Applied Mathematics E-Notes, 4(2004), 1–6 © ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

Complete Presentations Of Coxeter Groups*

Miguel A. Borges-Trenard †, Hebert Pérez-Rosés ‡

Received 9 March 2003

Abstract

A complete group presentation is a useful tool for performing computations with the specified group. Here we give complete presentations for the irreducible finite Coxeter groups $\mathbf{D_n}$, and prove some of its properties. With this result, it becomes possible to construct the complete presentation of any finite Coxeter group.

1 Introduction.

A **complete presentation** of a group or monoid M is a presentation of M that is complete when regarded as a string rewriting system. Such a presentation provides a straightforward solution to the **word problem** in M in a "syntactical" fashion, since any word on the generators of M can be rewritten in a unique way as a **canonical** or **normal form**. Thus, deciding whether two words represent the same group element amounts to comparing their canonical forms.

In general, complete presentations enable us to perform various computations with groups. In [4], we have shown how to use a complete group presentation for solving some problems in the given group, such as the discrete logarithm problem, of great importance in cryptograpy. If a group is to be used in a cryptographic system based on the complexity of the discrete logarithm problem, it must not be amenable to our methods. Thus, we have set out to investigate the complexity of the discrete logarithm problem in several classes of groups for potential cryptographic applications, including some Coxeter groups, like the class $\mathbf{D_n}$. This has provided the main motivation for the present paper.

Obtaining a complete presentation for M largely depends on a previously fixed ordering among the words on the generators of M. One of the most common such orderings is the **ShortLex** ordering, which first compares two words by their lengths, and then breaks ties lexicographically. Once we have fixed a generating set and an ordering on the words, there exists a unique complete **normalized** presentation on those generators, i.e. a presentation with no redundant rules (rules that can be derived from the others). For all details on the subject of complete rewriting systems, the reader can consult the classic monograph by Book and Otto [1].

*Mathematics Subject Classifications: 20F05, 20F10, 20F55, 68Q42.
†Department of Mathematics, University of Oriente, Santiago de Cuba 90500, Cuba
‡Department of Computer Science, University of Oriente, Santiago de Cuba 90500, Cuba

The derivation of complete presentations for **Coxeter groups** dates back to the 1980s with the work of Philippe le Chenadec [6, 7, 8], which has been pursued by other researchers in the last decade [10, 2, 9]. Du Cloux's paper [9] has come closest to giving a complete presentation for any finite Coxeter group on the standard generators, but there still remain some gaps to be filled. Du Cloux gives a set of directions that the reader has to follow in order to get an explicit complete presentation for a specific group; unfortunately, the method involves an induction step by the reader, who has to generalize some tables given by the author for particular groups.

In this paper we have set out to make that construction more explicit and rigorous for one of the families of irreducible finite Coxeter groups: the class $\mathbf{D_n}$. Those groups defy the Knuth-Bendix completion procedure for string rewriting systems; its execution time grows very rapidly as n increases, so that the procedure becomes soon impractical. As a consequence, no explicit formulas for the complete presentation of $\mathbf{D_n}$, based on the standard generators, had been available so far.

With this result, we can conclude a catalogue of complete presentations for all the irreducible finite Coxeter groups, which enables us to construct the complete presentation of any finite Coxeter group in way that is more straightforward than that of du Cloux's [3, 5].

2 Complete presentation of $\mathbf{D_n}$.

The class of groups $\mathbf{D_n}$ $(n \geq 4)$, of order $2^{n-1}n!$, is given by the following (standard) presentation on the generators $x_1, x_2, ..., x_n$, denoted $SP(n)$:

$$x_i^2 = 1 \text{ for } 1 \leq i \leq n,$$

$$(x_1x_3)^3 = 1,$$

$$(x_ix_{i+1})^3 = 1 \text{ for } 2 \leq i \leq n-1,$$

and finally,

$$(x_ix_j)^2 = 1$$

for all the other combinations of i and j $(i < j)$ not included above.

In this paper, the complete presentation for the group $\mathbf{D_n}$ will be obtained recursively, starting with a complete presentation for $\mathbf{D_4}$, and then producing the rules that need to be added in order to go from $\mathbf{D_{n-1}}$ to $\mathbf{D_n}$. The complete presentation of $\mathbf{D_4}$, denoted $CP(4)$, consists of the following 16 relations: [1]

$$x_i{}^2 \longrightarrow \mathbf{1}, \text{ para } 1 \leq i \leq 4,$$

$$x_2x_1 \longrightarrow x_1x_2, \;\; x_4x_1 \longrightarrow x_1x_4, \;\; x_4x_2 \longrightarrow x_2x_4,$$

$$x_3x_2x_3 \longrightarrow x_2x_3x_2, \;\; x_3x_1x_3 \longrightarrow x_1x_3x_1, \;\; x_4x_3x_4 \longrightarrow x_3x_4x_3,$$

$$x_3x_1x_2x_3x_1 \longrightarrow x_2x_3x_1x_2x_3, \;\; x_3x_1x_2x_3x_2 \longrightarrow x_1x_3x_1x_2x_3,$$

[1] This presentation was obtained with the aid of a Knuth-Bendix completion program written by us in GAP-3 [11].

$$x_4x_3x_1x_4 \longrightarrow x_3x_4x_3x_1,\ \ x_4x_3x_2x_4 \longrightarrow x_3x_4x_3x_2,$$
$$x_4x_3x_1x_2x_4 \longrightarrow x_3x_4x_3x_1x_2,$$
$$x_4x_3x_1x_2x_3x_4x_3 \longrightarrow x_3x_4x_3x_1x_2x_3x_4.$$

Now we define the words $\psi_j^{(n)}$, with $0 \leq j \leq 2n-1$:

$$\begin{aligned}
\psi_0^{(n)} &= \mathbf{1},\\
\psi_1^{(n)} &= x_n,\\
\psi_2^{(n)} &= x_nx_{n-1},\\
&\vdots\\
\psi_{n-2}^{(n)} &= x_nx_{n-1}x_{n-2}\dots x_3,\\
\psi_{n-1}^{(n)} &= x_nx_{n-1}x_{n-2}\dots x_3x_1,\\
\psi_n^{(n)} &= x_nx_{n-1}x_{n-2}\dots x_3x_2,\\
\psi_{n+1}^{(n)} &= x_nx_{n-1}x_{n-2}\dots x_3x_1x_2,\\
\psi_{n+2}^{(n)} &= x_nx_{n-1}x_{n-2}\dots x_3x_1x_2x_3,\\
&\vdots\\
\psi_{2n-1}^{(n)} &= x_nx_{n-1}x_{n-2}\dots x_3x_1x_2x_3\dots x_{n-1}x_n;
\end{aligned}$$

and we consider the following rule classes:

TYPE I: the rule ${x_n}^2 \longrightarrow \mathbf{1}$.

TYPE II: the rules $x_nx_i \longrightarrow x_ix_n$, for $1 \leq i \leq n-2$.

TYPE III: the rules $\psi_j^{(n)}x_n \longrightarrow x_{n-1}\psi_j^{(n)}$, with $2 \leq j \leq 2n-3$.

TYPE IV: the rule $\psi_{2n-1}^{(n)}x_{n-1} \longrightarrow x_{n-1}\psi_{2n-1}^{(n)}$.

We let $CP(n)$ be the presentation defined recursively as follows: For $n > 4$, $CP(n)$ is obtained from $CP(n-1)$ by adding the type I, II, III and IV relations just defined. We can now state the following result:

THEOREM 1. *$CP(n)$ is a complete normalized presentation of D_n, for all $n \geq 4$.*

Let us denote by $Irr(CP(n))$ the set of words in $x_1, x_2, ..., x_n$ that are irreducible with respect to the string rewriting system $CP(n)$. The proof of our theorem will consist of two parts:

1. Proving that $CP(n)$ and $SP(n)$ are algebraically equivalent.
2. Proving that $\|Irr(CP(n))\| = 2^{n-1}n!$.

As we shall see, those two facts suffice to conclude that $CP(n)$ is complete.

Let us start with the first part:

LEMMA 1. *$CP(n)$ and $SP(n)$ are algebraically equivalent.*

PROOF. All the relations in $SP(n)$ are contained in $CP(n)$, thus, we only have to show that the rules of $CP(n)$ are derivable from the relations in $SP(n)$; in particular, we only have to do this for the type III rules, except the first one, which is a trivial

consequence of $SP(n)$, and for the rule of type IV. In the case of the type III rules, it suffices to follow the process for the rule $\psi^{(n)}_{2n-3}x_n \longrightarrow x_{n-1}\psi^{(n)}_{2n-3}$, because in some sense, that is the most general situation.

On the right-hand side of each derivation step we give an indication of the rule that has been used, in the format "type.index"; for example, II.1 refers to the type II rule $x_nx_1 \longrightarrow x_1x_n$. We have

$$\begin{aligned}
& x_nx_{n-1}x_{n-2}\dots x_3x_1x_2x_3\dots x_{n-3}x_{n-2}x_n \\
\longleftrightarrow\ & x_nx_{n-1}x_{n-2}\dots x_3x_1x_2x_3\dots x_{n-3}x_nx_{n-2} && (II.n-2)\\
\longleftrightarrow\ & x_nx_{n-1}x_{n-2}\dots x_3x_1x_2x_3\dots x_nx_{n-3}x_{n-2} && (II.n-3)\\
& \vdots \\
\longleftrightarrow\ & x_nx_{n-1}x_nx_{n-2}\dots x_3x_1x_2x_3\dots x_{n-3}x_{n-2} && (II.n-2)\\
\longleftrightarrow\ & x_{n-1}x_nx_{n-1}x_{n-2}\dots x_3x_1x_2\dots x_{n-3}x_{n-2} && (III.2).
\end{aligned}$$

That is, we use the type II rules for permuting x_n with the other generators, and when the pattern $x_nx_{n-1}x_n$ appears, we use the rule III.2 to transform it into $x_{n-1}x_nx_{n-1}$. Hence, we have the equivalence

$$\begin{aligned}
& x_nx_{n-1}x_{n-2}\dots x_3x_1x_2x_3\dots x_{n-3}x_{n-2}x_n \\
\overset{*}{\longleftrightarrow}\ & x_{n-1}x_nx_{n-1}x_{n-2}\dots x_3x_1x_2x_3\dots x_{n-3}x_{n-2},
\end{aligned}$$

and since

$$x_nx_{n-1}\dots x_3x_1x_2x_3\dots x_{n-2}x_n > x_{n-1}x_nx_{n-1}\dots x_3x_1x_2x_3\dots x_{n-2}$$

in the ShortLex ordering, we can orient the rule as

$$x_nx_{n-1}\dots x_3x_1x_2x_3\dots x_{n-2}x_n \longrightarrow x_{n-1}x_nx_{n-1}\dots x_3x_1x_2x_3\dots x_{n-2}.$$

It is easy to see that the procedure above can be applied to all the other type III rules. As for the type IV rule, we have:

$$\begin{aligned}
& x_nx_{n-1}\cdots x_3x_1x_2x_3\cdots x_{n-1}x_nx_{n-1} \\
\longleftrightarrow\ & x_nx_{n-1}\cdots x_3x_1x_2x_3\cdots x_{n-2}x_nx_{n-1}x_n && (III.2)\\
\overset{*}{\longleftrightarrow}\ & x_nx_{n-1}x_nx_{n-2}\cdots x_3x_1x_2x_3\cdots x_{n-1}x_n && (II.i)\\
\longleftrightarrow\ & x_{n-1}x_nx_{n-1}x_{n-2}\cdots x_3x_1x_2\cdots x_{n-1}x_n, && (III.2).
\end{aligned}$$

which yields the rule

$$x_nx_{n-1}\cdots x_3x_1x_2\cdots x_{n-1}x_nx_{n-1} \longrightarrow x_{n-1}x_nx_{n-1}x_{n-2}\cdots x_3x_1x_2\cdots x_{n-1}x_n,$$

as desired.

Now we turn to the second assertion. Let us start with the following

LEMMA 2. $\alpha \in Irr(CP(n))$ if, and only if $\alpha = \alpha_1\psi^{(n)}_j$, for some $\alpha_1 \in Irr(CP(n-1))$ and $0 \le j \le 2n-1$.

PROOF. The "if" part is pretty obvious, so we turn to the "only if" part. In the trivial case, when α does not contain x_n, we have $\alpha = \alpha\psi^{(n)}_0 \in Irr(CP(n-1))$; so, let

us assume that α contains x_n. Let $\alpha = y_1 \cdots y_k$, and let i $(1 \leq i \leq k)$ be the smallest index such that $y_i = x_n$. Evidently, $y_1 \cdots y_{i-1} \in Irr(CP(n-1))$, hence we only have to show that $y_i y_{i+1} \cdots y_k$ coincides with one of the $\psi_j^{(n)}$. If $k = i$, $y_i y_{i+1} \cdots y_k$ coincides with $\psi_1^{(n)}$. Else, let the length of $y_i y_{i+1} \cdots y_k$ be smaller than $n-1$; thus y_{i+1} must be x_{n-1}, because otherwise, y_i and y_{i+1} could be swapped. Similarly, if it exists, y_{i+2} must be x_{n-2}, and so on, until y_{i+n-3}, which must be equal to x_3. Now, in the case when the length of $y_i y_{i+1} \cdots y_k$ is at least $n-1$, y_{i+n-2} could be x_2 or x_1. If $y_{i+n-2} = x_2$, there is no possibility for y_{i+n-1}; in the latter case, y_{i+n-1} must be x_2 (if it exists), y_{i+n} must be x_3, and so on, until y_{i+2n-2}, which must be equal to x_n again. The length of $y_i y_{i+1} \cdots y_k$ cannot exceed $2n-1$, because any symbol appearing after the final x_n will make α reducible.

Now, with the aid of induction, it is very straightforward to establish the following results.

COROLLARY 1. $\|Irr(CP(n))\| = 2^{n-1} n!$.

COROLLARY 2. If $\alpha \in Irr(CP(n))$, then $\alpha = \varphi \psi_{j_5}^{(5)} \cdots \psi_{j_{n-1}}^{(n-1)} \psi_{j_n}^{(n)}$, where $\varphi \in Irr(CP(4))$, and $1 \leq j_k \leq 2k-1$.

PROOF OF THEOREM 1. Let $X = \{x_1, x_2, ..., x_n\}$, $\langle X \rangle$ be the free monoid generated by X, and let $\langle SP(n) \rangle$ (resp. $\langle CP(n) \rangle$) denote the congruence on X generated by the presentation $SP(n)$ (resp. $CP(n)$). Since all the rules of $CP(n)$ can be derived from $SP(n)$ (Lemma 1), we can deduce that $\langle CP(n) \rangle \subseteq \langle SP(n) \rangle$, and hence,

$$\|\langle X \rangle / \langle SP(n) \rangle\| \leq \|\langle X \rangle / \langle CP(n) \rangle\| \leq \|Irr(CP(n))\| = \|\mathbf{D_n}\|.$$

That is, for each equivalence class modulo $CP(n)$, there exists one, and only one irreducible element, which means that $CP(n)$ is complete.

The fact that $CP(n)$ is normalized is fairly obvious.

References

[1] R. V. Book and F. Otto, String Rewriting Systems, Springer, Berlin, 1993.

[2] M. A. Borges-Trenard and H. Pérez-Rosés, G-presentations of Coxeter groups with three generators, Procs. First Int. Conf. Math. and Comp. Sc. (Santiago de Cuba, Nov. 1996), Publications of the National Autonomous Univ. of México, 1997.

[3] M. A. Borges-Trenard and H. Pérez-Rosés, Complete presentations of direct products of groups, Ciencias Matemáticas 19(1)(2001), 3–11.

[4] M. A. Borges-Trenard, H. Pérez-Rosés and M. Borges-Quintana, Gröbner basis property on elimination ideals in finite group theory, in K. Nakagawa (ed.), Procs. of the Conf. "Logic, Mathematics and Computer Science: Interactions" (Hagenberg, Austria, Oct. 20-22, 2002), 61–69.

[5] M. A. Borges-Trenard and H. Pérez-Rosés, Complete presentations of finite Coxeter groups, unpublished manuscript.

[6] Ph. Le Chenadec, A completion of some Coxeter groups, Procs. of the European Conf. on Computer Algebra (Linz, 1985), Lecture Notes in Computer Science 204, vol. 2., Springer, Berlin, 1985, 229–242.

[7] Ph. Le Chenadec, Canonical Forms in Finitely Presented Algebras, Pitman, London, 1986.

[8] Ph. Le Chenadec, A catalogue of complete group presentations, J. Symb. Comp. 2(4)(1986), 363–381.

[9] Fokko du Cloux, A transducer approach to Coxeter groups, J. Symb. Comp. 27(1999), 311–324.

[10] S. Hermiller, Rewriting systems for Coxeter groups, J. Pure Appl. Algebra 92(1994), 137–148.

[11] M. Schönert et al, GAP – Groups, Algorithms, and Programming, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, fifth edition, 1995.