ON 4-EQUIVALENCED ASSOCIATION SCHEMES

JEONG RYE PARK

Abstract. Let \((\Omega, S)\) be an association scheme where \(\Omega\) is a non-empty finite set and \(S\) is a partition of \(\Omega \times \Omega\). For a positive integer \(k\) we say that \((\Omega, S)\) is \(k\)-equivalenced if each non-diagonal element of \(S\) has valency \(k\). In this paper we focus on 4-equivalenced association schemes, and prove that they are transitive.

1. Introduction

Let \((\Omega, S)\) be an association scheme in the sense of [9] where \(\Omega\) is a non-empty finite set and \(S\) is a partition of \(\Omega \times \Omega\). An automorphism of \((\Omega, S)\) is a permutation of \(\Omega\) which fixes each element of \(S\) by the induced action on \(\Omega \times \Omega\). The set of all automorphisms of \((\Omega, S)\) is denoted by \(\text{Aut}(\Omega, S)\) and is called the automorphism group of \((\Omega, S)\). We say that \((\Omega, S)\) is Schurian if the set of orbits of the componentwise action of \(\text{Aut}(\Omega, S)\) on \(\Omega \times \Omega\) coincide with \(S\), transitive (resp. regular) if \(\text{Aut}(\Omega, S)\) is transitive (resp. regular) on \(\Omega\). For a positive integer \(k\), we say that an association scheme \((\Omega, S)\) is \(k\)-equivalenced if \(n_s = k\) for each non-diagonal \(s \in S\), where \(n_s\) is the valency of \(s\). It is an easy observation that the relation set of a 1-equivalenced association scheme form a group. This implies that every 1-equivalenced association scheme is regular (see [11]). Also, it is proved that every 2-equivalenced association scheme is Frobenius [10], and every 3-equivalenced association scheme is Frobenius [8], which implies that they are obtained by Frobenius groups. On the other hand, it is still an open problem whether a 4-equivalenced association scheme is Schurian (or Frobenius). The following is the main result of this paper.

Theorem 1.1. Every 4-equivalenced association scheme is transitive.

In [9], M. Muzychuk and I. Ponomarenko deal with pseudocyclic association schemes, and showed that every pseudocyclic association scheme \((\Omega, S)\) of valency \(k > 1\) is Frobenius if \(|S| \geq 4(k - 1)k^3\). In Section 4, we show that every 4-equivalenced association scheme \((\Omega, S)\) is Frobenius if \(|S| \geq 4 \cdot 41 + 1 = 165\).

Received November 19, 2014; Revised March 2, 2015.

2010 Mathematics Subject Classification. 05E30.

Key words and phrases. association schemes, equivalenced, Frobenius, schurian, transitive.
For the remainder of this section we assume that $(\Omega, S)$ is a 4-equivalenced association scheme. Applying [2, Theorem 3.1] for the adjacency algebra of $(\Omega, S)$, we obtain some equations on intersection numbers of $(\Omega, S)$ and these equations enable us to determine the local structure of the graph $(\Omega, s)$ where $s$ is a non-diagonal element in $S$. In this paper we determine the whole structure of $(\Omega, S)$ by using these equations and give a constructive proof of Theorem 1.1.

This paper is organized as follows. In Section 2, we prepare some terminologies and basic results about association schemes. In Section 3, we prove properties on 4-equivalenced association schemes. In Section 4, we give a sufficient condition for a 4-equivalenced association scheme to be Frobenius. In Section 5, we give a proof of Theorem 1.1. Section 6 consists of a proof of Theorem 3.5 according to the method given in the proof of [2, Theorem 3.1].

2. Preliminaries

We use the same notation on association schemes as in [9]. Let $\Omega$ be a non-empty finite set. We denote the set of $(\alpha, \alpha)$ with $\alpha \in \Omega$ by $1_\Omega$. For each subset $s$ of the Cartesian product $\Omega \times \Omega$, we define $s^*$ to be the set of $(\alpha, \beta)$ with $(\alpha, \beta) \in s$. For each element $\alpha$ in $\Omega$, and for each subset $s$ of $\Omega \times \Omega$, we define $\alpha s$ to be the set of all elements $\beta$ in $\Omega$ such that $(\alpha, \beta) \in s$.

Let $S$ be a partition of $\Omega \times \Omega$. We say that the pair $(\Omega, S)$ is an association scheme if it satisfies the following conditions (see [3], [11] and [12] for a background of the theory of association schemes):

(i) The diagonal set $1_\Omega$ belongs to $S$;
(ii) For each $s \in S$ we have $s^* \in S$;
(iii) For all $u, v, w \in S$ there exists a non-negative integer $c_{uw}$ such that $c_{uw} := |\alpha v \cap \beta w^*| \text{ whenever } (\alpha, \beta) \in u$.

The elements of $\Omega$, $S$ and $c_{uw}$ are called the points, the relations and the intersection numbers of $(\Omega, S)$, respectively.

We say that an association scheme $(\Omega, S)$ is symmetric if $s^* = s$ for all $s \in S$ and commutative if $c_{uw} = c_{wu}$ for all $u, v, w \in S$. It is well-known that each symmetric association scheme is commutative.

For the remainder of this paper we assume that $(\Omega, S)$ is an association scheme. We denote $S \setminus \{1_\Omega\}$ by $S^\#$. For each $s \in S$ we abbreviate $n_s := c_{ss^*}$, which is called the valency of $s$.

The following results are the basic properties about intersection numbers. We shall use it frequently without explicit mention.

**Lemma 2.1** ([11]). For all $u, v, w \in S$ we have the following:

(i) $c_{uv^*} = \delta_{uv}n_u$ where $\delta$ is the Kronecker’s delta;
(ii) $c_{uw} = c_{vw}^*$.
(iii) \( c_{uv}^w n_w = c_{vu}^w n_u = c_{wu}^v n_v \);
(iv) \( n_u n_v = \sum_{s \in S} c_{uv}^w n_s \).

The following is a direct consequence of [1, Theorem 2.2].

**Theorem 2.2.** Let \((\Omega, S)\) be a \(k\)-equivalenced association scheme. If \(k\) is even, 
\((\Omega, S)\) is symmetric and the following holds:

(1) \( \sum_{s \in S} c_{uu}^s c_{vv}^s \equiv \delta_{uv} \pmod{2} \).

Applying Lemma 2.1 for a \(k\)-equivalenced association scheme \((\Omega, S)\) we obtain the following:

(2) \( k = \delta_{vu} + \sum_{w \in S^\#} c_{uv}^w \) for all \( u, v \in S^\# \).

In [11], the **complex product** of two subsets \( U, V \subseteq S \) is defined to be

\[ UV := \left\{ w \in S \mid \sum_{u \in U, v \in V} c_{uv}^w \neq 0 \right\}. \]

For convenience we shall write \( uV \) and \( Uv \) instead of \( \{u\} V \) and \( U \{v\} \), respectively.

For a non-empty subset \( R \subseteq S \), we define

\[ R^* := \{ r^* \mid r \in R \}. \]

We say that \( R \) is **closed** if \( R^* R \subseteq R \). We define \( \langle R \rangle \) to be the intersection of all closed subsets of \( S \) which contain \( R \). We say that \( \langle R \rangle \) is generated by \( R \).

For \( s \in S \) we define a matrix \( A_s \) called the **adjacency matrix** of \( s \) as follows:

\[ (A_s)_{\alpha \beta} := \begin{cases} 1 & \text{if } (\alpha, \beta) \in s \\ 0 & \text{if } (\alpha, \beta) \notin s, \end{cases} \]

where the rows and columns of \( A_s \) are indexed by the elements of \( \Omega \). It follows from the definition of association schemes that

(3) \( A_u A_v = \sum_{w \in S} c_{uv}^w A_w \).

Recall that the hermitian product on \( \text{Mat}_{\Omega}(\mathbb{C}) \) is defined such that, for all \( A, B \in \text{Mat}_{\Omega}(\mathbb{C}) \),

\[ (A, B) = \frac{1}{|\Omega|} \text{Tr}(AB^*), \]

where \( B^* \) is the complex conjugate of \( B \).

As far as there is no confusion in the context we shall write just \( u \) instead of \( A_u \), and \( u \cdot v \) instead of \( A_u A_v \) in order to distinguish it from the complex product \( uv \) for all \( u, v \in S \). For example, we shall write (3) as

\[ u \cdot v = \sum_{w \in S} c_{uv}^w w. \]
Lemma 2.3. For all \(u, v, w \in S\) we have the following:

(i) \(\langle u, v \rangle = n_u \delta_{uv}\);
(ii) \(\langle u \cdot v, w \rangle = c \langle u, w \rangle = \langle u^* \cdot v, w \rangle\);
(iii) \(\langle u \cdot v, u \cdot v \rangle = c \langle u, v \rangle \).

Proof. (i) follows from Lemma 2.1, while (ii) and (iii) follow from the definition of \(\langle *, * \rangle\) and (i).

We use the same notation on group actions as in [6]. We denote the symmetric group of \(\Omega\) by \(\text{Sym}(\Omega)\). The unique relation containing a pair \((\alpha, \beta) \in \Omega \times \Omega\) is denoted by \(r(\alpha, \beta)\). We define the automorphism group of \((\Omega, S)\) to be the set of \(\sigma \in \text{Sym}(\Omega)\) such that, for all \(\alpha, \beta \in \Omega\),

\[ r(\alpha, \beta) = r(\alpha^\sigma, \beta^\sigma). \]

We denote it by \(\text{Aut}(\Omega, S)\).

3. Relations of 4-equivalenced association schemes

In this section we assume that \((\Omega, S)\) is a 4-equivalenced association scheme. It follows from Theorem 2.2 that \((\Omega, S)\) is symmetric.

Lemma 3.1. For any \(s \in S^\#\) one of the following holds:

(i) \(s \cdot s = 4 \cdot 1_\Omega + u + v + w\) for some distinct \(u, v, w \in S^\#\);
(ii) \(s \cdot s = 4 \cdot 1_\Omega + 2u + v\) for some distinct \(u, v \in S^\#\);
(iii) \(s \cdot s = 4 \cdot 1_\Omega + 3u\) for some \(u \in S^\#\).

Proof. Applying (2) with \(k = 4\) we have

\[ 4 = 1 + \sum_{t \in ss \setminus \{1_\Omega\}} c_{ss}^t. \]

Note that \(c_{ss}^t < n_t = 4\) for each \(t \in S^\#\). This completes the proof.

For the remainder of this paper, we use the following notation.

\[ S_i := \{ s \in S \mid |ss| = i \}. \]

It is clear that \(S_1 = \{1_\Omega\}\) and \(S^\#\) is the disjoint union of \(S_2, S_3\) and \(S_4\).

Lemma 3.2. For each \(s \in S_2, ss = \{1_\Omega, s\}\).

Proof. Suppose that \(s \cdot s = 4 \cdot 1_\Omega + 3t\) for some \(t \in S^\#\) with \(s \neq t\). For any \(\alpha \in \Omega\), \(as\) has exactly four elements. We set

\[ as := \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}. \]

Then \(r(\alpha_i, \alpha_j) = t\) whenever \(i \neq j\). This implies that the graph \((as, t \cap (as \times as))\) is the complete graph \(K_4\) (see Figure 1).
It is easy to see that \(c_{tt} \geq 2\). Applying (2) with \(k = 4\) we have
\[
4 = \sum_{u \in st} c_{st}^u.
\]
Since by Lemma 3.1 and by Lemma 2.1, \(c_{st}^s = c_{st}^t = 3\), we have
\[
40 \leq \langle s \cdot t, s \cdot t \rangle = \langle s \cdot t, s \cdot t \rangle = 40.
\]
This implies that \(c_{tt} = 2\). For each \(i = 1, 2, 3, 4\) there exists a unique \(\gamma \in \alpha_i t\) such that \(\gamma \notin \alpha s \cap \alpha_i t\). Since \(c_{tt} = |\alpha_i t \cap \gamma t| = 2\) and \((\alpha_i t \cap \gamma t) \subset \alpha s\), for \(\alpha_i, \alpha_i' \in \alpha_i t \cap \gamma t\),
\[
|\alpha_i t \cap \alpha_i' t| = c_{tt} = 3.
\]
This is a contradiction. □

By Lemma 3.1 (ii) we can define two mappings \(\varphi\) and \(\psi\) from \(S_3\) to \(S^\#\) such that \(s \cdot s = 4 \cdot 1_\Omega + 2s^\varphi + s^\psi\) for each \(s \in S_3\).

**Lemma 3.3.** For each \(s \in S_3\), \(s^\varphi \in S_3\) and \(s^\psi = (s^\varphi)^\varphi\).

**Proof.** Suppose that \(s \cdot s = 4 \cdot 1_\Omega + 2s^\varphi + s^\psi\) where \(s^\varphi \neq s^\psi\). For any \(\alpha \in \Omega\), we set
\[
\alpha s := \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}.
\]
Since by Lemma 2.1, \(c_{st}^s = c_{st}^t = 1\), for each \(i = 1, 2, 3, 4\) we have \(|\alpha s \cap \alpha_i s^\psi| = 1\). Without loss of generality, we may assume that \(r(\alpha_1, \alpha_3) = s^\psi\). It immediately follows that \(r(\alpha_2, \alpha_4) = s^\varphi\) and \((\alpha s, s^\varphi \cap (\alpha s \times \alpha s))\) is the cycle \(C_4\) (see Figure 2). Then we have
\[
\alpha_2, \alpha_4 \in \alpha_1 s^\varphi \cap \alpha_3 s^\psi \text{ and } \alpha_1, \alpha_3 \in \alpha_2 s^\psi \cap \alpha_4 s^\varphi.
\]
Since \(s^\varphi \neq s^\psi\), by Lemma 3.1 and Lemma 3.2 we have
\[
s^\varphi \cdot s^\psi = 4 \cdot 1_\Omega + 2s^\psi + (s^\varphi)^\psi.
\]
This completes the proof. □

**Lemma 3.4.** For all \(s, t \in S^\#\) with \(s \neq t\) one of the following holds:
Figure 2. Note that $c_{ss}^\alpha = 2$, there is an element in $\Omega$ which is not equal to $\alpha$.

(i) $s \cdot t = u_1 + u_2 + u_3 + u_4$ for some distinct $u_1, u_2, u_3, u_4 \in S^\#$;
(ii) $s \cdot t = 2u_1 + u_2 + u_3$ for some distinct $u_1, u_2, u_3 \in S^\#$;
(iii) $s \cdot t = 2u_1 + 2u_2$ for some distinct $u_1, u_2 \in S^\#$.

Proof. Applying (2) with $k = 4$ we have

$$4 = \sum_{u \in S^\#} c_{st}^u.$$

It suffices to show that $c_{st}^u < 3$ for each $u \in st$. If $c_{st}^u \geq 3$, then $(s \cdot t, s \cdot t) \in \{40, 64\}.$

Since $s \neq t$, by Lemma 3.1 and Lemma 3.2

$$(s \cdot s, t \cdot t) \in \{16, 20, 24, 28, 36, 40\}.$$ 

This implies that $c_{st}^u \neq 4$. Thus we may assume that $s \cdot t = 3u_1 + u_2$ for some distinct $u_1, u_2 \in S^\#$. Then by Lemma 3.1 and Lemma 3.2, $\{c_{sa}^v, c_{tb}^v\} = \{2, 3\}$ where $v \in \{s, t\}$. Without loss of generality $v = s$, then $c_{st}^s = c_{st}^t = 2$. This is a contradiction to our assumption.

In [2], they deal with homogeneous standard integral table algebras of degree 4. Applying [2] for adjacency algebra of $(\Omega, S)$, we obtain the following.

Theorem 3.5. The following properties hold:

(i) $\varphi$ is a permutation of $S_3$;
(ii) $\varphi^2 = \psi$;
(iii) $S_4 = \emptyset$.

Proof. The proof with the assumption that $|\langle s \rangle| > 4$ for each $s \in S^\#$ is given in [2, Theorem 3.1], and we give a proof without using the condition in Section 6.
By Theorem 3.5 and Lemma 3.2, we extends \( \varphi \) to the permutation of \( S \) whose restriction to \( S_1 \cup S_2 \) is the identity. From now on, we may regard \( \varphi \) as a permutation of \( S \).

**Lemma 3.6.** For all \( s, t \in S^\# \) with \( s \neq t \), if \( |st| = 2 \), then \( st = \{s, t\} \) and \( s = s^\varphi \), \( t = t^\varphi \).

**Proof.** We assume that \( s \cdot t = 2u_1 + 2u_2 \) for some distinct \( u_1, u_2 \in S^\# \). Then we have

\[
(s \cdot s, t \cdot t) = (s \cdot t, s \cdot t) = 32.
\]

It follows from Lemma 3.1 and Lemma 3.3 that \( t^\varphi = s^\varphi \) and \( t^\psi = s^\psi \). Thus we have \( t = s^\varphi \) and \( s = t^\varphi \).

By Lemma 2.1(ii) and (iii), \( c_{st}^s = c_{ss}^\varphi = 2 \) and \( c_{st}^t = c_{tt}^\varphi = 2 \). Therefore by Lemma 3.4 we have \( s \cdot t = 2s + 2t \). This completes the proof. \( \square \)

4. Frobenius schemes

4.1. Pseudocyclic schemes

An association scheme \((\Omega, S)\) is called pseudocyclic with valency \( k \) if the ratio \( k \) of the multiplicity and degree of its non-principal irreducible character does not depend on the choice of the character [9].

The indistinguishing number of a relation \( s \in S \) is defined to be the number

\[
c(s) = \sum_{t \in S} c_{st}^s.
\]

The maximum of \( c(s) \), \( s \in S^\# \), is called the indistinguishing number of \((\Omega, S)\).

The following results are suggested by Muzychuck and Ponomarenko.

**Theorem 4.1** ([9, Theorem 3.2]). The following are equivalent:

(i) \((\Omega, S)\) is a pseudocyclic association scheme with valency \( k \);

(ii) \((\Omega, S)\) is a \( k \)-equivalenced scheme with \( c(s) = k - 1 \) for all \( s \in S^\# \).

**Theorem 4.2** ([9, Theorem 7.4]). Every pseudocyclic association scheme \((\Omega, S)\) with valency \( k > 1 \) and \( |S| \geq 4(k - 1)k^3 \) is Frobenius.

It follows from Theorem 3.5 and Theorem 4.1 that every 4-equivalenced association scheme \((\Omega, S)\) is pseudocyclic. Moreover, it is Frobenius if \( |S| \geq 768 \) by Theorem 4.2. Hence, the bound \( |S| \) can be improved for 4-equivalenced association schemes.

**Theorem 4.3.** Every 4-equivalenced association scheme \((\Omega, S)\) with \( |S| \geq 165 \) is Frobenius.
Proof. For each \( u, v \in S^\# \) we denote
\[
D(u, v) := \{ w \in S^\# \mid (uvw) \cap ww = \{ 1_\Omega \} \}
\]
and
\[
\bar{D}(u, v) := S^\# \setminus D(u, v).
\]
Then by Theorem 3.5
\[
uvw = \{ 1_\Omega, u^\varphi, u^\psi, v^\varphi, v^\psi, u^\varphi v^\psi, u^\psi v^\varphi, u^\psi v^\psi \},
\]
and then by Lemma 3.4 \(|uvwv \setminus \{ 1_\Omega \}|\) is at most 20. Let \( t \in uuvv \) with \( t \neq 1_\Omega \).

By Theorem 3.5 if \( t \in S_2 \), then \( t \in D(u, v) \) and if \( t \in S_3 \), then \( t^{v^{-1}}, t^{v^{-1}} \in D(u, v) \). Thus we have \(|D(u, v)| \leq 40 < 41\). If \(|S^\#| \geq 4 \cdot 41\), then
\[
\bigcap_{a \in \{u, v\}} \bigcap_{b \in \{w, w'\}} D(a, b) \neq \emptyset, \quad w, w' \in D(u, v)
\]
and for all \( u, v, w \in S^\# \),
\[
D(u, v) \cap D(v, w) \cap D(w, u) \neq \emptyset
\]
are satisfied. The assertion holds by the same argument in the proof of [9, Theorème 5.4 and Theorem 7.1].

4.2. Affine schemes

For some background on affine spaces we refer to [4]. Let \( \Omega \) be a point set of a finite affine space. Denote by \( S \) the partition of \( \Omega \times \Omega \) containing \( 1_\Omega \) such that two pairs \( (\alpha, \beta), (\alpha', \beta') \in \Omega \times \Omega \), \( \alpha \neq \beta \), \( \alpha' \neq \beta' \), belong to the same class if and only if the lines \( \alpha \beta \) and \( \alpha' \beta' \) are equal or parallel. Then the pair \( (\Omega, S) \) is an association scheme called the affine scheme of an affine space. It was shown in [5] that an association scheme whose relations are involutions is an affine scheme.

Let \( (\Omega, S) \) be a 4-equivalenced association scheme such that \( S^\# = S_2 \). It follows from Lemma 3.2 that \( \langle s \rangle = \{ 1_\Omega, s \} \) for all \( s \in S^\# \). Thus \( (\Omega, S) \) is an affine scheme of an affine space of order 5.

**Theorem 4.4.** Every 4-equivalenced association scheme \( (\Omega, S) \) with \( S^\# = S_2 \) is Frobenius.

**Proof.** The number of points of the affine space which has order \( n \) and dimension \( d \) is equal to \( n^d \). It was proved in [9, Section 7.1] that every affine scheme of order 5 and dimension at least 3 is Frobenius. Since every affine scheme \( (\Omega, S) \) with \(|\Omega| \leq 25\) is classified [7], the assertion holds.

5. Main results

In this section we assume that \( (\Omega, S) \) is a 4-equivalenced association scheme.
5.1. Construction of lines

For $s \in S_3$ and $\alpha_0, \alpha_1, \ldots, \alpha_n \in \Omega$ with $n \geq 2$, a sequence $(\alpha_0, \alpha_1, \ldots, \alpha_n)$ is called an $s$-line if for each $i = 0, 1, \ldots, n - 1, j = 0, 1, \ldots, n - 2$, $r(\alpha_i, \alpha_{i+1}) = s$ and $r(\alpha_j, \alpha_{j+2}) = s^\psi$(see Figure 3).

\begin{figure}[h]
\centering
\includegraphics[scale=0.5]{figure3}
\caption{Figure 3}
\end{figure}

**Lemma 5.1.** Given a relation $s \in S_3$ and points $\alpha, \beta \in \Omega$ such that $r(\alpha, \beta) = s$, there exists $\gamma \in \Omega$ such that $(\alpha, \beta, \gamma)$ is an $s$-line.

**Proof.** By Theorem 3.5 and Lemma 2.1, $c_{ss} = c_{ss}^\psi = 1$. Since $r(\alpha, \beta) = s$, there exists a unique point $\gamma \in \alpha s \psi \cap \beta s$. Then $(\alpha, \beta, \gamma)$ satisfies the conditions of an $s$-line. \qed

The following corollary is immediate from Lemma 5.1.

**Corollary 5.2.** Let $(\alpha_0, \alpha_1, \ldots, \alpha_n)$ be an $s$-line. Then there exists a unique point $\alpha_{n+1} \in \Omega$ such that $(\alpha_0, \alpha_1, \ldots, \alpha_n, \alpha_{n+1})$ is an $s$-line.

**Lemma 5.3.** For any $s \in S_3$ with $s = s^\psi$, if $(\alpha_0, \alpha_1, \ldots, \alpha_n)$ be an $s$-line, then $\alpha_i = \alpha_j$ if and only if $i \equiv j \pmod{3}$.

**Proof.** By the definition of an $s$-lines, $\alpha_i \in \alpha_{i+1}s \cap \alpha_{i+2}s^\psi$ and $\alpha_{i+3} \in \alpha_{i+1}s^\psi \cap \alpha_{i+2}s$. Since $s = s^\psi$, we have $c_{ss} = c_{ss}^\psi = 1$ by Theorem 3.5. Thus $\alpha_i = \alpha_{i+3}$. This completes the proof. \qed

5.2. Construction of planes

For any $s \in S_3$ and $\alpha, \beta, \gamma \in \Omega$, we say that a triple $(\alpha, \beta, \gamma)_s$ is an $s$-triangle if $\beta, \gamma \in \alpha s$ and $r(\beta, \gamma) = s^\psi$. Let $(\alpha, \beta, \gamma)_s$ be an $s$-triangle. We define a map

$P(\alpha, \beta, \gamma)_s : \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \to \Omega$ by $(i, j) \mapsto \alpha_{i,j}$

as follows:

(i) $\alpha_{0,0} := \alpha, \alpha_{1,0} := \beta, \alpha_{0,1} := \gamma.$
We shall write \( (\alpha, \beta, \gamma) \) where \( \delta \).

Subsection 5.4. We say that the map \( (\alpha, \beta, \gamma) \) if \( (\alpha) \) are uniquely determined, and then for each \( s \) this implies that \( \epsilon \).

\[ \psi \]

\[ \phi \cap \gamma \]

\[ \beta \]

\[ \phi \cap \gamma \]

\[ \beta \]

\[ \phi \cap \gamma \]

\[ \beta \]

\[ \phi \cap \gamma \]

\[ \beta \]

\[ \phi \cap \gamma \]

\[ \beta \] for each \( i, j \) by Lemma 5.1 and Corollary 5.2.

Theorem 5.4. Let \( (\alpha, \beta, \gamma) \) and \( (\alpha', \beta', \gamma') \) be similar. We say that \( (\alpha, \beta, \gamma) \) and \( (\alpha', \beta', \gamma') \) are parallel if

\[ r(\gamma, P(\alpha, \beta, \gamma)_s(2, 0)) = r(\gamma', P(\alpha', \beta', \gamma')_s(2, 0)) \]
Throughout this subsection, we fix $s \in S_3$ with $s \neq s^{\psi}$. It follows from Theorem 3.5 that $c_{ss^\psi} = c_{ss} = 2$. Then by Lemma 3.4 and Lemma 3.6, 

$$s \cdot s^\psi = 2s + a + b$$

for some distinct $a, b \in S^\#$.

**Lemma 5.6.** Let $(\alpha_0, \alpha_1, \alpha_2)$ be an $s$-line. Then for each $a \in s^\psi s \setminus \{s\}$, there exists a unique point $\beta \in \Omega$ such that 

$$\beta \in \alpha_0 s \cap \alpha_1 s \cap \alpha_2 a.$$ 

**Proof.** By Theorem 3.5 and Lemma 2.1, $c_{ss^\psi} = c_{ss} = 2$, there exist distinct $\beta, \beta' \in \Omega$ such that 

$$\{\beta, \beta'\} = \alpha_0 s \cap \alpha_1 s \cap \alpha_2 a.$$ 

Now we assume that $r(\beta, \alpha_2) = r(\beta', \alpha_2)$. For short we set $t := r(\beta, \alpha_2)$. Then 

$$\beta, \beta' \in \alpha_1 s^\psi \cap \alpha_2 t.$$ 

This implies that $c_{ss^\psi} = c_{ss} \geq 2$. Since $s$ is the unique relation such that $c_{ss^\psi} = c_{ss} = 2$, we have $t = s$. It follows that $\beta, \beta' \in \alpha_0 s \cap \alpha_2 s$, which contradicts that $c_{ss^\psi} = 1$. We have 

$$\{r(\beta, \alpha_2), r(\beta', \alpha_2)\} = s^\psi s \setminus \{s\}.$$ 

Therefore, we can determine the point for each relation in $s^\psi s \setminus \{s\}$. \hfill $\square$

**Lemma 5.7.** Let $(\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4)$ be an $s$-line. For $i = 0, 1, 2$ we shall denote

$$\beta_i \in \alpha_i s \cap \alpha_{i+1} s^\psi \cap \alpha_{i+2} a$$

where $a \in s^\psi s \setminus \{s\}$. Then $(\beta_0, \beta_1, \beta_2)$ is an $s$-line.

**Proof.** There exists $\gamma \in \alpha_2 s$ such that $r(\beta_1, \gamma) = b$ where $b$ is a unique relation in $s^\psi s \setminus \{s, a\}$ (see Figure 5). Since 

$$r(\beta_1, \alpha_1) = s \text{ and } r(\beta_1, \alpha_3) = a,$$
we have $\gamma \notin \{\alpha_1, \alpha_3\}$. Thus $r(\alpha_1, \gamma) = s^\varphi$. If $r(\beta_0, \beta_1) = b$ (resp. $r(\beta_0, \beta_1) = a$), then $\gamma, \beta_0 \in \beta_1 b \cap \alpha_1 s^\varphi$ (resp. $\beta_1, \alpha_2 \in \beta_0 a \cap \alpha_2 s^\varphi$). Since $s$ is the unique relation such that $c^x_{ss^\varphi} = c^x_{ss^\varphi} = 2$, we have $c^y_{ss^\varphi} = c^y_{ss^\varphi} = 1$ and $c^x_{as^\varphi} = c^x_{as^\varphi} = 1$. It follows that $\gamma = \beta_0$ (resp. $\beta_1 = \alpha_2$), which contradicts that $s \neq a$ (resp. $s \neq 1_{\Omega}$). Since $r(\beta_0, \beta_1) \in r(\beta_0, \alpha_1) \cap r(\alpha_1, \beta_2)$, we obtain that $r(\beta_0, \beta_1) = s^\varphi$. Similarly, $r(\beta_1, \beta_2) = s^\varphi$. To complete the proof, it suffices to verify that $r(\beta_0, \beta_2) = s^\psi$. Since $\beta_1, \alpha_2 \in \alpha_1 s \cap \beta_2 s$, it follows that $r(\alpha_1, \beta_2) = s^\varphi$. Then
\[
\begin{align*}
\{r(\alpha_1, \alpha_0, \gamma), r(\alpha_1, \alpha_1, \gamma+1), r(\alpha_1, \alpha_1+1, \gamma+2), r(\alpha_1, \alpha_1+2, \gamma+1)\} = ss^\varphi \setminus \{s\}.
\end{align*}
\]
Therefore, $(\beta_0, \beta_1, \beta_2)$ satisfies the conditions of an $s$-line. \qed

By Lemma 5.1 and Corollary 5.2 for each $i$ the points $\alpha_{i,0}$ and $\alpha_{0,i}$ are uniquely determined. Also, by Lemma 5.7 for each $j \geq 1$ the sequence $(\alpha_{0,j}, \alpha_{1,j}, \alpha_{2,j}, \ldots)$ is an $s$-line and the points $\alpha_{i,j}$ is also uniquely determined by Lemma 5.6. Thus, $P(\alpha, \beta, \gamma)_s$ is well-defined.

Let $(\alpha, \beta, \gamma)_s$ be an $s$-triangle. For any $i, j \in \mathbb{Z}_{\geq 0}$, it follows immediately from the construction of the $s$-plane that

\begin{enumerate}
\item $r(\alpha_{i,j}, \alpha_{i+1,j+1}) = s^\varphi$ (see Figure 6)
\end{enumerate}

where $\alpha_{i,j} := P(\alpha, \beta, \gamma)_s(i, j)$.

**Lemma 5.8.** Let $(\alpha, \beta, \gamma)_s$ be an $s$-triangle. Then for any $i, j \in \mathbb{Z}_{\geq 0}$,

\[
\{r(\alpha_{i,j}, \alpha_{i+1,j+2}), r(\alpha_{i,j}, \alpha_{i+2,j+1})\} = ss^\varphi \setminus \{s\}.
\]

Moreover, $r(\alpha_{0,1}, \alpha_{2,0}) = r(\alpha_{i,j}, \alpha_{i+1,j+2})$ where $\alpha_{i,j} := P(\alpha, \beta, \gamma)_s(i, j)$ (see Figure 7).

**Figure 5**
Proof. From (4), we may assume that $i = j = 0$.

Note that

$r(\alpha_{0,0}, \alpha_{1,2}), r(\alpha_{0,0}, \alpha_{2,1}) \in ss^\psi$.

First, we will show that the left-hand side is contained in the right-hand side. If $r(\alpha_{0,0}, \alpha_{1,2}) = s$ (resp. $r(\alpha_{0,0}, \alpha_{2,1}) = s$), then $\alpha_{0,1}, \alpha_{1,2} \in \alpha_{0,0}s \cap \alpha_{0,2}s$ (resp. $\alpha_{1,0}, \alpha_{2,1} \in \alpha_{0,0}s \cap \alpha_{2,0}s$). Since $c_{ss}^\psi = 1$, we have $\alpha_{0,1} = \alpha_{1,2}$ (resp. $\alpha_{1,0} = \alpha_{2,1}$), which contradicts that $s^\psi \neq 1_\Omega$.

Secondly, we will show that the right-hand side is contained in the left-hand side. It suffices to show that $r(\alpha_{0,0}, \alpha_{1,2}) \neq r(\alpha_{0,0}, \alpha_{2,1})$. We set $t := r(\alpha_{0,0}, \alpha_{1,2})$ for short. If $r(\alpha_{0,0}, \alpha_{2,1}) = t$, then

$$\alpha_{1,2}, \alpha_{2,1} \in \alpha_{0,0}t \cap \alpha_{1,1}s.$$ 

By the construction of the $s$-plane, $r(\alpha_{1,2}, \alpha_{2,1}) = s^\psi$ and $\alpha_{1,2} \neq \alpha_{2,1}$. This implies $c_{ss}^\psi = c_{ss}^\psi \geq 2$. Since $s$ is the unique relation such that $c_{ss}^\psi = c_{ss}^\psi = 2$, we have $t = s$. This is a contradiction to the previous step.

To complete the proof, we assume that $r(\alpha_{0,1}, \alpha_{2,0}) = r(\alpha_{0,0}, \alpha_{2,1})$. For short $t := r(\alpha_{0,1}, \alpha_{2,0})$. Then by the construction of an $s$-plane, we have

$$t = r(\alpha_{0,2}, \alpha_{2,1}) = r(\alpha_{0,0}, \alpha_{2,1}).$$

Then

$$\alpha_{0,0}, \alpha_{0,2} \in \alpha_{1,1}s^\psi \cap \alpha_{2,1}s.$$ 

By the construction of the $s$-plane, $r(\alpha_{0,0}, \alpha_{0,2}) = s^\psi$ and $\alpha_{0,0} \neq \alpha_{0,2}$. This implies $c_{ss}^\psi = c_{ss}^\psi \geq 2$. It follows from the previous part that $t = s$. \qed

It follows from (4) and Lemma 5.8 that
(5) \((\alpha, \beta, \gamma)_s \sim (\alpha_{i+j}, \alpha_{i+j-1}, \alpha_{i+j+1})_s\)
\sim (\alpha_{i+j}, \alpha_{i+j-1}, \alpha_{i+j-1})_s \sim (\alpha_{i+j}, \alpha_{i+j+1}, \alpha_{i+j})_s\) (see Figure 8)

where the subscripts of \(\alpha\) are non-negative.

**Figure 8**

**Lemma 5.9.** For \(\alpha, \alpha' \in \Omega\) with \(r(\alpha, \alpha') = r(\beta, \beta')\), we shall denote \(\alpha' = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}\) and \(\beta' = \{\beta_1, \beta_2, \beta_3, \beta_4\}\). If \(r(\alpha, \alpha_i) = r(\beta, \beta_i)\) for each \(i = 1, 2, 3\), then \(r(\alpha, \alpha_4) = r(\beta, \beta_4)\) (see Figure 9).

**Figure 9**

**Proof.** For short we set \(u := r(\alpha, \alpha_4), v := r(\beta, \beta_4)\) and \(a := r(\alpha, \alpha') = r(\beta, \beta')\).

We assume that \(u \neq v\). Then
\[
as = \{r(\alpha, \alpha_1), r(\alpha, \alpha_2), r(\alpha, \alpha_3), u\}\n\]
and
\[
as = \{r(\beta, \beta_1), r(\beta, \beta_2), r(\beta, \beta_3), v\}.
\]
Since \(u, v \in as\),
\[
\{r(\beta, \beta_1), r(\beta, \beta_2), r(\beta, \beta_3)\} \subset u.
\]
and
\[
\{r(\alpha, \alpha_1), r(\alpha, \alpha_2), r(\alpha, \alpha_3)\} \subset v.
\]
Without loss of generality, we may assume that \( u = r(\beta, \beta_1) \) and \( v = r(\alpha, \alpha_2) \).
Since \( r(\beta, \beta_1) = r(\alpha, \alpha_1) \) and \( r(\alpha, \alpha_2) = r(\beta, \beta_2) \), we have
\[
\alpha_1, \alpha_4 \in au \cap \alpha's \text{ and } \beta_2, \beta_4 \in bv \cap \beta's.
\]
By Lemma 2.1, we have \( c_{us}^u = c_{us}^a \geq 2 \) and \( c_{us}^v = c_{us}^a \geq 2 \). It follows from Lemma 3.4 that
\[
a \cdot s = 2u + 2v.
\]
Thus by Lemma 3.6 we have \( s = s^\psi \), which is a contradiction. \( \square \)

**Proposition 5.10.** For any \( n \in \mathbb{Z}_{\geq 0} \) and \( \alpha, \beta, \gamma, \alpha', \beta', \gamma' \in \Omega \), if \((\alpha, \beta, \gamma)_s\) is similar to \((\alpha', \beta', \gamma')_s\), then \( r(\alpha, \mathcal{P}(\alpha, \beta, \gamma)_s(i, j)) = r(\alpha', \mathcal{P}(\alpha', \beta', \gamma')_s(i, j)) \) for all \( i, j \in \mathbb{Z}_{\geq 0} \) where \( 0 \leq i, j \leq n \).

**Proof.** We shall denote \( \mathcal{P}(\alpha, \beta, \gamma)_s(i, j) \) and \( \mathcal{P}(\alpha', \beta', \gamma')_s(i, j) \) by \( \alpha_{i,j} \) and \( \beta_{i,j} \), respectively. We proceed to use the induction on \( n \).

By the construction of \( s \)-planes, it is clear that
\[
\begin{align*}
r(\alpha_{0,0}, \alpha_{0,0}) &= r(\beta_{0,0}, \beta_{0,0}) = 1_\Omega, \\
r(\alpha_{0,0}, \alpha_{1,0}) &= r(\alpha_{0,0}, \alpha_{0,1}) = r(\beta_{0,0}, \beta_{1,0}) = r(\beta_{0,0}, \beta_{0,1}) = s, \\
r(\alpha_{0,0}, \alpha_{1,1}) &= r(\alpha_{0,1}, \alpha_{1,0}) = r(\beta_{0,1}, \beta_{1,1}) = r(\beta_{0,1}, \beta_{1,0}) = s^\psi
\end{align*}
\]
and
\[
r(\alpha_{0,0}, \alpha_{2,0}) = r(\alpha_{0,0}, \alpha_{0,2}) = r(\beta_{0,0}, \beta_{2,0}) = r(\beta_{0,0}, \beta_{0,2}) = s^\psi.
\]
Note that by Lemma 3.3
\[
r(\alpha_{0,0}, \alpha_{2,2}), r(\beta_{0,0}, \beta_{2,2}) \in s^\psi s^\psi \cap s^\psi s^\psi = \{1_\Omega, (s^\psi)^5\}.
\]
Since
\[
r(\alpha_{0,0}, \alpha_{2,2}) \in r(\alpha_{0,0}, \alpha_{1,0}) r(\alpha_{1,0}, \alpha_{2,2}) = sr(\alpha_{1,0}, \alpha_{2,2})
\]
and
\[
r(\beta_{0,0}, \beta_{2,2}) \in r(\beta_{0,0}, \beta_{1,0}) r(\beta_{1,0}, \beta_{2,2}) = sr(\beta_{1,0}, \beta_{2,2}),
\]
we have \( r(\alpha_{0,0}, \alpha_{2,2}) = r(\beta_{0,0}, \beta_{2,2}) = (s^\psi)^5 \). Since \( \alpha, \beta, \gamma, \alpha', \beta', \gamma' \) are arbitrary, it follows from Lemma 5.8 and (5) that the result holds if \( n = 2 \).

Now, we assume that \( r(\alpha_{0,0}, \alpha_{i,j}) = r(\beta_{0,0}, \beta_{i,j}) \) for \( 0 \leq i, j < n \). Since \( \alpha, \beta, \gamma, \alpha', \beta', \gamma' \) are arbitrary, it suffices to show that \( r(\alpha_{0,0}, \alpha_{n,j}) = r(\beta_{0,0}, \beta_{n,j}) \) for each \( j \). Note that by (4),
\[
(\alpha_{0,0}, \alpha_{1,0}, \alpha_{0,1}) \sim (\alpha_{0,1}, \alpha_{1,1}, \alpha_{0,2}) \text{ and } (\beta_{0,0}, \beta_{1,0}, \beta_{0,1}) \sim (\beta_{0,1}, \beta_{1,1}, \beta_{0,2}).
\]
Thus, we shall prove that \( r(\alpha_{0,1}, \alpha_{n,j+1}) = r(\beta_{0,1}, \beta_{n,j+1}) \) instead of \( r(\alpha_{0,0}, \alpha_{n,j}) = r(\beta_{0,0}, \beta_{n,j}) \) by some technical reason of subscripts.

By the induction hypothesis,
\[
r(\alpha_{1,2}, \alpha_{n,j+1}) = r(\beta_{1,2}, \beta_{n,j+1}), \quad r(\alpha_{2,1}, \alpha_{n,j+1}) = r(\beta_{2,1}, \beta_{n,j+1}),
\]
and
\[
r(\alpha_{1,0}, \alpha_{n,j+1}) = r(\beta_{1,0}, \beta_{n,j+1}).
\]
By substituting \( (\alpha_{n,j+1}, \alpha_{1,1}, \beta_{n,j+1}, \beta_{1,1}) \) instead of \( (\alpha, \alpha', \beta, \beta') \) in Lemma 5.9, the assertion holds. \( \square \)
5.5. Properties of planes

In this subsection, we fix \( s \in S_3 \).

**Lemma 5.11.** Given \( s \in S_3 \) and \( \alpha, \alpha', \beta, \beta' \in \Omega \) such that \( r(\alpha, \beta) = r(\alpha', \beta') \in \langle s \rangle \) and \( r(\alpha, \alpha') \neq r(\beta, \beta') \not\in \langle s \rangle \). For any \( \gamma \in \alpha s \), there exists a unique point \( \gamma' \in \alpha' r(\alpha, \gamma) \cap \beta' r(\beta, \gamma) \) such that \( r(\alpha, \alpha') = r(\gamma, \gamma') \) (see Figure 10).

![Figure 10](image)

**Proof.** For short we set \( u := r(\alpha, \alpha') = r(\beta, \beta') \), \( a := r(\alpha, \gamma) \) and \( b := r(\beta, \gamma) \).

Then \( r(\alpha', \gamma) \in r(\alpha', \alpha) r(\alpha, \gamma) = ua \) and \( r(\beta', \gamma) \in r(\beta', \beta) r(\beta, \gamma) = ub \).

Since \( a, b \in \langle s \rangle \) and \( u \not\in \langle s \rangle \),

\[
\langle u \cdot a, u \cdot a \rangle = \langle u \cdot u, a \cdot a \rangle = 16 \quad \text{and} \quad \langle u \cdot b, u \cdot b \rangle = \langle u \cdot u, b \cdot b \rangle = 16.
\]

By Lemma 3.4 we have

\[
1 = |\alpha' a \cap \gamma u| = |\alpha' a \cap \gamma u| \quad \text{and} \quad 1 = |\beta' b \cap \gamma u| = |\beta' b \cap \gamma u|.
\]

Thus, there exist unique points \( \delta \) and \( \delta' \) such that

\[
\delta \in \alpha' a \cap \gamma u \quad \text{and} \quad \delta' \in \beta' b \cap \gamma u.
\]

Since

\[
r(\delta, \delta') \in r(\delta, \alpha') r(\alpha', \beta') r(\beta', \delta') = ab(\alpha', \beta') b \subseteq \langle s \rangle
\]

and

\[
r(\delta, \delta') \in r(\delta, \gamma) r(\gamma, \delta') = uu,
\]

we have \( r(\delta, \delta') \in uu \cap \langle s \rangle = \{1 \_G\} \). By taking \( \gamma' = \delta = \delta' \), there exists \( \gamma' \in \alpha' a \cap \beta' b \) such that \( r(\gamma, \gamma') = u \). \( \square \)

**Lemma 5.12.** Let \( (\alpha, \beta, \gamma)_s \) and \( (\alpha', \beta', \gamma')_s \) be parallel. Then for any \( i, j \in \mathbb{Z}_{\geq 0} \), \( r(\mathcal{P}(\alpha, \beta, \gamma)_s(i, j), \mathcal{P}(\alpha', \beta', \gamma')_s(i, j)) \) is constant.

**Proof.** By our assumption, \( (\alpha, \beta, \gamma)_s \) is similar to \( (\alpha', \beta', \gamma')_s \). Since all of the points \( \mathcal{P}(\alpha, \beta, \gamma)_s(i, j) \) and \( \mathcal{P}(\alpha', \beta', \gamma')_s(i, j) \) are uniquely determined by \( (\alpha, \beta, \gamma)_s \) and \( (\alpha', \beta', \gamma')_s \), the result follows from Proposition 5.5, Proposition 5.10 and Lemma 5.11. \( \square \)
Lemma 5.13. Let $(\alpha, \beta, \gamma)_s$ and $(\alpha', \beta', \gamma')_s$ be parallel. Then for any $i, j \in \mathbb{Z}_{\geq 0}$, $(\alpha', \beta', \gamma')_s \simeq (\alpha_{i,j}, \alpha_{i+1,j}, \alpha_{i,j+1})_s$ where $\alpha_{i,j} := \mathcal{P}(\alpha, \beta, \gamma)_s(i,j)$.

Proof. From Proposition 5.5 and Proposition 5.10, we may assume that $r(\alpha, \alpha') \notin \langle s \rangle$. It follows from (4) that $(\alpha', \beta', \gamma')_s$ is similar to $(\alpha_{i,j}, \alpha_{i+1,j}, \alpha_{i,j+1})_s$ for any $i, j \in \mathbb{Z}_{\geq 0}$. Thus, it suffices to show that

$$(\alpha', \beta', \gamma')_s \simeq (\alpha_{1,0}, \alpha_{2,0}, \alpha_{1,1})_s.$$  

For short we set

$$u := r(\alpha', \alpha_{0,0}), \quad v := r(\alpha', \alpha_{1,0}) \text{ and } w := r(\alpha', \alpha_{2,0}).$$

Then $r(\delta', \alpha_{2,0}) = u$ where $\delta' \in \alpha' \cap \beta'. \text{ Note that }$

$$v \in r(\alpha', \alpha_{0,0})r(\alpha_{0,0}, \alpha_{1,0}) = us \text{ and } w \in r(\alpha', \alpha_{1,0})r(\alpha_{1,0}, \alpha_{2,0}) = vs.$$

Since $u \notin \langle s \rangle$, we have $v \notin \langle s \rangle$ and then

$$\langle u \cdot s, u \cdot s \rangle = (u \cdot u, s \cdot s) = 16 \text{ and } \langle v \cdot s, v \cdot s \rangle = (v \cdot v, s \cdot s) = 16.$$

Thus, by Lemma 3.4 $c^u_w = c^w_s = 1$ and $c^w_v = c^v_w = 1$. For $r(\delta', \alpha_{2,0}) = u$ and $r(\alpha', \alpha_{2,0}) = w$, $1 = |\delta' \cap \alpha_{2,0}v|$ and $1 = |\alpha' \cap \alpha_{2,0}v|$. Thus, there exist unique points $\eta$ and $\eta'$ such that

$$\eta \in \delta' \cap \alpha_{2,0}v \text{ and } \eta' \in \alpha' \cap \alpha_{2,0}v.$$  

Since

$$r(\eta, \eta') \in r(\eta, \delta')r(\delta', \alpha')r(\alpha', \eta') = ss\cap s \subseteq \langle s \rangle$$  

and

$$r(\eta, \eta') \in r(\eta, \alpha_{2,0})r(\alpha_{2,0}, \alpha') = vs,$$

we have $r(\eta, \eta') \in vv \cap \langle s \rangle = \{1_{\Omega}\}$. Since $\delta'$ is the unique point in $\alpha' \cap \delta'$, we have $\delta' = \eta = \eta'$ and $r(\delta', \alpha_{2,0}) = v$. Then by Lemma 5.1 and Lemma 5.11,

$$r(\alpha', \alpha_{1,0}) = r(\beta', \alpha_{2,0}) = r(\delta', \alpha_{3,0}).$$

Now, we shall prove that $r(\gamma', \alpha_{1,1}) = v$. Note that

$$\gamma' \in \alpha' \cap \beta' \cap s^\cap \text{ and } v \in us = r(\gamma', \alpha_{0,1})s.$$  

Since $\alpha_{1,1}$ is the unique point in $\alpha_{1,0}s \cap \alpha_{2,0}s \cap \alpha_{0,1}s$, by Lemma 5.11 we have $r(\gamma', \alpha_{1,1}) = v$. Also, by Lemma 5.1 and Lemma 5.11

$$r(\alpha', \alpha_{1,0}) = r(\gamma', \alpha_{1,1}) = r(\epsilon', \alpha_{1,2}),$$

where $\epsilon' \in \alpha' \cap \alpha_{0,1}$. Therefore, the s-triangle $(\alpha_{1,0}, \alpha_{2,0}, \alpha_{1,1})s$ is parallel to $(\alpha', \beta', \gamma')_s$.  

5.6. Proof of Theorem 5.4

Given a relation \( s \in S_3 \), we assume that \((\alpha, \beta, \gamma)_s \simeq (\alpha', \beta', \gamma')_s\) and \((\alpha, \beta, \gamma)_s \simeq (\alpha'', \beta'', \gamma'')_s\). From Proposition 5.5, Proposition 5.10 and Lemma 5.13, we may assume that \( r(\alpha, \alpha'), r(\alpha', \alpha'') \notin (s) \). We shall denote \( \mathcal{P}(\alpha, \beta, \gamma)_s(i, j), \mathcal{P}(\alpha', \beta', \gamma')_s(i, j) \) and \( \mathcal{P}(\alpha'', \beta'', \gamma'')_s(i, j) \) by \( \alpha_{ij}, \beta_{ij} \) and \( \gamma_{ij} \), respectively.

**Lemma 5.14.** For \( s \in S_3 \) with \( s = s^k \) and \( i = 0, 1, 2 \) if \( r(\beta_{0,i}, \gamma_{0,i}) \), \( r(\beta_{1,i}, \gamma_{1,i}) \) and \( r(\beta_{2,i}, \gamma_{2,i}) \) are constant, then \( r(\beta_{1,0}, \gamma_{1,0}) \) is constant.

**Proof.** For \( i = 0, 1, 2 \) we set

\[
\begin{align*}
\beta_{0,0} & = u_0, \quad \beta_{1,0} = u_1, \quad \beta_{2,0} = u_2, \\
\gamma_{0,0} & = v_0, \quad \gamma_{1,0} = v_1, \quad \gamma_{2,0} = v_2
\end{align*}
\]

Note that \( u_i, v_i, w_i \notin (s) \). For \( i \neq j \), if \( w_i = w_j \), then we are done by Lemma 5.1 and Lemma 5.11. By Lemma 5.13 we have the following:

\[
\begin{array}{c|ccc}
\alpha_{0,0} & u_0 & u_1 & u_2 \\
\alpha_{1,0} & u_2 & u_0 & u_1 \\
\alpha_{2,0} & u_1 & u_2 & u_0 \\
\beta_{0,0} & u_0 & u_1 & u_2 \\
\beta_{1,0} & u_1 & u_2 & u_0 \\
\beta_{2,0} & u_2 & u_0 & u_1 \\
\end{array}
\]

Note that \( \{\beta_{1,0}, \beta_{2,0}\} = \beta_{0,0}s \cap \beta_{0,2}s^2 \cap \beta_{0,2}s^2 \) and \( \{\gamma_{1,0}, \gamma_{2,0}\} = \gamma_{0,0}s \cap \gamma_{0,1}s^2 \cap \gamma_{0,2}s^2 \).

Then by our assumption and Lemma 5.11 we have

\[
w_0 = r(\beta_{1,0}, \gamma_{2,0}) = r(\beta_{2,0}, \gamma_{1,0}).
\]

Similarly, we have the following:

\[
\begin{array}{c|ccc}
\beta_{0,0} & \gamma_{0,0} & \gamma_{1,0} & \gamma_{2,0} \\
\beta_{1,0} & w_0 & w_1 & w_2 \\
\beta_{2,0} & w_1 & w_0 & w_2 \\
\end{array}
\]

Then,

\[
\begin{align*}
u_0 & = r(\alpha_{0,0}, \beta_{0,0}) \in r(\alpha_{0,0}, \gamma_{0,0})r(\gamma_{0,0}, \beta_{0,0}) = v_0 w_0, \\
u_1 & = r(\alpha_{1,0}, \beta_{2,0}) \in r(\alpha_{1,0}, \gamma_{1,0})r(\gamma_{1,0}, \beta_{2,0}) = v_0 w_0
\end{align*}
\]

and

\[
u_2 = r(\alpha_{2,0}, \beta_{1,0}) \in r(\alpha_{2,0}, \gamma_{2,0})r(\gamma_{2,0}, \beta_{1,0}) = v_0 w_0.
\]

This implies that \( v_0 = v_0 + u_1 = u_2 + x_0 \) for some \( x_0 \in S^# \). Similarly, there exist \( x_1, x_2 \in S^# \) such that

\[
v_1 = v_0 + u_1 + u_2 + x_1 \quad \text{and} \quad v_2 = v_0 + u_1 + u_2 + x_2.
\]

Then for \( i \neq j \),

\[
12 \leq (v_i, w_0, v_j, w_0) = (v_i, v_j, w_0, w_0).
\]
Note that \( \varphi \) is a permutation of \( S \). By Lemma 3.4 and Theorem 3.5 \( w_{ij}^s \in v_iv_j \).
Similarly, we can calculate that \( w_0, w_1, w_2 \in v_iu_k \) for each \( i, k = 0, 1, 2 \). Thus for \( i \neq j \),
\[
12 \leq \langle v_i \cdot u_k, v_j \cdot u_k \rangle = \langle v_i \cdot v_j, u_k \cdot u_k \rangle.
\]
By Lemma 3.4 and Theorem 3.5 we have \( u_k^s \in v_iv_j \). Since \( s \in v_iv_j \),
\[
v_i \cdot v_j = u_0^s + u_1^s + u_2^s + s.
\]
This implies that \( w_0^s \in \{u_0^s, u_1^s, u_2^s\} \), and then we have \( w_0 \in \{u_0, u_1, u_2\} \). Since for \( i = 0, 1, 2 \)
\[
v_i \cdot w_0 = u_0 + u_1 + u_2 + x_i,
\]
we have \( \{v_0, v_1, v_2\} \subseteq w_0 \setminus \{1 \Omega\} \). By Theorem 3.5 \( |w_0 \setminus \{1 \Omega\}| \leq 2 \). Without loss of generality, we may assume that \( v_0 = v_1 \). Since \( s = v_0v_1 \), we have \( v_0v_1 \in \langle s \rangle \), which contradicts \( v_0 \not\in \langle s \rangle \).

Note that each point is contained two \( s \)-lines and two \( s^2 \)-lines and \( \langle s \rangle = \{1 \Omega, s, s^2\} \). The Lemma 5.14 can be applied to \( s \)- or \( s^2 \)-lines which contain the same point.

The proof of Theorem 5.4 is divided into two parts. In the first part, we consider \( s = s^0 \). The second part of the proof deals with \( s \neq s^0 \).

**Proof of the first part.** For short we set \( u := r(\alpha_{0,0}, \beta_{0,0}) \) and \( v := r(\alpha_{0,0}, \gamma_{0,0}) \).

Since by Lemma 3.4 \( |uv| \leq 4 \),
\[
|\{r(\beta_{0,0}, \gamma_{0,0}), r(\beta_{1,0}, \gamma_{1,0}), r(\beta_{2,0}, \gamma_{2,0}), r(\beta_{0,1}, \gamma_{0,1}), r(\beta_{0,2}, \gamma_{0,2})\}| \leq 4.
\]
By the pigeonhole principle,
\[
r(\beta_{i,j}, \gamma_{i,j}) = r(\beta_{k,l}, \gamma_{k,l})
\]
where \( (i, j), (k, l) \in \{(0,0), (1,0), (2,0), (0,1), (0,2)\} \) such that \( (i, j) \neq (k, l) \).

Then we have the following:

(i) \( r(\beta_{i,j}, \beta_{k,l}) = s \);

(ii) \( r(\beta_{i,j}, \beta_{k,l}) = s^2 \).

By Lemma 5.3, we may assume that

(i) \( r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{0,1}, \gamma_{0,1}) \).

Then by Lemma 5.1 and Lemma 5.11,
\[
r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{0,1}, \gamma_{0,1}) = r(\beta_{0,2}, \gamma_{0,2}).
\]
If there exists \( (i, j) \in \{(1,0), (2,0), (1,1), (2,1), (1,2), (2,2)\} \) such that \( r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{i,j}, \gamma_{i,j}) \), then for each \( k, l \) the points \( \beta_{k,l} \) and \( \gamma_{k,l} \) are uniquely determined by \( \beta_{0,0}, \beta_{0,1}, \beta_{0,2}, \beta_{i,j} \) and \( \gamma_{0,0}, \gamma_{0,1}, \gamma_{0,2}, \gamma_{i,j} \). We are done by Lemma 5.11. Thus we have
\[
|\{r(\beta_{1,0}, \gamma_{1,0}), r(\beta_{2,0}, \gamma_{2,0}), r(\beta_{1,1}, \gamma_{1,1}), r(\beta_{2,1}, \gamma_{2,1}), r(\beta_{1,2}, \gamma_{1,2}), r(\beta_{2,2}, \gamma_{2,2})\}| \leq 3.
\]
By the pigeonhole principle and Lemma 5.3, we may assume that
\[ r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{1,j}, \gamma_{i,j}), \]
where \((i, j) \in \{(1, 1), (1, 2)\}\). If \((i, j) \in \{(2, 0), (2, 1), (2, 2)\}\), then there exists \(k, l\) such that \((\beta_{1,0}, \beta_{i,j}, \beta_{k,l})\) and \((\gamma_{1,0}, \gamma_{i,j}, \gamma_{k,l})\) are \(s\) or \(s^2\)-lines by Lemma 5.1.
Then by Lemma 5.3 \((k, l) \in \{(0, 0), (0, 1), (0, 2)\}\), by Lemma 5.11 we have
\[ r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{k,1}, \gamma_{k,1}) = r(\beta_{0,0}, \gamma_{0,0}). \]
Then for each \(m, n\) the points \(\beta_{m,n}\) and \(\gamma_{m,n}\) are uniquely determined by \(\beta_{0,0}, \beta_{0,1}, \beta_{1,0}\), and \(\gamma_{0,0}, \gamma_{0,1}, \gamma_{1,0}\). We are done by Lemma 5.11. Thus by Lemma 5.1 and Lemma 5.11,
\[ r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{1,1}, \gamma_{1,1}) = r(\beta_{1,2}, \gamma_{1,2}). \]
Also, we have
\[ |\{r(\beta_{2,0}, \gamma_{2,0}), r(\beta_{2,1}, \gamma_{2,1}), r(\beta_{2,2}, \gamma_{2,2})\}| \leq 2. \]
By the pigeonhole principle, Lemma 5.1 and Lemma 5.11,
\[ r(\beta_{2,0}, \gamma_{2,0}) = r(\beta_{2,1}, \gamma_{2,1}) = r(\beta_{2,2}, \gamma_{2,2}). \]
By Lemma 5.14
\[ r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{2,0}, \gamma_{2,0}). \]
Thus, we have \((\beta_{0,0}, \beta_{1,0}, \beta_{0,1}) \simeq (\gamma_{0,0}, \gamma_{1,0}, \gamma_{0,1})\).
(ii) \(r(\beta_{0,1}, \gamma_{0,1}) = r(\beta_{0,0}, \gamma_{0,0})\).
By the same argument in the case (i),
\[ r(\beta_{0,1}, \gamma_{0,1}) = r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{2,2}, \gamma_{2,2}), \]
\[ r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{1,2}, \gamma_{1,2}) = r(\beta_{2,1}, \gamma_{2,1}), \]
and
\[ r(\beta_{0,2}, \gamma_{0,2}) = r(\beta_{1,1}, \gamma_{1,1}) = r(\beta_{2,0}, \gamma_{2,0}). \]
Then each
\((\beta_{0,1}, \beta_{1,0}, \beta_{2,2}), (\beta_{0,0}, \beta_{1,2}, \beta_{2,1})\) and \((\beta_{0,2}, \beta_{1,1}, \beta_{2,0})\)
are \(s^2\)-lines, by Lemma 5.14
\[ r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{1,1}, \gamma_{1,1}) = r(\beta_{2,2}, \gamma_{2,2}). \]
Thus, we have \((\beta_{0,0}, \beta_{1,0}, \beta_{0,1}) \simeq (\gamma_{0,0}, \gamma_{1,0}, \gamma_{0,1})\). This completes the proof.

**Proof of the second part.** For short we set
\[ u := r(\alpha_{0,0}, \alpha_{0,0}), \quad v := r(\alpha_{0,0}, \gamma_{0,0}), \quad a := r(\alpha_{0,1}, \alpha_{2,0}), \quad b := r(\alpha_{0,2}, \alpha_{1,0}). \]
Note that by Lemma 5.8 \(a, b \in s_{s^2} \setminus \{s\}\) with \(a \neq b\). Since by Lemma 3.4
\[ |uv| \leq 4, \]
\[ |\{r(\beta_{0,0}, \gamma_{0,0}), r(\beta_{0,1}, \gamma_{0,1}), r(\beta_{2,0}, \gamma_{2,0}), r(\beta_{0,1}, \gamma_{0,1}), r(\beta_{0,2}, \gamma_{0,2})\}| \leq 4. \]
By the pigeonhole principle,
\[ r(\beta_{1,j}, \gamma_{i,j}) = r(\beta_{k,l}, \gamma_{k,l}). \]
where \((i,j),(k,l) \in \{(0,0),(1,0),(2,0),(0,1),(0,2)\}\) such that \((i,j) \neq (k,l)\).

Then we have the following:

(i) \(r(\beta_{i,j}, \beta_{k,l}) = s\) or \(s^\varphi\);

(ii) \(r(\beta_{i,j}, \beta_{k,l}) = s^\varphi\);

(iii) \(r(\beta_{i,j}, \beta_{k,l}) = ss^\varphi \setminus \{s\}\);

(iv) \(r(\beta_{i,j}, \beta_{k,l}) = (s^\varphi)^0\).

(i) There are six cases such that for each \(i,j \in \{0,1,2\}\) with \(i \neq j\):

\[r(\beta_{i,0}, \gamma_{i,0}) = r(\beta_{j,0}, \gamma_{j,0})\quad \text{and} \quad r(\beta_{0,i}, \gamma_{0,i}) = r(\beta_{0,j}, \gamma_{0,j}).\]

Then by Lemma 5.1 and Lemma 5.11,

\[r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{2,0}, \gamma_{2,0}),\]

(resp. \(r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{0,1}, \gamma_{0,1}) = r(\beta_{0,2}, \gamma_{0,2})\)).

Also, by Lemma 5.6 and Lemma 5.11

\[r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{0,1}, \gamma_{0,1})\quad \text{resp.} \quad r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{1,0}, \gamma_{1,0}).\]

Again, by Lemma 5.1 and Lemma 5.11

\[r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{0,2}, \gamma_{0,2}),\]

(resp. \(r(\beta_{0,0}, \gamma_{0,0}) = r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{0,2}, \gamma_{2,0})\)).

Thus, we have \((\beta_{0,0}, \beta_{0,0})_s \simeq (\gamma_{0,0}, \gamma_{1,0})_s\).

(ii) \(r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{0,1}, \gamma_{1,0})\).

Note that \(c_{ss^\varphi} = c_{ss^\varphi}^a = 1\). For \(r(\beta_{1,0}, \beta_{0,1}) = s^\varphi\) there exist unique points

\[\beta_{2,0} \in \beta_{1,0}s \cap \beta_{0,1}s\quad \text{and} \quad \gamma_{2,0} \in \gamma_{1,0}s \cap \gamma_{0,1}s.\]

By Lemma 5.11, we have

\[r(\beta_{2,0}, \gamma_{2,0}) = r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{0,1}, \gamma_{0,1}).\]

Then by case (i), we have \((\beta_{0,0}, \beta_{1,0}, \beta_{0,1})_s \simeq (\gamma_{0,0}, \gamma_{1,0}, \gamma_{0,1})_s\).

(iii) There are two cases such that

\[r(\beta_{0,1}, \gamma_{0,1}) = r(\beta_{2,0}, \gamma_{2,0})\quad \text{and} \quad r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{0,2}, \gamma_{0,2}).\]

Note that \(c_{ss^\varphi} = c_{ss^\varphi}^a = 1\) (resp. \(c_{ss^\varphi}^b = 1\)). For \(r(\beta_{0,1}, \beta_{2,0}) = a\) (resp. \(r(\beta_{0,2}, \beta_{1,0}) = b\)) there exist unique points

\[\beta_{1,0} \in \beta_{0,1}s^\varphi \cap \beta_{2,0}s\quad \text{resp.} \quad \beta_{0,1} \in \beta_{0,2}s \cap \beta_{1,0}s^\varphi\]

and

\[\gamma_{1,0} \in \gamma_{0,1}s^\varphi \cap \gamma_{2,0}s\quad \text{resp.} \quad \gamma_{0,1} \in \gamma_{0,2}s \cap \gamma_{1,0}s^\varphi.\]

By Lemma 5.11, we have

\[r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{0,1}, \gamma_{0,1}) = r(\beta_{2,0}, \gamma_{2,0}),\]

(resp. \(r(\beta_{0,1}, \gamma_{0,1}) = r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{0,2}, \gamma_{0,2})\)).

Then by case (i), we have \((\beta_{0,0}, \beta_{1,0}, \beta_{0,1})_s \simeq (\gamma_{0,0}, \gamma_{1,0}, \gamma_{0,1})_s\).
(iv) \( r(\beta_{2,0}, \gamma_{2,0}) = r(\beta_{0,2}, \gamma_{0,2}) \).

Since \((\beta_{2,0}, \beta_{1,1}, \beta_{0,2})\) and \((\gamma_{2,0}, \gamma_{1,1}, \gamma_{0,2})\) satisfy the conditions of an \( s^\varphi \)-line, by Lemma 5.1 and Lemma 5.11,

\[
r(\beta_{2,0}, \gamma_{2,0}) = r(\beta_{1,1}, \gamma_{1,1}) = r(\beta_{0,2}, \gamma_{0,2}).
\]

Note that \( e_{ab}^\varphi = e_{ba}^\varphi = 1 \). By Lemma 5.8, \( r(\beta_{0,2}, \beta_{1,0}) = r(\gamma_{0,2}, \gamma_{1,0}) = b \). For \( r(\beta_{1,1}, \beta_{0,2}) = s^\varphi \), there exist unique points

\[
\beta_{1,0} \in \beta_{1,1}s \cap \beta_{0,2}b \text{ and } \gamma_{1,0} \in \gamma_{1,1}s \cap \gamma_{0,2}b.
\]

By Lemma 5.11, we have

\[
r(\beta_{1,0}, \gamma_{1,0}) = r(\beta_{0,2}, \gamma_{0,2}) = r(\beta_{2,0}, \gamma_{2,0}).
\]

Then by case (i), we have \((\beta_{0,0}, \beta_{1,0}, \beta_{0,1}) \simeq (\gamma_{0,0}, \gamma_{1,0}, \gamma_{0,1}) \). This completes the proof.

### 5.7. Construction of automorphisms

**Lemma 5.15.** Let \((\alpha, \beta, \gamma)_s\) be an \( s \)-triangle. Then for each \( \alpha' \in \Omega \), there exists a unique \( s \)-triangle \((\alpha', \beta', \gamma')_s\) parallel to \((\alpha, \beta, \gamma)_s\).

**Proof.** It is clear \( \alpha = \alpha' \). We may assume that \( \alpha \neq \alpha' \) and we set \( u := r(\alpha, \alpha') \).

First, we assume that \( u \in \{s\} \). If \( s = s^\psi \), then by Proposition 5.5 for \( r(\alpha, \alpha') \in \{s, s^\varphi\} \), there exist unique \( s \)-lines \((\alpha', \beta', \delta')\) and \((\alpha', \gamma', \epsilon')\) such that

\[
r(\alpha, \alpha') = r(\beta, \beta') = r(\delta, \delta') \text{ and } r(\alpha, \alpha') = r(\gamma, \gamma') = r(\epsilon, \epsilon'),
\]

where \( \delta \in \alpha s \cap \beta s, \delta' \in \alpha's \cap \beta's, \epsilon \in \alpha s \cap \gamma s \) and \( \epsilon' \in \alpha's \cap \gamma's \). Thus, we may assume that \( s \neq s^\psi \). The existence follows from (4) and Proposition 5.10. To prove the uniqueness, we assume that

\[
(\alpha, \beta, \gamma)_s \simeq (\alpha', \beta', \gamma')_s \text{ and } (\alpha, \beta, \gamma)_s \simeq (\alpha', \beta'', \gamma'')_s.
\]

Then by Theorem 5.4,

\[
(\alpha', \beta', \gamma')_s \simeq (\alpha', \beta'', \gamma'')_s.
\]

Since \( r(\alpha', \alpha') = 1_\Omega, \beta' = \beta'' \) and \( \gamma' = \gamma'' \).

Now, we assume that \( u \notin \{s\} \). Then

\[
r(\alpha', \beta) \in r(\alpha', \alpha)r(\alpha, \beta) = us.
\]

Since \( u \notin \{s\} \),

\[
\langle u \cdot s, u \cdot s \rangle = \langle u \cdot u, s \cdot s \rangle = 16.
\]

By Lemma 3.4 we have

\[
1 = |\alpha' u \cap \beta s| = |\alpha' s \cap \beta u|.
\]

Thus, there exists a unique \( \beta' \in \alpha' s \cap \beta u \), and then by Lemma 5.11 there exists a unique \( \gamma' \in \alpha' s \cap \beta' s^\varphi \) such that

\[
u = r(\alpha, \alpha') = r(\beta, \beta') = r(\gamma, \gamma').
\]

It follows from Lemma 5.1 and Lemma 5.11 that the \( s \)-triangle \((\alpha', \beta', \gamma')_s\) is parallel to \((\alpha, \beta, \gamma)_s \). \qed
Lemma 5.16. For any $\alpha, \beta \in \Omega$ with $r(\alpha, \beta) \in S_3$, there exists $\sigma \in \text{Aut}(\Omega, S)$ such that $\alpha^\sigma = \beta$.

Proof. We denote $s := r(\alpha, \beta)$. Then for any $s$-triangle $(\alpha, \beta, \gamma)$, and $\alpha' \in \Omega$, there exists a unique $s$-triangle $(\alpha', \beta', \gamma')$, parallel to $(\alpha, \beta, \gamma)$, by Lemma 5.15. We define a map $\sigma$ from $\Omega$ to itself such that $(\alpha')^\sigma = \beta'$. Then $\sigma \in \text{Aut}(\Omega, S)$ by Theorem 5.4 and Lemma 5.12. □

Lemma 5.17. For any $s, t \in S \setminus \langle S_3 \rangle$ with $s \neq t$, $st \subseteq S_2$.

Proof. Since $s, t \in S_2$, $|\langle s, t \rangle| = 7$ by Lemma 3.4 and Theorem 3.5. We denote $n_{(s, t)} := \sum_{u \in \langle s, t \rangle} n_u$, then $n_{(s, t)} = 25$. Assume that there exists $v \in st$ such that $v \in S_3$. Then $\langle v \rangle$ is closed subset of $\langle s, t \rangle$, and then $n_{(v)}$ divides $n_{(s, t)}$. Since $v \in S_3$, $n_{(v)} = 25$. This implies that $\langle v \rangle = \langle s, t \rangle$, which contradicts $s, t \in S \setminus \langle S_3 \rangle$. □

Lemma 5.18. If $S_3 \neq \emptyset$, then $\langle S_3 \rangle = S$.

Proof. Given $\alpha, \beta, \gamma \in \Omega$ such that $r(\alpha, \beta) \in S_3$ and $r(\alpha, \gamma) \notin \langle S_3 \rangle$. If $r(\beta, \gamma) \in \langle S_3 \rangle$, then

$$r(\alpha, \gamma) \in r(\alpha, \beta)r(\beta, \gamma) \subseteq \langle S_3 \rangle,$$

a contradiction. If $r(\beta, \gamma) = r(\gamma, \beta) \notin \langle S_3 \rangle$, then by Lemma 5.17

$$r(\alpha, \beta) \in r(\alpha, \gamma)r(\gamma, \beta) \subseteq S_2,$$

which is a contradiction. Thus we have $\langle S_3 \rangle = S$. □

Lemma 5.19. If $S_3 \neq \emptyset$, then $\text{Aut}(\Omega, S)$ is transitive on $\Omega$.

Proof. Given $\alpha, \beta, \gamma \in \Omega$ such that $r(\alpha, \beta) = s$. If $s \in S_3$, then we are done by Lemma 5.16. Now we suppose $s \in S_2$. Then by Lemma 5.18, $s \in \langle S_3 \rangle$. We set

$$s = t_1 \cdots t_n$$

for some $t_i \in S_3$. We can choose $\gamma_0, \ldots, \gamma_n \in \Omega$ such that $\alpha = \gamma_0$, $\beta = \gamma_n$ and $r(\gamma_{i-1}, \gamma_i) = t_i$ for each $i = 1, \ldots, n$. Then by Lemma 5.16, for each $i = 1, \ldots, n$ there exists $\sigma_i \in \text{Aut}(\Omega, S)$ such that $\gamma_{i-1}^{\sigma_i} = \gamma_i$. We denote

$$\sigma := \sigma_1 \sigma_2 \cdots \sigma_n,$$

then $\alpha^\sigma = \beta$. □

Proof of Theorem 1.1. This is an immediate result of Lemma 5.19 and Theorem 4.4. □
6. Appendix

The main goal of this section is to prove Theorem 3.5. In this section, we refer to [2] and we use the same notation as in Section 3. We set

\[ S_3^\varphi := \{ s^\varphi \mid s \in S_3 \} , \]
\[ S_3^\psi := \{ s^\psi \mid s \in S_3 \} . \]

**Lemma 6.1** ([2, Proposition 3.6]).

(i) For each \( t \in S_3 \) and any \( s \in S \),

\[ c_{ss}^t \equiv 1 \pmod{2} \Rightarrow s = t, \ c_{ss}^t = 1 . \]

(ii) The map \( s \mapsto s^\psi, s \in S_3 \) is injective.

(iii) For each \( t \in S_3^\psi \) and any \( s \in S_4 \) it holds that \( t \not\in ss \).

**Proof.** (i) From (1) we have

\[ \delta_{st} = \sum_{u \in S^\#} c_{ss}^u c_{tt}^u = c_{ss}^t c_{tt}^t + c_{ss}^t c_{tt}^t \]
\[ = 2c_{ss}^t + c_{ss}^t \equiv c_{ss}^t \pmod{2} . \]

Since \( c_{ss}^t \equiv 1 \pmod{2} \), \( s = t \) and \( s \in S_3 \). This proves (i) by Lemma 3.3.

(ii) Let \( s^\psi = t^\psi \). Then \( c_{ss}^t = c_{ss}^t = 1 \) by Lemma 3.3. We obtain \( s = t \) by (i).

(iii) Since \( t \in S_3^\psi \), we may assume that \( t = r^\psi \) for some \( r \in S_3 \). Since \( s \in S_4 \), it is clear that \( r \neq s \). From (1) we have

\[ 0 = \delta_{st} = \sum_{u \in S^\#} c_{ss}^u c_{rr}^u = c_{ss}^t c_{rr}^t + c_{ss}^t c_{tt}^t \]
\[ = 2c_{ss}^t + c_{ss}^t \equiv c_{ss}^t \pmod{2} . \]

By Lemma 3.1 for any \( v \in ss \setminus \{ 1_\Omega \} \), \( c_{ss}^v = 1 \). Thus we obtain \( t \not\in ss \). \( \Box \)

**Lemma 6.2** ([2, Lemma 3.9]). \( \varphi \) is bijective.

**Proof.** It follows from Lemma 3.3 that \( S_3^\psi \subseteq S_3^\varphi \subseteq S_3 \). Since \( \psi \) is injective by Lemma 6.1(ii), we have \( |S_3| = |S_3^\varphi| \leq |S_3^\psi| \leq |S_3| \). This completes the proof. \( \Box \)

For each \( s \in S_4 \) we set

\[ \Delta_s := ss \setminus \{ 1_\Omega \} . \]

It follows from Lemma 3.1(i) that \( |\Delta_s| = 3 \) for each \( s \in S_4 \) and from (1) that \( |\Delta_u \cap \Delta_v| \in \{ 0, 2 \} \) for each \( u, v \in S_4 \) with \( u \neq v \).

For \( u, v \in S_4 \) we shall write \( u \sim v \) if and only if \( u = v \) or \( |\Delta_u \cap \Delta_v| = 2 \). Clearly, the relation \( \sim \) is reflexive and symmetric on \( S_4 \).

**Lemma 6.3** ([2, Proposition 3.10]). The relation \( \sim \) is an equivalence on \( S_4 \).
Proof. It suffices to show that the relation $\sim$ is transitive on $S_4$. Let $u, v, w \in S_4$ such that $u \sim v$ and $v \sim w$. If $u = v$ or $v = w$, then there is nothing to prove. Thus we suppose that $|\Delta_u \cap \Delta_v| = |\Delta_v \cap \Delta_w| = 2$. Since $\Delta_u \cap \Delta_v$ and $\Delta_v \cap \Delta_w$ are subsets of $\Delta_v$ and $|\Delta_v| = 3$, $\Delta_u \cap \Delta_w \neq \emptyset$. Thus we obtain $|\Delta_u \cap \Delta_w| = 2$. \[\square\]

Denote $[s]$ the equivalence class of $\sim$ generated by $s \in S_4$. The notation $\Delta_{[s]}$ as follows:

$$\Delta_{[s]} := \bigcup_{t \in [s]} \Delta_t.$$ 

Lemma 6.4 ([2, Proposition 3.11]). For each $s \in S_4$ it holds that $|[s]| \leq |\Delta_{[s]}|$, and the equality holds if and only if $|[s]| = |\Delta_{[s]}| = 4$.

Proof. Let $[s] = \{s_1, s_2, \ldots, s_m\}$. Then there are two possible cases:

(i) $\Delta_{s_i} \cap \Delta_{s_j} = \Delta_{s_i} \cap \Delta_{s_k}$ for any $k \in \{1, 2, \ldots, m\}$.

There exists $\{u, v\} \subseteq S$ such that $\Delta_{s_i} = \{u, v\} \cup \{w_i\}$. Thus

\[
\begin{align*}
s_i \cdot s_i &= 4 \cdot 1 + u + v + w_i, \\
s_j \cdot s_j &= 4 \cdot 1 + u + v + w_j, \\
\end{align*}
\]

\[\vdots\]

So, we obtain that $|[s]| = m < m + 2 = |\Delta_{[s]}|$. 

(ii) $\Delta_{s_i} \cap \Delta_{s_j} \neq \Delta_{s_i} \cap \Delta_{s_k}$ for some $k \in \{1, 2, \ldots, m\}$. 

There exists $\{u, v, w, t\} \subseteq S$ such that $\Delta_{s_i} \subseteq \{u, v, w, t\}$ for all $i$. Thus

\[
\begin{align*}
s_i \cdot s_i &= 4 \cdot 1 + u + v + w, \\
s_j \cdot s_j &= 4 \cdot 1 + u + v + t, \\
s_k \cdot s_k &= 4 \cdot 1 + u + w + t, \\
s_l \cdot s_l &= 4 \cdot 1 + v + w + t. \\
\end{align*}
\]

It is easy to see that the equality may hold only in the second case, when $m = 4$. \[\square\]

Lemma 6.5 ([2, Proposition 3.12]). For each $s \in S_4$, $|[s]| = 4$.

Proof. By Lemma 6.1(iii), $S^\psi_3 \cap (\bigcup_{s \in S_4} \Delta_s) = \emptyset$. Since $\psi$ is bijective, we obtain that $S_3 \cap (\bigcup_{s \in S_4} \Delta_s) = \emptyset$. 

Now for any $t \in S_2$ suppose that $t \in \Delta_s$ for some $s \in S_4$. Then applying Lemma 3.1 we obtain that $\langle s \cdot t, s \cdot t \rangle = 28$.

By Lemma 2.1, $c_{s,t}^2 = c_{s,s}^t = 1$. It follows from Lemma 3.4 that $\langle s \cdot t, s \cdot t \rangle \in \{16, 24\}$,
Thus we obtain $|\cup_{\alpha \in S_4}\Delta_{\alpha}| = |S_4|$. Since $S_4$ is the union of equivalence classes, say $[s_1], \ldots, [s_m]$, $\cup_{\alpha \in S_4}\Delta_{\alpha} = \cup_{i=1}^{m} \Delta_{[s_i]}$. By Lemma 6.4,

$$|S_4| = \sum_{i=1}^{m} |[s_i]| \leq \sum_{i=1}^{m} |\Delta_{[s_i]}| = |\bigcup_{s \in S_4} \Delta_s| \leq |S_4|.$$  

Thus we obtain $|[s_i]| = |\Delta_{[s_i]}|$ for $1 \leq i \leq m$, and by Lemma 6.4, $|[s_i]| = |\Delta_{[s_i]}| = 4$ for all $i$. □

\textbf{Lemma 6.6} ([2, Proposition 3.13]). If $S_4 \neq \emptyset$, then there exist $s, t \in S_4$ and $r \in S_3$ such that $c_{st}^r = 2$.

\textbf{Proof.} Take an arbitrary $s \in S_4$. By Lemma 6.5, $[s] = \{s, t, u, v\}$ where $s, t, u, v$ are pairwise distinct relations of $S_4$. Consider a pair $s, t \in [s]$. Then

$$(s \cdot t, s \cdot t) = (s \cdot s, t \cdot t) = 24.$$  

It follows from Lemma 3.4 that there exists $r \in S^\#$ such that $c_{st}^r = 2$. Note that $r \notin \{s, t\}$. If $r \in \{s, t\}$, then $c_{ss}^r = c_{tt}^r = 2$ or $c_{tt}^r = c_{st}^r = 2$, a contradiction. Claim that $r \in S_3$. Applying Lemma 3.1 if $r \in S_2$, then

$$(s \cdot s, r \cdot r) \in \{16, 28\},$$  

and if $r \in S_4$, then

$$(s \cdot s, r \cdot r) \in \{16, 20, 24, 28\}.$$  

Since $c_{ss}^t = c_{tt}^t = 2$,

$$(s \cdot r, s \cdot r) \in \{24, 32\}.$$  

Thus we obtain $r \nsim s$, whence $r \notin [s]$. Without loss of generality $r = u$. Now we can repeat these arguments with the pair $s, v \in [s]$. This yields an relation $r' \in [s] \setminus \{s, v\}$ with $c_{sv}^{r'} = 2$. If $r' = t$, then $s \cdot t = 2u + 2v$. If $r' = u$, then $s \cdot u = 2t + 2v$. Anyway we have two equivalent relations $a, b$ with $a \cdot b = 2d + 2e$. But in this case $(a \cdot b, a \cdot b) = 32$, contrary to $(a \cdot b, a \cdot b) = 24$. □

\textbf{Proof of Theorem 3.5.} (i) and (ii) follow from Lemma 3.3 and Lemma 6.2.

(iii) Suppose on the contrary that $S_4 \neq \emptyset$, then by Lemma 6.6 there exist $s, t \in S_4$ and $r \in S_3$ such that $c_{st}^r = 2$. This implies that

$$(s \cdot s, r \cdot r) = (s \cdot r, s \cdot r) \in \{24, 32\}.$$  

Therefore $\{r^*, r^{**}\} \cap \Delta_s \neq \emptyset$. But by Lemma 6.2, $r^* \in S_3^\#$. Hence by Lemma 6.1(ii) $S_3^\# \cap \Delta_s = \emptyset$. This completes the proof. □

\textbf{Acknowledgement.} The author would like to thank Professor Kijung Kim for his careful reading and valuable comments in writing the paper. This paper is a part of the author’s Ph. D. thesis, written under the supervision of Professor Mitsugu Hirasaka at the Pusan National University.
References


Department of Mathematics
Pusan National University
Busan 609-735, Korea
E-mail address: parkjr@pusan.ac.kr