TODD-COXETER ALGORITHM

by

MERRITT SPENCER, LAURA BARNES, TAYLOR NOVAK, AND DARREN ELIZONDO

MAT 3233 Modern Algebra

Dr. Dueñez

Fall 2024

TABLE OF CONTENTS

1. Introduction

1.1 Historical Context

1.1.1 History of Development

The Todd-Coxeter Algorithm was published in 1936 and created by mathematicians J. A. Todd and H. S. M. Coxeter [1]. Their procedure was so groundbreaking at the time that they had difficulty getting their paper published [2]. J. A. Todd, John Arthur Todd, focused on geometry and was a lecturer at Cambridge for much of his career [2]. H. S. M Coxeter, Harold Scott MacDonald Coxeter, primarily went by Donald [3]. His work was also focused on geometry and he spent the majority of his career at the University of Toronto [3]. When Todd and Coxeter proposed their method for hand calculations, it ended up likely being the first application of a pure mathematics non-trivial algorithm onto a digital computer[4]. By extension, it was the first implementation of a group theory program on a digital computer [5]. C.B. Haselgrove, an English mathematician, implemented the algorithm at Cambridge University on the EDSAC 1 computer[5]. The algorithm is known today as being within the subject of computational group theory [6]. Computational group theory is often used in cryptography and physics.

Stated by Todd and Coxeter themselves, the method of enumeration by cosets had long been in the field of abstract group theory [1]. The start of group theory likely stems from the early 19th century abstraction of geometry, late 18th century number theory, and the study of permutations at the end of the 18th century [7]. In 1761, Euler's work, although not stated in group theory terms, does have an example of an abelian group being decomposed into cosets of a subgroup [7]. Gauss built upon this foundation in 1801 with his work on modular arithmetic which led to theories about abelian groups. The first usage of the term "group" was from Evariste Galois during the 1830s, however this work was unknown until it was published in 1846 [7] [8]. When Cayley published papers in 1854, they were misunderstood, but by the 1870s, the definition of a group was generalized and his 1878 papers were very impactful in the field [7].

1.2 Current Applications in Computer Algebra Systems and Elsewhere

Until the early 1990s, computational group theory was rather unpopular with group theorists, but the introduction of Computer Algebra Systems improved popularity [6]. The Todd-Coxeter Algorithm was designed to calculate the cosets of a subgroup within a finite group [1]. There are current implementations of the algorithm in Computer Algebra Systems such as MAPLE, MAGMA, and GAP. Both MAPLE and MAGMA terminate the enumeration at a specific number of maximum cosets which is user definable [9] [10], while GAP has a tool that determines the step to stop at called Interactive Todd-Coxeter (ITC). Some users on the internet have also made programming scripts of the algorithm as well, typically in Python. Demonstrated in Section 4 of the paper, is the manual coset enumeration of the alternating group of degree 5, but to showcase the accuracy of ITC, the results of the algorithm will be shown below on the same group using GAP. For the sake of brevity, the relator tables will be shown at the end of section 4, but the results received from GAP do match the hand calculations.

Coset Table- HLT

	a	a^-1	b	b^-1
1	2	3	1	1
2	3	1	3	6
3	1	2	4	2
4	6	7	5	3
5	8	9	6	4
6	7	4	2	5
7	4	6	9	8
8	9	5	7	11
9	5	8	10	7
10	11	12	11	9
11	12	10	8	10
12	10	11	12	12

code adapted from Gap.app Help Manual

```
LoadPackage("itc");

F:= FreeGroup("a", "b");
a:= F.1; b:=F.2;
rels:= [a^3, b^5, (a*b)^2];
G:=F/rels;
a:=G.1; b:=G.2;
H:=Subgroup(G, [b]);
InteractiveTC(G, H);
```

2. Group Theory

2.1 Groups

A group is set that has been provided an operation that connects one element to any pair of elements such that the operation is associative, has an identity, and every element has an inverse. A presentation of a group G is defined to be $\langle X|R\rangle$ where G is generated by X such that all the equations in R hold true in the group G. X is the set of generators and R is the set of relations. What this all means is that every element of G can be made by a product of powers of some of the generators in X and of the relations between those generators in R. A Free Group is of the form $\langle X|\rangle$ where there are no nontrivial relations between the generators. A group isomorphism is a function between two groups that sets up a bijection between the elements of the two groups that renames all of the elements from one group into the elements of the other.

2.2 Coset Enumeration

2.2.1 What is a coset?

In group theory, a coset is one of a disjoint, equal sized subset of a group that is created by multiplying each element of a subgroup by an element of the group. There are two types of cosets: left cosets and right cosets. A left coset is made by multiplying each element of H by a fixed element g of G where

$$gH = gh : h \in H \text{ for } g \in G$$

A right coset is the same but with Hg and hg.

2.2.2 Lagrange's Theorem

Theorem: For any finite group G, the order of subgroup H of G divides the order of G.

Lemma 1: If G is a group with subgroup H, then there is a one to one correspondence between H and any coset of H.

Lemma 2: If G is a group with subgroup H, then the left coset relation $g1 \sim g2$ if and

only if $g1 \cdot H = g2 \cdot H$ is an equivalence relation.

Lemma 3: Let S be a set and $\sim$ be an equivalence relation on S. If A and B are two equivalence classes where $A \cap B = \emptyset$, then $A = B$.

Proof: Let G be a finite group of order b and H be a subgroup of G of order k. Also let $\sim$ be the left coset equivalence relation defined in Lemma 2. It follows from Lemma 2 that $\sim$ is an equivalence relation and by Lemma 3 any two distinct cosets of $\sim$ are disjoint. Hence there exists

$$G = (g1 \cdot H) \cup (g2 \cdot H) \cup ... \cup (gl \cdot H)$$

such that $gi \cdot H, i = 1, 2, ...l$ are the disjoint left cosets of H given by Lemma 3.
Lemma 1 states that the cardinality of these cosets is the same as $|H|$ meaning that

$$|G| = |H| \cdot |H| \cdot ... \cdot |H| \; |G| = |H| \cdot l \; |G| = k \cdot l$$

Therefore, $k|n$. □

2.2.3 A Todd-Coxeter Alternative

An alternative coset enumeration process includes the Knuth-Bendix process which may be particularly useful for infinite groups, something the Todd-Coxeter is not useful for [11]. That process has specifically been used for searching for "isomorphisms between two finitely presented groups" and determining equivalence of two given words from a group. A word within group theory represents an expression of a subgroup S that is made up of a string of generators $s1s2...si$ raised to the ± 1 where i is the length of the word. Each word in S represents an element of G [11].

3. What is the Todd-Coxeter Algorithm?

3.1 The Todd-Coxeter Algorithm

Given a finite group with unknown order G and given a subgroup H with known order $|G : H|$ it is possible to calculate $|G|$ through coset enumeration. Coset enumeration is the process of counting the number of cosets of a subgroup H of G. Lagrange's Theorem states that all cosets have the same order as the subgroup H and as such $|G| = |H| \cdot k$ where k is the number of cosets.

3.2 Proof of Termination within a Finite Subgroup

One of the main benefits of the Todd-Coxeter Algorithm is that the size of the Subgroup does not matter as long as it is finite. As such the following Theorem can be proved:

Theorem. *Consider a run of the Todd–Coxeter procedure in which the choices are made so that the following conditions are guaranteed to hold:*

(a) For each coset label x that is introduced, either x will eventually die or else x^s will eventually be defined for all $s \in S$.

(b) Coset 1 will eventually scan correctly under every generator of H.

(c) Each coset label x that is introduced and does not die will eventually scan correctly under every relator.

If $|G : H|$ is finite, then the procedure terminates.

By the given assumption $|G : H|$ is finite, so there can only be a finite number of distinct cosets of H in G. Let the index be $n = |G : H|$. This implies that the coset table can have at most n distinct rows.

Condition (a) ensures that every coset label either:

1. Dies by merging with another coset, or
2. Has all its transitions x^s defined

Since there are at most n distinct cosets, this process can introduce at most n distinct coset labels. Thus, the introduction of new coset labels must terminate.

Condition (b) guarantees that coset 1 (representing H) will eventually scan correctly under all generators $s \in S$.

Condition (c) guarantees that every surviving coset x will scan correctly under every relator.

Since the number of cosets is bound by n, the transitions for each coset are finite tasks, and each step either defines an entry or solves a conflict by merging cosets there can be no infinite loops and the process must terminate. □

3.3 Defining Schreier Graphs

Named after the well-known Austrian mathematician, Otto Schreier, these graphs provide a visual representation for understanding subgroup cosets. After a lecture he attended, held by Kurt Reidemeister, he was able to expand upon Reidemeister's method to arbitrary subgroups by choosing generators for the subgroup where he was able to prove that subgroups of free groups were also free [12], which is how Schreier graphs were formulated. This relates to the Todd-Coxeter algorithm by enumerating cosets of subgroups from a group. It allows the Schreier graph to browse through the cosets of a group to calculate the subgroup.

3.4 Defining Coset Tables

A coset table is crucial for the Todd-Coxeter algorithm. The coset tables enumerate the cosets of subgroup H in a finite group G. In the table, the rows represent the cosets while the columns are the generators. For the Todd-Coxeter procedure, names are made up for cosets which would be numbers and "draw in arrows for the action of the generators as we discover them" [13]. Once complete, the graph should show that all the relations are satisfied.

3.5 Definitions and Bonuses on the Relator Tables

As mentioned previously, a relator table is a tool used in the process of scanning when dealing with data that might be too complicated or too big for a Schreier Graph. Each relator has its own table where each row represents one coset such that it starts and ends in it. The entries within the table show the actions that a generator takes within each relator. Scanning is the "process of checking that a realtor is satisfied," [13]. A scan of a row is considered correct when the entire

row is filled [13]. However, it is possible that a row has been scanned both right to left and left to right and not be correct. In order to fill these rows a user is allowed to add "Definitions" where a blank entry is filled with a new coset such that $u^a = v$ where u is the existing coset, v is the newly defined coset, and a is the individual relator in between u and v on the table. As a result of this, it is possible that other definitions may arise due to applying the newly created definition; these are referred to as "Deductions" or "Bonuses" [14]. A relator table only ends once there are not any cosets created by definitions that haven't been satisfied on the Coset Table on any relator table that is part of the subgroup [13].

3.6 Felsch versus HLT

The sequence when enumerating is decided by the user [15]. Two common ways to scan are the HLT and Felsch techniques. A coset is scanned correctly if its vertex is within its Schreier Graph or if the row within its relator table is completely satisfied. Scanning is done from left to right, using a, and right to left, using $a - 1$. When enumerating cosets, there is the chance that a coincidence can occur. This is when the "defining relations" are mismatched [16]. If this is the case, then the group has only the identity element and any enumeration will collapse to one coset [15] [16]. This partial collapsing occurs cyclically– with the number of active cosets increasing and then decreasing when a coincident occurs [15]. The HLT method is named after Haselgrove, Leech, and Trotter and may also be known as the realtor based method [13]. Each coset is scanned against the relators, making definitions when needed to ensure all scans finish [15]. Any coincidences encountered are taken into account during the method [15]. The Felsch method aims to fill the table instead of aiming to finish scans [13]. It goes from each coset and tests each definition against all unique relator positions until coincidences are found [15].

4. The Todd Coxeter Algorithm on A_5

4.1 Coset Enumeration of the Alternating Group of Degree 5

Given the finite group $G = \langle a, b | a^3 = b^5 = (ab)^2 = 1 \rangle$ use the Todd Coxeter Algorithm to perform coset enumeration with respect to subgroup $H = \langle b \rangle$. *It is also possible to enumerate with respect to a, however there would be 20 cosets instead of 12.*

To begin, create the b relator table scanning correctly where $1^b = 1$ which will be listed under the bonus column and the coxeter table will be updated to show this.

b	
1	1

Definition	Bonus
	$1^b = 1$

	a	b
1		1

Thus, starting from the first coset for our remaining tables we have:

	a	a	a
1			1

	b	b	b	b	b
1	1	1	1	1	1

	a	b	a	b
1			1	1

Define $1^a = 2$, $2^a = 3$ so that the so that the first coset of the aaa table scans correctly from left to right. The bonus $3^a = 1$ is acquired as part of this process. By applying these definitions to the $abab$ table and scanning from right to left, the bonus $2^b = 3$ is obtained by applying $1^{a^{-1}} = 3$, the inverse of $3^a = 1$.

	a	a	a
1	2	3	1

	b	b	b	b	b
1	1	1	1	1	1

	a	b	a	b
1	2	3	1	1

Definition	Bonus
	$1^b = 1$
$1^a = 2$	$3^a = 1$
$2^a = 3$	$2^b = 3$

	a	b
1	2	1
2	3	3
3	1	

Moving to the second coset, upon using the current definitions and bonuses to scan from left to right results in a correctly scanned coset in the aaa table. To scan the coset correctly on the $bbbbb$ table define $b^3 = 4$, $b^4 = 5$, and $b^5 = 6$ which will provide the bonus of $b^6 = 2$. These definitions are used to correctly scan the second coset in the $abab$ table giving the second bonus of $4^a = 6$ after scanning from both left to right and right to left.

	a	a	a
1	2	3	1
2	3	1	2

	b	b	b	b	b
1	1	1	1	1	1
2	3	4	5	6	2

	a	b	a	b
1	2	3	1	1
2	3	4	6	2

Definition	Bonus
	$1^b = 1$
$1^a = 2$	$3^a = 1$
$2^a = 3$	$2^b = 3$
$b^3 = 4$	
$b^4 = 5$	$b^6 = 2$
$b^5 = 6$	$4^a = 6$

	a	b
1	2	1
2	3	3
3	1	4
4	6	5
5		6
6		2

For the sake of brevity from this point onward, only the current coset row will be shown (along with which definitions, if any, will be added along with any bonuses obtained from the coset) during each concurrent step. While these are shown separately it is important to remember that they are all parts of the same table.

For the third coset, there are no new definitions required in order to scan correctly and as such no bonuses are gained.

	a	a	a
3	1	2	3

	b	b	b	b	b
3	4	5	6	2	3

	a	b	a	b
3	1	1	2	3

For the fourth coset, define $6^a = 7$ resulting in a bonus of $7^a = 4$.

	a	a	a
4	6	7	4

	b	b	b	b	b
4	5	6	2	3	4

	a	b	a	b
4	6	2	3	4

For the fifth coset, define $5^a = 8$ and $8^a = 9$ resulting in a bonus of $9^a = 5$ and $8^b = 7$.

	a	a	a
5	8	9	5

	b	b	b	b	b
5	6	2	3	4	5

	a	b	a	b
5	8	7	4	5

For the sixth coset, there are no required definitions, but the bonus $7^b = 9$ is gained by scanning the $abab$ table from right to left.

	a	a	a
6	7	4	6

	b	b	b	b	b
6	2	3	4	5	6

	a	b	a	b
6	7	9	5	6

For the seventh coset, define $9^b = 10$ and $10^b = 11$ resulting in a bonus of $11^b = 8$.

	a	a	a
7	4	6	7

	b	b	b	b	b
7	9	10	11	8	7

	a	b	a	b
7	4	5	8	7

For the eighth coset, the bonus $10^a = 11$ is gained by scanning the $abab$ table.

	a	a	a
8	9	5	8

	b	b	b	b	b
8	7	9	10	11	8

	a	b	a	b
8	9	10	11	8

For the ninth coset, there are no new definitions required in order to scan correctly and as such no bonuses are gained.

	a	a	a
9	5	8	9

	b	b	b	b	b
9	10	11	8	7	9

	a	b	a	b
9	5	6	7	9

For the tenth coset, define $11^a = 12$ resulting in a bonus of $12^a = 10$.

	a	a	a
10	11	12	10

	b	b	b	b	b
10	11	8	7	9	10

	a	b	a	b
10	11	8	9	10

For the eleventh coset, the bonus $12^b = 12$ is obtained by scanning the $abab$ table.

	a	a	a
11	12	10	11

	b	b	b	b	b
11	8	7	9	10	11

	a	b	a	b
11	12	12	10	11

For the twelfth coset there are no new definitions required in order to scan correctly and as such no bonuses are gained. As there are no more open definitions this is the last coset.

	a	a	a
12	10	11	12

	b	b	b	b	b
12	12	12	12	12	12

	a	b	a	b
12	10	11	12	12

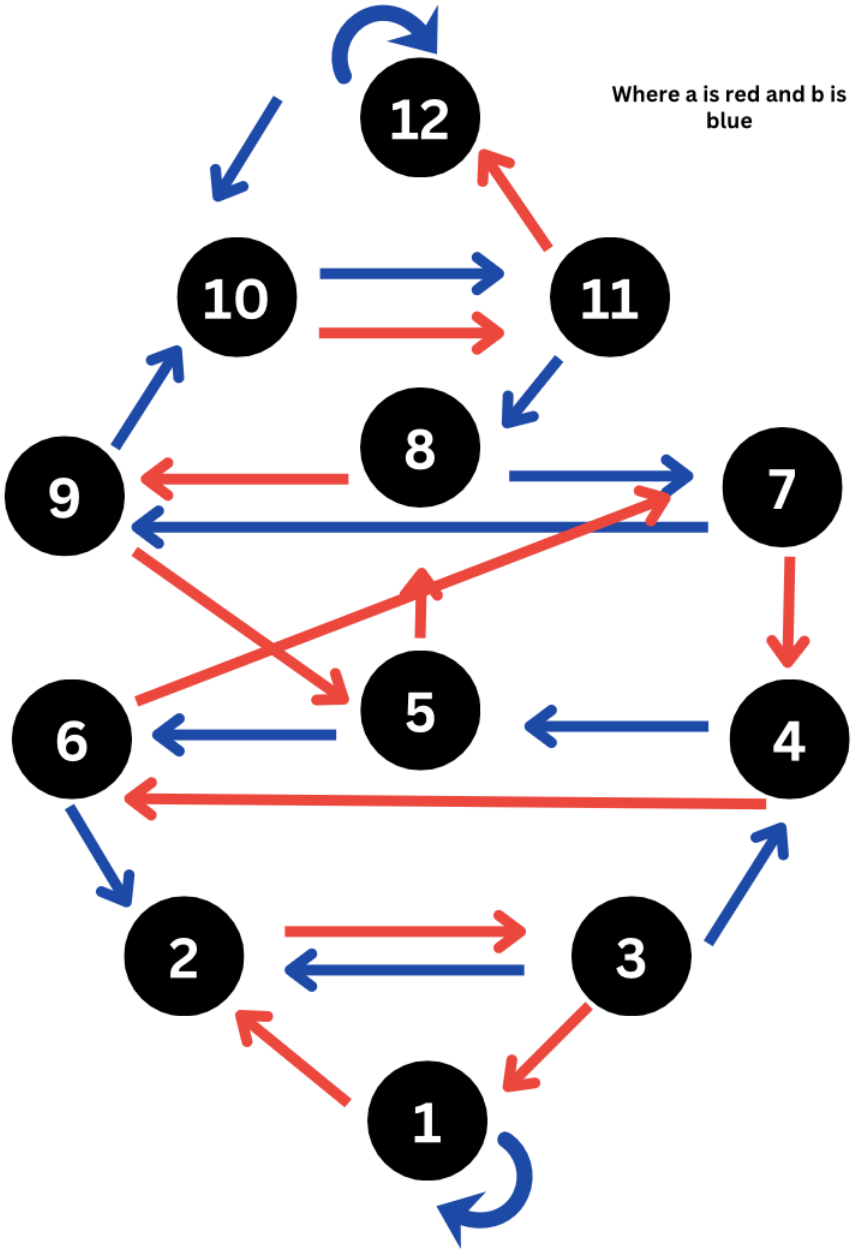
The final coset table is:

	1	2	3	4	5	6	7	8	9	10	11	12
a	2	3	1	6	8	7	4	9	5	11	12	10
b	1	3	4	5	6	2	9	7	10	11	8	12

From this it is deducible that $|G : H| = 12$. Furthermore, the permutation representation for the generators a, b is $a = (123)(467)(589)(101112) \quad b = (23456)(7891011)$.

Since b of G is a nontrivial generator it follows that $|H| = 5$ meaning that $|G| = 60$. □

Below is the Schreier Graph that represents the work done above.



4.2 Results of the GAP Coset Enumeration

Below is the relator tables.

Relator 1: a^3 - Gap S...

Sheet

a	a	a	
1	2	3	1
2	3	1	2
3	1	2	3
4	6	7	4
5	8	9	5
6	7	4	6
7	4	6	7
8	9	5	8
9	5	8	9
10	11	12	10
11	12	10	11
12	10	11	12

Relator 2: b^5 - Gap Session 1

Sheet

b	b	b	b	b	b
1	1	1	1	1	1
2	3	4	5	6	2
3	4	5	6	2	3
4	5	6	2	3	4
5	6	2	3	4	5
6	2	3	4	5	6
7	9	10	11	8	7
8	7	9	10	11	8
9	10	11	8	7	9
10	11	8	7	9	10
11	8	7	9	10	11
12	12	12	12	12	12

Relator 3: a*b*a*b - Gap Sess...

Sheet

a	b	a	b	
1	2	3	1	1
2	3	4	6	2
3	1	1	2	3
4	6	2	3	4
5	8	7	4	5
6	7	9	5	6
7	4	5	8	7
8	9	10	11	8
9	5	6	7	9
10	11	8	9	10
11	12	12	10	11
12	10	11	12	12

REFERENCES

[1] J. A. Todd and H. S. M. Coxeter, “A practical method for enumerating cosets of a finite abstract group,” *Proceedings of the Edinburgh Mathematical Society*, vol. 5, pp. 26–34, 1936.

[2] MacTutor from the University of St Andrews, "John Arthur Todd," https://mathshistory.st-andrews.ac.uk/Biographies/Todd/.

[3] MacTutor from the University of St Andrews, "Harold Scott MacDonald Coxeter," https://mathshistory.st-andrews.ac.uk/Biographies/Coxeter/.

[4] S. A. Linton, “Computational algebra and number theory,” 1995.

[5] Cambridge Press, "Article", https://www.cambridge.org/core/books/groups-st-andrews-1981/an-elementary-introduction-to-coset-table-methods-in-computational-group-theory/4AEEF4EA224BA06964D46D51A3ED1D89.

[6] R. F. M. Luise-Charlotte Kappe, Arturo Magidin, *Computational Group Theory and the Theory of Groups*. American Mathematical Society, 2007.

[7] MacTutor from the University of St Andrews, "The development of group theory," https://mathshistory.st-andrews.ac.uk/HistTopics/Development_group_theory/.

[8] M. D. Woba, “Application of the todd-coxeter algorithm in the computation of group theory,” 2023.

[9] MAGMA, "Documentation", https://magma.maths.usyd.edu.au/magma/handbook/text/86710093.

[10] MAPLE, "Online Help", https://www.maplesoft.com/support/helpJP/Maple/view.aspx?path=group/pres.

[11] D. Epstein and P. Sanders, “"knuth-bendix for groups with infinitely many rules",” 2024.

[12] MacTutor from the University of St Andrews, "Otto Schreier," https://mathshistory.st-andrews.ac.uk/Biographies/Schreier/.

[13] The Todd-Coxeter Procedure, "Ken Brown," https://pi.math.cornell.edu/ kbrown/7350/toddcox.pdf, Sept. 2013.

[14] D. L. Johnson, “Presentations of groups,” 1998.

[15] G. Havas and C. Ramsay, “Proving a group trivial made easy: A case study in coset enumeration,” *62*, pp. 105–118, 2000.

[16] J. Leech, “Coset enumeration on digital computers,” *Cambridge University Press*, 2008.