CHINESE JOURNAL OF
MATHEMATICS
Volume 18, Number 3, September 1990

SCHUR RINGS OVER DIHEDRAL GROUPS

by

WAI-CHEE SHIU (邵慰慈)

Abstract. Let G be a finite group and $\mathcal{P} = \{D_0 = \{e\}, D_1, \cdots, D_d\}$ be a partition of G. Suppose, for each i, j, $0 \leq i,j \leq d$, $\{g \in G | g^{-1} \in D_i\} = D_{i*} \in \mathcal{P}$ for some $0 \leq i* \leq d$ and $\bar{D}_i \bar{D}_j = \sum_{k=0}^{d} p_{ij}^k \bar{D}_k$ where $\bar{D}_m = \sum_{g \in D_m} g \in \mathbb{C}[G]$. Then the subalgebra of $\mathbb{C}[G]$ spanned by $\bar{D}_0, \cdots, \bar{D}_d$ is called a Schur ring (S-ring). Such an object is known to have application on group theory and combinatorial design theory. In this paper, we study the structure of Schur rings over dihedral group $\mathfrak{D}_n$. Special attention is paid to the case when $n = p$ where p is an odd prime.

1. INTRODUCTION

Let G be a finite group and let e be the identity of G. For any $D \subseteq G$, $t \in \mathbb{Z}$, we define $D^{(t)} = \{d^t | d \in D\}$ and $\bar{D} = \sum_{d \in D} d \in \mathbb{C}[G]$ where $\mathbb{C}[G]$ denotes the group algebra of G over $\mathbb{C}$. Let $\mathcal{P} = \{D_0 = \{e\}, D_1, \cdots, D_d\}$ be a family of nonempty subsets of G satisfying the following conditions:

[S1] $\mathcal{P}$ is a partition of G;

[S2] for each $D_i \in \mathcal{P}$, $D_i^{(-1)} = D_{i*}$ for some $i* \in \{0, 1, \cdots, d\}$;

[S3] $\bar{D}_i \bar{D}_j = \sum_{k=0}^{d} p_{ij}^k \bar{D}_k$ for all i, j where $p_{ij}^k \in \{0, 1, 2, \cdots\} = \mathbb{N}$.

Received August 28, 1989; Revised May 30, 1990.
Key words and phrases: Schur ring, Association scheme, Difference sets.
A.M.S. classification codes (1980):20C05,05B99.

The subalgebra, denoted by $\mathfrak{S} = (G; \mathcal{P})$, of $\mathbb{C}[G]$ generated by $\bar{D}_0, \cdots, \bar{D}_d$ is called a Schur ring (for short, S-ring) of dimension $d+1$ over G. We call an S-ring trivial if its dimension is less than 3. The integers p_{ij}^k are called the intersection numbers of the S-ring $\mathfrak{S}$. Each $\bar{D}_i$ is called a principal basis element of $\mathfrak{S}$ and each D_i is called an $\mathfrak{S}$-principal subset of G.

Given an S-ring $\mathfrak{S}$ of dimension $d+1$ over a group G. For each i, $0 \leq i \leq d$, we define the relation R_i by $(h, g) \in R_i$ if and only if $h^{-1}g \in D_i$. It is known that $\mathcal{X} = (G; R_0, \cdots, R_d)$ is an association scheme with d classes on G and the intersection numbers of the scheme $\mathcal{X}$ are exactly the intersection numbers of the S-ring $\mathfrak{S}$. $\mathcal{X}$ is said to be the association scheme induced by $\mathfrak{S}$ (see [1]: p.104-105). We have

$$
\begin{aligned}
&\text{(a) } p_{0j}^k = \delta_{jk};\\
&\text{(b) } p_{i0}^k = \delta_{ik};\\
&\text{(c) } \sum_{j=0}^{d} p_{ij}^k = v_i = |D_i|;\\
&\text{(d) } p_{ij}^0 = v_i \delta_{ij*}; \text{ and}\\
&\text{(e) } v_k p_{ij}^k = v_j p_{i*k}^j = v_i p_{kj*}^i \quad \text{(see [1]: P.55–56).}
\end{aligned} \tag{1.1}
$$

2. GENERAL PROPERTIES OF S-RINGS

An S-ring $\mathfrak{S} = (G; \mathcal{P})$ (of dimension $d+1$) over G is called primitive if $< D_i >= G$ for each $D_i \in \mathcal{P}$, $1 \leq i \leq d$. Otherwise it is called imprimitive. Clearly, $\mathfrak{S}$ is primitive if and only if no $D_i \in \mathcal{P}$,$1 \leq i \leq d$, is contained in a proper subgroup of G.

Let $\mathfrak{S} = (G; \mathcal{P})$ be an S-ring over G. Suppose $H \leq G$ and $\mathcal{P}' \subseteq \mathcal{P}$ are such that $\mathfrak{S}' = (H; \mathcal{P}')$ is an S-ring over H, then we call $\mathfrak{S}'$ a Schur subring (for short, S-subring) of $\mathfrak{S}$, and call $\mathfrak{S}'$ normal if H is a normal subgroup of G. $\mathfrak{S}$ is called simple if it contains only two normal S-subrings $\mathfrak{S}$ and $\mathfrak{S}_0 = (\{e\}; \{D_0\})$.

Lemma 2.1. *Let $\mathfrak{S} = (G; \mathcal{P})$ be an S-ring. Let $\phi \neq \mathcal{P}' \subseteq \mathcal{P}$ satisfy*

(a) $D_{i*} \in \mathcal{P}'$ *for each* $D_i \in \mathcal{P}'$.

(b) $\bar{D}_i\bar{D}_j$ *is a linear combination of* $\bar{D}_k \in \mathcal{P}'$ *for all* $D_i, D_j \in \mathcal{P}'$.

Then $H = \bigcup_{D \in \mathcal{P}'} D$ *is a subgroup of* G *and* $\mathfrak{S}' = (H; \mathcal{P}')$ *is an S-subring of* $\mathfrak{S}$.

Proposition 2.2. $\mathfrak{S} = (G; \mathcal{P})$ *is an imprimitive S-ring iff* $\mathfrak{S}$ *contains a proper S-subring* $\mathfrak{S}' \neq (\{e\}; \{D_0\})$. *Hence a primitive S-ring is simple.*

Proof. Sufficiency: It is obvious.

Necessity: Suppose $\exists D_i \in \mathcal{P}, i \neq 0$, such that $< D_i >= H$ which is a proper subgroup of G. Let

$$\mathcal{P}' = \left\{ D \in \mathcal{P} \,\middle|\, \begin{array}{l} \bar{D} \text{ appears in the expression of } (\bar{D}_i)^s \text{ as a} \\ \text{linear combination of } \bar{D}_0, \cdots, \bar{D}_d \text{ for some } s > 0 \end{array} \right\}$$
$$= \{D \in \mathcal{P} | D \subset D_i^s \text{ for some } s > 0\},$$

where $D_i^s = \{g \in G | g = g_1 g_2 \cdots g_s \text{ for some } g_j \in D_i \quad 1 \leq j \leq s\}$.

Then $\mathcal{P}'$ satisfies condition (b) in Lemma 2.1.

Since $p_{ij}^0 = v_i \delta_{ij*}$, the appearance of e in $(\bar{D}_j)^s$ implies that $\bar{D}_{j*}$ appears in the linear combination expression of $(\bar{D}_j)^{s-1}$. So $D_{i*} \in \mathcal{P}'$ and hence $D_{j*} \in \mathcal{P}'$ if $D_j \in \mathcal{P}'$. ∎

An S-ring $\mathfrak{S} = (G; \mathcal{P})$ (of dimension $d+1$) is called commutative if $\bar{D}_i\bar{D}_j = \bar{D}_j\bar{D}_i$ for all i, j, $0 \leq i, j \leq d$. $\mathfrak{S}$ is called symmetric if $D_i^{(-1)} = D_{i*} = D_i$ for all i, $0 \leq i \leq d$.

Consider a group homomorphism (or antihomomorphism) $\varphi : G_1 \to G_2$, it can be extended to an algebra homomorphism (or antihomomorphism) from $\mathbb{C}[G_1]$ into $\mathbb{C}[G_2]$ in the usual way (see [3]: §2.2). We denote this extension by φ^*. In particular, we let $G_1 = G_2 = G$ and $\varphi = \iota : g \mapsto g^{-1}$ for all $g \in G$. Then

$$\bar{D}_{j*}\bar{D}_{i*} = \iota^*(\bar{D}_j)\iota^*(\bar{D}_i) = \iota^*(\bar{D}_i\bar{D}_j) \sum_{k=0}^{d} p_{ij}^k \iota^*(\bar{D}_k) = \sum_{k=0}^{d} p_{ij}^k \bar{D}_{k*}.$$

Hence a symmetric S-ring must be commutative.

Throughout the remaining sections of this paper, all groups are finite and non-trivial, and all S-rings are nontrivial.

3. PROPERTIES OF S–RINGS OVER $\mathfrak{C}_p$

Let G be an abelian group with exponent n and let $\Delta = \mathbb{Z}_n^*$ be the multiplicative group of units in $\mathbb{Z}_n$. Let Δ act on G by $(s, g) = g^s$, $g \in G, s \in \Delta$. For a fixed $s \in \Delta$, we define $\vartheta : G \to G$ by $\vartheta(g) = g^s$.

Lemma 3.1. *(Wielandt; see* [8]: § *23) Let* $\mathfrak{S} = (G; \mathcal{P})$ *be an S–ring over* G. *Then* $\vartheta^*(\mathfrak{S}) = \mathfrak{S}$ *(i.e.* ϑ *permutes the* $\mathfrak{S}$*–principal subsets). Hence* Δ *is a permutation group on* $\mathcal{P}$.

Now let us consider $G = \mathfrak{C}_p =< \rho >, \Delta = \mathbb{Z}_p^* =< t >$ where p is an odd prime, let $\mathfrak{S} = (G; \mathcal{P})$ be an S–ring over G of dimension $m + 1$. Then Δ is a transitive permutation group on $\mathcal{P}\backslash\{D_0\}$. So $m = [\Delta{:}\mathrm{stab}(D_1)]$. We denote $\mathrm{stab}(D_1)$ by Δ_m and assume that $\rho \in D_1$.

Let $\Delta = \Delta_m \cup t\Delta_m \cup \cdots \cup t^{m-1}\Delta_m$. By renumbering we can write $D_i = D_1^{(t^{i-1})}$. Since $\sum_{i=1}^{m} |D_i| = |\Delta|$. by counting $D_1 = \rho^{\Delta_m} = \{\rho^s | s \in \Delta_m\}$. We have

Theorem 3.2. *An S–ring* $(\mathfrak{C}_p; \mathcal{P})$ *over* $\mathfrak{C}_p =< \rho >$ *of dimension* m *is formed by* $(\mathfrak{C}_p; \{D_0 = \{e\}, D_1 = \rho^{\Delta_m}, D_2 = \rho^{t\Delta_m}, \cdots, D_m = \rho^{t^{m-1}\Delta_m}\})$ *uniquely, where* $\Delta_m =< t^m >$ *is the unique subgroup of* $\mathbb{Z}_p^* =< t >$ *of index* $m, m|p-1$.

Proof. The axiom **[S3]** follows from the addition of cyclotomic classes (see [7]: p.24-25). ∎

Remark 3.3. In general, the structure of S–rings over cyclic groups of prime power orders is thoroughly determined (see [4]).

4. S-RINGS OVER DIHEDRAL GROUPS

Let $\mathfrak{D}_n =< \rho, \sigma | \rho^n = \sigma^2 = e, \sigma\rho\sigma = \rho^{-1} >$ be the dihedral group of order $2n$ and $\mathfrak{C}_n =< \rho >$ be the cyclic subgroup of $\mathfrak{D}_n$ generated by ρ.

Let $\mathfrak{S} = (\mathfrak{D}_n; \mathcal{P} = \{D_0, D_1, \cdots, D_d\})$ be an S–ring over $\mathfrak{D}_n$. For each i, D_i is of the form $D_i = A_i \cup \sigma B_i$ uniquely, where $A_i, B_i \subseteq \mathfrak{C}_n$. (We shall keep these notations till the end of this paper).

Proposition 4.1.

(a) *If* $\bar{D}_i \bar{D}_j = \sum_k p_{ij}^k \bar{D}_k$, *then*

$$\sum_k p_{ij}^k \bar{A}_k = \bar{A}_i \bar{A}_j + \overline{B_i^{(-1)}} \bar{B}_j \tag{4.1}$$

$$\sum_k p_{ij}^k \bar{B}_k = \overline{A_i^{(-1)}} \bar{B}_j + \bar{A}_j \bar{B}_i \tag{4.2}$$

In the above formulas we define $\bar{A}_k = 0$ *and* $\bar{B}_k = 0$ *if* $A_k = \phi$ *and* $B_k = \phi$ *respectively.*

(b) $A_i^{(-1)} = A_{i*}, B_i = B_{i*}$. *Moreover if* $D_i \neq D_{i*}$ *then* $D_i = A_i$

(*Here* $A_{i*} \cup \sigma B_{i*} = D_{i*}$).

Remark 4.2.

(a) $\{\bar{A}_0 = e, \bar{A}_1 \cdots, \bar{A}_d, \bar{B}_1, \cdots, \bar{B}_d\}$ is a commutative subset of $\mathbb{C}[\mathfrak{C}_n]$.

(b) In general $B_i^{(-1)} \neq B_{i*}$.

Theorem 4.3. *Any non-symmetric S-ring* $\mathfrak{S}$ *over* $\mathfrak{D}_n$ *has a proper normal S-subring* $\mathfrak{S}'$ *which is a nontrivial S-ring over a subgroup of* $\mathfrak{C}_n$(*i.e. the dimension of* $\mathfrak{S}'$ *is greater than 2*). *Hence* $\mathfrak{S}$ *is not simple.*

Proof. Suppose $\mathfrak{S}$ is non–symmetric. By Proposition 4.1(b) and renumbering the indices of the $\mathfrak{S}$–principal subsets of $\mathfrak{D}_n$, we may assume that they are $D_0 = A_0, D_1 = A_1, \cdots, D_r = A_r, D_{r+1} = A_{r+1} \cup \sigma B_{r+1}, \cdots, D_d = A_d \cup \sigma B_d$, where $A_i \subseteq \mathfrak{C}_n$ for $0 \leq i \leq d$, and $\phi \neq B_s \subseteq \mathfrak{C}_n$ for $2 \leq r+1 \leq s \leq d$. By Lemma 2.1, $H = \bigcup_{k=0}^{r} A_k$ is a subgroup of $\mathfrak{C}_n$ and hence $\mathfrak{S}' = (H; \{A_0, \cdots, A_r\})$ is a normal S-subring of $\mathfrak{S}$ (since any subgroup of $\mathfrak{D}_n$ lying in $\mathfrak{C}_n$ is normal).

Theorem 4.4. (*Wielandt*) *No non-trivial primitive Schur ring exists over* $\mathfrak{D}_n$ (*see*[9], [5] : *p*.416 – 422).

5. Nonsimple S–rings over $\mathfrak{D}_p$

Consider the dihedral group $\mathfrak{D}_p$, where p is an odd prime. Let $\mathfrak{S}$ be a nonsimple S–ring over $\mathfrak{D}_p$. By definition, $\mathfrak{S}$ contains a proper normal S–subring $\mathfrak{S}'$, which is an S–ring over a proper normal subgroup $H \neq \{e\}$ of $\mathfrak{D}_p$. Hence $H = \mathfrak{C}_p$ and $\mathfrak{S}'$ is an S–ring over $\mathfrak{C}_p$. Thus any $\mathfrak{S}$–principal subset of $\mathfrak{D}_p$ is of the form A or σB where A and B are subsets of $\mathfrak{C}_p$.

By Theorem 3.2 we have

$$\mathfrak{S}' = (\ \mathfrak{C}_p; \{A_0 = \{e\}, A_1 = \rho^{\Delta m}, A_2 = \rho^{t\Delta m}, \cdots, A_m = \rho^{t^{m-1}\Delta m}\})$$

where Δ_m is the unique subgroup of $\mathbb{Z}_p^* =< t >$ of index $m, m|p-1$. Hence

$$\mathfrak{S} = (\ \mathfrak{D}_p; \{A_0, \cdots, A_m, \sigma B_{m+1}, \cdots, \sigma B_d\}).$$

Let us call a nonsimple S–ring over $\mathfrak{D}_p$ a (p,m)–S–ring if it contains a (unique) normal S–subring $\mathfrak{S}'$ over $\mathfrak{C}_p$ of the form
$\mathfrak{S}' = (\ \mathfrak{C}_p; \{A_0 = \{e\}, A_1 = \rho^{\Delta m},\ A_2 = \rho^{t\Delta m}, \cdots, A_m = \rho^{t^{m-1}\Delta m}\})$,
$m|p-1$, $\Delta_m =< t^m >$ being the unique subgroup of $\mathbb{Z}_p^* =< t >$ of index m.

Let $\mathfrak{S} = (\ \mathfrak{D}_p; \{A_0, \cdots, A_m, \sigma B_{m+1}, \cdots, \sigma B_d\})$ be a (p,m)-S-ring and write $\bar{B}_\alpha = \sum_{j \in \mathbb{Z}_p} \alpha_j \rho^j$, $\bar{B}_\beta = \sum_{k \in \mathbb{Z}_p} \beta_k \rho^k$, $m+1 \leq \alpha, \beta \leq d$, where α_j, β_k are either 0 or 1. Then

$$\overline{B_\alpha^{(-1)}} \bar{B}_\beta = \sum_{h \in \mathbb{Z}_p} P_{\alpha\beta}(h) \rho^h$$

where $P_{\alpha\beta}(h) = \sum_{j \in \mathbb{Z}_p} \alpha_{j-h} \beta_j$.

Proposition 5.1. $|B_\alpha||B_\beta| = \sum_{h \in \mathbb{Z}_p} P_{\alpha\beta}(h) \equiv P_{\alpha\beta}(0)\ (\mathrm{mod}\ v)$,
i.e. $|B_\alpha||B_\beta| \equiv \delta_{\alpha\beta}|B_\alpha|\ (\mathrm{mod}\ v)$, *where* $v = \frac{p-1}{m} = |\Delta_m|$.

Proof. Since

$$P_{\alpha\beta}(0) = \sum_{j\in \mathbb{Z}_p} \alpha_{j-0}\beta_j = |B_\alpha \cap B_\beta| = \delta_{\alpha\beta}|B_\alpha| \text{ and}$$

$$\overline{B_\alpha^{(-1)}}\bar{B}_\beta = \sum_\gamma p_{\alpha\beta}^\gamma \bar{A}_\gamma,$$

$$P_{\alpha\beta}(j) = P_{\alpha\beta}(k) \text{ if } j^{-1}k \in \Delta_m \forall \alpha, \beta. \tag{5.1}$$

So we have the proposition. ∎

Corollary 5.2. *Let* $\bar{B}_\alpha = \sum_{i\in \mathbb{Z}_p} \alpha_i \rho^i$ *be defined as above, then the periodic (of period* p*) binary sequences* $(\alpha_0, \alpha_1, \cdots, \alpha_{p-1})$ *has autocorrelation (see appendix) of level at most* $m+1$*. If* $m = 1$ *then each* B_α *is a cyclic difference set in* $\mathfrak{C}_p$*(see appendix).*

Proof. It follows from (5.1) and the theorem in appendix. ∎

Let $\mathfrak{S} = (\mathfrak{D}_p; \{A_0, \cdots, A_m, \sigma B_{m+1}, \cdots, \sigma B_d\})$ be a commutative (p, m)–S–ring. Without loss of generality we may assume that $e \in B_{m+1}$. By commutativity we have

$$\overline{B_i^{(-1)}}\bar{B}_j = \overline{\sigma B_i}\overline{\sigma B_j} = \sum_{k=0}^{m} p_{ij}^k \bar{A}_k = \overline{\sigma B_j}\overline{\sigma B_i} = \overline{B_j^{(-1)}}\bar{B}_i.$$

Let $\chi : \rho \mapsto \zeta = e^{2\pi i/p}$ be the character of $\mathfrak{C}_p$ then $\overline{\chi^*(\bar{B}_i)}\chi^*(\bar{B}_j) \in \mathbb{R}$.

In the remaining part of this section, we keep the notations defined above.

Lemma 5.3. $\mathcal{R}e\chi^*(\bar{B}_k) \neq 0$ *for each* $k = m+1, \cdots, d$ *unless* $B_{m+1} = \mathfrak{C}_p$.

Proof. Let $z = \chi^*(\bar{B}_k) = \sum_{j=0}^{p-1} \alpha_j \zeta^j, \alpha_j = 0$ or 1. Suppose $\mathcal{R}ez = 0$ then

$$\sum_{j=0}^{p-1} (\alpha_j + \alpha_{p-j})\zeta^j = 0,$$

where α_p is defined to be α_0. Then the irreducible polynomial $1 + x + \cdots + x^{p-1}$ divides the polynomial $\sum_{j=0}^{p-1}(\alpha_j + \alpha_{p-j})x^j$ in $\mathbb{Z}[x]$ and then

$$\alpha_j + \alpha_{p-j} = 2\alpha_0 \; \forall j = 0, 1, \cdots, p-1.$$

For $k > m+1$, we get $\alpha_j + \alpha_{p-j} = 0$ and $\alpha_j = 0 \; \forall j$.

For $k = m+1$, $\alpha_j + \alpha_{p-j} = 2\ \forall j$. Since $a_j = 0$ or $1, \alpha_j = 1\ \forall j$. Hence $B_{m+1} = \mathfrak{C}_p$. ∎

Theorem 5.4. *Keep the notations as in Lemma 5.3. If one of the B_j is symmetric (i.e. $B_j = B_j^{(-1)}$) then all B_k, $m+1 \le k \le d$, are symmetric.*

Proof. Suppose $B_{m+1} \neq \mathfrak{C}_p$. Since $\overline{\chi^*(\bar{B}_j)}\chi^*(\bar{B}_k) \in \mathbb{R}$ for all $j, k, \exists c \in \mathbb{R}$ such that $\chi^*(\bar{B}_h) = a_h + ca_h i$ for some $a_h, b_h \in \mathbb{R}\ \forall h\ (m+1 \le h \le d)$. The theorem follows from Lemma 5.3. ∎

A (p,m)–S–ring is symmetric iff $A_{1*} = A_1^{(-1)} = A_1$ iff $-1 \in \Delta_m$ iff $2m|p-1$. Hence, if a (p,m)–S–ring is not symmetric, then m is even and $A_i \neq A_{i*} \forall 1 \le i \le m$. By a rearrangement of the indices of the A_i, $\mathfrak{S}'$ can be written as

$$(\ \mathfrak{C}_p; \{A_0 = \{e\}, A_1, \cdots, A_{m/2}, A_1^{(-1)} = A_{1*}, \cdots, A_{m/2}^{(-1)} = A_{(m/2)*}\}).$$

In particular, a nonsymmetric $(p,2)$–S–ring over $\mathfrak{D}_p$ exists only if $p \equiv 3 \pmod 4$, in which $\mathfrak{S}' = (\ \mathfrak{C}_p; A_0 = \{e\}, A_1 = \rho^{\Delta_2}, A_2 = A_{1*}\})$ where $\Delta_2 = < t^2 >$.

Theorem 5.5. *Let $\mathfrak{S}$ be a nonsymmetric (p,2)–S–ring over $\mathfrak{D}_p$ and p be an odd prime, $p \equiv 3\ (mod\ 4)$. Let σB be an $\mathfrak{S}$–principal subset of $\mathfrak{D}_p$ in $\mathfrak{D}_p \setminus \mathfrak{C}_p$, then B is a cyclic difference set of $\mathfrak{C}_p$.*

Proof. Applying (4.1) to the $\mathfrak{S}$–principal subset σB of $\mathfrak{D}_p$, we have

$$\overline{B^{(-1)}}\bar{B} = |B|e + a\bar{A}_1 + b\bar{A}_{1*} \tag{5.2}$$

Let $\iota : \mathfrak{C}_p \to \mathfrak{C}_p$ be an automorphism of $\mathfrak{C}_p$ defined by $\iota : \rho \mapsto \rho^{-1}$. By applying ι^* on (5.2) we have $\overline{B^{(-1)}}\bar{B} = |B|e + a\bar{A}_{1*} + b\bar{A}_1$. This implies $a = b$, i.e. $\overline{B^{(-1)}}\bar{B} = |B|e + a\overline{(\ \mathfrak{C}_p \setminus \{e\})}$, hence B is a $(p, |B|, a)$–cyclic difference set of $\mathfrak{C}_p$. ∎

Remark 5.6. By a similar proof we see that A_1, defined above, is a $(p, \frac{p-1}{2}, \frac{p+1}{4})$–cyclic difference set containing ρ.

Proposition 5.7. *Let $\mathfrak{S}$ be a commutative but not symmetric (p,m)–S–ring*

with the normal S–subring $\mathfrak{S}' = (\mathfrak{C}_p; \mathcal{P}')$ *where*

$$\mathcal{P}' = \{A_0, A_1, \cdots, A_{m/2}, A_1^{(-1)} = A_{1*}, \cdots, A_{m/2}^{(-1)} = A_{(m/2)*}\}.$$

Let σB *and* $\sigma B'$ *be any* $\mathfrak{S}$*–principal subsets of* $\mathfrak{D}_p$ *in* $\mathfrak{D}_p \setminus \mathfrak{C}_p$, *then*

$$\overline{B'^{(-1)}}\bar{B} = a_0 e + a_1(\bar{A}_1 + \bar{A}_{1*}) + \cdots + a_{m/2}(\bar{A}_{m/2} + \bar{A}_{(m/2)*}) \text{ for some } a_i \in \mathbb{N}.$$

Proof. Since $\overline{\sigma B'}\overline{\sigma B} = \overline{\sigma B \sigma B'}$,

$$\overline{B'^{(-1)}}\bar{B} = a_0 e + a_1\bar{A}_1 + \cdots + a_{m/2}\bar{A}_{m/2} + b_1\bar{A}_{1*} + \cdots + b_{m/2}\bar{A}_{(m/2)*} = \overline{B^{(-1)}}\bar{B}'.$$

By applying ι^*, which is defined in Theorem 5.5, we have $a_i = b_i$ for $1 \le i \le m/2$. ∎

Corollary 5.8. *Keeping the notations as in Proposition 5.7, let* $\mathfrak{S} = (\mathfrak{D}_p : \mathcal{P}' \cup \{\sigma B_{m+1}, \cdots, \sigma B_d\})$ *be a commutative S–ring and let* $E_i = A_i \cup A_{i*}$, $0 \le i \le m/2$. *Then* $\mathfrak{S}'' = (\mathfrak{C}_p; \{E_0, E_1, \cdots, E_{m/2}\} = \mathcal{P}'')$ *is a normal S–subring of a symmetric* $(p, \frac{m}{2})$*–S–ring* $\mathfrak{S}_1 = (\mathfrak{D}_p; \mathcal{P}'' \cup \{\sigma B_{m+1}, \cdots, \sigma B_d\})$ *over* $\mathfrak{D}_p$ *of dimension* $d - \frac{m}{2} + 1$.

Proof. By Proposition 5.7, $\Delta_m \cup (-\Delta_m) = \Delta_{m/2}$, and, $\overline{\sigma B_i}\overline{E_j} = \sigma\bar{B}_i(\bar{A}_j + \bar{A}_{j*})$ is a linear combination of $\overline{\sigma B_k}$. ∎

If $\mathfrak{S}$ is an S–ring over G and $\mathfrak{S}_1$ is a subalgebra of $\mathfrak{S}$ such that $\mathfrak{S}_1$ is also an S–ring over G, then we say that $\mathfrak{S}$ can be reduced to $\mathfrak{S}_1$. Hence any nonsymmetric commutative (p, m)–S–ring can be reduced to a symmetric $(p, \frac{m}{2})$–S–ring.

6. Simple S–rings over $\mathfrak{D}_p$

In this section, we assume $\mathfrak{S}$ is a nontrivial simple (and hence symmetric) S–ring over $\mathfrak{D}_p$ where p is an odd prime. By Theorem 4.4 and Proposition 2.2 $\mathfrak{S}$ contains an S–subring $\mathfrak{S}'$ which is an S–ring over a proper nontrivial subgroup H which is not normal. Then $|H| = 2$ and $H = \{e, \sigma p^i\}$ for some i. By replacing the generator $\sigma\rho^i$ by σ we may assume $H = \{e, \sigma\}$ and $\mathfrak{S}' = (H; D_0 = \{e\}$,

$D_{0'} = \{\sigma\}$). So $\mathfrak{S} = (\mathfrak{D}_p; \{D_0, D_{0'}, D_1, \cdots, D_d\})$ where $D_i = A_i \cup \sigma B_i$ for $0 \leq i \leq d$ or $i = 0'$, $A_0 = \{e\} = B_{0'}$, $A_{0'} = \phi = B_0$ and $B_j \neq \phi$ for $1 \leq j \leq d$.

Since $\mathfrak{S}$ is symmetric, $\bar{D}_{0'}\bar{D}_i = \bar{D}_i\bar{D}_{0'}$. So we have

$$\sigma\bar{A}_i + \bar{B}_i = \bar{A}_i\sigma + \overline{\sigma B_i}\sigma = \sigma\overline{A_i^{(-1)}} + \overline{B_i^{(-1)}}.$$

Hence $A_i = A_i^{(-1)} = A_{i*}$ (Proposition 4.1(b)) and $B_i = B_i^{(-1)}$ for each i.

Proposition 6.1. *Let $\mathfrak{S} = (\mathfrak{D}_p; \{D_0, D_{0'}, D_1, \cdots, D_d\})$ be a symmetric S-ring over $\mathfrak{D}_p$. Then σD_j is an $\mathfrak{S}$-principal subset of $\mathfrak{D}_p$. Moreover, either $A_j = B_j$ or $A_j \cap B_j = \phi$.*

Proof. Apply (4.1) and (4.2) to $\bar{D}_{0'}\bar{D}_j$ we have

$$\bar{B}_j = \sum_k p^k_{0'j}\bar{A}_k \text{ and } \bar{A}_j = \sum_k p^k_{0'j}\bar{B}_k \quad \forall j \geq 1.$$

Clearly, we have $p^k_{0'j} = 0$ or $1 \quad \forall j, k$. Thus for $j \geq 1$ we have

$$\bar{A}_j = \sum_{k,h} p^k_{0'j}p^h_{0'k}\bar{A}_h \text{ and } \sum_k p^k_{0'j}p^h_{0'k} = \delta_{jh}.$$

In particular, $\sum_k p^k_{0'j}p^j_{0'k} = 1$, hence $p^k_{0'j}p^j_{0'k} = 0$ for all k except one, say j'.

By (1.1) (e) and $0'* = 0$' we have $(p^k_{0'j})^2 = 0$ except $k = j'$. Hence $A_j = B_{j'}$, $B_j = A_{j'}$ and $\sigma D_j = D_{j'}$ is an $\mathfrak{S}$-principal subset of $\mathfrak{D}_p$.

If $A_j \cap B_j \neq \phi$ then $D_j \cap D_{j'} \neq \phi$ and hence $A_j = B_j$. ∎

In the above case, we denote σD_j by $D_{j'}$.

For convenience, let us call a symmetric S-ring $\mathfrak{S}$ over $\mathfrak{D}_p$ a reflective symmetric S-ring over $\mathfrak{D}_p$ if $\mathfrak{S} = (\mathfrak{D}_p; \{E_0, E_{0'}, E_1 \cdots, E_u\})$ where $E_0 = \{e\}, E_{0'} = \{\sigma\}$ $E_i = A_i \cup \sigma A_i$, $A_i \subseteq \mathfrak{C}_p$ for $1 \leq i \leq u$, i.e. $\sigma E_i = E_i$ for $1 \leq i \leq u$.

Let $\mathfrak{S}$ be the S-ring of dimension $d+2$ as in Proposition 6.1. By renumbering the indices of D_i, let s be the least integer ≥ 1 such that $\forall j \geq s$, $D_j = A_j \cup \sigma B_j$, $A_j \cap B_j = \phi$. More explicitly, $\mathfrak{S} = (\mathfrak{D}_p; \mathcal{P})$ where

$$\mathcal{P} = \left\{ \begin{array}{c} D_0, D_{0'}, D_1 = A_1 \cup \sigma A_1, \cdots, D_{s-1} = A_{s-1} \cup \sigma A_{s-1}, \\ D_s = A_s \cup \sigma B_s, \cdots, D_u = A_u \cup \sigma B_u, \\ D_{s'} = A_{s'} \cup \sigma B_{s'} \cdots, D_{u'} = A_{u'} \cup \sigma B_{u'} \end{array} \middle| \begin{array}{l} A_j, B_k \subset \mathfrak{C}_p \ \forall j, k \\ \text{and } A_j \cap B_j = \phi \ \forall j \geq s \end{array} \right\},$$

where $u = \frac{d+s-1}{2}$. For convenience, let us call such a symmetric S–ring a [p,s,u]–S–ring.

Remark 6.2.

(a) $j = j'$ for each $1 \leq j \leq s-1$;

(b) $(j')' = j$ for all j;

(c) $p_{0'j}^k = \delta_{kj'}$ for all j, k;

(d) Since $\bar{A}_i\bar{A}_j + \bar{B}_i\bar{B}_j + \sigma(\bar{A}_i\bar{B}_j + \bar{A}_j\bar{B}_i) = \bar{D}_i\bar{D}_j = p_{ij}^0 e + p_{ij}^{0'}\sigma + \cdots$, $p_{ij}^{0'} = \delta_{ij'}v_i$ where $v_i = |D_i|$.

(e) Since $\bar{D}_i\bar{D}_j = \bar{D}_{i'}\bar{D}_{j'}, p_{ij}^k = p_{i'j'}^k$ for all i, j, k.

(f) If $1 \leq i \leq s-1$ then $\bar{D}_i\bar{D}_j = \bar{D}_{i'}\bar{D}_j = \sigma\bar{D}_i\bar{D}_j$ and hence $p_{ij}^k = p_{ij}^{k'}$.

Theorem 6.3. *Let $\mathfrak{S}$ be defined above, and let $E_j = D_j \cup \sigma D_j \quad j \geq s$. Assume $E_s, \cdots, E_u$ are all distinct subsets among the E_j. (In fact $u = \frac{d+s-1}{2}$) Then $\mathfrak{S}_R = (\mathfrak{D}_p; \{D_0, D_{0'}, D_1, \cdots, D_{s-1}, E_s, \cdots, E_u\})$ is a reflective symmetric S–ring of dimension u+2 over $\mathfrak{D}_p$. Such a [p,s,u]–S–ring $\mathfrak{S}$ over $\mathfrak{D}_p$ can be reduced to the reflective symmetric S–ring $\mathfrak{S}_R$. We shall call $\mathfrak{S}_R$ the reflex of $\mathfrak{S}$.*

Proof. Obviously, axioms **[S1]** and **[S2]** hold.

Using Remark 6.1(f) and computing directly, we obtain

$$(6.1)\quad \bar{D}_i\bar{D}_j = \sum_{k=0}^{s-1} p_{ij}^k \bar{D}_k + \sum_{k=s}^{d} p_{ij}^k \bar{D}_k + p_{ij}^{0'}\bar{D}_{0'} = \sum_{k=0}^{s-1} p_{ij}^k \bar{D}_k + \sum_{k=s}^{u} p_{ij}^k \bar{E}_k + p_{ij}^{0'}\bar{D}_{0'}$$

for $1 \leq i, j \leq s-1$;

$$\bar{D}_i\bar{E}_j = 2\left[\sum_{k=1}^{s-1} p_{ij}^k \bar{D}_k + \sum_{k=s}^{u} p_{ij}^k \bar{E}_k\right]$$

for $1 \leq i \leq s-1$ and $s \leq j \leq u$ (note that, in this case $p_{ij}^0 = p_{ij}^{0'} = 0$.) and for $s \leq i, j \leq u$,

$$(6.2)\quad \bar{E}_i\bar{E}_j = 2\left[(p_{ij}^0 + p_{ij}^{0'})e + (p_{ij}^0 + p_{ij}^{0'})\sigma + 2\sum_{k=1}^{s-1} p_{ij}^k \bar{D}_k + \sum_{k=s}^{u}(p_{ij}^k + p_{ij}^{k'})\bar{E}_k\right]$$

Hence axiom **[S3]** holds. ∎

Thus, to study the structure of a simple S–ring over $\mathfrak{D}_p$, we have to consider a reflective symmetric S–ring first.

Now let us denote a reflective symmetric S–ring of dimension $u+2$ by $\mathfrak{S}_R = (\mathfrak{D}_p; \mathcal{P})$ where $\mathcal{P} = \{E_0 = \{e\}, E_{0'} = \{\sigma\}, E_1, \cdots, E_u\}$, $E_i = \mathcal{A}_i \cup \sigma\mathcal{A}_i$ for $1 \le i \le u$ and $\mathcal{A}_0 = \{e\}$. Let $\mathcal{P}_{ij}^k$ be the intersection numbers of $\mathfrak{S}_R$.

Theorem 6.4. *$(\mathfrak{C}_p; \{\mathcal{A}_0, \mathcal{A}_1, \cdots, \mathcal{A}_u\})$ is a symmetric S-ring over $\mathfrak{C}_p$.*

Proof. For $1 \le i, j \le u$, by (4.1) we have

$$2\bar{\mathcal{A}}_i\bar{\mathcal{A}}_j = \mathcal{P}_{ij}^0\bar{\mathcal{A}}_0 + \sum_{k=1}^{u}\mathcal{P}_{ij}^k\bar{\mathcal{A}}_k.$$

(Note that, since $j = j'$ for $j \ge 1$, $\mathcal{P}_{ij'}^{0'} = \mathcal{P}_{ij}^{0'} = \mathcal{P}_{ij}^0 = \delta_{ij}v_i = 2\delta_{ij}|\mathcal{A}_i|$.) Clearly, $\mathcal{A}_{i*} = \mathcal{A}_i^{(-1)} = \mathcal{A}_i$ for all i and $\cup_i \mathcal{A}_i = \mathfrak{C}_p$. ∎

Corollary 6.5. *$\mathfrak{S} = (\mathfrak{D}_p; \{D_0 = \{e\}, D_{0'} = \{\sigma\}, D_1, \cdots, D_u\})$ is a (simple) reflective symmetric S–ring over $\mathfrak{D}_p$ of dimension $u+2$, where p is an odd prime, if and only if $\mathfrak{S} = \mathfrak{S}_R$ and $\mathcal{A}_i = \rho^{t^{i-1}\Delta_u}$, $1 \le i \le u$, where $\Delta_u = <t^u>$ is a subgroup of $\mathbb{Z}_p^* = <t>$ and $2u|p-1$. For convenience let us call such $\mathfrak{S}_R$ a $\{p,u\}$–S–ring.*

Corollary 6.6. *Let $\mathfrak{S}$ be a $[p,s,u]$–S–ring of dimension $2u-s+3$ and let $\mathfrak{S}_R$ be the reflex of $\mathfrak{S}$ of dimension $u+2$. Let p_{ij}^k and $\mathcal{P}_{ij}^k$ be the intersection numbers of $\mathfrak{S}$ and $\mathfrak{S}_R$ respectively.*
Then $\mathcal{P}_{0j}^k = \delta_{jk}$, $\mathcal{P}_{0'j}^k = \delta_{j'k}$ and

$$\mathcal{P}_{ji}^k = \mathcal{P}_{ij}^k = \begin{cases} p_{ij}^k & \text{if } 1 \le i, j \le s-1 \\ 2p_{ij}^k & \text{if } 1 \le i \le s-1 \text{ and } s \le j \le u \\ 2(p_{ij}^k + p_{ij}^{k'}) & \text{if } s \le i, j \le u \end{cases}$$

Proof. Compare the coefficients of (6.1) and (6.2) and use Remark 6.2(c). ∎

Remark 6.7.

(a) By the proof of the Theorem 6.4, $\mathcal{P}_{ij}^{k}$ are even for $1 \leq i, j \leq u$.

(b) In this section, all results except Corollary 6.5 can be extended to $\mathfrak{D}_n$.

(c) If $\mathfrak{S}$ is a reflective symmetric S–ring over $\mathfrak{D}_q$ where q is a power of prime then all the $\mathfrak{S}$–principal subsets of $\mathfrak{D}_q$ can be determined and we can list all $\mathfrak{S}$–principal subsets of $\mathfrak{D}_q$ for $u \leq 5$ (see [4]: §3).

7. EXAMPLE: S–RINGS OVER $\mathfrak{D}_7$

Consider $G = \mathfrak{D}_7$ as an example, by applying the results in the preceding sections, we can find all nontrivial S–rings over $\mathfrak{D}_7$ which are listed below (up to the naming of the generators):

Nonsimple case:

(7,1)–S–ring : $(\mathfrak{D}_7; \{A_0, A_1, \sigma B, \sigma B*\})$ where $A_1 = \mathfrak{C}_7 \backslash \{e\}$, B is a cyclic difference set of $\mathfrak{C}_7$ and $B*$ is the complementary cyclic difference set of B.

(7,2)–S–ring : $(\mathfrak{D}_7; \{A_0, A_1, A_2, \sigma\, \mathfrak{C}_7\})$ where $A_1 = \{\rho, \rho^2, \rho^4\}$, $A_2 = A_1^{(-1)} = \{\rho^3, \rho^5, \rho^6\}$.

(7,3)–S–ring : (a) $(\mathfrak{D}_7; \{A_0, A_1, A_2, A_3, \sigma\, \mathfrak{C}_7\})$.

(b) $(\mathfrak{D}_7; \{A_0, A_1, A_2, A_3, \{\sigma\}, \sigma A_1, \sigma A_2, \sigma A_3\})$.

In the both cases, $A_1 = \{\rho, \rho^{-1}\}$, $A_2 = \{\rho^2, \rho^{-2}\}$ and $A_3 = \{\rho^3, \rho^{-3}\}$.

(7,6)–S–ring : (a) $(\mathfrak{D}_7; \{A_0, A_1, \cdots, A_6, \sigma\, \mathfrak{C}_7\})$ where $A_i = \{\rho^i\}, 0 \leq i \leq 6$.

(b) $\mathbb{C}[\mathfrak{D}_7]$. (The only noncommutative case.)

Simple case :

$\{7,1\}$–S–ring: $(\mathfrak{D}_7; E_0, E_{0'}, \mathfrak{D}_7 \backslash \{e, \sigma\})$.

$\{7,3\}$–S–**ring** : $(\mathfrak{D}_7; \mathcal{P})$ where

$$\mathcal{P} = \left\{ \begin{array}{c} E_0, E_{0'}, \{\rho, \rho^{-1}, \sigma\rho, \sigma\rho^{-1}\}, \{\rho^2, \rho^{-2}, \sigma\rho^2, \sigma\rho^{-2}\}, \\ \{\rho^3, \rho^{-3}, \sigma\rho^3, \sigma\rho^{-3}\} \end{array} \right\}.$$

8. APPENDIX

A set $D = \{d_1, d_2, \cdots, d_k\}$ of k elements from an abelian group G of order v is called a (v, k, λ)–difference set for $1 \leq \lambda \leq k \leq v$, if for each $g \neq e \in G$, there exist exactly λ ordered pairs (i, j) with $i \neq j$ such that $d_i d_j^{-1} = g$. A difference set of G is called a cyclic difference set if G is cyclic (see [2]:p.1-10).

Clearly, D is a (v, k, λ)–difference set if and only if

$$\bar{D}\overline{D^{(-1)}} = \lambda\bar{G} + (k - \lambda)e$$

A binary sequence $\{a_0, a_1, a_2, \cdots\}$ is called periodic of period v if $a_i = a_{i+v}$ for all i. Sometimes we write a binary periodic sequence of period v by $\mathbf{a} = (a_0, a_1, \cdots, a_{v-1})$.

For a binary periodic sequence $\mathbf{a} = (a_0, a_1, \cdots, a_{v-1})$. we define the binary periodic autocorrelation function of $\mathbf{a}$ by

$$BP(t) = \sum_{i=0}^{v-1} a_i a_{i+t} \text{ (see [6])},$$

where the indices run through the residues mod v.

A binary periodic sequence $\mathbf{a} = (a_0, a_1, \cdots, a_{v-1})$ is said to possess m–level autocorrelation if the binary periodic autocorrelation function of $\mathbf{a}$ assumes m distinct values.

Theorem: (*Theorem* 3.4 *in* [6]) *A binary periodic sequence possessing 2-level autocorrelation corresponds to a cyclic difference set.*

Example: If **a** =(100110101111000) then it corresponds to $D = \{0,3,4,6,8,9,10,11\}$ in the additive cyclic group $\mathbb{Z}_{15}$. Since $BP(t) = \begin{cases} 8 & \text{if } t \equiv 0 \pmod{15} \\ 4 & \text{if otherwise} \end{cases}$, D is a cyclic (15,8,4)-difference set.

REFERENCES

1. E. Bannai and T. Ito, Algebraic Combinatorics I : Association schemes, Benjamin/ Cumming, Menlo Park, 1984.
2. L.D. Baumert, Cyclic Difference Sets (Lecture Notes in Maths., 182), Springer-Verlag, Berlin, Heidelberg, New York, 1971.
3. G. Karpilovsky, "Commutative Group Algebras", Dekker, 1983.
4. K.H. Leung and S.L. Ma, The structure of Schur rings over cyclic groups, Research Report, Department of Mathematics, National University of Singapore, 1988.
5. W.R. Scott, "Group Theory", Prentice Hall, New Jersey, 1964.
6. M.K. Siu, From binary sequences to combinatorial designs, to appear in *J. Math. Res. and Expos.*
7. T. Storer, "Cyclotomy and Difference sets", Markham, Chicago, 1967.
8. H. Wielandt, "Finite Permutation Groups", Academic Press, New York, 1964.
9. H. Wielandt, Zur Theorie der einfach transitiven Permutationsgruppen II, *Math. Zeit.*, **52** (1949), 384-393.

Department of Mathematics
Hong Kong Baptist College
224 Waterloo Road, Kowloon,
Hong Kong