Constructions of Semi-regular Relative Difference Sets[1]

Ka Hin Leung, San Ling, and Siu Lun Ma

Department of Mathematics, National University of Singapore, Singapore 117543
E-mail: matlkh@nus.edu.sg, matlings@nus.edu.sg, matmasl@nus.edu.sg

J. A. Davis, J. Jedwab, and M. Mowbray (1998, *Des. Codes Cryptogr.* **13**, 131–146) gave two new constructions for semi-regular relative difference sets (RDSs). They asked if the two constructions could be unified. In this paper, we show that the two constructions are closely related. In fact, the second construction should be viewed as an extension of the first. Furthermore, we generalize the second construction to obtain new RDSs.

1. INTRODUCTION

Let G be a group of order mu and U a normal subgroup of G of order u. A k element subset R of G is called an (m, u, k, λ)-*relative difference set* in G relative to U if the expressions gh^{-1}, $g, h \in R$ and $g \neq h$, represent each element in $G \backslash U$ exactly λ times and do not represent any element in $U \backslash \{1\}$. For reference on relative difference sets, we refer the reader to a survey by Pott [8].

We call an (m, u, k, λ)-*relative difference set* R semi-regular if $k = u\lambda$. In the case mu is a power of a prime, i.e., the order of the group involved is a prime power there are many known families of semi-regular difference sets. For reference, we refer the reader to [7, Chap. 4]. However, semi-regular difference sets in groups of non-prime power order are very rare. Pott remarked in his book [7] that the only known semi-regular RDS with mu not a prime-power were $(m, 2, m, m/2)$-difference sets. It is also known that the existence of $(m, 2, m, m/2)$-RDS is related to the existence of a certain Hadamard difference set. For further details, refer to [7, Chap. 2]. In [2], Davis *et al.* give two new

[1] The first and the third authors are partially supported by NUS Research Grant, Project RP 3982723; and the second author is partially supported by NSTB/MOE Grant RP 960668/M.

constructions of semi-regular relative difference sets with $u > 2$ and mu not a prime-power. In their first construction, m is not a 2-power but u can be any 2-power. Whereas in the second construction, the forbidden subgroup has order 3. At the end of the paper, they ask if the two constructions can be unified. The answer would be clearer if the second construction can be modified to obtain a $(2^p(2^p-1)^{2a}, 2^{p-i}, 2^p(2^p-1)^{2a}, 2^i(2^p-1)^{2a})$-semi-regular RDS in $\mathbb{Z}_{(2^p-1)^{2a}}^2 \times \mathbb{Z}_{2^p}^2$ relative to a subgroup isomorphic to $\mathbb{Z}_{2^p}$ in the case where $2^p - 1$ is a prime. In this paper, we show that such a modification is possible and thus obtain many semi-regular difference sets with new parameters. Our construction is actually inductive in nature and the first step is based on the first construction in [2]. With a slight variation, it also allows us to recover the second construction in [2] as well.

Not only are we able to construct semi-regular difference sets with new parameters, but also obtain new semi-regular difference sets with old parameters. Note that all $(2^{2a}3, 3, 2^{2a}3, 2^{2a})$-RDSs constructed in [2, Theorem 4.1] are contained in a group isomorphic to $\mathbb{Z}_{2^a}^2 \times \mathbb{Z}_3^2$. We may ask if it is possible to construct a $(2^{2a}3, 3, 2^{2a}3, 2^{2a})$-RDS in a group not isomorphic to $\mathbb{Z}_{2^a}^2 \times \mathbb{Z}_3^2$, i.e., the 2-Sylow subgroup is not ismorphic to $\mathbb{Z}_{2^a}^2$. Indeed, we shall show that the 2-Sylow subgroup can be isomorphic to $\mathbb{Z}_{2^{t+1}}^{2l'} \times \mathbb{Z}_{2^t}^{2l-2l'}$ where t, l, l' are nonnegative integers with $a = tl + l'$ and $l' < l$. The key is to observe that in [2, Theorem 4.1], the 2-Sylow subgroup of G can be viewed as the additive group, $\mathbb{Z}_{2^a} \times \mathbb{Z}_{2^a}$. However, $\mathbb{Z}_{2^a} \times \mathbb{Z}_{2^a}$ may be viewed as the direct product of two copies of the local ring $\mathbb{Z}_{2^a}$. Thus, we may try to replace $\mathbb{Z}_{2^a}$ by a finite chain ring of the same order.

2. THE CONSTRUCTION

To facilitate the study of relative difference sets in a group G, we often make use of the group ring $\mathbb{Z}[G]$. Throughout this article, we identify a subset of a group with its corresponding element in the group ring. A subset E of G is an (m, u, k, λ)-relative difference set relative to a normal subgroup U if and only if

$$EE^{(-1)} = k + \lambda(G - U).$$

When G is abelian, we often apply character sums to determine if a set E is an RDS in G. In [2], Theorem 3.3 and Theorem 4.1 are proved by using character sums. Our construction is motivated by our attempt to find algebraic proofs for the two constructions given in [2]. As it turns out, the algebraic proofs shed light on what the "correct" construction should be.

Finite local principal chain rings have often been used in the construction of various types of difference sets. In [1, 3–5, 9], the difference sets constructed are actually the additive groups of finite chain rings.

Let p be a prime. Given any positive integers n, l with $l < n$, there exist integers t, l' such that $n = tl + l'$ and $l' < l$. By [6, Theorem XVII.5], the ring $R = \mathbb{Z}_{p^{t+1}}[X]/(X^l - p, p^t X^{l'})$ is a local principal ideal ring. Let π denote the element $X + (X^l - p, p^t X^{l'})$ in R. Obviously, (π) is the maximal ideal of R. For convenience, we denote (π) by $\mathfrak{m}$. Clearly, $R/\mathfrak{m} \cong \mathbb{F}_p$. Moreover, by [6, Theorem XVII.5], the nilpotence of $\mathfrak{m}$ is $l' + tl = n$. Hence, $\pi^{n-1} \neq 0$ and $\pi^n = 0$. By [6, Lemma XVII.4 (c) and (d)], we conclude that as an additive group, $R \cong \mathbb{Z}_{p^{t+1}}^{l'} \times \mathbb{Z}_{p^t}^{l-l'}$. Note that R has p^n elements.

From now on, we assume R, $\mathfrak{m}$, and π as defined above. Writing $\oplus$ for the ring addition in R, we then have

$$R = \{b_0 \oplus b_1 \pi \oplus \cdots \oplus b_{n-1} \pi^{n-1} : b_i \in \{0, 1, \ldots, p-1\}\}.$$

We also define $R' = \{b_0 \oplus b_1 \pi \oplus \cdots \oplus b_{n-2} \pi^{n-2} : b_i \in \{0, 1, \ldots, p-1\}\}$ if $n \geq 2$ and $R' = \{0\}$ when $n = 1$.

Let $K = \{(\alpha, \beta) : \alpha, \beta \in R\}$, with a multiplicative group operation given by

$$(\alpha, \beta)(\alpha', \beta') = (\alpha \oplus \alpha', \beta \oplus \beta').$$

There is a natural action of the additive group of R on K. For $x = (\alpha, \beta) \in K$ and $r \in R$, we use the notation x^r to denote the element $(r\alpha, r\beta)$ of K. It is clear that this notation is consistent with the multiplication defined on K. Moreover, we use $\langle\langle x \rangle\rangle$ to denote the set $\{x^r : r \in R\}$, which is the orbit of x under the action of R.

The proof of the following lemma is straightforward, so we omit it.

LEMMA 2.1. (i) *For any $x \in K$, $\langle\langle x \rangle\rangle$ is a subgroup of K.*

(ii) *For $x \in K$ and $r, s \in R$, if $r \in (s)$, then $\langle\langle x^r \rangle\rangle \subseteq \langle\langle x^s \rangle\rangle$.*

(iii) *For $x \in K$, $\langle\langle x \rangle\rangle \supset \langle x \rangle$ and $\langle\langle x^{\pi^{n-1}} \rangle\rangle = \langle x^{\pi^{n-1}} \rangle$. Here $\langle x \rangle$ denotes the subgroup generated by x in K.*

Remark. In view of Lemma 2.1 (iii), we often write $\langle x^{\pi^{n-1}} \rangle$ instead of $\langle\langle x^{\pi^{n-1}} \rangle\rangle$.

For $0 \leq i \leq p$, we define elements x_i, y_i of K as

$$x_i = \begin{cases} (1, i) & \text{if } i \neq p \\ (0, 1) & \text{if } i = p, \end{cases} \quad \text{and} \quad y_i = \begin{cases} (0, 1) & \text{if } i \neq p \\ (1, 0) & \text{if } i = p. \end{cases}$$

For $0 \leq i \leq p$ and $k \in R'$, we use $I_{i,k}$ to denote the subgroup $\langle\langle x_i y_i^{\pi k} \rangle\rangle$. When expressed as elements in $R \times R$, $x_i y_i^{\pi k} = (1, i + \pi k)$ when $i < p$ and

$x_p y_p^{\pi k} = (\pi k, 1)$. Hence,

$$\langle\langle x_i y_i^{\pi k}\rangle\rangle = \begin{cases} \{r(1, i + \pi k) : r \in R\} & \text{when } i < p, \\ \{r(\pi k, 1) : r \in R\} & \text{when } i = p. \end{cases}$$

It is easy to see that $I_{i,k}$ has p^n elements. Observe that $y_i^{\pi^{n-1}} = (0, \pi^{n-1}) \neq (0, 0)$ when $i \neq p$ and $y_p^{\pi^{n-1}} = (\pi^{n-1}, 0) \neq (0, 0)$. However, $(y_i^{\pi^{n-1}})^p = (0, p\pi^{n-1}) = (0, 0)$ and $(y_p^{\pi^{n-1}})^p = (p\pi^{n-1}, 0) = (0, 0)$. Hence $\langle y_i^{\pi^{n-1}}\rangle$ is a cyclic subgroup of order p.

Remark. When $n = 1$, R is none other than the finite field $\mathbb{F}_p$, $R \times R$ is a two-dimensional vector space over $\mathbb{F}_p$, and the $I_{i,k}$ are lines in $\mathbb{F}_p^2$ going through the origin. When $n > 1$, R is no longer a finite field, but $I_{i,k}$ can still be regarded as rank 1 free R-submodules of $R \times R$.

From now on, we assume $p = 2$ or p is a Mersenne prime with $p = 2^a - 1$. It turns out that K is not the group where in which we shall construct our relative difference sets. Instead we shall construct semi-regular relative difference sets in $K \times H$ relative to U where

$$H = \begin{cases} \mathbb{Z}_4^a & \text{if } p = 2^a - 1 \\ \mathbb{Z}_3^2 & \text{if } p = 2, \end{cases}$$

and $U \subset H$ is a subgroup isomorphic to $\mathbb{Z}_2^a$ if $p = 2^a - 1$, and isomorphic to $\mathbb{Z}_3$ if $p = 2$. From now on, H and U are fixed throughout the paper.

Remark. It will be shortly seen that U may be identified with the additive group of the finite field $\mathbb{F}_{p+1}$.

The second ingredient for our construction involves subsets in $K \times U$ that satisfy a certain condition. In the case where $p = 2^a - 1$ is a Mersenne prime, Davis *et al.* [2, Lemma 3.1] found a set S in the group $\mathbb{Z}_p \times \mathbb{Z}_2^a$ such that $SS^{(-1)} = \mathbb{Z}_p \times \mathbb{Z}_2^a - \mathbb{Z}_p - \mathbb{Z}_2^a + (p + 1)$. This set turns out to be crucial in our construction as well. Here, we give another view on how S is found.

Actually, such an S exists as long as $p + 1$ is a prime power. In other words, S exists even in the case when $p = 2$. Note that when $p + 1$ is a prime power, the finite field $\mathbb{F}_{p+1}$ exists. Consider the ring $W = \mathbb{F}_{p+1}[X]/(X^2) = \mathbb{F}_{p+1} + \mathbb{F}_{p+1}\gamma$, where $\gamma = X + (X^2)$. Note that $\gamma^2 = 0$. Let W^* be the group of units in W. Clearly,

$$W^* = \{c + b\gamma : c \neq 0, b \in \mathbb{F}_{p+1}\} = \mathbb{F}_{p+1}^* \cdot \{1 + b\gamma : b \in \mathbb{F}_{p+1}\}.$$

For convenience, we define $U' = \{1 + b\gamma : b \in \mathbb{F}_{p+1}\}$. Clearly, U' is a subgroup of order $p+1$. Hence $U' \cong \mathbb{Z}_3$ if $p = 2$. If $p + 1 = 2^a$, then for any $b \in \mathbb{F}_{p+1}$, $(1 + b\gamma)^{-1} = (1 + b\gamma)$ as $\mathrm{char}\mathbb{F}_{p+1} = 2$ and $\gamma^2 = 0$. Hence, $U' \cong \mathbb{Z}_2^a$ when $p \neq 2$. On the other hand, it is well known that $\mathbb{F}_{p+1}^*$ is a cyclic group of order p. Hence, W^* is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_2^a$ when $p \neq 2$ and $W^* \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ when $p = 2$.

Let S' be the set $\{\alpha(1 + \alpha^{-1}\gamma) : \alpha \in \mathbb{F}_{p+1}^*\}$,

$$S'S'^{(-1)} = \sum_{\alpha \in \mathbb{F}_{p+1}^*} \sum_{\beta \in \mathbb{F}_{p+1}^*} \alpha\beta^{-1}(1 + \alpha^{-1}\gamma)(1 - \beta^{-1}\gamma)$$

$$= \sum_{\alpha \in \mathbb{F}_{p+1}^*} \sum_{\beta \in \mathbb{F}_{p+1}^*} \alpha\beta^{-1}(1 - (\alpha^{-1} - \beta^{-1})\gamma).$$

Let $t = \alpha\beta^{-1}$. Then $(\alpha^{-1} - \beta^{-1})\gamma = \alpha^{-1}(1 - t)\gamma$. Hence,

$$S'S'^{(-1)} = \sum_{t \in \mathbb{F}_{p+1}^*} \sum_{\alpha \in \mathbb{F}_{p+1}^*} t(1 - \alpha^{-1}(1 - t)\gamma).$$

When $t = 1$, $\sum_{\alpha \in \mathbb{F}_{p+1}^*} t[1 - \alpha^{-1}(1 - t)\gamma] = p$. When $t \neq 1$, $\sum_{\alpha \in \mathbb{F}_{p+1}^*} t[1 - \alpha^{-1}(1 - t)\gamma] = tU' - t$. Hence, we obtain

$$S'S'^{(-1)} = \mathbb{F}_{p+1}^* U' - U' - \mathbb{F}_{p+1}^* + (p + 1).$$

Observe that S' does not contain the identity. However, if we choose $d \in S'$ and set $S = d^{-1}S'$, then S contains the identity and

$$SS^{(-1)} = \mathbb{F}_{p+1}^* U' - U' - \mathbb{F}_{p+1}^* + (p + 1).$$

Furthermore, as $\mathbb{F}_{p+1}^*$ is a group of order p, $(p - \mathbb{F}_{p+1}^*)\mathbb{F}_{p+1}^* = 0$. Therefore,

$$(p - \mathbb{F}_{p+1}^*)SS^{(-1)} = (p - \mathbb{F}_{p+1}^*)(p + 1 - U').$$

Observe that for each $\alpha \in \mathbb{F}_{p+1}^*$, there exists exactly one element in $S \cap \alpha U'$. Therefore, if we let y be a generator of $\mathbb{F}_{p+1}^*$, then for each $j = 0, \ldots, p-1$, there exist $u_0, u_1, \ldots, u_{p-1}$ in U' such that $y^j u_j \in S$. Thus, $S = \{u_0, u_1 y, \ldots, u_{p-1} y^{p-1}\}$. Recall that $y_i^{\pi^{n-1}}$ is an element of order p and $U \cong U'$. After identifying y and U' with $y_i^{\pi^{n-1}}$ and U respectively, we rename S as A_i and we obtain the following result.

LEMMA 2.2. *Let U and $y_i^{\pi^{n-1}}$ be as defined above for $i = 0, \ldots, p$. There is an ordering $u_0, u_1, \ldots, u_{p-1}$ of the elements of U, with $u_0 = 1$, such that the subset*

$$A_i = \{u_0, u_1 y_i^{\pi^{n-1}}, \ldots, u_{p-1} y_i^{\pi^{n-1}(p-1)}\} \subset \langle y_i^{\pi^{n-1}} \rangle \times U$$

satisfies

$$A_i A_i^{(-1)} = \langle y_i^{\pi^{n-1}} \rangle \times U - \langle y_i^{\pi^{n-1}} \rangle - U + (p+1) \tag{1}$$

and

$$(p - \langle y_i^{\pi^{n-1}} \rangle) A_i A_i^{(-1)} = (p - \langle y_i^{\pi^{n-1}} \rangle)(p + 1 - U). \tag{2}$$

In the above lemma, we assume $u_0, \ldots, u_{p-1} \in U$ and they will be fixed from now on. Recall that

$$R = \{b_0 \oplus b_1 \pi \oplus \cdots \oplus b_{n-1} \pi^{n-1} : b_i \in \{0, 1, \ldots, p-1\}\}$$

and $R' = \{b_0 \oplus b_1 \pi \oplus \cdots \oplus b_{n-2} \pi^{n-2} : b_i \in \{0, 1, \ldots, p-1\}\}$ if $n \geq 2$ while $R' = \{0\}$ when $n = 1$. We define u_k for all $k \in R'$ as follows. For $k = k_0 \oplus k_1 \pi \oplus \cdots \oplus k_{n-2} \pi^{n-2} \in R'$, with $k_i \in \{0, 1, \ldots, p-1\}$, we define

$$u_k = u_{k_0} u_{k_1} \cdots u_{k_{n-2}} \in U.$$

The last ingredient needed for our construction is a $(p+1, p+1, p+1, 1)$-relative difference set of H relative to U. As is well known, such a relative difference set of H relative to U exists. For a reference, see Pott [8]. Let D be a $(p+1, p+1, p+1, 1)$-relative difference set of H relative to U. We label the elements of D as $d_0, d_1, \ldots, d_p$. In particular, we may identify D with $\sum_{i=0}^{p} d_i$ and hence

$$DD^{(-1)} = (H - U) + (p+1).$$

Before we write down our construction explicitly, we define for $i = 0, \ldots, p$,

$$D_i = \bigcup_{k \in R'} y_i^k u_k I_{i,k} A_i.$$

The main result of this paper is:

THEOREM 2.3. *The subset* $\bigcup_{i=0}^{p} D_i d_i$ *is a semi-regular* $((p+1)p^{2n}, p+1, (p+1)p^{2n}, p^{2n})$*-relative difference set in* $K \times H$ *relative to* U, *with*

$$\left(\sum_{i=0}^{p} D_i d_i\right)\left(\sum_{i=0}^{p} D_i d_i\right)^{(-1)} = p^{2n}(KH - U) + p^{2n}(p+1).$$

Before we proceed with the proof, we first give some examples to illustrate our construction. We only consider the case when $p = 3$. Now, let $H = \langle u \rangle \times$

$\langle v\rangle$ where u, v are of order 4 and $U = \langle u^2, v^2\rangle$. Let $\langle z\rangle$ be a group of order 3. It is known that there exists a $(4, 4, 4, 1)$ RDS $\{d_0, d_1, d_2, d_3\}$ in H relative to U. Moreover, in $\langle z\rangle \times U$, if we set $S = \{1, zu^2, z^2v^2\}$, it is straightforward to check that

$$SS^{(-1)} = \langle z\rangle \times U - \langle z\rangle - U + 4.$$

EXAMPLE 1. $p = 3$ and $n = 1$. In this case, $R \times R = K$ is a 3-group of order 9 and $R' = \{0\}$. We write $K = \langle x\rangle \times \langle y\rangle$ where x, y are of order 3. In this case, $I_{0,0} = \langle x\rangle$, $I_{1,0} = \langle xy\rangle$, $I_{2,0} = \langle xy^2\rangle$ and $I_{3,0} = \langle y\rangle$. Recall that $u_0 = 1$.

Using S constructed above, we see that $A_0 = A_1 = A_2 = \{1, yu^2, y^2v^2\}$ and $A_3 = \{1, xu^2, x^2v^2\}$. Hence, the RDS we construct is

$$\langle x\rangle\{1, yu^2, y^2v^2\}d_0 \cup \langle xy\rangle\{1, yu^2, y^2v^2\}d_1 \cup \langle xy^2\rangle\{1, yu^2, y^2v^2\}d_2$$

$$\cup \langle y\rangle\{1, xu^2, x^2v^2\}d_3.$$

EXAMPLE 2. $p = 3$; $n = 2$ and $l = 1$. Hence, $l' = 0$ and $t = 2$. Thus, $R \cong \mathbb{Z}_9$ and $K = \langle x\rangle \times \langle y\rangle$ where x, y are of order 9. In this case, $R' = \{0, 1, 2\}$. Consequently,

$$\begin{aligned}
I_{0,0} &= \langle x\rangle, & I_{0,1} &= \langle xy^3\rangle, & I_{0,2} &= \langle xy^6\rangle,\\
I_{1,0} &= \langle xy\rangle, & I_{1,1} &= \langle xy^4\rangle, & I_{1,2} &= \langle xy^7\rangle,\\
I_{2,0} &= \langle xy^2\rangle, & I_{2,1} &= \langle xy^5\rangle, & I_{2,2} &= \langle xy^8\rangle,\\
I_{3,0} &= \langle y\rangle, & I_{3,1} &= \langle x^3y\rangle, & I_{3,2} &= \langle x^6y\rangle.
\end{aligned}$$

Now, $A_0 = A_1 = A_2 = \{1, y^3u^2, y^6v^2\}$ and $A_3 = \{1, x^3u^2, x^6v^2\}$. In particular, $u_0 = 1$, $u_1 = u^2$, and $u_2 = v^2$. Thus, the RDS that we get is

$$d_0A_0(\langle x\rangle \cup yu^2\langle xy^3\rangle \cup y^2v^2\langle xy^6\rangle) \cup d_1A_1(\langle xy\rangle \cup yu^2\langle xy^4\rangle \cup y^2v^2\langle xy^7\rangle) \cup$$

$$d_2A_2(\langle xy^2\rangle \cup yu^2\langle xy^5\rangle \cup y^2v^2\langle xy^8\rangle) \cup d_3A_3(\langle y\rangle \cup xu^2\langle x^3y\rangle \cup x^2v^2\langle x^6y\rangle).$$

As we have observed earlier, when $n = 1$, K is an elementary p-group with $|K| = p^2$ and $R' = \{0\}$. Hence, $I_{i,0} = \langle\langle x_i\rangle\rangle = \langle x_i\rangle$ for $i \neq p$ and $I_{p,0} = \langle\langle y_p\rangle\rangle = \langle y_p\rangle$. If we set $u_0 = 1$, the RDS we get is then $\bigcup_{i=0}^{p} D_i = \bigcup_{i=0}^{p} I_{i,0}A_i = \bigcup_{i=0}^{p}\langle x_i\rangle A_i$. This coincides with the S_i' defined in Theorem 3.3 in [2]. Consequently, the RDS constructed in Theorem 2.3 is the same as the $(2^a(2^a-1)^2, 2^a, 2^a(2^a-1)^2, (2^a-1)^2)$-relative difference set defined in [2].

To get back all the other RDSs constructed in [2, Theorem 3.3], we only need to apply [7, Lemma 2.6].

Observe that, in the construction of R, the only requirement is $l \leq n$, even though when $|R|$ is fixed, $(R, +)$ changes as l varies. For example, when $l = 1$, $l' = 0$, and $t = n$, $R \cong \mathbb{Z}_{p^n}$ as groups, whereas if we take $l = n$, $t = 1$, and $l' = 0$, $R \cong \mathbb{Z}_p^n$ as groups. Therefore, we have quite a number of choices for the additive group structure of R. Thus even in the case $p = 2$, we do get new RDSs compared with those constructed in [2]. Though at this point, our construction does not seem to cover the second construction given in [2], we will see in the last section that with a slight modification to our present construction, we will get back those RDSs constructed in [2]. Furthermore, it will be shown there why the second construction given in [2] cannot be extended to Mersenne primes.

To prove Theorem 2.3, we first observe that

$$\left(\sum_{i=0}^{p} D_i d_i\right)\left(\sum_{i=0}^{p} D_i d_i\right)^{(-1)} = \sum_{0 \leq i \neq j \leq p} D_i D_j^{(-1)} d_i d_j^{-1} + \sum_{i=0}^{p} D_i D_i^{(-1)}. \tag{3}$$

In Section 3, we prove

PROPOSITION 2.4. *Let R and the D_i's be defined as before Theorem 2.3. Then*

$$\sum_{0 \leq i \neq j \leq p} D_i D_j^{(-1)} d_i d_j^{-1} = p^{2n}(KH - KU).$$

After some lemmas in Section 4, we prove in Section 5

PROPOSITION 2.5. *Let R and the D_i's be defined as before Theorem 2.3. Then*

$$\sum_{i=0}^{p} D_i D_i^{(-1)} = p^{2n}(KU - U) + p^{2n}(p + 1).$$

Applying Propositions 2.4 and 2.5 to (3), we obtain

$$\begin{aligned}\left(\sum_{i=0}^{p} D_i d_i\right)\left(\sum_{i=0}^{p} D_i d_i\right)^{(-1)} &= p^{2n}(KH - KU) + p^{2n}(KU - U) + p^{2n}(p + 1) \\ &= p^{2n}(KH - U) + p^{2n}(p + 1),\end{aligned}$$

thus completing the proof of Theorem 2.3.

As shown in [2], it is possible to combine RDSs to obtain new RDSs. Using the new RDSs constructed here, we can then obtain results analogous

to [2, Corollaries 3.10, 4.4]. However, we are not going to discuss it here as that does not shed any new light on the construction of RDSs.

3. PROOF OF PROPOSITION 2.4

We begin this section with a lemma.

LEMMA 3.1. *For $0 \le i, j \le p$ and $k, \ell \in R'$, if $i \ne j$, then $I_{i,k} \cap I_{j,\ell}$ is trivial. Consequently, $I_{i,k} I_{j,\ell} = K$.*

Proof. We assume first that both i and j are different from p. Let $(r, r(i \oplus \pi k)) = (s, s(j \oplus \pi \ell))$ be in the intersection $I_{i,k} \cap I_{j,\ell}$, for some $r, s \in R$. Then, $r = s$ and hence $r((i-j) \oplus \pi(k-\ell)) = 0$.

If $r \ne 0$, write

$$r = r_m \pi^m \oplus r_{m+1} \pi^{m+1} \oplus \cdots, \qquad r_m \ne 0, m \ge 0.$$

Then we have $r_m(i-j) = 0$, which implies that $i = j$. The first statement of the lemma then follows for the case $i \ne p$, $j \ne p$.

Next we suppose $i \ne p$ and $j = p$. In this case, let $(r, r(i \oplus \pi k)) = (s\pi\ell, s)$ be an element in the intersection $I_{i,k} \cap I_{j,\ell}$, for some $r, s \in R$. Then we have $\pi s \ell (i \oplus \pi k) = s$, i.e., $s(\pi\ell(i \oplus \pi k) - 1) = 0$. Since $\pi\ell(i \oplus \pi k) - 1 \notin \mathfrak{m}$, it follows that $s = 0$. This completes the proof of the first statement of the lemma.

The second statement follows immediately from the first by considering cardinality. ∎

Now we consider the term $D_i D_j^{(-1)}$ for $i \ne j$. Recall that by Lemma 3.1, $I_{i,k} I_{j,\ell} = K$ when $i \ne j$. Therefore,

$$\begin{aligned} D_i D_j^{(-1)} &= \left(\sum_{k \in R'} y_i^k u_k I_{i,k} A_i \right) \left(\sum_{\ell \in R'} y_j^{-\ell} u_\ell^{-1} I_{j,\ell} A_j^{(-1)} \right) \\ &= \sum_{k,\ell \in R'} y_i^k y_j^{-\ell} u_k u_\ell^{-1} I_{i,k} I_{j,\ell} A_i A_j^{(-1)} \\ &= \sum_{k,\ell \in R'} y_i^k y_j^{-\ell} u_k u_\ell^{-1} K A_i A_j^{(-1)}. \end{aligned}$$

Since $y_i^k, y_j^{-\ell} \in K$ for all $k, \ell \in R$, $KA_i = K(\sum_{k'=0}^{p-1} u_{k'})$ and $KA_j^{(-1)} = K(\sum_{\ell'=0}^{p-1} u_{\ell'}^{-1})$. Consequently,

$$D_i D_j^{(-1)} = \left(\sum_{k,\ell \in R'} u_k u_\ell^{-1} \right) K \left(\sum_{k'=0}^{p-1} u_{k'} \right) \left(\sum_{\ell'=0}^{p-1} u_{\ell'}^{-1} \right).$$

This shows that $D_i D_j^{(-1)}$ $(i \neq j)$ is independent of i and j. Hence,

$$\sum_{0 \le i \ne j \le p} D_i D_j^{(-1)} d_i d_j^{-1} = \left(\sum_{k,\ell \in R'} u_k u_\ell^{-1} \right) K \left(\sum_{k'=0}^{p-1} u_{k'} \right) \left(\sum_{\ell'=0}^{p-1} u_{\ell'}^{-1} \right)$$

$$\times \left(\sum_{0 \le i \ne j \le p} d_i d_j^{-1} \right)$$

$$= \left(\sum_{k,\ell \in R'} u_k u_\ell^{-1} \right) K \left(\sum_{k',\ell'=0}^{p-1} u_{k'} u_{\ell'}^{-1} \right) (H - U)$$

$$= p^{2n} K(H - U),$$

since $u_k, u_\ell, u_{k'}, u_{\ell'} \in U$ and, for any $h \in U$, $h(H - U) = H - U$ as $H - U$ is a union of cosets of U. This completes the proof of Proposition 2.4. ■

4. SOME PRELIMINARY LEMMAS

We begin this section with a few lemmas.

Let $\bar{R}$ denote the quotient ring $R/\mathfrak{m}^{n-1}$ and let $\bar{K}$ be the analogue of K, with $\bar{R}$ playing the role of R in its definition. Let $\rho: K \times H \to \bar{K} \times H$ be the map that acts as the identity map on H and as the reduction map on K. Let J denote the kernel of ρ. It is easy to see that $J = \langle x_i^{\pi^{n-1}} \rangle \langle y_i^{\pi^{n-1}} \rangle$. In the case $n = 1$, we have $J = K$. We also let $\overline{x_i}, \overline{y_i}, \bar{I}_{i,k}, \overline{A_i}, \overline{D_i}$ be the analogues of $x_i, y_i, I_{i,k}, A_i, D_i$, respectively, with $\bar{R}$ replacing R. Note that we may assume $\overline{x_i} = \rho(x_i)$, $\overline{y_i} = \rho(y_i)$, and $\bar{I}_{i,k} = \rho(I_{i,k})$. This will be assumed in this section and Section 5. However, $\overline{D_i} \neq \rho(D_i)$. In fact,

$$\overline{D_i} = \bigcup_{k \in \bar{R}'} \overline{y_i}^k u_k \bar{I}_{i,k} \left(\bigcup_{j=0}^{p-1} \overline{y_i}^{j\pi^{n-2}} u_j \right) = \rho \left(\bigcup_{k \in R'} y_i^k u_k I_{i,k} \right) \neq \rho(D_i).$$

Note also that we have abused our notation in the definition of $\overline{y_i}^{j\pi^{n-2}}$. Strictly speaking, we should replace π^{n-2} by the corresponding element $\bar{\pi}^{n-2}$ in $\bar{R}$.

LEMMA 4.1. *For $k, \ell \in R'$ with $k \neq \ell$, we have $\langle x_i^{\pi^{n-1}} \rangle \subseteq I_{i,k}$ and $J \subseteq I_{i,k} I_{i,\ell}$.*

Proof. Since $x_i y_i^{\pi k} \in I_{i,k}$, $x_i^{\pi^{n-1}} = (x_i y_i^{\pi k})^{\pi^{n-1}} \in I_{i,k} \subseteq I_{i,k} I_{i,\ell}$. Clearly, $y_i^{\pi(k-\ell)} \in I_{i,k} I_{i,\ell}$. Since $k \neq \ell$, it follows that $y_i^{\pi^{n-1}} \in \langle \langle y_i^{\pi(k-\ell)} \rangle \rangle \subseteq I_{i,k} I_{i,\ell}$ by Lemma 2.1 (ii). Hence $J \subseteq I_{i,k} I_{i,\ell}$. ■

LEMMA 4.2. *We have the identity*

$$\sum_{k,\ell\in R',k\neq\ell} y_i^k y_i^{-\ell} u_k u_\ell^{-1} I_{i,k} I_{i,\ell} = \rho^{-1}(\overline{D_i}\,\overline{D_i}^{(-1)}) - p^{n-1}\sum_{k\in R'} I_{i,k}\langle y_i^{\pi^{n-1}}\rangle. \tag{4}$$

Proof. Recall that $\overline{y_i} = \rho(y_i)$, $\bar{I}_{i,k} = \rho(I_{i,k})$ and

$$\overline{D_i} = \rho\left(\bigcup_{k\in R'} y_i^k u_k I_{i,k}\right) = \bigcup_{k\in R'} \overline{y_i}^k u_k \bar{I}_{i,k}.$$

We thus have

$$\begin{aligned}\overline{D_i}\,\overline{D_i}^{(-1)} &= \left(\sum_{k\in R'} \overline{y_i}^k u_k \bar{I}_{i,k}\right)\left(\sum_{\ell\in R'} \overline{y_i}^{-\ell} u_\ell^{-1} \bar{I}_{i,\ell}\right)\\ &= \sum_{k,\ell\in R',k\neq\ell} \overline{y_i}^k \overline{y_i}^{-\ell} u_k u_\ell^{-1} \bar{I}_{i,k}\bar{I}_{i,\ell} + \sum_{k\in R'} \bar{I}_{i,k}\bar{I}_{i,k}.\end{aligned} \tag{5}$$

To find $\rho^{-1}(\overline{D_i}\,\overline{D_i}^{(-1)})$, we look at the pre-image of the two sums in the final line of (5).

Since $\rho(\sum_{k\in R'} I_{i,k}) = \sum_{k\in R'} \bar{I}_{i,k}$ and, by Lemma 4.1, $\langle x_i^{\pi^{n-1}}\rangle \subseteq I_{i,k}$, it follows that

$$\rho^{-1}\left(\sum_{k\in R'} \bar{I}_{i,k}\bar{I}_{i,k}\right) = \rho^{-1}\left(p^{n-1}\sum_{k\in R'} \bar{I}_{i,k}\right) = p^{n-1}\sum_{k\in R'} I_{i,k}\langle y_i^{\pi^{n-1}}\rangle. \tag{6}$$

Note also that $\rho\left(\sum_{k,\ell\in R',k\neq\ell} y_i^k y_i^{-\ell} u_k u_\ell^{-1} I_{i,k} I_{i,\ell}\right) = \sum_{k,\ell\in R',k\neq\ell} \overline{y_i}^k \overline{y_i}^{-\ell} u_k u_\ell^{-1} \bar{I}_{i,k}\bar{I}_{i,\ell}$ and by Lemma 4.1, $J \subseteq I_{i,k} I_{i,\ell}$ for $k \neq \ell$. We have

$$\rho^{-1}\left(\sum_{k,\ell\in R',k\neq\ell} \overline{y_i}^k \overline{y_i}^{-\ell} u_k u_\ell^{-1} \bar{I}_{i,k}\bar{I}_{i,\ell}\right) = \sum_{k,\ell\in R',k\neq\ell} y_i^k y_i^{-\ell} u_k u_\ell^{-1} I_{i,k} I_{i,\ell}. \tag{7}$$

As $\rho^{-1}(\overline{D_i}\,\overline{D_i}^{(-1)})$ is the sum of the left hand sides of (7) and (6), the lemma follows. ■

LEMMA 4.3. *We have the identity*

$$\left(\sum_{k\in R'} I_{i,k}\right)(p - \langle y_i^{\pi^{n-1}}\rangle) = p^n\langle x_i^{\pi^{n-1}}\rangle - p^{n-1}J = p^{n-1}\langle x_i^{\pi^{n-1}}\rangle(p - \langle y_i^{\pi^{n-1}}\rangle). \tag{8}$$

Proof. From the definition of $I_{i,k}$, we have

$$\sum_{k\in R'} I_{i,k} = \sum_{k\in R'}\sum_{t\in R} x_i^t y_i^{\pi kt} = \sum_{t\in R} x_i^t \left(\sum_{k\in R'} y_i^{\pi kt}\right) = \sum_{t\in R} x_i^t \langle\langle y_i^{\pi t}\rangle\rangle \frac{p^{n-1}}{|\langle\langle y_i^{\pi t}\rangle\rangle|}.$$

Therefore, the left hand side of (8) is equal to

$$\sum_{t\in R} x_i^t \langle\langle y_i^{\pi t}\rangle\rangle \frac{p^{n-1}}{|\langle\langle y_i^{\pi t}\rangle\rangle|} (p - \langle y_i^{\pi^{n-1}}\rangle)$$

$$= \sum_{t\notin \mathfrak{m}^{n-1}} x_i^t \langle\langle y_i^{\pi t}\rangle\rangle \frac{p^{n-1}}{|\langle\langle y_i^{\pi t}\rangle\rangle|} (p - \langle y_i^{\pi^{n-1}}\rangle)$$

$$+ \sum_{t\in \mathfrak{m}^{n-1}} x_i^t p^{n-1}(p - \langle y_i^{\pi^{n-1}}\rangle).$$

Now, we observe that

$$\sum_{t\in \mathfrak{m}^{n-1}} x_i^t p^{n-1}(p - \langle y_i^{\pi^{n-1}}\rangle) = p^n \langle x_i^{\pi^{n-1}}\rangle - p^{n-1}\langle x_i^{\pi^{n-1}}\rangle\langle y_i^{\pi^{n-1}}\rangle$$

$$= p^n \langle x_i^{\pi^{n-1}}\rangle - p^{n-1} J.$$

When $t\notin \mathfrak{m}^{n-1}$, using Lemma 2.1 (ii), $\langle y_i^{\pi^{n-1}}\rangle$ is a subgroup in $\langle\langle y_i^{\pi t}\rangle\rangle$. It follows therefore that $\sum_{t\notin m^{n-1}} x_i^t \langle\langle y_i^{\pi t}\rangle\rangle (p^{n-1}/|\langle\langle y_i^{\pi t}\rangle\rangle|)(p - \langle y_i^{\pi^{n-1}}\rangle) = 0$.

The proof of the lemma is now complete. ∎

LEMMA 4.4. *We have the identity*

$$\sum_{i=0}^{p} \langle x_i^{\pi^{n-1}}\rangle = J + p.$$

Proof. Since

$$\langle x_i^{\pi^{n-1}}\rangle = \begin{cases} \{(r\pi^{n-1}, ri\pi^{n-1}) : r\in R\} & \text{if } i\neq p \\ \{(0, r\pi^{n-1}) : r\in R\} & \text{if } i = p, \end{cases}$$

it follows that

$$\sum_{i=0}^{p} \langle x_i^{\pi^{n-1}}\rangle = p + \sum_{\alpha,\beta=0}^{p-1} (\alpha\pi^{n-1}, \beta\pi^{n-1}) = J + p. \qquad \blacksquare$$

5. PROOF OF PROPOSITION 2.5

We will now prove Proposition 2.5 by induction on n.

First, we prove Proposition 2.5 when $n = 1$, i.e., $R \cong \mathbb{Z}_p$. Recall that, in this case, $J = K = \langle x_i \rangle \langle y_i \rangle$. Note also that $R' = \{0\}$, so $D_i = I_{i,0} A_i = \langle x_i \rangle A_i$. Therefore,

$$D_i D_i^{(-1)} = I_{i,0} I_{i,0} A_i A_i^{(-1)} = p(KU - K - \langle x_i \rangle U + (p+1)\langle x_i \rangle),$$

using (1).

Invoking Lemma 4.4, it follows that

$$\begin{aligned}
\sum_{i=0}^{p} D_i D_i^{(-1)} &= (p+1)\, p(KU - K) - pU \sum_{i=0}^{p} \langle x_i \rangle + p(p+1) \sum_{i=0}^{p} \langle x_i \rangle \\
&= (p+1)\, p(KU - K) + (p(p+1) - pU)(K + p) \\
&= p^2(KU - K) + p^2(p+1).
\end{aligned}$$

We have thus finished the proof for $n = 1$.

Next, we assume $n > 1$. We note first that by applying Lemmas 4.2 and 4.3,

$$\begin{aligned}
D_i D_i^{(-1)} &= \left(\sum_{k \in R'} y_i^k u_k I_{i,k} A_i \right) \left(\sum_{\ell \in R'} y_i^{-\ell} u_\ell^{-1} I_{i,\ell} A_i^{(-1)} \right) \\
&= \left(\sum_{k,\ell \in R', k \neq \ell} y_i^k y_i^{-\ell} u_k u_\ell^{-1} I_{i,k} I_{i,\ell} + \sum_{k \in R'} I_{i,k} I_{i,k} \right) A_i A_i^{(-1)} \\
&= \left(\rho^{-1}(\overline{D_i}\, \overline{D_i}^{(-1)}) - p^{n-1} \sum_{k \in R'} I_{i,k} \langle y_i^{\pi^{n-1}} \rangle + \sum_{k \in R'} p^n I_{i,k} \right) A_i A_i^{(-1)} \\
&= \rho^{-1}(\overline{D_i}\, \overline{D_i}^{(-1)})\, A_i A_i^{(-1)} + p^{2n-2} \langle x_i^{\pi^{n-1}} \rangle (p - \langle y_i^{\pi^{n-1}} \rangle) A_i A_i^{(-1)}.
\end{aligned}$$

By (2), we obtain

$$\begin{aligned}
\langle x_i^{\pi^{n-1}} \rangle (p - \langle y_i^{\pi^{n-1}} \rangle)\, A_i A_i^{(-1)} &= \langle x_i^{\pi^{n-1}} \rangle (p + 1 - U)(p - \langle y_i^{\pi^{n-1}} \rangle) \\
&= (p + 1 - U)(p \langle x_i^{\pi^{n-1}} \rangle - J).
\end{aligned}$$

By Lemma 4.4 again, we see that

$$\begin{aligned} & p^{2n-2}\textstyle\sum_{i=0}^{p}\langle x_i^{\pi^{n-1}}\rangle(p-\langle y_i^{\pi^{n-1}}\rangle)A_iA_i^{(-1)} \\ &= p^{2n-2}(p+1-U)(p^2-J) \\ &= p^{2n}(p+1)-p^{2n-2}(p+1)J-p^{2n}U+p^{2n-2}JU. \end{aligned} \tag{9}$$

Since the kernel J of $\rho: K\times H\to \bar{K}\times H$ is a $\langle y_i^{\pi^{n-1}}\rangle$ coset, $\rho^{-1}(\overline{D_i}\,\overline{D_i}^{(-1)})$ is also a $\langle y_i^{\pi^{n-1}}\rangle$ coset. From (1), it follows that

$$\begin{aligned} & \rho^{-1}(\overline{D_i}\,\overline{D_i}^{(-1)})\,A_iA_i^{(-1)} \\ &= \rho^{-1}(\overline{D_i}\,\overline{D_i}^{(-1)})(pU-p-U+(p+1)) \\ &= ((p-1)U+1)\rho^{-1}(\overline{D_i}\,\overline{D_i}^{(-1)}). \end{aligned}$$

Recall that $\overline{D_i}$ is the analogue for D_i for the local ring $\bar{R}$. By the inductive hypothesis,

$$\sum_{i=0}^{p}\overline{D_i}\,\overline{D_i}^{(-1)}=p^{2n-2}(\bar{K}U-U)+p^{2n-2}(p+1).$$

Hence, by the definition of J and (1), we obtain

$$\begin{aligned} & \textstyle\sum_{i=0}^{p}A_iA_i^{(-1)}\rho^{-1}(\overline{D_i}\,\overline{D_i}^{(-1)}) \\ &= ((p-1)U+1)(p^{2n-2}(KU-JU)+p^{2n-2}(p+1)J) \\ &= p^{2n}KU-p^{2n-2}JU+p^{2n-2}(p+1)J. \end{aligned} \tag{10}$$

Finally, by adding (9) and (10), we get

$$\sum_{i=0}^{p}D_iD_i^{(-1)}=p^{2n}(KU-U)+p^{2n}(p+1).$$

This completes the proof of Proposition 2.5.

6. TWO MORE GENERAL CONSTRUCTIONS

As we have seen in Section 5, our proof for Proposition 2.5 is inductive. In fact, the construction would have been clearer by using an inductive

argument. However, we feel that it is useful to give an explicit description of the RDSs that we construct, so, we choose to describe the general situation in the last section.

As before, we assume throughout this section that $\{d_0, d_1, \ldots, d_p\}$ is a $(p+1, p+1, p+1, 1)$-RDS in H relative to U. Let $g_k \in U$ for all $k \in R'$ and let $E_i = \bigcup_{k \in R'} y_i^k g_k I_{i,k} A_i$. Observe that in the proof of Proposition 2.4, u_k's do not play any role at all. So, it is easy to see that

$$\sum_{0 \le i \ne j \le p} E_i E_j^{(-1)} d_i d_j^{-1} = p^{2n}(KH - KU).$$

On the other hand, in the proof of Proposition 2.5, the key is to observe that

$$\bigcup_{i=0}^{p} \rho(y_i^k u_k I_{i,k}) = \overline{D_i} \quad \text{and} \quad \sum_{i=0}^{p} \overline{D_i}\,\overline{D_i}^{(-1)} = p^{2n-2}(\bar{K}U - U) + p^{2n-2}(p+1).$$

Therefore, if $\bigcup_{i=0}^{p} \bigcup_{k \in R'} \rho(y_i^k I_{i,k}) g_k d_i$ is an RDS in $\bar{K} \times H$ relative to U, then we can apply the same argument to see that

$$\sum_{i=0}^{p} E_i E_i^{(-1)} = p^{2n}(KU - U) + p^{2n}(p+1).$$

We have thus obtained the following

THEOREM 6.1. *Let $g_k \in U$ for all $k \in R'$. $\bigcup_{i=0}^{p} \bigcup_{k \in R'} y_i^k g_k I_{i,k} A_i d_i$ is a semi-regular $((p+1)p^{2n}, p+1, (p+1)p^{2n}, p^{2n})$-RDS in $K \times H$ relative to U if $\bigcup_{i=0}^{p} \bigcup_{k \in R'} \rho(y_i^k I_{i,k}) g_k d_i$ is an RDS in $\bar{K} \times H$ relative to U.*

Theorem 6.1 gives us more flexibility in constructing RDSs. The whole idea is that once we construct an RDS in $\bar{K} \times H$, we can then lift it to one in $K \times H$. Note that the A_i's depend on the choice of A in Lemma 2.1 and there are many choices for A. For example, we could take a translate of A. So, if we choose a different A each time we lift our RDS, the resulting RDS would be quite different from the one we construct in Section 2. Let us illustrate our idea by considering the following example.

EXAMPLE. Let $R_n = \mathbb{Z}_{2^n}$ and $R_n' = \{0, 1, \ldots, 2^{n-1} - 1\}$. We may assume $R_n \times R_n = \langle x \rangle \cdot \langle z \rangle$. Let H be isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. We assume $H = \langle u, v \rangle$. Let $\{d_0, d_1, d_2\}$ be a $(3,3,3,1)$-RDS in H relative to $U = \langle u \rangle$. We define $x_0 = x, x_1 = z, x_2 = xz, y_0 = z, y_1 = x$ and $y_2 = x$. Let $A_{i,n} = \{1, y_i^{2^{n-1}} u^{2^{n-1}}\}$. (Note that $A_{i,n}$ depends on i and n.) As 3 does not divide 2^{n-1},

$$A_{i,n} A_{i,n}^{(-1)} = \langle y_i^{2^{n-1}} \rangle U - \langle y_i^{2^{n-1}} \rangle - U + 3.$$

Note that $\langle\langle t\rangle\rangle = \langle t\rangle$ for all t in $R_1 \times R_1$. We claim that

$$F_n = \bigcup_{i=0}^{2} \bigcup_{j=0}^{2^{n-1}-1} \langle x_i y_i^{2j}\rangle u^j y_i^j A_{i,n} d_i$$

is an RDS.

When $n = 1$, F_1 is the same as the one we define in Theorem 2.3. Thus, F_1 is an RDS in $R_1 \times R_1 \times H$ relative to U.

Let ρ be as defined before. By Theorem 6.1, F_n is an RDS in $R_n \times R_n \times H$ relative to U if we show that the set $\bigcup_{i=0}^{2} \bigcup_{j=0}^{2^{n-1}-1} \rho(\langle x_i y_i^{2j}\rangle u^j y_i^j)\, d_i$ is an RDS in $R_{n-1} \times R_{n-1} \times H$ relative to U. Clearly,

$$\bigcup_{i=0}^{2} \bigcup_{j=0}^{2^{n-1}-1} \rho(\langle x_i y_i^{2j}\rangle u^j y_i^j)\, d_i = \bigcup_{i=0}^{2} \bigcup_{j=0}^{2^{n-2}-1} \langle \overline{x_i}\, \overline{y_i}^{2j}\rangle u^j \overline{y_i}^j (1 + u^{2^{n-2}} \overline{y_i}^{2^{n-2}})\, d_i = F_{n-1}.$$

By induction, F_{n-1} is an RDS in $R_{n-1} \times R_{n-1} \times H$ relative to U.

We have thus proved F_n is an RDS. Note also that

$$F_n = \bigcup_{i=0}^{2} \bigcup_{j=0}^{2^{n-1}-1} \langle x_i y_i^{2j}\rangle u^j y_i^j (1 + u^{2^{n-1}} y_i^{2^{n-1}})\, d_i = \bigcup_{i=0}^{2} \bigcup_{j=0}^{2^n-1} \langle x_i y_i^{2j}\rangle u^j y_i^j d_i.$$

Remarks. (i) In the above example, our RDS is different from that in [2, Theorem 4.1] even though the parameters are the same.

(ii) The above construction works only when $p = 2$. When $n > 1$, it does not work if we replace 2 by a Mersenne prime p and the $(3, 3, 3, 1)$-RDS by an appropriate RDS. The reason is that the induction step fails as

$$1 + u^{p^{n-2}} \overline{y_i}^{p^{n-2}} + u^{2p^{n-2}} \overline{y_i}^{2p^{n-2}} + \cdots + u^{(p-1)p^{n-2}} \overline{y_i}^{(p-1)p^{n-2}}$$

does not satisfy (1) if $p \neq 2$. This also explains why the second construction in [2] cannot be extended to Mersenne primes.

Next, we describe another modification which gives us the second construction in [2]. For any $k \in R'$, we let $g'_k \in U$ and define

$$E'_i = \bigcup_{k \in R'} y_i^k g'_k I_{i,k} B_i,$$

where each $B_i \subset \langle y_i^{\pi^{n-1}}\rangle \times U$ and

$$B_i B_i^{(-1)} = \langle y_i^{\pi^{n-1}}\rangle U - U - \langle y_i^{\pi^{n-1}}\rangle + (p + 1).$$

THEOREM 6.2. *Let $\eta : K \times H \to H$ be the natural projection. Suppose*

$$\bigcup_{i=0}^{p} \bigcup_{k \in R'} \rho(y_i^k I_{i,k}) g_k' d_i \qquad \text{and} \qquad \bigcup_{i=0}^{p} \eta(B_i d_i)$$

are respectively an RDS in $\bar{K} \times H$ relative to U and a $(p+1, p+1, p(p+1), (p^2-1), p^2)$ divisible difference set in H relative to U. Then $\bigcup_{i=0}^{p} E_i' d_i$ is a semi-regular $((p+1)p^{2n}, p+1, (p+1)p^{2n}, p^{2n})$- RDS in $K \times H$ relative to U.

Proof. As we have mentioned, when $\bigcup_{i=0}^{p} \bigcup_{k \in R'} \rho(y_i^k I_{i,k}) g_k' d_i$ is an RDS in $\bar{K} \times H$ relative to U, we then have

$$\sum_{i=0}^{p} E_i' E_i'^{(-1)} = p^{2n}(KU - U) + p^{2n}(p+1).$$

Note that $Ud_0, \ldots, Ud_p$ are all the distinct U-cosets in H. Therefore,

$$\sum_{0 \le i \ne j \le p} \eta(B_i d_i)\, \eta(B_j d_j)^{(-1)} = p^2(H - U).$$

Therefore,

$$\begin{aligned}
\sum_{0 \le i \ne j \le p} E_i' E_j'^{(-1)} d_i d_j^{-1} &= \sum_{0 \le i \ne j \le p} \left(\sum_{k,\ell \in R'} g_k' g_\ell'^{-1} \right) K B_i d_i B_j^{(-1)} d_j^{-1} \\
&= \sum_{0 \le i \ne j \le p} \left(\sum_{k,\ell \in R'} g_k' g_\ell'^{-1} \right) K \eta(B_i d_i) \eta(B_j d_j)^{(-1)} \\
&= \left(\sum_{k,\ell \in R'} g_k' g_\ell'^{-1} \right) K \left(\sum_{0 \le i \ne j \le p} \eta(B_i d_i)\, \eta(B_j d_j)^{(-1)} \right) \\
&= \left(\sum_{k,\ell \in R'} g_k' g_\ell'^{-1} \right) K p^2 (H - U) = p^{2n} K (H - U).
\end{aligned}$$

It is now clear that $\bigcup_{i=0}^{p} E_i' d_i$ is an RDS. ∎

We now come back to the second construction given in [2]. We follow the notation used in the previous example. First we set $d_0 = u, d_1 = v$, and $d_2 = v^2$. It is straightforward to check that $\{u, v, v^2\}$ is an RDS in H relative to $U = \langle u \rangle$. Observe that F defined in [2, Theorem 4.1] can be rewritten as

$$\bigcup_{i=0}^{2} \bigcup_{j \in R_n'} \langle x_i y_i^{2j} \rangle u^j y_i^j B_i d_i,$$

where $B_0 = \{1, uy_0^{2^{a-1}}\}, B_1 = \{1, u^2 y_1^{2^{a-1}}\}$, and $B_2 = \{1, u^2 y_2^{2^{a-1}}\}$. It is clear that for each i,

$$B_i B_i^{(-1)} = \langle y_i^{2^{a-1}} \rangle U - U - \langle y_i^{2^{a-1}} \rangle + 3.$$

Moreover if $\eta : R_n \times R_n \times H \to H$ is the natural projection, then

$$\bigcup_{i=0}^{2} \eta(B_i d_i) = \{u, u^2, v, u^2 v, v^2, u^2 v^2\}$$

is a $(3, 3, 6, 3, 4)$-DDS in H relative to U. Furthermore,

$$\bigcup_{i=0}^{2} \bigcup_{j \in R_n'} \rho(\langle x_i y_i^{2j} \rangle u^j y_i^j) d_i = F_{n-1},$$

where F_{n-1} is as defined in the previous example. By Theorem 6.2, F is an RDS in $R_n \times R_n \times H$ relative to U.

ACKNOWLEDGMENT

We thank the referees for their suggestions that have improved the exposition of this paper.

REFERENCES

1. 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.
2. J. A. Davis, J. Jedwab, and M. Mowbray, New families of semi-regular relative difference sets, *Des. Codes Cryptogr.* **13** (1998), 131–146.
3. K. H. Leung and S. L. Ma, Constructions of partial difference sets and relative difference sets on p-groups, *Bull. London Math. Soc.* **22** (1990), 533–539.
4. K. H. Leung and S. L. Ma, Partial difference sets with Paley parameters, *Bull. London Math. Soc.* **27** (1995), 553–564.
5. K. H. Leung and S. L. Ma, A construction of partial difference sets in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^2}$, *Des. Codes Cryptogr.* **8** (1996), 167–172.
6. B. R. McDonald, "Finite Rings with Identity," Dekker, New York, 1974.
7. A. Pott, "Finite Geometry and Character Theory," Springer-Verlag, New York/Berlin, 1995.
8. A. Pott, A survey on relative difference sets, *in* "Groups, Difference Sets, and the Monster, Proceedings of a Special Research Quarter at The Ohio State University, Spring 1993," de Gruyter, Berlin, 1996.
9. D. K. Ray-Chaudhuri and Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings, *Des. Codes Cryptogr.* **8** (1996), 215–227.