Journal of Algebraic Combinatorics **12** (2000), 145–153


# Two Generalized Constructions of Relative Difference Sets

XIANG-DONG HOU* xhou@euler.math.wright.edu
*Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435, USA*

SURINDER K. SEHGAL sehgal@math.ohio-state.edu
*Department of Mathematics, Ohio State University, Columbus, Ohio 43210, USA*

*Received March 11, 1998*

**Abstract.** We give two generalizations of some known constructions of relative difference sets. The first one is a generalization of a construction of RDS by Chen, Ray-Chaudhuri and Xiang using the Galois ring $GR(4, m)$. The second one generalizes a construction of RDS by Ma and Schmidt from the setting of chain rings to a setting of more general rings.

**Keywords:** bent function, exponential sum, finite quasi-Frobenius local ring, relative difference set

## 1. Introduction

Let $N \lhd G$ be finite groups such that $|N| = n$ and $|G| = mn$. A $k$-subset $R$ of $G$ is called an $(m, n, k, \lambda)$ relative difference set (RDS) of $G$ relative to $N$ if the differences $r_1 r_2^{-1}$ $(r_1, r_2 \in R)$ represent each element of $G\backslash N$ exactly $\lambda$ times but represent no element of $N\backslash\{e\}$. If we identify $R$ with $\sum_{g\in R} g \in \mathbb{Z}[G]$, then $R$ is an $(m, n, k, \lambda)$ RDS relative to $N$ if and only if the equation

$$RR^{(-1)} = ke + \lambda(G\backslash N) \tag{1.1}$$

is satisfied in the group ring $\mathbb{Z}[G]$, where $R^{(-1)} = \sum_{g\in R} g^{-1}$. When $G$ is abelian, (1.1) holds if and only if for every character $\chi$ of $G$,

$$|\chi(R)|^2 = \begin{cases} k^2, & \text{if } \chi \text{ is principal,} \\ k - \lambda n, & \text{if } \chi \text{ is principal on } N \text{ but not on } G, \\ k, & \text{if } \chi \text{ is not principal on } N. \end{cases} \tag{1.2}$$

An $(m, n, k, \lambda)$ RDS with $k = \lambda n$ is called semi-regular. Thus $R$ is an $(m, n, k, k/n)$ semi-regular RDS in a finite abelian group $G$ relative to $N$ if and only if for every character

*This work was done during the first author's sabbatical visit to the Ohio State University. Support from Wright State University and hospitality from the Ohio State University are gratefully acknowledged.

$\chi$ of $G$,

$$|\chi(R)|^2 = \begin{cases} k^2, & \text{if } \chi \text{ is principal,} \\ 0, & \text{if } \chi \text{ is principal on } N \text{ but not on } G, \\ k & \text{if } \chi \text{ is not principal on } N. \end{cases} \tag{1.3}$$

The RDS's constructed in this paper are semi-regular.

For a survey of results on relative difference sets up to 1995, we refer the reader to Pott [11]. Since then, there have been some new constructions of relative difference sets in abelian groups using certain ring structures on the groups. Roughly speaking, the required ring structure on an abelian group $G$ enables us to generate all additive characters of $G$ from any "nondegenerate" character. Chen, Ray-Chaudhuri and Xiang [2] constructed a family of RDS in abelian 2-groups using Galois rings. Let $G = GR(4, 2t+1) \times W$, where $GR(4, 2t+1)$ is the Galois ring of characteristic 4 and size $4^{2t+1}$ and $W = \mathbb{Z}_4^r \times (\mathbb{Z}_2 \times \mathbb{Z}_2)^s$, $r+s = t$. Their result is a family of RDS of $G$ relative to the maximal ideal of $GR(4, 2t+1)$. We will generalize this construction to $GR(4, m) \times W$, where $m$ is not necessarily odd and $W$ is any abelian 2-group with $|W| \leq 2^m$ and $\exp W \leq 4$. Another recent construction of RDS was by Ma and Schmidt [8] using finite commutative principal ideal local rings. We shall see that their construction can be generalized to a larger class of rings—finite rings with a unique minimal left ideal. The purpose of this paper is not only to provide more general ways to construct RDS's but also to demonstrate some connections between RDS and other interesting topics such as quasi-Frobenius rings and generalized bent functions. The reader will find that the proofs here differ from those in [2] and [8] considerably.

## 2. A generalized construction of RDS using the Galois ring $GR(4, m)$

Let $p$ be a prime, $t > 0$ and $f \in \mathbb{Z}_{p^t}[x]$ a monic polynomial of degree $m$ whose image $\bar{f}$ in $\mathbb{Z}_p[x]$ is irreducible. The ring structure of $\mathbb{Z}_{p^t}[x]/(f)$ depends only on $m$. $\mathbb{Z}_{p^t}[x]/(f)$ is called a Galois ring of characteristic $p^t$ and is denoted by $GR(p^t, m)$. We refer the reader to McDonald [9] for a comprehensive treatment of Galois rings. For the role of Galois rings in some recent important discoveries in coding theory, we refer the reader to [1, 5].

The Galois ring needed here is $GR(4, m)$. It is a local ring with maximal ideal $2GR(4, m)$. The group of units $GR(4, m)^*$ of $GR(4, m)$ contains a unique cyclic subgroup $T^*$ of order $2^m - 1$. $T = T^* \cup \{0\}$ is called the Teichmuller set of $GR(4, m)$. $GR(4, m)/2GR(4, m)$ is the Galois field $GF(2^m)$ and $T$ is a system of coset representatives of $2GR(4, m)$ in $GR(4, m)$. Each element $a \in GR(4, m)$ has a unique 2-adic representation $a = x_0 + 2x_1$ where $x_0, x_1 \in T$. The map $\sigma : GR(4, m) \to GR(4, m) : x_0 + 2x_1 \mapsto x_0^2 + 2x_1^2$ $(x_0, x_1 \in T)$ is the Frobenius map of $GR(4, m)$. $\sigma$ is an automorphism of $GR(4, m)$ of order $m$ and $\langle\sigma\rangle$ is the full automorphism of $GR(4, m)$.The trace of $GR(4, m)$ is the map $\mathrm{Tr} : GR(4, m) \to \mathbb{Z}_4$ defined by $\mathrm{Tr}(a) = \sum_{i=0}^{m-1} \sigma^i(a)$.

Let $\xi = \sqrt{-1}$. Then for $x_0 \in T^*$ and $x_1 \in T$,

$$\sum_{x \in T} \xi^{\mathrm{Tr}((x_0+2x_1)x)} = \xi^{-\mathrm{Tr}(x_1/x_0)} \sum_{x \in T} \xi^{\mathrm{Tr}(x)}. \tag{2.1}$$

This is a result of Calderbank whose proof can be found in [2]. The exponential sum $\sum_{x\in T}\xi^{\mathrm{Tr}(x)}$ was determined up to 4 possibilities in [1] and was completely determined in [12]. For our purpose here, we shall only need the fact that

$$\left|\sum_{x\in T}\xi^{\mathrm{Tr}(x)}\right| = 2^{m/2}. \tag{2.2}$$

Let $W$ be a finite abelian group and $h : W \to T$ any function. Let $G = GR(4, m) \times W$ and

$$R = \bigcup_{w\in W}((1 + 2h(w))T, w) \subset G. \tag{2.3}$$

We shall explore conditions on $W$ and $h$ that will make $R$ a semi-regular RDS in $G$ relative to $N = 2GR(4, m) \times \{0\}$. We need the following notion of generalized bent functions [6].

**Definition 2.1** Let $A$ be a finite abelian group with character group $A^*$ and let $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. A function $f : A \to S^1$ is called a bent function if for every $\chi \in A^*$,

$$\left|\sum_{x\in A} f(x)\chi(x)\right| = |A|^{1/2}. \tag{2.4}$$

**Theorem 2.2** *The set $R$ in* (2.3) *is a semi-regular RDS of $G$ relative to $N$ if and only if for each $z \in T$, the function*

$$\begin{aligned} f_z : W &\to S^1 \\ w &\mapsto \xi^{\mathrm{Tr}(h(w)+2zh(w))} \end{aligned} \tag{2.5}$$

*is a bent function on $W$.*

**Proof:** Sufficiency. Assume $\chi \times \lambda$ is a nonprincipal character of $G$ where $\chi$ and $\lambda$ are characters of $GR(4, m)$ and $W$ respectively.

*Case 1.* $\chi$ is principal on $2GR(4, m)$. Then $\chi(\cdot) = \xi^{\mathrm{Tr}(a\cdot)}$ for some $a \in 2GR(4, m)$. Then

$$\begin{aligned} (\chi \times \lambda)(R) &= \sum_{w\in W}\lambda(w)\sum_{x\in T}\xi^{\mathrm{Tr}(a(1+2h(w))x)} \\ &= \sum_{w\in W}\lambda(w)\cdot\sum_{x\in T}\xi^{\mathrm{Tr}(ax)}. \end{aligned} \tag{2.6}$$

If $a \in 2GR(4, m)\backslash\{0\}$, then $\sum_{x\in T}\xi^{\mathrm{Tr}(ax)} = 0$; if $a = 0$, then $\lambda$ is nonprincipal on $W$ and $\sum_{w\in W}\lambda(w) = 0$. Thus we always have

$$(\chi \times \lambda)(R) = 0 \tag{2.7}$$

in this case.

*Case 2.* $\chi$ is nonprincipal on $2GR(4, m)$. Then $\chi(\cdot) = \xi^{\mathrm{Tr}(a\cdot)}$ for some $a = x_0 + 2x_1$ where $x_0 \in T^*$, $x_1 \in T$. Then

$$\begin{aligned}(\chi \times \lambda)(R) &= \sum_{w\in W} \lambda(w) \sum_{x\in T} \xi^{\mathrm{Tr}(a(1+2h(w))x)} \\ &= \sum_{w\in W} \lambda(w) \sum_{x\in T} \xi^{\mathrm{Tr}(1+2(h(w)+z))x)} \end{aligned} \tag{2.8}$$

where $z = x_1/x_0$. Note that $h(w)+z \equiv h(w)+z+2\sigma^{m-1}(zh(w)) \pmod{2GR(4, m)}$ and that $h(w) + z + 2\sigma^{m-1}(zh(w)) = (\sigma^{m-1}(h(w)) + \sigma^{m-1}(z))^2 \in T$, since $T$ consists of all the squares of $GR(4, m)$. Using (2.1) and (2.2) in (2.8), we have

$$\begin{aligned}|(\chi \times \lambda)(R)| &= \left| \sum_{w\in W} \lambda(w) \cdot \xi^{-\mathrm{Tr}(h(w)+z+2\sigma^{m-1}(zh(w)))} \sum_{x\in T} \xi^{\mathrm{Tr}(x)} \right| \\ &= 2^{m/2} \left| \sum_{w\in W} \lambda(w) \cdot \xi^{-\mathrm{Tr}(h(w)+2zh(w))} \right| \\ &= 2^{m/2} \left| \sum_{w\in W} \overline{\lambda(w)}\, f_z(w) \right| \\ &= 2^{m/2} |W|^{1/2}. \end{aligned} \tag{2.9}$$

Therefore $R$ is a semi-regular RDS of $G$ relative to $N$.

Necessity. It follows from (2.9). □

For any $x \in T$, the 2-adic expansion of $\mathrm{Tr}(x) \in \mathbb{Z}_4$ is known (cf. [5]):

$$\mathrm{Tr}(x) = (\iota \circ \mathrm{tr} \circ \pi)(x) + 2Q(\pi(x)). \tag{2.10}$$

In (2.10), $\pi : GR(4, m) \to GR(4, m)/2GR(4, m) = GF(2^m)$ is the canonical projection; $\mathrm{tr} : GF(2^m) \to \mathbb{Z}_2$ is the trace of $GF(2^m)$; $\iota : \mathbb{Z}_2 \to \{0, 1\} \subset \mathbb{Z}_4$ is the obvious inclusion; $Q : GF(2^m) \to \mathbb{Z}_2$ is given by

$$Q(y) = \sum_{0\le i<j\le m-1} \rho^i(y)\rho^j(y), \tag{2.11}$$

where $\rho$ is the Frobenius map of $GF(2^m)$. $Q$ is a quadratic function on $GF(2^m) = \mathbb{Z}_2^m$. For each $a \in GF(2^m)$, the function $D_aQ : GF(2^m) \to \mathbb{Z}_2$ is defined by $(D_aQ)(y) = Q(y+a) - Q(y)$, $y \in GF(2^m)$. It's easy to determine that

$$\dim\{a \in GF(2^m) : D_aQ \equiv 0 \pmod{\mathbb{Z}_2}\} = \begin{cases} 0, & \text{if } m \text{ is even,} \\ 1, & \text{if } m \text{ is odd.} \end{cases} \tag{2.12}$$

(In fact, $\{a \in GF(2^m) : D_a Q \equiv 0 \pmod{\mathbb{Z}_2}\}$ is $\{0\}$ for even $m$ and is $\mathbb{Z}_2$ for odd $m$.) Then using the well-known canonical forms of quadratic functions on $\mathbb{Z}_2^m$ (cf. [4]), we can identify $GF(2^m)$ with $\mathbb{Z}_2^m$ suitably such that

$$Q(x_1, \ldots, x_m) = x_1x_2 + x_3x_4 + \cdots + x_{2\lfloor m/2 \rfloor - 1}x_{2\lfloor m/2 \rfloor} + l(x_1, \ldots, x_m) \tag{2.13}$$

for all $(x_1, \ldots, x_m) \in GF(2^m)$, where $l(x_1, \ldots, x_m)$ is a linear function of $(x_1, \ldots, x_m)$. Let

$$\mathrm{tr}(x_1, \ldots, x_m) = a_1x_1 + \cdots + a_mx_m, \quad (x_1, \ldots, x_m) \in GF(2^m), \tag{2.14}$$

where $a_i \in \mathbb{Z}_2$. Note that when $m$ is odd, $a_m \neq 0$. (To see this, one only has to check that $D_a Q \not\equiv \mathrm{tr} (\mathrm{mod}\, \mathbb{Z}_2)$ for all $a \in GF(2^m)$.) Therefore, by a suitable linear transformation of $(x_1, \ldots, x_m)$ in (2.13), we may further assume, in addition to (2.13), that

$$\mathrm{tr}(x_1, \ldots, x_m) = x_m \quad \text{for } (x_1, \ldots, x_m) \in GF(2^m). \tag{2.15}$$

From now on, we assume that $GF(2^m)$ is so identified with $\mathbb{Z}_2^m$ such that both (2.13) and (2.15) hold.

**Corollary 2.3** *Let $W$ be a finite abelian group and $h : W \to T$ a function. Let*

$$\pi \circ h = (\alpha_1, \ldots, \alpha_m) : W \to GF(2^m) = \mathbb{Z}_2^m. \tag{2.16}$$

*Then $R = \bigcup_{w \in W}((1 + 2h(w))T, w) \subset GR(4, m) \times W = G$ is a semi-regular RDS of $G$ relative to $2GR(4, m) \times \{0\}$ if and only if*

$$\xi^{\iota \circ \alpha_m}(-1)^{\alpha_1\alpha_2 + \cdots + \alpha_{2\lfloor m/2 \rfloor - 1}\alpha_{2\lfloor m/2 \rfloor} + a_1\alpha_1 + \cdots + a_m\alpha_m} \tag{2.17}$$

*is a bent function on $W$ for all $(a_1, \ldots, a_m) \in \mathbb{Z}_2^m$.*

**Proof:** By (2.10), (2.13), (2.15) and (2.16), for each $z \in T$, $w \in W$,

$$\begin{aligned} \xi^{\mathrm{Tr}(h(w) + 2zh(w))} &= \xi^{\mathrm{Tr}(h(w))}(-1)^{\mathrm{tr}(\pi(z)\pi(h(w)))} \\ &= \xi^{(\iota \circ \mathrm{tr} \circ \pi \circ h)(w) + 2(Q \circ \pi \circ h)(w)}(-1)^{\mathrm{tr}(\pi(z)\pi(h(w)))} \\ &= \xi^{\iota(\alpha_m(w))}(-1)^{\alpha_1(w)\alpha_2(w) + \cdots + \alpha_{2\lfloor m/2 \rfloor - 1}(w)\alpha_{2\lfloor m/2 \rfloor}(w) + a_1\alpha_1(w) + \cdots + a_m\alpha_m(w)} \end{aligned} \tag{2.18}$$

where $(a_1, \ldots, a_m) \in \mathbb{Z}_2^m$ is determined by $z$. As $z$ runs over $T$, $(a_1, \ldots, a_m)$ runs over $\mathbb{Z}_2^m$. Thus the corollary follows from Theorem 2.2. □

In order for the construction of RDS in Corollary 2.3 to work, we only have to find functions $\alpha_1, \ldots, \alpha_m : W \to \mathbb{Z}_2$ such that the function (2.17) is bent on $W$ for all $(a_1, \ldots, a_m) \in \mathbb{Z}_2^m$.

**Lemma 2.4**

(i) *Let $\alpha : \mathbb{Z}_2 \to \mathbb{Z}_2$ be a bijection and $a \in \mathbb{Z}_2$. Then $\xi^{\iota\circ\alpha}(-1)^{a\alpha}$ is bent on $\mathbb{Z}_2$.*

(ii) *Let $(\alpha_1, \alpha_2) : \mathbb{Z}_2 \to \mathbb{Z}_2^2$ be such that $\alpha_2$ is a bijection and $a_1, a_2 \in \mathbb{Z}_2$. Then $\xi^{\iota\circ\alpha_2}(-1)^{\alpha_1\alpha_2+a_1\alpha_1+a_2\alpha_2}$ is bent on $\mathbb{Z}_2$.*

(iii) *Let $(\alpha_1, \alpha_2) : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ be a bijection and $a_1, a_2 \in \mathbb{Z}_2$. Then $\xi^{\iota\circ\alpha_2}(-1)^{\alpha_1\alpha_2+a_1\alpha_1+a_2\alpha_2}$ is bent on $\mathbb{Z}_2^2$.*

(iv) *Let $(\alpha_1, \alpha_2) : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ be a bijection such that $\alpha_2(0) = \alpha_2(2)$ and $a_1, a_2 \in \mathbb{Z}_2$. Then $\xi^{\iota\circ\alpha_2}(-1)^{\alpha_1\alpha_2+a_1\alpha_1+a_2\alpha_2}$ is bent on $\mathbb{Z}_4$.*

(v) *Let $W = \mathbb{Z}_2^2$ or $\mathbb{Z}_4$, $(\alpha_1, \alpha_2) : W \to \mathbb{Z}_2^2$ a bijection and $a_1, a_2 \in \mathbb{Z}_2$. Then $(-1)^{\alpha_1\alpha_2+a_1\alpha_1+a_2\alpha_2}$ is bent on $W$.*

(vi) *Let $\pi$ be a permutation of $\mathbb{Z}_2^s$ and let $(\alpha_1, \ldots, \alpha_{2s}) : \mathbb{Z}_2^{2s} \to \mathbb{Z}_2^{2s}$ be defined by*

$$\begin{aligned}&(\alpha_1, \alpha_3, \ldots, \alpha_{2s-1}, \alpha_2, \alpha_4, \ldots, \alpha_{2s})(x_1, \ldots, x_{2s})\\ &\quad = (x_1, \ldots, x_s, \pi(x_{s+1}, \ldots, x_{2s})), (x_1, \ldots, x_{2s}) \in \mathbb{Z}_2^{2s}.\end{aligned} \tag{2.19}$$

*Then for any $a_1, \ldots, a_{2s} \in \mathbb{Z}_2$, $(-1)^{\alpha_1\alpha_2+\cdots+\alpha_{2s-1}\alpha_{2s}+a_1\alpha_1+\cdots+a_{2s}\alpha_{2s}}$ is bent on $\mathbb{Z}_2^{2s}$.*

**Proof:** (i)–(v) can be easily checked because the groups there are only of orders 2 and 4. The function in (vi) is the well-known Maiorana-McFarland bent function [11]. □

Let $W_1$ and $W_2$ be two finite abelian groups. If $f_1$ is bent on $W_1$ and $f_2$ is bent on $W_2$, then $f_1 \cdot f_2$ is bent on $W_1 \times W_2$ [6]. Another obvious fact is that any function $f : \{0\} \to S^1$ is bent on $\{0\}$. Using these two facts and Lemma 2.4, we conclude that if $W$ is an abelian 2-group such that $|W| \leq 2^m$ and $\exp W \leq 4$, there are many ways to choose functions $\alpha_1, \ldots, \alpha_m : W \to \mathbb{Z}_2$ such that the function (2.17) is bent on $W$ for all $(a_1, \ldots, a_m) \in \mathbb{Z}_2^m$. For each such $W$ and each such choice of $\alpha_1, \ldots, \alpha_m$, we have a semi-regular RDS of $GR(4, m) \times W$ relative to $2GR(4, m) \times \{0\}$ by Corollary 2.3. The construction given here generalizes the one in [2].

## 3. A generalized construction of RDS using local rings

Let $R$ be a finite ring with identity. A character $\chi$ of $(R, +)$ is called nondegenerate if $\ker \chi$ does not contain any nonzero left ideal of $R$. (In the definition of a nondegenerate character, the words "left ideal" can be replaced by "right ideal".) If $\chi$ is a nondegenerate character of $R$, then $\chi(a\cdot)$ gives all the additive characters of $R$ as $a$ runs over $R$ and the same is true for $\chi(\cdot a)$. For any subset $S$ of a ring $R$, the left and right annihilators of $S$ are

$$l(S) = \{x \in R : xs = 0 \text{ for all } s \in S\}, \tag{3.1}$$

$$r(S) = \{x \in R : sx = 0 \text{ for all } s \in S\}. \tag{3.2}$$

The rings used for our construction of RDS are finite local rings with a nondegenerate character. (Cf. [6] for the use of such rings for constructions of bent functions and partial

difference sets.) In the following proposition, we list some characterizations and properties of such rings without proof. (When the ring is commutative, the proof of Proposition 3.1 can be found in [6]. The proof in the noncommutative case is similar.)

**Proposition 3.1** *Let $R$ be a finite ring with identity. Then the following are equivalent.*

(i) *$R$ is local and has a nondegenerate character.*
(ii) *$R$ is local and for any left ideal $L$ and right ideal $J$ of $R$, $l(r(L)) = L$, $r(l(J)) = J$. Equivalently, $R$ is local and quasi-Frobenius.*
(iii) *$R$ has a unique (nonzero) minimal left ideal.*
(iv) *$R$ has a unique (nonzero) minimal right ideal.*

*Assume that one of* (i)–(iv) *is satisfied, then the minimal left ideal and the minimal right ideal of $R$ coincide; they are $r(M) = l(M)$, where $M$ is the unique maximal ideal of $R$. Furthermore, for any left ideal $L$ and right ideal $J$ of $R$, $R/r(L) \cong L$ and $R/l(J) \cong J$ as abelian groups.*

**Theorem 3.2** *Let $R$ be a finite local ring with a nondegenerate character $\chi$. Let $M$ be the unique maximal ideal of $R$, $A$ a system of coset representatives of $R/M$, $B$ a system of coset representatives of $M/r(M)$, and $f : A \to R\backslash M$ any function. For each $a \in A$, define*

$$D_a = \{(au + b(f(a) + u), u) : u \in M, b \in B\} \subset M \times M. \tag{3.3}$$

*Then we have the following conclusions.*

(i) *For each $a \in A$ and each character $\lambda$ of $M \times M$,*

$$|\lambda(D_a)| = \begin{cases} \frac{|M|^2}{|r(M)|}, & \text{if } \lambda \text{ is principal,} \\ 0, & \text{if } \lambda \text{ is principal on } r(M) \times \{0\} \text{ but not on } M \times M, \\ 0 \text{ or } |M|, & \text{if } \lambda \text{ is not principal on } r(M) \times \{0\}. \end{cases} \tag{3.4}$$

*Furthermore, if $\lambda$ is not principal on $r(M) \times \{0\}$, there is exactly one $a \in A$ such that $|\lambda(D_a)| = |M|$. In the terminology of* [3, 7], *$\{D_a : a \in A\}$ form a $(|M|^2/|r(M)|, |M|, |r(M)|)$ building set of $M \times M$ relative to $r(M) \times \{0\}$.*

(ii) *Let $G \supset M \times M$ be any group such that $[G : M \times M] = |r(M)|$ and $M \times M$ is contained in the center of $G$. Then for any system of coset representatives $\{g_a : a \in A\}$ of $G/M \times M$, $\bigcup_{a \in A}(g_a + D_a)$ is a semi-regular RDS of $G$ relative to $r(M) \times \{0\}$.*

**Proof:** (ii) is the well known construction of semi-regular RDS from building sets [3, 7]. We only have to prove (i). Let $\lambda$ be a character of $M \times M$ and $a \in A$. Then $\lambda = \chi(\alpha \cdot) \times \chi(\beta \cdot)$ where $\chi$ is a nondegenerate character of $R$ and $\alpha, \beta \in R$.

*Case 1.* $\lambda$ is principal. Then

$$|\lambda(D_a)| = |D_a| = \frac{|M|^2}{|r(M)|}. \tag{3.5}$$

*Case 2.* $\lambda$ is principal on $r(M)\times\{0\}$ but not principal on $M\times M$. Then $\alpha\in M$. If $\alpha\notin r(M)$, we have

$$\begin{aligned}\lambda(D_a) &= \sum_{u\in M}\chi(\alpha a u)\chi(\beta u)\sum_{b\in B}\chi(\alpha b(f(a)+u))\\ &= 0.\end{aligned} \tag{3.6}$$

(Note that $\sum_{b\in B}\chi(\alpha b(f(a)+u))=0$ since $B(f(a)+u)$ is a system of coset representatives of $M/r(M)$ and $\chi(\alpha\cdot)$ is a nonprincipal character of $M/r(M)$.) If $\alpha\in r(M)$, then $\beta\notin r(M)$ since $\lambda$ is nonprincipal on $M\times M$. Then we have

$$\lambda(D_a) = |B|\sum_{u\in M}\chi(\beta u) = 0. \tag{3.7}$$

*Case 3.* $\lambda$ is not principal on $r(M)\times\{0\}$. Then $\alpha\in R\backslash M$. We have

$$\lambda(D_a) = \sum_{b\in B}\chi(\alpha b f(a))\sum_{u\in M}\chi((\alpha(a+b)+\beta)u). \tag{3.8}$$

If $a\not\equiv -\beta/\alpha \pmod M$, the inner sum in (3.8) is 0 for all $b\in B$, since $\alpha(a+b)+\beta\notin r(M)$. If $a\equiv -\beta/\alpha \pmod M$, there is a unique $b_0\in B$ such that $b_0\equiv -a-\beta/\alpha \pmod{r(M)}$, and

$$\lambda(D_a) = \chi\big(\alpha b_0 f(a)\big)|M|. \tag{3.9}$$

Therefore

$$|\lambda(D_a)| = \begin{cases}0, & \text{if } a\not\equiv -\beta/\alpha \pmod M,\\ |M|, & \text{if } a\equiv -\beta/\alpha \pmod M.\end{cases} \tag{3.10}$$

The proof of (i) is now completed. □

When $R$ is a chain ring, i.e., a finite commutative principal ideal local ring, the construction in Theorem 3.2 coincides with the construction by Ma and Schmidt [8]. However, the category of finite rings with a unique minimal left ideal is much larger than the category of chain rings. We give some examples of finite rings with a unique minimal left ideal without proofs. In these examples, the rings are not chain rings in general.

**Example 3.3** Let $R$ be a finite ring with a unique minimal left ideal $L$ and let $n_1,\dots,n_k>1$ be integers. Then

$$\mathcal{R} = R[X_1,\dots,X_k]\big/\big(X_1^{n_1},\dots,X_k^{n_k}\big) \tag{3.11}$$

is a finite ring with a unique minimal left ideal $L\cdot\bar{X}_1^{n_1-1}\cdots\bar{X}_k^{n_k-1}$, where $\bar{X}_i$ is the image of $X_i$ in $\mathcal{R}$.

**Example 3.4** Let $R$ be a finite ring with a unique minimal left ideal $L$. Let $\phi \in \mathrm{Aut}(R)$. Then

$$\mathcal{R} = \left\{ \begin{bmatrix} a & b \\ 0 & \phi(a) \end{bmatrix} : a, b \in R \right\} \tag{3.12}$$

is a finite ring with a unique minimal left ideal

$$\mathcal{L} = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} : b \in L \right\}. \tag{3.13}$$

**Example 3.5** Let $R$ be a finite ring with a unique minimal left ideal $L$. Since $R$ is local, $\mathrm{char}(R) = p^k$ for some prime $p$. Let $G$ be any finite $p$-group. Then $R[G]$ is a finite ring with a unique minimal left ideal $L \cdot \sum_{g \in G} g$.

## References


1. S. Boztaş, R. Hammons, and P.V. Kumar, "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inform. Theory* **38** (1992), 1101–1113.
2. Y. Chen, D.K. Ray-Chaudhuri, and Q. Xiang, "Constructions of partial difference sets and relative difference sets using Galois rings II," *J. Combin. Theory, Ser A* **76** (1996), 179–196
3. J.A. Davis and J. Jedwab, "A unifying construction for difference sets," *J. Combin. Theory, Ser A* **80** (1997), 13–78.
4. L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover, New York, 1958.
5. A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory* **40** (1994), 301–319.
6. X. Hou, "Bent functions, partial difference sets, and quasi-Frobenius local rings," *Designs, Codes and Cryptogor.*, **20** (2000), 251–268.
7. X. Hou and S.K. Sehgal, "An extension of building sets," *J. Combin. Designs* **8** (2000), 50–57.
8. S.L. Ma and B. Schmidt, "Relative $(p^a, p^b, p^a, p^{a-b})$-difference sets: A unified exponent bound and a local ring construction," preprint.
9. B.R. McDonald, *Finite Rings with Identity*, Dekker, New York, (1974).
10. A. Pott, "A survey on relative difference sets," in *Groups, Difference Sets, and the Monster*, K.T. Arasu et al. (eds.), de Gruyter, Berlin, 1996, pp. 195–232.
11. O.S. Rothaus, "On "bent" functions," *J. Combin. Theory, Ser A* **20** (1976), 300–305.
12. K. Yang, T. Helleseth, P.V. Kumar, and A.G. Shanbhag, "On the weight hierarchy of Kerdock codes over $\mathbb{Z}_4$," *IEEE Trans. Inform. Theory* **42** (1996), 1587–1593.