Disjoint difference families from Galois rings

Koji Momihara*
Faculty of Education
Kumamoto University
2-40-1 Kurokami, Kumamoto 860-8555, Japan
momihara@educ.kumamoto-u.ac.jp

Submitted: Mar 11, 2016; Accepted: Jul 21, 2017; Published: Aug 11, 2017
Mathematics Subject Classifications: 05B05, 05B10

Abstract

In this paper, we give new constructions of disjoint difference families from Galois rings. The constructions are based on choosing cosets of the unit group of a subring in the Galois ring $\mathrm{GR}(p^2, p^{2s})$. Two infinite families of disjoint difference families are obtained from the Galois rings $\mathrm{GR}(p^2, p^{4n})$ and $\mathrm{GR}(2^2, 2^{2s})$.

Keywords: disjoint difference family; difference set; Galois ring

1 Introduction

Let G be an additively written abelian group of order v, and let D_i, $i = 1, 2, \ldots, b$, be disjoint k-subsets of G. We call $\{D_i : i = 1, 2, \ldots, b\}$ a *disjoint difference family in G with parameters* (v, k, λ, b) if the multiset

$$\{x - y : x, y \in D_i, x \neq y, i = 1, 2, \ldots, b\}$$

covers every nonzero element of G exactly λ times. If $b = 1$, it is called a (v, k, λ) *difference set in G*. If D_i's form a partition of G (or $G \setminus \{0\}$), it is called *partition type* (or *nearly-partition type*, respectively) following the terminologies of [13]. It is clear that a disjoint difference family with $bk = v$ is of partition type. Furthermore, a disjoint difference family with $bk = v - 1$ can be transformed to be of nearly-partition type by taking a translation.

For $X, Y \subseteq G$ and $a \in G$, define multisets $X + Y := \{x + y : x \in X, y \in Y\}$ and $X + a := \{x + a : x \in X\}$. Given disjoint subsets D_i's of G form a disjoint difference family if and only if $\sum_{i=1}^{b} |D_i \cap (D_i + a)| = \lambda$ for every nonzero element a of G.

Disjoint difference families have rich applications to coding theory, communications and information security. For these connections, we refer the reader to [13] and references

*Supported by JSPS under Grant-in-Aid for Young Scientists (B) 25800093.

therein. Disjoint difference families are closely related to other combinatorial objects such as external difference families (or perfect difference systems of sets) and zero-difference balanced functions [3, 4, 12]. A zero-difference balanced function is equivalent to a partition type disjoint difference family. A disjoint difference family such that the union of D_i's forms a difference set in G is an external difference family. In this sense, a lot of constructions of disjoint difference families have been known [2, 3, 4, 5, 6, 7, 8, 9, 12, 16, 17, 18]. Most of the constructions are based on finite fields, in particular, cyclotomic cosets and trace functions of finite fields.

In this paper, we are inspired by the following well-known construction of disjoint difference families. Let $\mathbb{F}_q$ be the finite field of order q and C be a multiplicative subgroup of index e. Then, the family of all cosets of C in the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ forms a disjoint difference family in $(\mathbb{F}_q, +)$. The proof is as follows. We compute $\sum_{i=0}^{e-1} |\gamma^i C \cap (\gamma^i C + a)|$ for each $a \in \mathbb{F}_q^*$, where γ is a primitive element of $\mathbb{F}_q$. Since the equation $\gamma^i x = \gamma^i y + a$ is reformulated as $xy^{-1} = a\gamma^{-i}y^{-1} + 1$, where $x, y \in C$, we have

$$\sum_{i=0}^{e-1} |\gamma^i C \cap (\gamma^i C + a)| = \sum_{i=0}^{e-1} |C \cap (a\gamma^{-i} C + 1)| = |C \cap (\mathbb{F}_q^* + 1)|,$$

which is constant not depending on a. Hence, $\{\gamma^i C : i = 0, 1, \ldots, e-1\}$ forms a disjoint difference family in $(\mathbb{F}_q, +)$.

In this paper, we consider an analogy of this construction. More precisely, we consider cosets of the unit group of a subring of the Galois ring $\mathrm{GR}(p^2, p^{2s})$. Then, we choose carefully some of the cosets and take the union together with the maximal ideal of the subring removing the zero. Then, we have a family of subsets of the Galois ring by multiplying the union by some elements in the Teichmüller set. Our new construction yields disjoint difference families of nearly-partition type. In particular, we obtain two infinite families of disjoint difference families in the additive groups of the Galois rings $\mathrm{GR}(p^2, p^{4n})$ and $\mathrm{GR}(2^2, 2^{2s})$ with parameters $(v, k, \lambda, b) = (p^{4n}, (p^{2n}+1)(p^n-1), p^{3n} - p^{2n} + p^n - 2, p^n + 1)$ and $(2^{2s}, 2^s + 1, 2^s, 2^s - 1)$, respectively. In addition, we find one example of a disjoint difference family with parameters $(v, k, \lambda, b) = (729, 56, 55, 13)$ from $\mathrm{GR}(3^2, 3^6)$.

Note that disjoint difference families with the same parameters above can be constructed by using the cosets of the multiplicative subgroups of order $(p^{2n}+1)(p^n-1)$ and $2^s + 1$ of the finite field of order p^{4n} and 2^{2s}, respectively, as described above while the groups are distinct; the difference families obtained by the construction using finite fields are in the groups $\mathbb{Z}_p^{4n}$ and $\mathbb{Z}_2^{2s}$, and our new difference families are in the groups $\mathbb{Z}_{p^2}^{2n}$ and $\mathbb{Z}_{2^2}^{s}$. Furthermore, as far as the author knows, there has been no construction of disjoint difference families with the parameters above in Galois rings. This will be explained in the last section.

2 Preliminaries

In this section, we introduce notations about Galois rings used throughout this paper. See [15] for general background of Galois rings.

Let p be a prime and let $g(x) \in \mathbb{Z}_{p^2}[x]$ be a primitive basic irreducible polynomial of degree s and denote a root of order $p^s - 1$ of $g(x)$ by ξ. Then $\mathbb{Z}_{p^2}[x]/\langle g(x)\rangle$ is called a *Galois ring* of characteristic p^2 and of an extension degree s, and denoted by $\mathrm{GR}(p^2, p^{2s})$. The algebraic extension of $\mathbb{Z}_{p^2}$ obtained by adjoining ξ is isomorphic to $\mathbb{Z}_{p^2}[x]/\langle g(x)\rangle$. $\mathrm{GR}(p^2, p^{2s})$ has a unique maximal ideal $\mathcal{I}_{p^s} = p\mathrm{GR}(p^2, p^{2s})$ and the residue ring $\mathrm{GR}(p^2, p^{2s})/\mathcal{I}_{p^s}$ is isomorphic to $\mathbb{F}_{p^s}$. We take $\mathcal{T}_{p^s} = \{0, 1, \xi, \ldots, \xi^{p^s-2}\}$ as a set of representatives of $\mathrm{GR}(p^2, p^{2s})/\mathcal{I}_{p^s}$, called the *Teichmüller set*. An arbitrary element $\alpha \in \mathrm{GR}(p^2, p^{2s})$ is uniquely represented as $\alpha = \alpha_0 + p\alpha_1$, $\alpha_0, \alpha_1 \in \mathcal{T}_{p^s}$. We denote the set of all units in $\mathrm{GR}(p^2, p^{2s})$ by $\mathrm{GR}(p^2, p^{2s})^*$ and also denote $\mathcal{I}^*_{p^s} := \mathcal{I}_{p^s} \setminus \{0\}$.

We define the map $\tau : \mathrm{GR}(p^2, p^{2s})^* \to \mathcal{T}^*_{p^s} (:= \mathcal{T}_{p^s} \setminus \{0\})$ as $\tau(\alpha) = \alpha^{p^s}$. The kernel of τ is the group $\mathbb{P}_{p^s}$ of principal units, which are elements of the form $1 + p\beta, \beta \in \mathcal{T}_{p^s}$, i.e., $\mathbb{P}_{p^s} = 1 + \mathcal{I}_{p^s} = 1 + p\mathcal{T}_{p^s}$. By noting that $(1 + p\alpha)(1 + p\beta) = 1 + p(\alpha + \beta) \in \mathbb{P}_{p^s}$ for any $\alpha, \beta \in \mathcal{T}_{p^s}$, $\mathbb{P}_{p^s}$ is isomorphic to the additive group of $\mathbb{F}_{p^s}$ by the isomorphism $1 + pa \in \mathbb{P}_{p^s} \longmapsto a + p\mathcal{T}_{p^s} \in \mathrm{GR}(p^2, p^{2s})/\mathcal{I}_{p^s}$. It is clear that $\mathrm{GR}(p^2, p^{2s})^*$ is the direct product of $\mathbb{P}_{p^s}$ and the cyclic group $\mathcal{T}^*_{p^s}$ of order $p^s - 1$. In other words, every element of $\mathrm{GR}(p^2, p^{2s})^*$ is uniquely represented as $\alpha_0(1 + p\alpha_1)$, $\alpha_0, \alpha_1 \in \mathcal{T}_{p^s}, \alpha_0 \neq 0$.

In Section 3, we treat the case where s is even, say, $s = 2n$. In Section 4, we treat the case where $p = 2$ and s an arbitrary positive integer.

3 Disjoint difference families from $\mathrm{GR}(p^2, p^{4n})$

In this section, we follow the notations of Section 2. In particular, we set $s = 2n$ and consider the unique subring $\mathrm{GR}(p^2, p^{2n})$ of $\mathrm{GR}(p^2, p^{4n})$.

Recall that

$$\mathcal{T}_{p^{2n}} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^{2n}-2}\},$$

which is a system of representatives for $\mathrm{GR}(p^2, p^{4n})/\mathcal{I}_{p^{2n}}$. Hence,

$$\mathrm{GR}(p^2, p^{4n}) = \{s + t \,:\, s \in \mathcal{T}_{p^{2n}}, t \in \mathcal{I}_{p^{2n}}\}.$$

On the other hand, any element of $\mathrm{GR}(p^2, p^{4n})$ can be uniquely expressed as

$$a_0 + a_1\xi, \;\; a_0, a_1 \in \mathrm{GR}(p^2, p^{2n}),$$

i.e., $\mathrm{GR}(p^2, p^{4n})$ is an extension ring of $\mathrm{GR}(p^2, p^{2n})$ obtained by adjoining ξ. Define a subset of $\mathcal{T}_{p^{2n}}$:

$$\mathcal{T}_{p^n} = \{0, 1, \xi^{p^n+1}, \xi^{2(p^n+1)}, \ldots, \xi^{(p^n-2)(p^n+1)}\},$$

which is the Teichmüller set of the subring $\mathrm{GR}(p^2, p^{2n})$ [15, Corollary 14.28]. Hence,

$$R_{p^n} = \{a(1 + pb) \,:\, a \in \mathcal{T}^*_{p^n}, \; b \in \mathcal{T}_{p^n}\}$$

is the unit group $\mathrm{GR}(p^2,p^{2n})^*$ of $\mathrm{GR}(p^2,p^{2n})$, and $p\mathcal{T}_{p^n}$ is the maximal ideal $\mathcal{I}_{p^n}$ of $\mathrm{GR}(p^2,p^{2n})$.

Note that the additive group of $\mathcal{I}_{p^{2n}}$ is isomorphic to $(\mathbb{F}_{p^{2n}},+)$. Let pS be a system of representatives for $\mathcal{I}_{p^{2n}}/\mathcal{I}_{p^n}(\simeq \mathbb{F}_{p^{2n}}/\mathbb{F}_{p^n})$. Since $\mathcal{I}_{p^{2n}}=p\mathcal{T}_{p^{2n}}$ and $\mathcal{I}_{p^n}=p\mathcal{T}_{p^n}$, each element of pS can be written as px for $x\in\mathcal{T}_{p^{2n}}$, i.e., $pS=\{px : x\in S\}$ for some subset S of $\mathcal{T}_{p^{2n}}$. Write $S=\{x_i : i=0,1,\ldots,p^n-1\}\subseteq\mathcal{T}_{p^{2n}}$. Define

$$P=\{p\xi^{j(p^n+1)+p^n} : j=0,1,\ldots,p^n-2\}.$$

Then, $P=\xi^{p^n}\mathcal{I}^*_{p^n}=p\xi^{p^n}\mathcal{T}^*_{p^n}$, that is, a coset of $\mathcal{I}^*_{p^n}$ in $\mathcal{I}^*_{p^{2n}}$.

Theorem 1. *Let*

$$D_i=\xi^i\left(P\cup\left(\bigcup_{j=0}^{p^n-1}\xi^j(1+px_j)R_{p^n}\right)\right),\ 0\leqslant i\leqslant p^n. \tag{1}$$

Then, $\{D_0,D_1,\ldots,D_{p^n}\}$ forms a disjoint difference family in $(\mathrm{GR}(p^2,p^{4n}),+)$ with parameters $(v,k,\lambda,b)=(p^{4n},(p^{2n}+1)(p^n-1),p^{3n}-p^{2n}+p^n-2,p^n+1)$.

It is clear that $\bigcup_{i=0}^{p^n}\xi^iP=\bigcup_{i=0}^{p^n}\xi^i\mathcal{I}^*_{p^n}=\mathcal{I}^*_{p^{2n}}$. Furthermore,

$$\begin{aligned}\bigcup_{i=0}^{p^n}\bigcup_{j=0}^{p^n-1}\xi^{i+j}(1+px_j)R_{p^n}=&\left(\bigcup_{i=0}^{p^n}\xi^i\mathcal{T}^*_{p^n}\right)\left(\bigcup_{j=0}^{p^n-1}(1+px_j)(1+p\mathcal{T}_{p^n})\right)\\ =&\mathcal{T}^*_{p^{2n}}(1+p(S+\mathcal{T}_{p^n}))=\mathrm{GR}(p^2,p^{4n})^*.\end{aligned}$$

Hence, D_i, $i=0,1,\ldots,p^n$, partition $\mathrm{GR}(p^2,p^{4n})\setminus\{0\}$.

Example 2. Consider the case where $p=3$ and $n=1$. The polynomial $x^2+4x+8\in\mathbb{Z}_9[x]$ is a monic basic irreducible polynomial having a root ξ of order $3^2-1=8$. Then,

$$\mathcal{T}_9=\{0,1,\xi,\xi^2,\xi^3,\xi^4,\xi^5,\xi^6,\xi^7\}.$$

Let

$$S=\{0,\xi,\xi^2\}.$$

Then, $1+pS$ forms a system of representatives for $\mathbb{P}_{3^2}/\mathbb{P}_3$. Define

$$R_3:=\{1,2,4,5,7,8\}(=\mathbb{Z}_9^*)$$

and

$$P=\{3\xi^3,3\xi^7\}.$$

Then, the sets

$$D_i=\xi^i(R_3\cup\xi(1+3\xi)R_3\cup\xi^2(1+3\xi^2)R_3\cup P),\ 0\leqslant i\leqslant 3,$$

form a disjoint difference family in $(\mathrm{GR}(3^2,3^4),+)\simeq\mathbb{Z}_9^2$ with parameters $(v,k,\lambda,b)=(81,20,19,4)$.

3.1 Proof of Theorem 1

It is clear that $|D_i| = p^{2n}(p^n-1)+(p^n-1) = (p^{2n}+1)(p^n-1)$. We expect that $\lambda = p^{3n}-p^{2n}+p^n-2$. So, we show that for any nonzero $a \in \mathrm{GR}(p^2, p^{4n})$

$$\sum_{i=0}^{p^n} |D_i \cap (D_i + a)| = \lambda = p^{3n} - p^{2n} + p^n - 2 \tag{2}$$

by a series of lemmas below.

Lemma 3. *If $\xi^x(1+py) \notin R_{p^n}$ and $\xi^x \notin \mathcal{T}_{p^n}$,*

$$\begin{aligned} R_{p^n} + \xi^x(1+py)R_{p^n} = \mathrm{GR}(p^2,p^{4n}) \setminus \big(&\mathcal{I}_{p^{2n}} \cup \{u(1+pv) \,:\, u \in \mathcal{T}_{p^n}^*,\ v \in \mathcal{T}_{p^{2n}}\} \\ &\cup \{\xi^x u(1+pv) \,:\, u \in \mathcal{T}_{p^n}^*,\ v \in \mathcal{T}_{p^{2n}}\}\big). \end{aligned}$$

Proof. It is clear that

$$\begin{aligned} R_{p^n} + \xi^x(1+py)R_{p^n} = \mathrm{GR}(p^2,p^{4n}) \setminus \Big(&\big(\mathcal{I}_{p^n} + \mathcal{I}_{p^n}\xi^x(1+py)\big) \\ &\cup \big(R_{p^n} + \mathcal{I}_{p^n}\xi^x(1+py)\big) \cup \big(\mathcal{I}_{p^n} + R_{p^n}\xi^x(1+py)\big)\Big). \end{aligned}$$

On the other hand, we have

$$\begin{aligned} \mathcal{I}_{p^n} + \mathcal{I}_{p^n}\xi^x(1+py) &= \{pu + pv\xi^x \,:\, u,v \in \mathcal{T}_{p^n}\} \\ &= \{p(u+v\xi^x) \,:\, u,v \in \mathcal{T}_{p^n}\} = \mathcal{I}_{p^{2n}}. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} R_{p^n} + \mathcal{I}_{p^n}\xi^x(1+py) &= \{u(1+pc) + pd\xi^x \,:\, u \in \mathcal{T}_{p^n}^*, c,d \in \mathcal{T}_{p^n}\} \\ &= \{u(1+p(c+d\xi^x)) \,:\, u \in \mathcal{T}_{p^n}^*, c,d \in \mathcal{T}_{p^n}\} \\ &= \{u(1+pv) \,:\, u \in \mathcal{T}_{p^n}^*, v \in \mathcal{T}_{p^{2n}}\} \end{aligned}$$

and

$$\begin{aligned} \mathcal{I}_{p^n} + R_{p^n}\xi^x(1+py) &= \{pd + u(1+pc)\xi^x(1+py) \,:\, u \in \mathcal{T}_{p^n}^*,\ c,d \in \mathcal{T}_{p^n}\} \\ &= \{u\xi^x(1+p(c+y+d\xi^{-x})) \,:\, u \in \mathcal{T}_{p^n}^*,\ c,d \in \mathcal{T}_{p^n}\} \\ &= \{u\xi^x(1+pv) \,:\, u \in \mathcal{T}_{p^n}^*,\ v \in \mathcal{T}_{p^{2n}}\}. \end{aligned}$$

This completes the proof of the lemma. □

Lemma 4. *For $j, j' = 0, 1, \ldots, p^n-1$ with $j \neq j'$ and any $a \in \mathrm{GR}(p^2,p^{4n})^*$,*

$$\sum_{i=0}^{p^n} |\xi^{i+j}(1+px_j)R_{p^n} \cap (\xi^{i+j'}(1+px_{j'})R_{p^n} + a)| = p^n - 1.$$

Proof. It is enough to compute the frequency of an element $a \in \mathrm{GR}(p^2, p^{4n})^*$ appearing in the multiset

$$A := \bigcup_{i=0}^{p^n} \big(\xi^{i+j}(1+px_j)R_{p^n} - \xi^{i+j'}(1+px_{j'})R_{p^n}\big).$$

Then, since $R_{p^n} = -R_{p^n}$, we have

$$A = \bigcup_{i=0}^{p^n} \xi^{i+j}\big((1+px_j)R_{p^n} + \xi^{j'-j}(1+px_{j'})R_{p^n}\big). \tag{3}$$

Furthermore, since ξ^{i+j}, $i = 0, 1, \ldots, p^n$, form a system of representatives for $\mathcal{T}^*_{p^{2n}}/\mathcal{T}^*_{p^n}$, the right hand side of (3) is rewritten as

$$\bigcup_{i=0}^{p^n} \xi^i(1+px_j)\big(R_{p^n} + (\xi^{j'-j}(1+p(x_{j'}-x_j))R_{p^n}\big). \tag{4}$$

Since $j'-j \neq 0$ and $\xi^{j'-j}(1+p(x_{j'}-x_j)) \notin R_{p^n}$, continuing from (3), we have by Lemma 3 that

$$A = \bigcup_{i=0}^{p^n} \xi^i\Big(\mathrm{GR}(p^2, p^{4n}) \setminus \big(\mathcal{I}_{p^{2n}} \cup \{u(1+pv) \,:\, u \in \mathcal{T}^*_{p^n},\ v \in \mathcal{T}_{p^{2n}}\} \cup \{\xi^{j'-j}u(1+pv) \,:\, u \in \mathcal{T}^*_{p^n},\ v \in \mathcal{T}_{p^{2n}}\}\big)\Big).$$

Hence, each element $a \in \mathrm{GR}(p^2, p^{4n})^*$ appears in A exactly $p^n - 1$ times. □

Lemma 5. *For any nonzero element $a \in \mathrm{GR}(p^2, p^{4n})$,*

$$\sum_{i=0}^{p^n}\sum_{j=0}^{p^n-1} |\xi^{i+j}(1+px_j)R_{p^n} \cap (\xi^{i+j}(1+px_j)R_{p^n} + a)| = \begin{cases} p^{2n}(p^n-1), & \text{if } a \in \mathcal{I}^*_{p^{2n}}, \\ p^n(p^n-2), & \text{if } \mathrm{GR}(p^2, p^{4n})^*, \end{cases}$$

where $\mathcal{I}^*_{p^{2n}} = \mathcal{I}_{p^{2n}} \setminus \{0\}$.

Proof. We consider the following set:

$$\{\xi^{i+j}(1+px_j)x - \xi^{i+j}(1+px_j)y \,:\, x, y \in R_{p^n}, x \neq y, i = 0, 1, \ldots, p^n, j = 0, 1, \ldots, p^n - 1\}. \tag{5}$$

If x and y have the form $x = \xi^u(1+ps)$ and $y = \xi^u(1+pt)$ with $s \neq t$, respectively, we have

$$\xi^{i+j}(1+px_j)x - \xi^{i+j}(1+px_j)y = p\xi^{i+j+u}(s-t) \in \mathcal{I}^*_{p^{2n}}.$$

Hence, each element of $\mathcal{I}^*_{p^{2n}}$ appears in the multiset (5) exactly $p^{2n}(p^n-1)$ times.

If x and y have the form $x = \xi^u(1+ps)$ and $y = \xi^v(1+pt)$ with $u \neq v$, respectively, we have

$$\xi^{i+j}(1+px_j)x - \xi^{i+j}(1+px_j)y = \xi^{i+j}(1+px_j)(\xi^u(1+ps) - \xi^v(1+pt)) \in \mathrm{GR}(p^2, p^{4n})^*.$$

Since $\xi^u(1+ps), \xi^v(1+pt) \in \mathrm{GR}(p^2, p^{2n})^*$, the differences $\xi^u(1+ps) - \xi^v(1+pt)$ represent every element of $\mathrm{GR}(p^2, p^{2n})^*$ exactly $p^n(p^n-2)$ times. □

Lemma 6. *For any* $a \in \mathrm{GR}(p^2, p^{4n})^*$,

$$\sum_{i=0}^{p^n} \sum_{j=0}^{p^n-1} \left|\xi^{i+j}(1+px_j)R_{p^n} \cap (\xi^i P + a)\right| = p^n - 1.$$

Proof. We compute the frequency of an element $a \in \mathrm{GR}(p^2, p^{4n})^*$ appearing in the multiset

$$B := \bigcup_{i=0}^{p^n} \bigcup_{j=0}^{p^n-1} (\xi^{i+j}(1+px_j)R_{p^n} - \xi^i P).$$

Let $u \in \mathcal{T}_{p^n}$ and $\xi^s, v \in \mathcal{T}_{p^n}^*$. Since

$$\xi^{i+j+s}(1+px_j)(1+pu) - pv\xi^{i+p^n} = \xi^{i+j+s}(1+p(x_j+u-v\xi^{p^n-j-s})),$$

we have

$$\begin{aligned}\xi^{i+j}(1+px_j)R_{p^n} - \xi^i P = \left\{\xi^{i+j+s}(1+p(x_j+u-v\xi^{p^n-j-s})) \,:\, \xi^s \in \mathcal{T}_{p^n}^*,\, u,v \in \mathcal{T}_{p^n}\right\} \\ \setminus \left\{\xi^{i+j+s}(1+p(x_j+u)) \,:\, \xi^s \in \mathcal{T}_{p^n}^*,\ u \in \mathcal{T}_{p^n}\right\}.\end{aligned}$$

Since $\xi^{p^n-j-s} \notin \mathcal{T}_{p^n}^*$, we have

$$\{p(u - v\xi^{p^n-j-s}) \,:\, u,v \in \mathcal{T}_{p^n}\} = p\mathcal{T}_{p^{2n}}.$$

Hence,

$$\left\{\xi^{i+j+s}(1+p(x_j+u-v\xi^{p^n-j-s})) \,:\, \xi^s \in \mathcal{T}_{p^n}^*,\, u,v \in \mathcal{T}_{p^n}\right\} = \xi^{i+j}\mathcal{T}_{p^n}^*(1+p\mathcal{T}_{p^{2n}}).$$

It is clear that

$$\bigcup_{i=0}^{p^n} \bigcup_{j=0}^{p^n-1} \xi^{i+j}\mathcal{T}_{p^n}^*(1+p\mathcal{T}_{p^{2n}})$$

contains every element of $\mathrm{GR}(p^2, p^{4n})^*$ exactly p^n times. On the other hand, we have

$$\begin{aligned}&\bigcup_{i=0}^{p^n} \bigcup_{j=0}^{p^n-1} \left\{\xi^{i+j+s}(1+p(x_j+u)) \,:\, \xi^s \in \mathcal{T}_{p^n}^*,\ u \in \mathcal{T}_{p^n}\right\} \\ =\ &\mathcal{T}_{p^{2n}}^* \bigcup_{j=0}^{p^n-1} \left\{(1+p(x_j+u)) \,:\, u \in \mathcal{T}_{p^n}\right\},\end{aligned}$$

which contains every element of $\mathrm{GR}(p^2, p^{4n})^*$ exactly once. Hence, B contains every element of $\mathrm{GR}(p^2, p^{4n})^*$ exactly $p^n - 1$ times. □

Lemma 7. *For any* $a \in \mathcal{I}_{p^{2n}}^*$,

$$\sum_{i=0}^{p^n} |\xi^i P \cap (\xi^i P + a)| = p^n - 2.$$

Proof. We consider the multiset

$$C := \bigcup_{i=0}^{p^n} \{\xi^{i+p^n} p\xi^{(p^n+1)s} - \xi^{i+p^n} p\xi^{(p^n+1)t} : s, t = 0, 1, \ldots, p^n - 2, s \neq t\}.$$

Since the multiset $\{p(\xi^{(p^n+1)s} - \xi^{(p^n+1)t}) : s, t = 0, 1, \ldots, p^n - 2, s \neq t\}$ covers every element of $\mathcal{I}^*_{p^n}$ exactly $p^n - 2$ times, C covers every element of $\mathcal{I}^*_{p^{2n}}$ exactly $p^n - 2$ times. □

We are now ready for proving Theorem 1.

Proof of Theorem 1. For any nonzero $a \in \mathrm{GR}(p^2, p^{4n})$, by Lemmas 4–7, we have

$$\begin{aligned}
\sum_{i=0}^{p^n} |D_i \cap (D_i + a)| = & \sum_{j \neq j'; j, j' = 0}^{p^n - 1} \sum_{i=0}^{p^n} |\xi^{i+j}(1 + px_j)R_{p^n} \cap (\xi^{i+j'}(1 + px_{j'})R_{p^n} + a)| \\
& + \sum_{i=0}^{p^n} \sum_{j=0}^{p^n - 1} |\xi^{i+j}(1 + px_j)R_{p^n} \cap (\xi^{i+j}(1 + px_j)R_{p^n} + a)| \\
& + \sum_{i=0}^{p^n} \sum_{j=0}^{p^n - 1} \left|\xi^{i+j}(1 + px_j)R_{p^n} \cap (\xi^i P + a)\right| \\
& + \sum_{i=0}^{p^n} \sum_{j=0}^{p^n - 1} \left|\xi^i P \cap (\xi^{i+j}(1 + px_j)R_{p^n} + a)\right| + \sum_{i=0}^{p^n} |\xi^i P \cap (\xi^i P + a)| \\
= & \begin{cases} p^{2n}(p^n - 1) + p^n - 2, & \text{if } a \in \mathcal{I}_{p^{2n}}, \\ p^n(p^n - 1)(p^n - 1) + p^n(p^n - 2) + 2(p^n - 1), & \text{if } \mathrm{GR}(p^2, p^{4n})^*, \end{cases} \\
= & p^{3n} - p^{2n} + p^n - 2.
\end{aligned}$$

This completes the proof of Theorem 1. □

4 Disjoint difference families from $\mathrm{GR}(2^2, 2^{2s})$

In this section, we follow the notations of Section 2. In particular, we treat the case where $p = 2$ and s an arbitrary positive integer. We present an infinite family of disjoint difference families from $\mathrm{GR}(2^2, 2^{2s})$ by using cosets of the unit group $\{1, 3\}$ of the subring $\mathrm{GR}(2^2, 2^2)$.

4.1 A bijection between $\mathbb{F}_{2^s}/\mathbb{F}_2$ and a $(2^s - 1, 2^{s-1}, 2^{s-2})$ difference set in $\mathbb{F}^*_{2^s}$

We begin with finding a "good" bijection from $\mathbb{F}_{2^s}/\mathbb{F}_2$ to a $(2^s - 1, 2^{s-1}, 2^{s-2})$ difference set in $\mathbb{F}^*_{2^s}$.

Let r be a fixed element of $\mathbb{F}_{2^s}$ such that $\mathrm{Tr}_{2^s/2}(r) = 1$, where $\mathrm{Tr}_{2^s/2}$ is the trace function from $\mathbb{F}_{2^s}$ to $\mathbb{F}_2$. It is clear that

$$\{x : \mathrm{Tr}_{2^s/2}(x) = 1, x \in \mathbb{F}^*_{2^s}\} = \{\beta^2 + \beta + r : \beta \in \mathbb{F}_{2^s}\}. \tag{6}$$

Note that the set (6) forms a difference set in $\mathbb{F}_{2^s}^*$ [14, Theorem 2.1.1]. Then, we consider the following bijection g from $\mathbb{F}_{2^s}/\mathbb{F}_2$ to the $(2^s-1, 2^{s-1}, 2^{s-2})$ difference set $D := \{x^{-1} : \mathrm{Tr}_{2^s/2}(x) = 1, x \in \mathbb{F}_{2^s}^*\}$:

$$g(\beta + \mathbb{F}_2) = (\beta^2 + \beta + r)^{-1}.$$

Put $f := g^{-1}$. Let γ be a fixed primitive element of $\mathbb{F}_{2^s}$. For each γ^i, $1 \leqslant i \leqslant 2^s - 2$, there are 2^{s-2} pairs $(u, v) \in D^2$ such that $uv^{-1} = \gamma^i$. Let $\mathcal{P}_i$ be the set of such pairs, i.e., $\mathcal{P}_i := \{(u, v) \in D^2 : uv^{-1} = \gamma^i\}$.

Lemma 8. *The bijection $f : D \to \mathbb{F}_{2^s}/\mathbb{F}_2$ defined above satisfies that for each i,*

$$\bigcup_{(u,v)\in\mathcal{P}_i} (f(u)\gamma^i + f(v)) = \mathbb{F}_{2^s}. \tag{7}$$

Proof. We compute the frequency of each element $t \in \mathbb{F}_{2^s}$ appearing in the multiset $\bigcup_{(u,v)\in\mathcal{P}_i}(f(u)\gamma^i + f(v))$. This number can be described in terms of characters as follows:

$$\begin{aligned}
&\frac{1}{2^{2s}} \sum_{x,y\in\mathbb{F}_{2^s}} \sum_{\alpha,\beta\in\mathbb{F}_{2^s}} \psi(y(\beta\gamma^i + \alpha + t))\psi(x((\beta^2 + \beta + r)\gamma^i - (\alpha^2 + \alpha + r))) \\
=&\frac{1}{2^{2s}} \sum_{x,y\in\mathbb{F}_{2^s}} \sum_{\alpha,\beta\in\mathbb{F}_{2^s}} \psi(x\alpha^2 + x\alpha + y\alpha)\psi(x\beta^2\gamma^i + x\beta\gamma^i + y\beta\gamma^i)\psi(yt + xr\gamma^i + xr),
\end{aligned}$$

where ψ is the canonical additive character of $\mathbb{F}_{2^s}$. Here,

$$\sum_{\alpha\in\mathbb{F}_{2^s}} \psi(x\alpha^2 + x\alpha + y\alpha) = \begin{cases} 2^s, & \text{if } x = (x+y)^2, \\ 0, & \text{otherwise,} \end{cases}$$

and

$$\sum_{\beta\in\mathbb{F}_{2^s}} \psi(x\beta^2\gamma^i + x\beta\gamma^i + y\beta\gamma^i) = \begin{cases} 2^s, & \text{if } x\gamma^i = (x\gamma^i + y\gamma^i)^2, \\ 0, & \text{otherwise.} \end{cases}$$

By noting that $i \neq 0$, since $x = (x+y)^2$ and $x\gamma^i = (x\gamma^i + y\gamma^i)^2$ can not happen simultaneously except for the trivial case $x = y = 0$, we have

$$\frac{1}{2^{2s}} \sum_{x,y\in\mathbb{F}_{2^s}} \sum_{\alpha,\beta\in\mathbb{F}_{2^s}} \psi(x\alpha^2 + x\alpha + y\alpha)\psi(x\beta^2\gamma^i + x\beta\gamma^i + y\beta\gamma^i)\psi(yt + xr\gamma^i + rx) = 1.$$

This completes the proof of the lemma. □

Lemma 9. *The bijection $f : D \to \mathbb{F}_{2^s}/\mathbb{F}_2$ satisfies that*

$$\bigcup_{u\in D} (f(u) - u^{-1}) = \mathbb{F}_{2^s}. \tag{8}$$

Proof. The assertion follows from the following transformation:

$$\bigcup_{u\in D} (f(u) - u^{-1}) = \{\beta - (\beta^2 + \beta + r) : \beta \in \mathbb{F}_{2^s}\} = \{\beta^2 + r : \beta \in \mathbb{F}_{2^s}\} = \mathbb{F}_{2^s}.$$ □

4.2 Construction and proof

The bijection $f : D \to \mathbb{F}_{2^s}/\mathbb{F}_2$ defined in the previous subsection also induces a bijection between a difference set X in $\mathcal{T}_{2^s}^*$ and $\mathcal{I}_{2^s}/\mathcal{I}_2$ via the following maps: $\sigma_1 : \mathbb{F}_{2^s}^* \to \mathcal{T}_{2^s}^*$ defined by $\sigma_1(\gamma^i) = \xi^i$ and $\sigma_2 : \mathbb{F}_{2^s}/\mathbb{F}_2 \to \mathcal{I}_{2^s}/\mathcal{I}_2$ defined by $\sigma_2(\gamma^i + \mathbb{F}_2) = 2(\xi^i + \mathcal{T}_2)$. Let h be the induced map from X to $\mathcal{I}_{2^s}/\mathcal{I}_2$.

Consider the set

$$D_i = \xi^i \left(P \cup \left(\bigcup_{x \in X} x(1 + h(x)) \right) \right), \ \ 0 \leqslant i \leqslant 2^s - 2, \tag{9}$$

where $P = \{2\}$.

Theorem 10. *Let h be the bijection from X to $\mathcal{I}_{2^s}/\mathcal{I}_2$ defined above. Then, the sets D_i, $i = 0, 1, \ldots, 2^s - 2$, defined in (9) form a disjoint difference family in $(\mathrm{GR}(2^2, 2^{2s}), +)$ with parameters $(v, k, \lambda, b) = (2^{2s}, 2^s + 1, 2^s, 2^s - 1)$.*

It is clear that $\bigcup_{i=0}^{2^s-2} \xi^i P = \mathcal{I}_{2^s}^*$. Furthermore, since $\bigcup_{x \in X}(1 + h(x)) = \mathbb{P}_{2^s}$ by the definition of h, we have

$$\begin{aligned} \bigcup_{i=0}^{2^s-2} \bigcup_{x \in X} \xi^i x(1 + h(x)) &= \left(\bigcup_{i=0}^{2^s-2} \xi^i \right) \left(\bigcup_{x \in X} (1 + h(x)) \right) \\ &= \mathcal{T}_{2^s}^* \mathbb{P}_{2^s} = \mathrm{GR}(2^2, 2^{2s})^*. \end{aligned}$$

Hence, D_i, $i = 0, 1, \ldots, 2^s - 2$, partition $\mathrm{GR}(2^2, 2^{2s}) \setminus \{0\}$.

We now prove this theorem by the following two lemmas.

Lemma 11. *Let $\mathcal{P}_i' := \{(x, y) \in X^2 : xy^{-1} = \xi^i\}$. For each $i = 1, 2, \ldots, 2^s - 2$,*

$$\mathcal{T}_{2^s}^* \bigcup_{(x,y) \in \mathcal{P}_i'} (x(1 + h(x)) + y(1 + h(y))) = \mathrm{GR}(2^2, 2^{2s})^*.$$

Proof. Note that

$$\mathcal{T}_{2^s}^* \bigcup_{(x,y) \in \mathcal{P}_i'} (x(1 + h(x)) + y(1 + h(y))) = \mathcal{T}_{2^s}^* \bigcup_{(x,y) \in \mathcal{P}_i'} (\xi^i(1 + h(x)) + (1 + h(y))).$$

Write $h(x) = 2(x' + \mathcal{T}_2)$ and $h(y) = 2(y' + \mathcal{T}_2)$. Then, $\xi^i(1 + h(x)) + (1 + h(y))$ is expressed as

$$\xi^i(1 + 2x' + 2\mathcal{T}_2) + (1 + 2y' + 2\mathcal{T}_2) = \xi^i + 1 + 2(\xi^i(x' + \mathcal{T}_2) + y' + \mathcal{T}_2).$$

Put $\xi^i + 1 = \xi^{k_i}(1 + 2\ell_i)$. Then,

$$\xi^i + 1 + 2(\xi^i(x' + \mathcal{T}_2) + y' + \mathcal{T}_2) = \xi^{k_i}(1 + 2(\ell_i + \xi^{-k_i}(\xi^i(x' + \mathcal{T}_2) + y' + \mathcal{T}_2))).$$

We now consider the set $\bigcup_{(x,y)\in\mathcal{P}_i'} 2(\xi^i(x'+\mathcal{T}_2)+y'+\mathcal{T}_2)$. By the isomorphism σ from $\mathcal{I}_{2^s}$ to $\mathbb{F}_{2^s}$ mapping $2\xi^i$ to γ^i, $0\leqslant i\leqslant 2^s-2$, and $0\in\mathcal{I}_{2^s}$ to $0\in\mathbb{F}_{2^s}$, we have

$$\sigma(\bigcup_{(x,y)\in\mathcal{P}_i'} 2(\xi^i(x'+\mathcal{T}_2)+y'+\mathcal{T}_2)) = \bigcup_{(u,v)\in\mathcal{P}_i} (\gamma^i f(u)+f(v)).$$

By Lemma 8, this set coincides with $\mathbb{F}_{2^s}$. In other words, $\bigcup_{(x,y)\in\mathcal{P}_i'} 2(\xi^i(x'+\mathcal{T}_2)+y'+\mathcal{T}_2)) = \mathcal{I}_{2^s}$. This completes the proof of the lemma. □

Lemma 12. *It holds that*

$$\mathcal{T}_{2^s}^* \bigcup_{x\in X}(x(1+h(x))+P) = \mathrm{GR}(2^2,2^{2s})^*.$$

Proof. Write $h(x)=2(x'+\mathcal{T}_2)$. Then, $\mathcal{T}_{2^s}^*\bigcup_{x\in X}(x(1+h(x))+P)$ is expressed as

$$\mathcal{T}_{2^s}^* \bigcup_{x\in X} x(1+2(x'+\mathcal{T}_2-x^{-1})).$$

We now consider the set $\bigcup_{x\in X} 2(x'+\mathcal{T}_2-x^{-1})$. By the isomorphism σ, we have

$$\sigma(\bigcup_{x\in X} 2(x'+\mathcal{T}_2-x^{-1})) = \bigcup_{u\in D}(f(u)-u^{-1}).$$

By Lemma 9, this set coincides with $\mathbb{F}_{2^s}$. In other words, $\bigcup_{x\in X} 2(x'+\mathcal{T}_2-x^{-1}) = \mathcal{I}_{2^s}$. This completes the proof of the lemma. □

We are now ready for proving our main theorem of this section.

Proof of Theorem 10. For each nonzero $a\in\mathrm{GR}(2^2,2^{2s})$, we compute the number

$$\sum_{i=0}^{2^s-2} |D_i\cap(D_i+a)|.$$

By Lemma 11, for each $a\in\mathrm{GR}(2^2,2^{2s})^*$, we have

$$\sum_{i=0}^{2^s-2} \Big|\xi^i\bigcup_{x\in X} x(1+h(x))\cap\big(\xi^i\bigcup_{x\in X} x(1+h(x))+a\big)\Big| = 2^s-2.$$

On the other hand, since the number of elements in $\mathcal{I}_{2^s}^*$ occurring as differences between elements in $xh(x)$ is two, for each $a\in\mathcal{I}_{2^s}^*$

$$\sum_{i=0}^{2^s-2} \Big|\xi^i\bigcup_{x\in X} x(1+h(x))\cap\big(\xi^i\bigcup_{x\in X} x(1+h(x))+a\big)\Big| = 2^s.$$

Finally, by Lemma 12, for each $a\in\mathrm{GR}(2^2,2^{2s})^*$, we have

$$\sum_{i=0}^{2^s-2} \Big|\xi^i\bigcup_{x\in X} x(1+h(x))\cap\big(\xi^iP+a\big)\Big| + \sum_{i=0}^{2^s-2} \Big|\xi^iP\cap\big(\xi^i\bigcup_{x\in X} x(1+h(x))+a\big)\Big| = 2.$$

This completes the proof of Theorem 10. □

$x \in \mathcal{T}_{3^3}^*/\mathcal{T}_3^*$	$\mathcal{T}_3^*\xi^2$	$\mathcal{T}_3^*\xi^4$	$\mathcal{T}_3^*\xi^5$	$\mathcal{T}_3^*\xi^6$	$\mathcal{T}_3^*\xi^7$
$h(x) \in \mathcal{I}_{3^3}/\mathcal{I}_3$	$3\xi^{17}+\mathcal{I}_3$	$3\xi^{6}+\mathcal{I}_3$	$3\xi^{2}+\mathcal{I}_3$	$3\xi^{15}+\mathcal{I}_3$	$3\xi^{4}+\mathcal{I}_3$

$x \in \mathcal{T}_{3^3}^*/\mathcal{T}_3^*$	$\mathcal{T}_3^*\xi^8$	$\mathcal{T}_3^*\xi^{10}$	$\mathcal{T}_3^*\xi^{11}$	$\mathcal{T}_3^*\xi^{12}$
$h(x) \in \mathcal{I}_{3^3}/\mathcal{I}_3$	$3\xi^{8}+\mathcal{I}_3$	$3\xi^{5}+\mathcal{I}_3$	$3\xi+\mathcal{I}_3$	$\mathcal{I}_3$

Table 1: A bijection between a $(13, 9, 6)$ difference set in $\mathcal{T}_{3^3}^*/\mathcal{T}_3^*$ and $\mathcal{I}_{3^3}/\mathcal{I}_3$

5 Disjoint difference families from $\mathrm{GR}(3^2, 3^6)$

In this section, we consider a generalization of the construction of disjoint difference families given in Section 4. Let p be a prime and s, n be positive integers such that $n \mid s$. Let X be a $(\frac{p^s-1}{p^n-1}, p^{s-n}, p^{s-2n}(p^n-1))$ difference set on $\mathcal{T}_{p^s}^*/\mathcal{T}_{p^n}^*$ and set $Y = \mathcal{I}_{p^s}/\mathcal{I}_{p^n}$. Let h be a bijection from X to Y. Consider the set

$$D_i = \xi^i \left(P \cup \left(\bigcup_{x \in X} x(1 + h(x)) \right) \right), \ \ 0 \leqslant i \leqslant \frac{p^s - p^n}{p^n - 1}, \tag{10}$$

where $P = p\mathcal{T}_{p^n}^*$.

Problem 13. Find a bijection h such that $\{D_0, D_1, \ldots, D_{(p^s-p^n)/(p^n-1)}\}$ forms a disjoint difference family in $(\mathrm{GR}(p^2, p^{2s}), +)$.

We checked by computer that such a disjoint difference family exists in the case where $(p, s, n) = (3, 3, 1)$. The polynomial $x^3 + 2x^2 + 3 + 1 \in \mathbb{Z}_9[x]$ is a monic basic irreducible polynomial having a root ξ of order $3^3 - 1 = 26$. Then, $\mathcal{T}_{3^3} = \{0, 1, \xi, , \ldots, \xi^{25}\}$ and $P = \{3, 6\}$. Let

$$S = \{0, \xi, \xi^2, \xi^4, \xi^5, \xi^6, \xi^8, \xi^{15}, \xi^{17}\}.$$

Then, $1 + 3S$ forms a system of representatives for $\mathbb{P}_{3^3}/\mathbb{P}_3$. Furthermore, the set

$$X := \mathcal{T}_3^*\{\xi^2, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8, \xi^{10}, \xi^{11}, \xi^{12}\}$$

is a $(13, 9, 6)$ difference set in $\mathcal{T}_{3^3}^*/\mathcal{T}_3^*$. Define the map $h : X \to \mathcal{I}_{3^3}/\mathcal{I}_3$ as in Table 1. Then, the sets

$$D_i = \xi^i \Big(P \cup \Big(\bigcup_{x \in X} x(1 + h(x)) \Big) \Big), \ \ 0 \leqslant i \leqslant 12,$$

form a disjoint difference family in $(\mathrm{GR}(3^2, 3^6), +) \simeq \mathbb{Z}_9^3$ with parameters $(v, k, \lambda, b) = (729, 56, 55, 13)$.

Remark 14. We could not generalize this example into an infinite family. When we try to generalize the example, it is natural to consider the equality

$$\{x \in \mathbb{F}_{p^s} : \mathrm{Tr}_{p^s/p^n}(x) = 1\} = \{\beta^{p^n} - \beta + r : \beta \in \mathbb{F}_{p^s}\},$$

where r is a fixed element of $\mathbb{F}_{p^s}$ satisfying $\mathrm{Tr}_{p^s/p^n}(r) = 1$, similarly to (6). Then, analogous to the construction given in Section 4, we can consider the map g from $\mathbb{F}_{p^s}/\mathbb{F}_{p^n}$ to the difference set $\{x^{-1}\mathbb{F}_{p^n}^* : \mathrm{Tr}_{p^s/p^n}(x) = 1, x \in \mathbb{F}_{p^s}\} \subseteq \mathbb{F}_{p^s}^*/\mathbb{F}_{p^n}^*$ defined by

$$g(\beta + \mathbb{F}_{p^n}) = (\beta^{p^n} - \beta + r)^{-1}\mathbb{F}_{p^n}^*.$$

However, this map does not yield a disjoint difference family in $(\mathrm{GR}(3^2, 3^6), +)$. Hence, we need a modification of this construction. We leave this as an open problem to the readers.

6 Concluding remarks

In this paper, we give two constructions of disjoint difference families from Galois rings by carefully choosing cosets of the unit group of a subring. In this section, we explain how our constructions are related to known constructions of disjoint difference families in finite rings.

As far as the author knows, two general constructions of disjoint difference families in finite rings (not finite fields) have been known; one is a recursive construction using *difference matrices*, and the other is a construction using cosets of a unit subgroup of the ring similarly to our construction. However, both of the constructions can not fit with our constructions as explained below.

A typical recursive construction given in [1] assumes the existence of two difference families in groups of order u and u', respectively, with the same block size $k \leqslant u, u'$ and a combinatorial object, called a *difference matrix*. Then, the resulting difference family is of order $v = uu'$ and with block size k. In this case, it is clear that $v \geqslant k^2$. On the other hand, our new difference families satisfy that $v < k^2$. Hence, our difference families can not be obtained from the recursive construction.

Also, the following basic construction of disjoint difference families in finite rings was given in [11, Theorem 3.7] (see also [10, Theorem 3.3]). Let R be a finite commutative ring with an identity and B be a subgroup of the unit group U of R such that the differences occurring in B are all in U. Define a relation "$x \sim y$" for $x, y \in R\backslash\{0\}$ by $xB = yB$, which gives an equivalence relation. Let S be a system of representatives for the equivalence classes modulo B in $R \setminus \{0\}$. Then, $\{sB : s \in S\}$ forms a disjoint difference family in $(R, +)$. On the other hand, each block of our difference family is a union of cosets of the unit group of a subgring together with a coset of the maximal ideal of the subring removing the zero. Hence, the known construction can not fit with our new construction.

Acknowledgements

The author wishes to thank my graduate student Taishi Tanaka for assisting me to find the example of a disjoint difference family in $\mathrm{GR}(3^2, 3^6)$. Also, the author would like to thank the reviewers for their helpful comments for improving the readability of this paper.

References

[1] R. J. R. Abel and M. Buratti. Difference families. In: C. J. Colbourn and J. H. Dinitz. (Eds.) *The CRC Handbook of Combinatorial Designs, 2nd edn*, pages 392–409. Chapman & Hall/CRC Press, Boca Raton, FL, 2006.

[2] C. Carlet, G. Gong, and Y. Tan. Quadratic zero-difference balanced functions, APN functions and strongly regular graphs. *Des. Codes Cryptogr.*, 78:629–654, 2016.

[3] Y. Chang and C. Ding. Constructions of external difference families and disjoint difference families. *Des. Codes Cryptogr.*, 40:167–185, 2006.

[4] C. Ding. Optimal constant composition codes from zero-difference balanced functions. *IEEE Trans. Inform. Theory*, 54:5766–5770, 2008.

[5] C. Ding, Q. Wang, and M. Xiong. Three new families of zero-difference balanced functions with applications. *IEEE Trans. Inform. Theory*, 60:2407–2413, 2014.

[6] H. Cai, X. Zeng, T. Helleseth, X. Tang, and Y. Yang. A new construction of zero-difference balanced functions. *IEEE Trans. Inform. Theory*, 59:5008–5015, 2013.

[7] C. Fan, J. Lei, and Y. Chang. Constructions of difference systems of sets and disjoint difference families. *IEEE Trans. Inform. Theory*, 54:3195–3201, 2008.

[8] C. Fan and J. Lei. Constructions of difference systems of sets from finite projective geometry. *IEEE Trans. Inform. Theory*, 58:130–138, 2012.

[9] R. Fuji-Hara, A. Munemasa, and V. Tonchev. Hyperplane partitions and difference systems of sets. *J. Combin. Theory, Ser. A*, 113:1689–1698, 2006.

[10] S. Furino. Difference families from rings. *Discrete Math.*, 97:177–190, 1991.

[11] S. Kageyama and Y. Miao. Difference families with applications to resolvable designs. *Hiroshima Math. J.*, 25:475–485, 1995.

[12] Y. Mutoh and V. Tonchev. Difference systems of sets and cyclotomy. *Discrete Math*, 308:2959–2969, 2008.

[13] S.-L. Ng and M. B. Paterson. Disjoint difference families and their applications. *Des. Codes Cryptogr.*, 78:103–127, 2016.

[14] A. Pott. *Finite Geometry and Character Theory.* Lecture Note in Mathematics, 1601, Springer, Berlin, 1995.

[15] Z.-X. Wan. *Finite Fields and Galois Rings.* World Scientific, Singapore, 2010.

[16] Q. Wang and Y. Zhou. Sets of zero-difference balanced functions and their applications. *Adv. Math. Commun.*, 8:83–101, 2014.

[17] J. Yin, X. Shan, and Z. Tian. Constructions of partitioned difference families. *European J. Combin.*, 29:1507–1519, 2008.

[18] Z. Zhou and X. Tang. Optimal and perfect difference systems of sets from q-ary sequences with difference-balanced property. *Des. Codes Cryptogr.*, 57:215–223, 2010.