p}-\mathfrak{p}^2$ | $0$ | $\pm 2^{\frac{n+1}{2}s-1}$ | $0$ | $0$ | $0$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $\mathfrak{p}^l-\mathfrak{p}^{l+1}$ | $0$ | $0$ | $\pm 2^{\frac{n+1}{2}s-1}$ | $0$ | $0$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $\mathfrak{p}^{\frac{n-3}{2}}-\mathfrak{p}^{\frac{n-1}{2}}$ | $0$ | $0$ | $0$ | $\pm 2^{\frac{n+1}{2}s-1}$ | $0$ |
| $\mathfrak{p}^{\frac{n-1}{2}}-\mathfrak{p}^{\frac{n+1}{2}}$ | $0$ | $0$ | $0$ | $0$ | $2^{\frac{n+1}{2}s-1}u$ |
| $\mathfrak{p}^{\frac{n+1}{2}}-\mathfrak{p}^{\frac{n+3}{2}}$ | $0$ | $0$ | $0$ | $0$ | $-2^{\frac{n+1}{2}s-1}$ |
| $\mathfrak{p}^{\frac{n+3}{2}}-\mathfrak{p}^{\frac{n+5}{2}}$ | $0$ | $0$ | $0$ | $-2^{\frac{n+3}{2}s-1}$ | $2^{\frac{n+1}{2}s-1}(2^s-1)$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $\mathfrak{p}^{n-l}-\mathfrak{p}^{n-l+1}$ | $0$ | $0$ | $-2^{(n-l)s-1}$ | $2^{\frac{n+3}{2}s-1}(2^s-1)$ | $2^{\frac{n+1}{2}s-1}(2^s-1)$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $\mathfrak{p}^{n-1}-\mathfrak{p}^n$ | $0$ | $-2^{(n-1)s-1}$ | $2^{(n-l)s-1}(2^s-1)$ | $2^{\frac{n+3}{2}s-1}(2^s-1)$ | $2^{\frac{n-1}{2}s-1}(2^s-1)$ |
| $\mathfrak{p}^n-\{0\}$ | $-2^{ns-1}$ | $2^{(n-1)s-1}(2^s-1)$ | $2^{(n-l)s-1}(2^s-1)$ | $2^{\frac{n+3}{2}s-1}(2^s-1)$ | $2^{\frac{n-1}{2}s-1}(2^s-1)$ |

It is easily verified that $\psi_\beta(\mathcal{D}) = 2^{\frac{n+1}{2}s-1}u$ for $0 \le l \le \frac{n-1}{2}$ where $u$ is a unit of a cyclotomic field $Q(\zeta_{2^{n+1}})$ from the above table. The construction shows a family of these Menon-Hadamard difference sets has an embedded structure.

## References


[1] A.R. Calderbank, N.J.A. Sloane, Modular and $p$-adic Cyclic Codes, Des. Codes and Cryptogr. 6, 21–35 (1995)

[2] D. Jungnickel, A. Pott and K.W. Smith, Difference sets, in: C. J. Colbourn and J. H. Dinitz (eds), Handbook of Combinatorial Designs, Chapman & Hall/CRC, New York, 419-435 (2007)

[3] D. Jungnickel, Difference sets, in: J. H. Dinitz and D. R. Stinson (eds), Contemporary Design Theory, Wiley, New York, 241–324 (1992)

[4] F.Q. Gouvêa, $p$-adic Numbers: An Introduction, Springer, Berlin Heidelberg (1997)

[5] N.Koblitz, $p$-adic Analysis: a Short Course on Recent Work, Cambridge Univ. Press, New York (1980)

[6] N. Lagorce, A Convolutional-like Approach to $p$-adic Codes, Discrete Applied Math. 1114, 139–155 (2001)

[7] B.R.McDonald, Finite Rings with Identity, Marcel Dekker, New York (1974)

[8] J.Neukirch, Class Field Theory, Springer-Verlag, Berlin Heidelberg (1986)

[9] M. Yamada, Difference sets over the Galois ring $GR(2^n, 2)$, Europ. J. Combinatorics 23, 239–252 (2002)

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