Another proof of Hiramine’s theorem on three-dimensional Schur rings

Tsuyoshi Atsumi (厚見寅司)
Department of Mathematics
Faculty of Science, Kagoshima University, Kagoshima, 890 Japan
atsumi@sci.kagoshima-u.ac.jp

1 Introduction

Let \( G \) be a finite group. For a subset \( S \) of \( G \), let \( S^{-1} = \{ x^{-1} | x \in S \} \), \( \overline{S} = \sum_{x \in S} x (\in C[G]) \).

Let \( G = S_0 \cup S_1 \cup S_2 \) be a partition of \( G \) of order \( n^2 \) such that \( S_0 = \{1\}, S_1 = S_1^{-1}, S_2 = S_2^{-1} \) and \( \overline{S_i} = \sum_{k=0}^{2} \nu_i^k \overline{S_k} \), where \( \nu_i^k \) are nonnegative integers (0 \( \leq i, j \leq 2 \)). The subring \( \mathcal{R} = \langle \overline{S}_0, \overline{S}_1, \overline{S}_2 \rangle \) of \( Z[G] \) is called a three-dimensional (3D) Schur ring over \( G \). It is well known that the concept of a (3D) Schur ring is equivalent to that of a strongly regular Cayley graph (cf. [1]).

We say that \( \mathcal{R} \) is rational if the eigenvalues of the corresponding strongly regular Cayley graph are rational. \( \mathcal{R} \) is called primitive if \( S_i \) generates \( G \) for all \( i \neq 0 \). \( \mathcal{R} \) is said to be of \((n,r)\)-type if \( |S_1| = r(n-1) \) for some \( r (1 \leq r \leq n) \). We here note that by definition \( \mathcal{R} \) is a Schur ring of \((n,r)\) - type if and only if it is of \((n,n-r+1)\)-type.

We now give an example.

Example 1 Let \( G \) be an group of order \( n^2 \). Let \( \{H_1, H_2, \ldots, H_r\} \) (1 \( \leq r \leq n \)) be a partial spread of \( G \) with degree \( r \). We set \( S_0 = \{1\}, S_1 = H_1 \cup H_2 \cup \ldots H_r - \{1\}, S_2 = G - S_0 \cup S_1. \) Then \( \langle \overline{S}_0, \overline{S}_1, \overline{S}_2 \rangle \) is a Schur ring of \((n,r)\)-type over \( G \).

We note that the Schur ring of the example above satisfies an equation

\[
\overline{S}_1^2 = r(n-1)\overline{S}_0 + (n+r^2-3r)\overline{S}_1 + r(r-1)\overline{S}_2. \tag{A}
\]
A Schur ring of $(n, r)$-type is said to be of Latin square type [2] if it satisfies [A].

We state a conjecture due to [2].

**Conjecture 1** Let $\mathcal{R} = \langle \overline{S}_0, \overline{S}_1, \overline{S}_2 \rangle$ be a Schur ring of $(n, r)$-type over an abelian group $G$ of order $n^2$. Then $\mathcal{R}$ is of Latin square type.

Hiramine [2] verified the conjecture for the case $n > f'(r)$, where $f'(r) = 4r^5 - 8r^4 - 2r^3 - 10r^2 - 3r - 1$.

In this note we shall verify the conjecture for the case $n > f(r)$, where $f(r) = r^5 - 2r^4 + r^3 + 3r^2 - r$.

Notation. We follow the notation and terminology of [2].

## 2 Preliminary results

Assume that $\mathcal{R} = \langle \overline{S}_0, \overline{S}_1, \overline{S}_2 \rangle$ is a Schur ring of $(n, r)$-type over a group $G$ of order $n^2$. By [3] we have

**Lemma 1** The following hold.

(i) $\mathcal{R}$ is primitive unless $r \in \{1, n\}$.

(ii) $\mathcal{R}$ is rational.

In the rest of paper let us assume that $\mathcal{R} = \langle \overline{S}_0, \overline{S}_1, \overline{S}_2 \rangle$ is a Schur ring of $(n, r)$-type over an abelian group $G$ of order $n^2$. We have the following, which is due to [2].

**Lemma 2** Set $\overline{S}_1^2 = a\overline{S}_0 + b\overline{S}_1 + c\overline{S}_2$, where $a, b$ and $c$ are some nonnegative integers. Then,

(i) $a = r(n - 1)$ and $(c - r^2)n + r^2 + (b - c + 1)r + c = 0$.

(ii) If $n > 2r - 1$, then $c$ is even.

(iii) Set $m = \sqrt{(b - c)^2 + 4(rn - r - c)}$. Then $m$ is an integer and $m | n^2$.

**Lemma 3** $c \neq 0$.

**Proof.** If $c = 0$, then $\mathcal{R}$ is non-primitive. This fact contradicts Lemma 1 (ii).

$\blacksquare$
Lemma 4 If \( r = 1 \), then the conjecture is true.

Proof. If \( r = 1 \), then \((n-1)^2 = (n-1) + b(n-1) + c(n^2 - (n-1))\). From this we see that \( c = 0 \) and \( b = n - 2 \), which show that \( \mathcal{R} \) is of Latin square type. □

3 Sketch of Proof

If \( c = r^2 - r \), then \( b = n + r^2 - 3r \) and so the conjecture is true. Our proof is by contradiction. Therefore, we assume that \( 2 \leq r \leq n-1 \), and \( c \neq r^2 - r \).

Lemma 5 \( c \neq r^2 \).

Proof. See [2]. □

Lemma 6 \( 2 \leq c \leq r^2 - 1 \).

Proof. By Lemma 2 (i),

\[
c = r^2 + \frac{r^3 - 2r^2 - (b+1)r}{n-r+1} < r^2 + \frac{r^3 - 2r^2 - r}{f(r) - r + 1} < r^2 + 1.
\]

Hence \( c \leq r^2 - 1 \) by Lemma 5. Lemmas 3 and 2 show that \( 2 \leq c \). □

Assume \( g = r^2 - c \), where \( 1 \leq g \leq r^2 - 2 \). Set \( d = g(n+1)/r \). Then \( d \) is a positive integer. After some calculations we have the following lemma, which is due to Hiramine [2].

Lemma 7

\[(gd + 2r^2 - 2rg - g + gm)|2(r - g)^2(r^2 - g)\]

Proof. See [2]. □

We now distinguish two cases.

(i) The case when \( 2 \leq c < r^2 - r \). The following is a key to our proof of the conjecture.
**Lemma 8** If \( n > f(r) \), then
\[
m^2 - n^2 = ((r - c/r)^2 - 1)n^2 + (2c^2/r^2 + 2c/r + 2r - 2r^2)n
+ 1 - 2c + c^2/r^2 + 2c/r - 2r + r^2
> 0.
\]

**Proof.** Set \( h(n) = r^2(m^2 - n^2) \). Recall that \( g = r^2 - c \). So \( r + 1 \leq g < r^2 - 1 \). Hence
\[
r^2(1 - 2c + c^2/r^2 + 2c/r - 2r + r^2) > 0. \tag{B}
\]
Observe that in case (i)
\[
(r^2 - c)^2 - r^2 > 0. \tag{C}
\]
From (B) and (C) it follows that
\[
h(n) > h'(n) = ((r^2 - c)^2 - r^2)n^2 + (2c^2 + 2cr + 2r^3 - 2r^4)n
= n[(r^2 - c)^2 - r^2)n + 2c^2 + 2cr + 2r^3 - 2r^4]
> 0, \quad \text{when } n \geq \frac{-1(2c^2 + 2cr + 2r^3 - 2r^4)/((r^2 - c)^2 - r^2)}.
\]
On the other hand, since \( r + 1 \leq g < r^2 - 1 \), it follows that \( 2r^3 - 3r - 1 > -1(2c^2 + 2cr + 2r^3 - 2r^4)/((r^2 - c)^2 - r^2). \) Hence if \( n(> f(r)) > 2r^3 - 3r - 1 \), then \( h(n) > 0 \). This completes the proof of this lemma.

So if \( n > f(r) \), then \( m > n \). From this inequality and Lemma 7 we have
\[
gd + 2r^2 - 2rg - g + gn < 2(r - g)^2(r^2 - g). \tag{D}
\]
Since \( gd > gn \), substitution of \( gn \) in \( gd \) of the inequality (D) yields
\[
2gn < 2(r - g)^2(r^2 - g) - 2r^2 - 2rg + g.
\]
So
\[
n < [(r - g)^2(r^2 - g) - r^2 - rg + g/2]/g. \tag{E}
\]
Since \( r + 1 \leq g \leq r^2 - 2 \), the right hand side of (E) is less than \( r^4 + r^3 - 5r^2 - 7r - 1/2 \), which contradicts our assumption. So we complete the proof of our conjecture in this case.

(ii) The case when \( r^2 - r < c \leq r^2 - 1 \). Elaborate arguments show that if \( n > f(r) \), then \( gn/r \leq m \). From this inequality and Lemma 7 we have a contradiction, so we complete the proof of our conjecture. ■
References

