0.0 Abstract

This is an example of referencing: citeBourbaki[**?**]

The word problem for a group presentation $\langle S \mid R \rangle$ involves finding an algorithm to reduce any word in the group W into a reduced word. In this paper, we solve this problem for Coxeter groups, and, more generally, for all systems satisfying the exchange condition, which is encapsulated in Tits' Theorem.

The proof of this result is divided into several steps:

- First, we show that every Coxeter group satisfies the exchange condition.
- Next, we examine when two reduced words represent the same element in the group.
- Lastly, we discuss how to reduce a word in a system satisfying the exchange condition.

The hardest part of the proof is the first one, and we will focus on this in more detail.

0.1 Exchange Condition

Definition 0.1.1. A system is a tuple (W, S), where W is a group and S is a set of generators for G, such that $S = S^{-1}$ and $1 \notin S$.

Definition 0.1.2. For $w \in W$, the sequence $\mathbf{s} = (s_1, \ldots, s_q)$, where $s_i \in S$ for all $i \in \mathbb{N}$, is called a **reduced representation** of w if and only if $w = s_1 s_2 \ldots s_q$ and q is the smallest such number satisfying this condition. We define $l(w) = q$, which is called the **length** of w.

Proposition 0.1.3. For $w, w' \in W$, we have the following facts:

- (1) $l(ww') \leq l(w) + l(w')$
- (2) $l(w^{-1}) = l(w)$
- (3) $|l(w) - l(w')| \leq l(ww'^{-1})$

Proof. (1) and (2) are straightforward. From (1), we see $l(w) \leq l(ww'^{-1}) + l(w')$ and $l(w') \leq l(w'w^{-1}) + l(w)$. From (2), we know $l(w'w^{-1}) = l(ww'^{-1})$. Combining these, we obtain (3). $\square$

Definition 0.1.4. If a system (W, S) satisfies the following conditions:

- (1) Every element in S has order 2.
- (2) Let $m(s,t)$ denote the order of st, and define $I = \{(s,t) \mid s,t \in S, m(s,t) < \infty\}$, then the presentation $\langle S \mid (st)^{m(s,t)} = 1, (s,t) \in I \rangle$ describes W.

Then we say that (W, S) is a Coxeter System, and W is a Coxeter group.

Remark 0.1.5. A Coxeter system (W, S) satisfies the following universal property: For any group G and map $\psi : S \to G$ such that $\psi(st)^{m(st)} = e_G$ for all $(s,t) \in I$, there exists a unique homomorphism $\phi \in \mathrm{Hom}(W, G)$ such that $\psi = \phi \circ l$, where l is the natural inclusion from S to W. This is simply the composition of the universal properties of free groups and quotient groups.

Example 0.1.6. By the universal property of Coxeter systems, the map $s \mapsto -1$ for all $s \in S$ extends to a homomorphism $\epsilon : W \to \{-1, 1\}$, such that $\epsilon(w) = (-1)^{l(w)}$. We call $\epsilon(w)$ the sign of w.

Now we want to find an invariant among different representations of the same word. For this, we define the following:

Definition 0.1.7. For a Coxeter system (W, S), let T denote the union of the conjugacy classes of all elements in S. For a sequence $\mathbf{s} = (s_1, \ldots, s_q)$, where $s_i \in S$ for all i, define $\Phi(\mathbf{s}) = (t_1, \ldots, t_q)$, where $t_j = (s_1 \ldots s_{j-1}) s_j (s_1 \ldots s_{j-1})^{-1}$. For $t \in T$, define $n(\mathbf{s}, t) := \#\{1 \leq j \leq q \mid t_j = t\}$. Finally, define $R = \{\pm 1\} \times T$.

Note that we have $s_1 \ldots s_j = t_j \ldots t_1$.

Lemma 0.1.8. For a Coxeter System (W, S), we have the following facts:

1. For $w \in W$ and $t \in T$, for every sequence $\mathbf{s} = (s_1, \ldots, s_q)$ such that $w = s_1 \ldots s_q$, the value $(-1)^{n(\mathbf{s},t)}$ is constant. We call this value $\eta(w, t)$.
2. For $w \in W$, consider the map $U_w : R \to R$ defined as

$$U_w(\epsilon, t) = (\epsilon \eta(w, t), wtw^{-1}),$$

then the map $w \mapsto U_w$ is a homomorphism from W to the permutation group of R.

Proof. For $s \in S$, define $U_s : R \to R$ by:

$$U_s(\epsilon, t) = (\epsilon(-1)^{\delta(\mathbf{s},t)}, sts^{-1}),$$

where $\delta_{s,t}$ is the Kronecker delta. For a sequence $\mathbf{s} = (s_1, \ldots, s_q)$ in S, let $w = s_q \ldots s_1$, then

$$U_s = U_{s_q} \circ \cdots \circ U_{s_1}.$$

We prove that $U_{\mathbf{s}}(\epsilon, t) = (\epsilon(-1)^{n(\mathbf{s},t)}, wtw^{-1})$ by induction.

$(*)$ In the case when $q = 0$ or 1, the proof is trivial.

For $q > 1$, assume the induction hypothesis holds for $\mathbf{s}' = (s_1, \ldots, s_{q-1})$ with $w' = s_{q-1} \ldots s_1$. Then

$$U_{\mathbf{s}'} = U_{s_q}(\epsilon(-1)^{n(\mathbf{s}',t)}, w'tw'^{-1}).$$

Thus, it remains to prove that

$$n(\mathbf{s}, t) = \delta_{s_q, w'tw'^{-1}} + n(\mathbf{s}', t).$$

Notice that $\Phi(\mathbf{s}) = (\Phi(\mathbf{s}'), w'^{-1} s_q w')$, so the proof is trivial.

We now prove that the map $s \mapsto U_s$ can be extended to a homomorphism from W. By the universal property of Coxeter systems, it suffices to prove that for all $s, s' \in S$ such that $m(s, s') < \infty$, we have

$$(U_s \circ U_{s'})^{m(s,s')} = 1.$$

Define $\mathbf{s} = (s_1, \ldots, s_{2m(s,s')})$ such that $s_i := s$ for odd i and $s_i := s'$ for even i. It suffices to prove that

$$U_{\mathbf{s}} = \mathrm{Id}.$$

Notice that here we have $t_j = (ss')^{j-1} s$, so $t_i \neq t_j$ for all $1 \leq i < j \leq m(s, s')$ and $t_i = t_{i+m(s,s')}$.

Hence, for $t \in T$, $n(\mathbf{s}, t)$ is either 0 or 2. Applying the result in the previous paragraph, we see that $U_{\mathbf{s}} = \mathrm{Id}$.

Therefore, the map $w \mapsto U_w$ is a homomorphism from W. Specifically, U_w does not depend on the representation chosen for w. From $(*)$, we conclude that $n(\mathbf{s}, t)$ is invariant across different representations. This gives us statement (1). Statement (2) follows easily. $\square$

Theorem 0.1.9. For a Coxeter System (W, S), consider a sequence $\mathbf{s} = (s_1, \ldots, s_q)$, $\Phi(\mathbf{s}) = (t_1, \ldots, t_q)$, and $w = s_1 \ldots s_q$. Then $\mathbf{s}$ is a reduced representation of w if and only if $t_i \neq t_j$ for all $i \neq j$. Define

$$T_w := \{t \in T \mid \eta(w, t) = -1\},$$

then in the case that $\mathbf{s}$ is a reduced representation of w, we have $T_w = \{t_1, \ldots, t_q\}$ and $|T_w| = l(w)$.

Proof. For all $t \in T_w$, we have $n(w, t) \neq 0$. By the definition of $n(w, t)$, we deduce that for all $t \in T_w$, $t \in \{t_1, \ldots, t_q\}$. Moreover, since $\eta(w, t)$ is independent of the choice of representation of w, the set T_w depends only on w. Hence, $|T_w| \leq l(w)$.

In the case where $t_i \neq t_j$ for all $i \neq j$, we have $n(s, t) = 0$ or 1, and thus $T_w = \{t_1, \ldots, t_q\}$. Since $q = |T_w| \leq l(w)$, it follows that $\mathbf{s}$ is a reduced representation of w.

Conversely, if there exist $i \neq j$ such that $t_i = t_j$, without loss of generality, assume $i < j$. Consider the subsequence $u = s_{i+1} \ldots s_{j-1}$, then we have

$$s_i = u s_j u^{-1}.$$

Hence, we have

$$\begin{aligned} s_1 \ldots s_q = s_1 \ldots s_{i-1}(u s_j u^{-1}) u s_j s_{j+1} \ldots s_q &= s_1 \ldots s_{i-1} u s_j s_j s_{j+1} \ldots s_q \\ &= s_1 \ldots s_{i-1} s_{i+1} \ldots s_{j-1} s_{j+1} \ldots s_q. \end{aligned}$$

Thus, $\mathbf{s}$ is not a reduced representation. □

Note that now we have a necessary and sufficient condition to check whether a word is reduced or not. We want to improve this result and develop an algorithm for reducing words.

Definition 0.1.10. Definition 6.1.10. For a system (W, S), if it satisfies: for all $w \in W$ and $s \in S$, if $l(sw) \leq l(w)$, then for any reduced representation $\mathbf{s} = (s_1, \ldots, s_q)$, there exists $1 \leq j \leq q$ such that $s s_1 \ldots s_{j-1} = s_1 \ldots s_j$, then we say (W, S) satisfies the *exchange condition*.

Theorem 0.1.11. If (W, S) is a Coxeter System, then it satisfies the exchange condition.

Proof. Consider $w \in W$ and $s \in S$ such that $l(sw) \leq l(w)$. For any reduced representation $\mathbf{s} = (s_1, \ldots, s_q)$ of w, consider $w' := sw$. By Example 6.1.6, we have

$$l(w') \equiv l(w) + 1 \pmod 2.$$

Proposition 6.1.3(3) gives that $|l(w) - l(w')| \leq 1$, so we conclude that $l(w') = l(w) - 1$. Now, pick $(s'_1, \ldots, s'_{l(w)-1})$ as a reduced representation of w', then $\mathbf{s}' = (s, s'_1, \ldots, s'_{p-1})$ is a reduced representation of w.

Take $\Phi(\mathbf{s}') = (t'_1, \ldots, t'_p)$, then by definition, we have $t'_1 = s$. However, Theorem 6.1.9 shows that $t'_i \neq t'_j$ if $i \neq j$, so we have

$$n(\mathbf{s}', s) = 1.$$

By Lemma 6.1.8, we know that

$$n(\mathbf{s}', s) \equiv n(\mathbf{s}, s) \pmod 2,$$

so $n(\mathbf{s}, s) \neq 0$. Hence, there exists an index j such that $s = t_j$, where t_j is an element in $\Phi(\mathbf{s})$. By the definition of t_j, we have

$$s s_1 \ldots s_{j-1} = s_1 \ldots s_j.$$

Thus, the claim is proved. □

0.2 M-operations

Definition 0.2.1. Consider a system (W, S). The sequence $\mathbf{s} = (s_1, \dots, s_q)$, where $s_i \in S$ for all i, is called a word in S, and $w := s_1 \dots s_q$ is called the element in W expressed by $\mathbf{s}$. An elementary M-operation on a word in $\mathbf{s}$ is one of the following two types of operations:

- **(MI)** Delete a subword of the form (s, s) from $\mathbf{s}$.
- **(MII)** Replace an alternating subword of the form $(s, t, s, \dots)$ by another alternating subword of the form $(t, s, t, \dots)$, both of length $m(s, t)$.

We say a word is M-reduced if and only if its length cannot be shortened by M-operations. Clearly, any reduced word is M-reduced.

Lemma 0.2.2. For a system (W, S) with the exchange condition, two reduced representations express the same element in W if and only if one can be transformed into the other by MII operations.

Proof. Let $\mathbf{s} = (s_1, \dots, s_q)$ and $\mathbf{r} = (r_1, \dots, r_q)$ be two reduced representations, both expressing $w \in W$. We will prove the lemma by induction.

In the case when $q = 0$, the proof is trivial. If $s_1 = r_1$, we can reduce the length of both words by 1, and the induction hypothesis can be applied directly. It suffices to prove the case where $s_1 \neq r_1$. Let $m := m(s_1, r_1)$.

Claim. m is finite, and there is another reduced expression $\mathbf{u}$ of w that starts with an alternating subword $(s_1, r_1, s_1, \dots)$ of length m.

With the claim, the remaining proof is easy. Since $\mathbf{s}$ and $\mathbf{u}$ both start with s_1, by the induction hypothesis, $\mathbf{s}$ can be transformed into $\mathbf{u}$ by MII operations. Now, apply MII on $\mathbf{u}$ to get another word $\mathbf{u}'$ that starts with $(r_1, s_1, r_1, \dots)$ of length m. Since $\mathbf{u}'$ and $\mathbf{r}$ both start with r_1, again by the induction hypothesis, $\mathbf{u}'$ can be transformed into $\mathbf{r}$ through MII operations. The combination of all the above MII operations gives the result.

The converse of the proposition is trivial. □

Proof of Claim. To prove that m is finite, consider the following. Since $\mathbf{r}$ is a reduced representation of w starting with r_1, it follows that $l(r_1 w) < l(w)$. By the exchange condition, there exists an index i such that

$$r_1 s_1 \dots s_{i-1} = s_1 \dots s_i.$$

Moreover, since $(s_1, \dots, s_i)$ is a subword of $\mathbf{s}$, which is reduced, we know that the word

$$v := (r_1, s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_q)$$

is also a reduced representation of w.

Note that $i \neq 1$. Otherwise, $(s_1, s_2, \dots, s_q) = (r_1, s_2, \dots, s_q)$, which would imply $s_1 = r_1$, a contradiction.

Next, define S_q to be the alternating word ending in s_1, with each term in the set $\{s_1, r_1\}$ of length q. Suppose $\mathbf{s}'$ is a word that starts with S_{q-1}, and let s' be the element of $\{s_1, r_1\}$ that $\mathbf{s}'$ does not start with.

Looking at the relationship between $\mathbf{s}$ and $\mathbf{r}$, we see that $l(s'w) < l(w)$. Applying the exchange condition, we obtain a reduced representation of $\mathbf{s}'$ starting with s'. Importantly, the removed element in this exchange process cannot lie in S_{q-1}, since any reduced representation with a length not equal to m in a group like D_{2m} is unique. This fact is learned in the Year 2 module *Groups and Rings*. If the removed term were from S_{q-1}, we would get two different reduced representations of the same element in D_{2m} with lengths not equal to m, which would be a contradiction.

Therefore, we obtain a reduced representation starting with S_q from $\mathbf{s}'$. By induction, we conclude that w has a reduced expression starting with S_q for any $q \leq m(s_1, r_1)$, but since $q \leq l(w) < \infty$, we have that m is finite.

Finally, by replacing $S_{m(s_1,r_1)}$ with $(s_1, r_1, s_1, \dots)$ using an MII operation, we obtain the desired reduced expression $\mathbf{u}$. □

0.3 Tits' Theorem

Theorem 0.3.1 (Tits')**.** A word in a system (W, S) with the exchange condition is reduced if and only if it is M-reduced.

Proof. Suppose the word $\mathbf{s} = (s_1, \dots, s_k)$ is M-reduced. We will show that $\mathbf{s}$ is reduced by induction on k. The base case $k = 1$ is trivial.

For $k > 1$, by the induction hypothesis, $\mathbf{s}' = (s_2, \dots, s_k)$ is reduced. Let w' be the element expressed by $\mathbf{s}'$. Suppose $\mathbf{s}$ is not reduced, then

$$l(w) = l(s_1\mathbf{s}') \leq k - 1 < l(\mathbf{s}').$$

Thus, by the exchange condition, there exists an index i such that

$$w' = s_1 s_2 \dots s_{i-1} s_{i+1} \dots s_k.$$

That is, w' has a reduced representation starting with s_1. Applying Lemma 6.2.2, we see that $\mathbf{s}'' := (s_1, s_2, \dots, s_{i-1}, s_{i+1}, \dots, s_k)$ can be transformed from $\mathbf{s}'$ by an MII operation. This gives a reduced representation of w starting with (s_1, s_1), which is a contradiction.

The other direction of the theorem is obvious. □

Remark 0.3.2. Tits' Theorem is far from trivial. For example, when considering a group like $G = \langle x, y \mid x^n = y^2 = (xy)^2 = 1_G \rangle$, it is not immediately clear how to reduce the word of the group, as shown in the Groups and Rings module of Year 2.

Example 0.3.3. Consider the group $G := \langle x, y \mid xyxyx = yxyxy \rangle$. This can be rewritten as:

$$G \cong \langle x, y, a \mid xyxyx = yxyxy, a = xy \rangle \cong \langle x, a \mid aax = x^{-1}aaa \rangle \cong$$

$$\langle x, a, b \mid a^2x = x^{-1}a^3, b = xa^2 \rangle \cong \langle a, b \mid a^2 = b^5 \rangle.$$

In this example, we can see that while the relations defining the group G are clear, the process of simplifying or reducing these relations is far from trivial. The transition from the group generated by x and y to the one generated by a and b involves several non-trivial steps, and the operations required to perform this reduction are not immediately obvious. This illustrates the difficulty in finding a direct reduction, even when the relations are relatively simple.

There are general tools such as Tietze transformations and coset enumeration that can be used to explore what operations can be performed on a general group presentation to reduce it. However, these methods go beyond the scope of this project and are typically covered in more advanced group theory courses.

In conclusion: while Tits' Theorem provides a powerful framework for reducing words in Coxeter groups, its non-triviality is highlighted by the complexity of group presentations and the reductions that need to be applied. The example above demonstrates how the word problem in even seemingly simple groups can become quite intricate and challenging.