Groups With Two Generators Having Unsolvable Word Problem And Presentations of Mihailova Subgroups

Xiaofeng Wang, Chen Xu, Guo Li*, and Hanling Lin
School of Mathematics, Shenzhen University
Shenzhen 518060, P. R. China

Abstract. A presentation of a group with two generators having unsolvable word problem and an explicit countable presentation of Mihailova subgroup of $F_2 \times F_2$ with finite number of generators are given. Where Mihailova subgroup of $F_2 \times F_2$ enjoys the unsolvable subgroup membership problem. One then can use the presentation to create entities' private keys in a public key cryptsystem.

Key words: word problem, subgroup membership problem, Mihailova subgroup, insolvability

1 Introduction

In 1997, Shor published in [37] his distinguished quantum computational algorithms and he pointed out in this paper that with his algorithms the factorization of an integer and the computation of discrete logarithm are computable in a polynomial time. Therefore, the most used public key cryptsystems (such as RSA, ECC, et cetera) are really in jeopardy since people believe that quantum computers or quantum computation systems are in fact not far from the reality. Therefore, one of the most urgent task for the cryptologists is to find new public key cryptsystems which are much more safe and free of the quantum computational attack.

In the last decade, due to the works done by Anshel *et al*[1], and Ko *et al*[24], the decision problems from combinatorial group theory (i.e. the conjugacy search problem, the decomposition problem, the root extraction search problem, and the subgroup membership problem) have been intensively employed as the core for the establishment of alleged secure and effective cryptographic primitives. In particular, due to having very complicated structures, very nice geometrical interpretations, exponential growth, and unique normal form for all words representing any fixed element, the non-commutative braid groups B_n have been used as the platforms of setting up cryptographic schemes [2, 3, 25, 8, 13, 27, 38, 40, 41, 42, 44, 45] with the hope that the corresponding protocols have high level security. Unfortunately, it was shown that some of these primitives are feasible to the attackers, for examples see [9, 14, 15, 16, 17, 19, 21, 22, 23, 26, 28, 29, 30, 31, 34, 36].

Clearly, one of the resolutions is to find a group with word problem solvable in polynomial time and with some decision problem very hard decidable. Followed then, taking the group as the platform one can try to set up public key cryptographic primitives with safety guaranteed by the hard decision problem.

Collins [12] proved that there are subgroups of a braid group B_n with $n \geq 6$ which are isomorphic to the group $F_2 \times F_2$, where the group F_2 is the free group of rank 2. Then, as Shpilrain and Ushakov have pointed out in [39] that there are some Mihailova subgroups [32] in a braid group B_n with $n \geq 6$ such that the subgroup membership problem of these subgroups is unsolvable. Therefore, one of the key points of this undecidability is able to be applied to propose new cryptsystems is to give an explicit presentation of Mihailova subgroups of B_n.

*Correspondence author.

2 Subgroups with unsolvable GWP

2.1 Some decision problems of groups

In this section, for the use in the sequel, we present some decision problems of groups.

A presentation of a group G is as the following

$$\mathcal{P} = \langle x_1, x_2, x_3, \cdots | R_1, R_2, R_3, \cdots \rangle$$

where the set $X = \{x_1, x_2, x_3, \cdots\}$ is called an alphabet and the R_j's are words on $X \cup X^{-1}$ with $X^{-1} = \{x_1^{-1}, x_2^{-1}, x_3^{-1}, \cdots\}$. The group presented by $\mathcal{P}$ denoted $G(\mathcal{P})$ is the quotient group of the free group on X by the normal closure of the set $\{R_1, R_2, R_3, \cdots\}$ in the free group. Usually it is not necessary to distinguish so carefully between a group and its presentation and we often write simply

$$G = \langle x_1, x_2, x_3, \cdots | R_1, R_2, R_3, \cdots \rangle$$

to mean the G is the group defined by the given presentation, and we call that the elements in X are generators of G, the words R_j's are defining relators. When the sets X is finite we then say that G is finitely generated, and when both sets X and $\{R_1, R_2, R_3, \cdots\}$ are finite we then say that G is finitely presented. Sometimes, one may uses so-called *defining relations* of the form $R_l = R_r$ (which is equivalent to being a relator of the form $R_l R_r^{-1}$) to replace relators in a presentation of a group G.

Suppose that G is a finitely presented group defined by a presentation as above. We present some decision problems in G.

Word problem (WP):
Given any two words w and u on $X \cup X^{-1}$, decide if $w = u$ in G.

Generalized word problem or subgroup membership problem (GWP):
Given a subgroup H of G generated by elements $a_1, a_2, \cdots, a_l$, and an element g of G, decide if g is an element of H, or equivalently if g can be written as a word on the set

$$\{a_1, a_2, \cdots, a_l\} \cup \{a_1^{-1}, a_2^{-1}, \cdots, a_l^{-1}\}$$

2.2 Presentation of groups with two generators having unsolvable WP

Novikov [35] and Boone [4] independently proved that there is a finitely presented group having unsolvable word problem. In 1969, Borisov [6] gave an elegant simplification on Boone's approach. Then in 1986, applying to a Céjtin's [7] semigroup presentation with Borisov's method, Collins [11] set up a simple finite group presentation having unsolvable word problem with 10 generators and 27 relations as the following.

Presentation A

Generators:

$$c_1,\ c_2,\ c_3,\ c_4,\ c_5,\ c_6,\ c_7,\ c_8,\ c_9,\ c_{10}$$

Relations:

$$c_1^{-1}c_7^{10}c_1 = c_7,\ c_2^{-1}c_7^{10}c_2 = c_7,\ c_3^{-1}c_7^{10}c_3 = c_7,\ c_4^{-1}c_7^{10}c_4 = c_7,\ c_5^{-1}c_7^{10}c_5 = c_7,$$

$$c_1^{-1}c_8c_1 = c_8^{10},\ c_2^{-1}c_8c_2 = c_8^{10},\ c_3^{-1}c_8c_3 = c_8^{10},\ c_4^{-1}c_8c_4 = c_8^{10},\ c_5^{-1}c_8c_5 = c_8^{10},$$

$$c_9^{-1}c_1c_9 = c_1,\ c_9^{-1}c_2c_9 = c_2,\ c_9^{-1}c_3c_9 = c_3,\ c_9^{-1}c_4c_9 = c_4,\ c_9^{-1}c_5c_9 = c_5,$$

$$c_{10}^{-1}c_7c_{10} = c_7,\ c_{10}^{-1}c_8c_{10} = c_8, c_6^{-1}c_1^{-3}c_{10}c_1^3c_6 = c_1^{-3}c_{10}c_1^3$$

$$c_9^{-1}c_7c_1c_3c_8c_9 = c_7c_3c_1c_8,\ c_9^{-1}c_7^2c_1c_4c_8^2c_9 = c_7^2c_4c_1c_8^2,\ c_9^{-1}c_7^3c_2c_3c_8^3c_9 = c_7^3c_3c_2c_8^3,$$

$$c_9^{-1}c_7^4c_2c_4c_8^4c_9 = c_7^4c_4c_2c_8^4,\ c_9^{-1}c_7^5c_3c_5c_8^5c_9 = c_7^5c_5c_3c_1c_8^5,\ c_9^{-1}c_7^6c_4c_5c_8^6c_9 = c_7^6c_5c_4c_2c_8^6,$$

$$c_9^{-1}c_7^7c_3c_4c_3c_8^7c_9 = c_7^7c_3c_4c_3c_5c_8^7,\ c_9^{-1}c_7^8c_3c_1^3c_8^8c_9 = c_7^8c_1^3c_8^8,\ c_9^{-1}c_7^9c_4c_1^3c_8^9c_9 = c_7^9c_1^3c_8^9$$

We denote C the group defined by the above presentation. By a remarkable embedding theorem [20] of G. Higman, B. H. Neumann and H. Neumann's, one can embed C in the group defined by the following presentation.

Presentation B

$$\langle J, t;\ v = t^{-1}ut,\ t^{-1}v^{-1}uvt = c_1u^{-1}vu,\ t^{-1}v^{-2}uv^2t = c_2u^{-2}vu^2,\ t^{-1}v^{-3}uv^3t = c_3u^{-3}vu^3$$
$$t^{-1}v^{-4}uv^4t = c_4u^{-4}vu^4,\ t^{-1}v^{-5}uv^5t = c_5u^{-5}vu^5,\ t^{-1}v^{-6}uv^6t = c_6u^{-6}vu^6,\ t^{-1}v^{-7}uv^7t = c_7u^{-7}vu^7$$
$$t^{-1}v^{-8}uv^8t = c_8u^{-8}vu^8,\ t^{-1}v^{-9}uv^9t = c_9u^{-9}vu^9,\ t^{-1}v^{-10}uv^{10}t = c_{10}u^{-10}vu^{10}\rangle$$

where $J = C * \langle u, v\rangle$ is the free product of the group C and the free group generated by letters u and v.

By Lemma 2.1 of [33] we then have the following.

Proposition 2.1 *The word problem for the group defined by* Presentation B *is unsolvable.*

Now we apply Tietze transformations [43] as pointed in [20] to replace all the occurrences of v by $t^{-1}ut$ and replace all occurrences of c_i by

$$c_i = t^{-1}t^{-1}u^{-i}tut^{-1}u^ittu^{-i}t^{-1}u^{-1}tu^i, \qquad i = 1, 2, \cdots, 10$$

in the relations in Presentation B, and then eliminate all generators (by using Tieze transformations agian) c_i, $i = 1, 2, \cdots, 10$ and v to get a finite presentation with only two generators as follows.

Presentation C

Two generators: u, t

27 relations:

R_1: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^{10}t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu$
$= t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tut^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7$

R_2: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^{10}t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2$
$= t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7$

R_3: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^{10}t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$= t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7$

R_4: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^{10}t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4$
$= t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7$

R_5: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^{10}t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5$
$= t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7$

R_6: $t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu$
$= t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^{10}$

R_7: $t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2$
$= t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^{10}$

R_8: $t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$= t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^{10}$

R_9: $t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4$
$= t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^{10}$

R_{10}: $t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5$
$= t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^{10}$

R_{11}: $t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu$
$= t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tut^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$

R_{12}: $t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2$
$= t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$

R_{13}: $t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$= t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$

R_{14}: $t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4$
$= t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$

R_{15}: $t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5$
$= t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$

R_{16}: $t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7t^{-2}u^{-10}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}$
$= t^{-2}u^{-10}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7$

R_{17}: $t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-10}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}$
$= t^{-2}u^{-10}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8$

R_{18}: $(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^{-3}t^{-2}u^{-10}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^3$
$t^{-2}u^{-6}tut^{-1}u^6t^2u^{-6}t^{-1}u^{-1}tu^6$
$= t^{-2}u^{-6}tut^{-1}u^6t^2u^{-6}t^{-1}u^{-1}tu^6(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^{-3}t^{-2}u^{-10}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}$
$(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^3$

R_{19}: $t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tut^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tut^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8$

R_{20}: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^2t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tut^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^2t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^2t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4$
$t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^2$

R_{21}: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^3t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^3t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^3t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^3$

R_{22}: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^4t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^4t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^4t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4$
$t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^4$

R_{23}: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^5t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^5t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^5t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5$
$t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^5$

R_{24}: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^6t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^6t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^6t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5$
$t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^6$

R_{25}: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^7t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4$
$t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^7t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^7t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^7$

R_{26}: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^8t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^3$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^8t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^8(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^3$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^8$

R_{27}: $(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^9t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^3$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^9t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9$
$= t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^9(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^3$
$(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^9$

By removing a number of inverse pairs on the relations in the above presentation we then have the following presentation.

Presentation C′

Two generators: u, t

27 relations:

R'_1: $u^{-6}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^9t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}t$
$= tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tut^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^6$

R'_2: $u^{-5}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^9t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}t$
$= tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^5$

R'_3: $u^{-4}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^9t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}t$
$= tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^4$

R'_4: $u^{-3}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^9t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}t$
$= tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^3$

R'_5: $u^{-2}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7(t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7)^9t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}t$
$= tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^2$

R'_6: $u^{-7}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}t$
$= tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^9t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^7$

R'_7: $u^{-6}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}t$
$= tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^9t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^6$

R'_8: $u^{-5}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}t$
$= tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^9t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^5$

R'_9: $u^{-4}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}t$
$= tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^9t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^4$

R'_{10}: $u^{-3}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}t$
$= tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5(t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8)^9t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^3$

R'_{11}: $u^{-8}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}t$
$= tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tut^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^8$

R'_{12}: $u^{-7}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-2}tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}t$
$= tut^{-1}u^2t^2u^{-2}t^{-1}u^{-1}tu^2t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^7$

R'_{13}: $u^{-6}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}t$
$= tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^6$

R'_{14}: $u^{-5}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-4}tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}t$
$= tut^{-1}u^4t^2u^{-4}t^{-1}u^{-1}tu^4t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^5$

R'_{15}: $u^{-4}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^9t^{-2}u^{-5}tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}t$
$= tut^{-1}u^5t^2u^{-5}t^{-1}u^{-1}tu^5t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu^4$

R'_{16}: $tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7t^{-2}u^{-10}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^3$
$= u^{-3}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}t^{-2}u^{-7}tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}t$

R'_{17}: $tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-10}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^2$
$= u^{-2}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}t$

R'_{18}: $(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^{-2}u^{-1}t^{-1}utut^{-2}u^{-1}tu^{-1}t^{-1}u^{-9}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}$
$(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^3t^{-2}u^{-6}tut^{-1}u^6t^2u^{-6}t^{-1}u^{-1}tu^5$
$= t^{-2}u^{-6}tut^{-1}u^6t^2u^{-6}t^{-1}u^{-1}tu^5t^{-1}utut^{-2}u^{-1}tu^{-1}t^{-1}ut^2u^{-1}t^{-1}utut^{-2}u^{-1}tu^{-1}t^{-1}ut^2$
$u^{-1}t^{-1}utut^{-2}u^{-1}tu^{-1}t^{-1}u^{-9}tut^{-1}u^{10}t^2u^{-10}t^{-1}u^{-1}tu^{10}$
$(t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tu)^2t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}t$

R'_{19}: $tut^{-1}u^7t^2u^{-7}t^{-1}u^{-1}tu^7t^{-2}u^{-1}tut^{-1}ut^2u^{-1}t^{-1}u^{-1}tut^{-2}u^{-3}tut^{-1}u^3t^2u^{-3}t^{-1}u^{-1}tu^3$
$t^{-2}u^{-8}tut^{-1}u^8t^2u^{-8}t^{-1}u^{-1}tu^8t^{-2}u^{-9}tut^{-1}u^9t^2u^{-9}t^{-1}u^{-1}tu$

$$
\begin{aligned}
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}\\
&\quad t^{-2}u^{-1}tut^{-1}ut^{2}u^{-1}t^{-1}u^{-1}tut^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

$$
\begin{aligned}
R'_{20}:\quad & tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}t^{-2}u^{-1}tut^{-1}ut^{2}u^{-1}t^{-1}u^{-1}tu\\
& t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{2}t^{-2}u^{-9}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu\\
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{2}t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}\\
& t^{-2}u^{-1}tut^{-1}ut^{2}u^{-1}t^{-1}u^{-1}tut^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8}t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

$$
\begin{aligned}
R'_{21}:\quad & tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{2}t^{-2}u^{-2}tut^{-1}u^{2}t^{2}u^{-2}t^{-1}u^{-1}tu^{2}\\
& t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{3}t^{-2}u^{-9}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu\\
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{3}t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}\\
& t^{-2}u^{-2}tut^{-1}u^{2}t^{2}u^{-2}t^{-1}u^{-1}tu^{2}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{2}t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

$$
\begin{aligned}
R'_{22}:\quad & tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{3}t^{-2}u^{-2}tut^{-1}u^{2}t^{2}u^{-2}t^{-1}u^{-1}tu^{2}\\
& t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{4}t^{-2}u^{-9}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu\\
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{4}t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}\\
& t^{-2}u^{-2}tut^{-1}u^{2}t^{2}u^{-2}t^{-1}u^{-1}tu^{2}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{3}t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

$$
\begin{aligned}
R'_{23}:\quad & tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{4}t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}\\
& t^{-2}u^{-5}tut^{-1}u^{5}t^{2}u^{-5}t^{-1}u^{-1}tu^{5}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{5}t^{-2}u^{-9}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu\\
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{5}t^{-2}u^{-5}tut^{-1}u^{5}t^{2}u^{-5}t^{-1}u^{-1}tu^{5}\\
& t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}t^{-2}u^{-1}tut^{-1}ut^{2}u^{-1}t^{-1}u^{-1}tu\\
& (t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{4}t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

$$
\begin{aligned}
R'_{24}:\quad & tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{5}t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}\\
& t^{-2}u^{-5}tut^{-1}u^{5}t^{2}u^{-5}t^{-1}u^{-1}tu^{5}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{6}t^{-2}u^{-9}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu\\
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{6}t^{-2}u^{-5}tut^{-1}u^{5}t^{2}u^{-5}t^{-1}u^{-1}tu^{5}\\
& t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}t^{-2}u^{-2}tut^{-1}u^{2}t^{2}u^{-2}t^{-1}u^{-1}tu^{2}\\
& (t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{5}t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

$$
\begin{aligned}
R'_{25}:\quad & tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{6}t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}\\
& t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}\\
& (t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{7}t^{-2}u^{-9}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu\\
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{7}t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}\\
& t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}t^{-2}u^{-5}tut^{-1}u^{5}t^{2}u^{-5}t^{-1}u^{-1}tu^{5}\\
& (t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{6}t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

$$
\begin{aligned}
R'_{26}:\quad & tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{7}t^{-2}u^{-3}tut^{-1}u^{3}t^{2}u^{-3}t^{-1}u^{-1}tu^{3}\\
& (t^{-2}u^{-1}tut^{-1}ut^{2}u^{-1}t^{-1}u^{-1}tu)^{3}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{8}t^{-2}u^{-9}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu\\
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{8}(t^{-2}u^{-1}tut^{-1}ut^{2}u^{-1}t^{-1}u^{-1}tu)^{3}\\
& (t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{7}t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

$$
\begin{aligned}
R'_{27}:\quad & tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{8}t^{-2}u^{-4}tut^{-1}u^{4}t^{2}u^{-4}t^{-1}u^{-1}tu^{4}\\
& (t^{-2}u^{-1}tut^{-1}ut^{2}u^{-1}t^{-1}u^{-1}tu)^{3}(t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{9}t^{-2}u^{-9}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu\\
&= u^{-2}tut^{-1}u^{9}t^{2}u^{-9}t^{-1}u^{-1}tu^{9}(t^{-2}u^{-7}tut^{-1}u^{7}t^{2}u^{-7}t^{-1}u^{-1}tu^{7})^{9}(t^{-2}u^{-1}tut^{-1}ut^{2}u^{-1}t^{-1}u^{-1}tu)^{3}\\
& (t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}tu^{8})^{8}t^{-2}u^{-8}tut^{-1}u^{8}t^{2}u^{-8}t^{-1}u^{-1}t
\end{aligned}
$$

We denote by H the group defined by Presentation C$'$. Since H is isomorphic to the group defined by Presentation B [43], we have the following theorem.

Theorem 2.2 *The word problem for the group H defined by* Presentation C$'$ *is unsolvable.*

3 Presentations of Mihailova subgroups of $F_2 \times F_2$

Let H be a group defined by a presentation $\mathcal{P} = \langle x_1, x_2, \cdots, x_k | R_1, R_2, \cdots, R_m \rangle$ with integer $k \geq 2$, and let F_k be the free group on $\{x_1, x_2, \cdots, x_k\}$. Then, in her influent paper [32], Mihailova associated to H the *Mihailova subgroup* $M(H)$ of the direct product of $F_k \times F_k$ defined by

$$M(H) = \{(w_1, w_2) | w_1 = w_2 \text{ in } H\}$$

Mihailova then proved the following theorem.

Theorem 3.1 (Mihailova) *The membership problem for $M(H)$ in $F_k \times F_k$ is solvable if and only if the word problem for H is solvable.*

Thus, taking H the group defined by Presentation C$'$ generated by two elements, the Mihailova subgroup $M(H)$ of $F_2 \times F_2$ has a unsolvable membership problem, namely there is no algorithm to decide if any element x of $F_2 \times F_2$ written as a word on the generators of $F_2 \times F_2$ is an element of $M(H)$.

By a result of Grunewald's [18], if H enjoys a unsolvable word problem then the Mihailova subgroup $M(H)$ can not be finitely presented. However, Bogopolski and Venturawe [5] have gaven an explicit countable presentation with finite generators and countably infinite relators for Mihailova subgroup $M(H)$ of $F_k \times F_k$ $(k \geq 2)$ provided that the group H can be defined by a finite, concise and Peiffer aspherical presentation as the following theorem.

Theorem 3.2 (Bogopolski and Venturawe) *Let F_k be the free group on $\{x_1, \cdots, x_k\}$, and let $H = \langle x_1, \cdots, x_k | \, R_1, \cdots, R_m\rangle$ be a finite, concise and Peiffer aspherical presentation. Then Mihailova's group $M(H) \leq F_k \times F_k$ admits the following presentation*

$$\langle d_1, \cdots, d_k, t_1, \cdots, t_m | \, [t_j, \, d^{-1}t_i^{-1}r_i d], \, [t_i, \, \mathrm{root}(r_i)], \, 1 \leq i, j \leq m, \, d \in D_k\rangle$$

where D_k is the free group with basis $\{d_1, \cdots, d_k\}$, r_i denotes the word in D_k obtained from R_i by replacing each x_l to d_l $(1 \leq l \leq k)$, $\mathrm{root}(r_i)$ denotes the unique element $s_i \in D_k$ such that r_i is a positive power of s_i but s_i itself is not a proper power, and the elements d_i and t_j correspond, respectively, to the elements (x_i, x_i) and $(1, R_j)$ of $M(H)$ $(1 \leq i \leq k, \, 1 \leq j \leq m)$.

To apply the above theorem on Presentation C$'$ we must show that Presentation C$'$ is concise and Peiffer aspherical.

A group presentation $\mathcal{P} = \langle x_1, x_2, \cdots, x_k | R_1, R_2, \cdots, R_m\rangle$ is called concise if every relation R_i is non-trivial and reduced, and every two relators $R_i, R_j, i \neq j$, are not conjugate to each other, or to the inverse of each other. A direct check shows that Presentation C$'$ is concise.

One can refer [5] for the definition of being Peiffer aspherical. Theorems 3.1 and 4.2, and Lemma 5.1 in [10] imply that respectively, the Peiffer asphericity is preserved under HNN-extensions, under free products, and under Tietze transformations. Therefore, it is sufficient to show that Presentation C (as well as Presentation C$'$) can be obtained from a free group by performing a number of HNN-extensions, free products, and Tietze transformations.

First, Presentation A can be gained from a free group by three consecutive HNN-extensions as follows.

The first HNN-extension is performed by taking the free group A generated by c_7, c_8 as the associated subgroup, and $c_1, c_2, c_3, c_4, c_5, c_{10}$ as the stable letters to get an HNN-extension J_1 defined by the following presentation.

$$\begin{gathered}\mathcal{P}_1 = \langle A, \, c_1, \, c_2, \, c_3, \, c_4, \, c_5, \, c_{10} \, | \\ c_1^{-1}c_7^{10}c_1 = c_7, \, c_2^{-1}c_7^{10}c_2 = c_7, \, c_3^{-1}c_7^{10}c_3 = c_7, \, c_4^{-1}c_7^{10}c_4 = c_7, \, c_5^{-1}c_7^{10}c_5 = c_7, \, c_{10}^{-1}c_7c_{10} = c_7, \\ c_1^{-1}c_8c_1 = c_8^{10}, \, c_2^{-1}c_8c_2 = c_8^{10}, \, c_3^{-1}c_8c_3 = c_8^{10}, \, c_4^{-1}c_8c_4 = c_8^{10}, \, c_5^{-1}c_8c_5 = c_8^{10}, \, c_{10}^{-1}c_8c_{10} = c_8\rangle\end{gathered}$$

Then, by taking the subgroup K_1 of J_1 generated by the the following subset

$$\begin{gathered}\{c_1, \, c_2, \, c_3, \, c_4, \, c_5, \, c_7c_1c_3c_8, \, c_7c_3c_1c_8, \, c_7^2c_1c_4c_8^2, \, c_7^2c_4c_1c_8^2, \, c_7^3c_2c_3c_8^3, \, c_7^3c_3c_2c_8^3, \, c_7^4c_2c_4c_8^4, \, c_7^4c_4c_2c_8^4, \, c_7^5c_3c_5c_8^5, \\ c_7^5c_5c_3c_1c_8^5, \, c_7^6c_4c_5c_8^6, \, c_7^6c_5c_4c_2c_8^6, \, c_7^7c_3c_4c_3c_8^7, \, c_7^7c_3c_4c_3c_5c_8^7, \, c_7^8c_3c_1^3c_8^8, \, c_7^8c_1^3c_8^8, \, c_7^9c_4c_1^3c_8^9, \, c_7^9c_1^3c_8^9\}\end{gathered}$$

as the associated subgroup and c_9 as the stable letter we have the HNN-extension J_2 defined by the following presentation.

$$\begin{gathered}\mathcal{P}_2 = \langle J_1, c_9 \, | \, c_9^{-1}c_1c_9 = c_1, \, c_9^{-1}c_2c_9 = c_2, \, c_9^{-1}c_3c_9 = c_3, \, c_9^{-1}c_4c_9 = c_4, \, c_9^{-1}c_5c_9 = c_5, \\ c_9^{-1}c_7c_1c_3c_8c_9 = c_7c_3c_1c_8, \, c_9^{-1}c_7^2c_1c_4c_8^2c_9 = c_7^2c_4c_1c_8^2, \, c_9^{-1}c_7^3c_2c_3c_8^3c_9 = c_7^3c_3c_2c_8^3, \\ c_9^{-1}c_7^4c_2c_4c_8^4c_9 = c_7^4c_4c_2c_8^4, \, c_9^{-1}c_7^5c_3c_5c_8^5c_9 = c_7^5c_5c_3c_1c_8^5, \, c_9^{-1}c_7^6c_4c_5c_8^6c_9 = c_7^6c_5c_4c_2c_8^6, \\ c_9^{-1}c_7^7c_3c_4c_3c_8^7c_9 = c_7^7c_3c_4c_3c_5c_8^7, \, c_9^{-1}c_7^8c_3c_1^3c_8^8c_9 = c_7^8c_1^3c_8^8, \, c_9^{-1}c_7^9c_4c_1^3c_8^9c_9 = c_7^9c_1^3c_8^9\rangle\end{gathered}$$

The third one HNN-extension is then clearly performed by taking the subgroup K_2 of J_2 generated by the the element $c_1^{-3}c_{10}c_1^3$ as the associated subgroup and c_6 the stable letter to obtain the HNN-extension C defined by Presentation A.

Now, it is obvious that the group defined by Presentation B is also an HNN-extension by taking the subgroup J as the associated subgroup and t as the stble letter, where J is the free product of group C and the free group generated by two letters u and v.

Finally and clearly, we already have known that Presentation C (as well as Presentation C′) is obtained by performing a number of Tietze transformations from Presentation B. Thus, by the results in [10] we have the following theorem.

Theorem 3.3 *Presentation C and Presentation C′ are Peiffer aspherical, and Presentation C′ is concise.*

Since the group H defined by Presentation C′ is generated by two elements u, t, we now can apply Theorem 3.2 to present an explicit countable presentation for Mihailova subgroup $M_{F_2\times F_2}(H)$ of $F_2 \times F_2$ with F_2 generated by $\{u, t\}$. To do so we need some notations as follows.

For each $i = 1, 2, \cdots, 27$, if a relation R'_i in Presentation C′ is of the form

$$R'_i : R_i^{(l)}(u, t) = R_i^{(r)}(u, t)$$

with both $R_i^{(l)}(u, t)$ and $R_i^{(r)}(u, t)$ being words on $\{u, t, u^{-1}, t^{-1}\}$ then we denote

$$S_i = (R_i^{(r)}(u, t))^{-1} R_i^{(l)}(u, t)$$

Clearly, one can check that $\mathrm{root}(S_i) = S_i$, $i = 1, 2, \cdots, 27$. Thus, we then have

$$r_i = (R_i^{(r)}((u, u), (t, t)))^{-1} R_i^{(l)}((u, u), (t, t)), \quad i = 1, 2, \cdots, 27$$

where r_i is as defined as in the the presentation given in Theorem 3.2.

Finally, by Theorem 3.2 we then have an explicit countable presentation with 56 generators for Mihailova subgroup $M_{F_2\times F_2}(H)$ of $F_2 \times F_2$ as the following.

Presentation D

29 generators:

$$(u, u),\ (t, t),\ (1, S_i), \quad i = 1, 2, \cdots, 27$$

Countable number of relators:

$$S_i^{-1}(\delta^{-1}S_k^{-1}r_k^{-1}\delta)^{-1}S_i(\delta^{-1}S_k^{-1}r_k^{-1}\delta), \quad S_i^{-1}r_i^{-1}S_i r_i, \quad i, k = 1, 2, \cdots, 27$$

where $\delta \in F_2 \times F_2$.

Now, since the word problem of the group G defined by Presentation C is unsolvable, Mihailova's theorem (Theorem 3.1) implies the following conclusion.

Theorem 3.4 *The membership problem for Mihailova subgroup $M_{F_2\times F_2}(H)$ of $F_2 \times F_2$ is unsolvable.*

Finally, for being used with applications, we give the descriptions of each S_i's in the generators $(1, S_i)$, $i = 1, 2, \cdots, 27$ in Presentation D as follows where for the simplicity we replace all occurrences of (u, u) by δ_u and all occurrences of (t, t) by δ_t.

S_1: $(\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^6)^{-1}$
$\delta_u^{-6}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7)^9$
$\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_2: $(\delta_t\delta_u\delta_t^{-1}\delta_u^2\delta_t^2\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^2\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^5)^{-1}$
$\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7)^9$
$\delta_t^{-2}\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^2\delta_t^2\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_3: $(\delta_t\delta_u\delta_t^{-1}\delta_u^3\delta_t^2\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^3\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^4)^{-1}$
$\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7)^9$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^3\delta_t^2\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_4: $(\delta_t\delta_u\delta_t^{-1}\delta_u^4\delta_t^2\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^4\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^3)^{-1}$
$\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7)^9$
$\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^4\delta_t^2\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_5: $(\delta_t\delta_u\delta_t^{-1}\delta_u^5\delta_t^2\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^5\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^2)^{-1}$
$\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7)^9$
$\delta_t^{-2}\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^5\delta_t^2\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_6: $(\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8)^9$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7)^{-1}$
$\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_7: $(\delta_t\delta_u^2\delta_t^{-1}\delta_u^2\delta_t^2\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^2(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8)^9$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^6)^{-1}$
$\delta_u^{-6}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_8: $(\delta_t\delta_u^3\delta_t^{-1}\delta_u^3\delta_t^2\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^3(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8)^9$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^5)^{-1}$
$\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_9: $(\delta_t\delta_u^4\delta_t^{-1}\delta_u^4\delta_t^2\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8)^9$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^4)^{-1}$
$\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_{10}: $(\delta_t\delta_u^5\delta_t^{-1}\delta_u^5\delta_t^2\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8)^9$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^3)^{-1}$
$\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_{11}: $(\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8)^{-1}$
$\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^9\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_{12}: $(\delta_t\delta_u\delta_t^{-1}\delta_u^2\delta_t^2\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^2\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7)^{-1}$
$\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^9\delta_t^{-2}\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^2\delta_t^2\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_{13}: $(\delta_t\delta_u\delta_t^{-1}\delta_u^3\delta_t^2\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^3\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^6)^{-1}$
$\delta_u^{-6}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^9\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^3\delta_t^2\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_{14}: $(\delta_t\delta_u\delta_t^{-1}\delta_u^4\delta_t^2\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^4\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^5)^{-1}$
$\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^9\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^4\delta_t^2\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_{15}: $(\delta_t\delta_u\delta_t^{-1}\delta_u^5\delta_t^2\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^5\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^4)^{-1}$
$\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^9\delta_t^{-2}\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^5\delta_t^2\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t$

S_{16}: $(\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{10}\delta_t^2\delta_u^{-10}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{10}\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7\delta_t^{-2}\delta_u^{-10}\delta_t\delta_u\delta_t^{-1}\delta_u^{10}\delta_t^2\delta_u^{-10}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^3$

S_{17}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{10}\delta_t^2\delta_u^{-10}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{10}\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8\delta_t^{-2}\delta_u^{-10}\delta_t\delta_u\delta_t^{-1}\delta_u^{10}\delta_t^2\delta_u^{-10}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^2$

S_{18}: $(\delta_t^{-2}\delta_u^{-6}\delta_t\delta_u\delta_t^{-1}\delta_u^6\delta_t^2\delta_u^{-6}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^5\delta_t^{-1}\delta_u\delta_t\delta_u\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u^{-1}\delta_t^{-1}\delta_u\delta_t^2$
$\delta_u^{-1}\delta_t^{-1}\delta_u\delta_t\delta_u\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u^{-1}\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u\delta_t\delta_u\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u^{-1}\delta_t^{-1}\delta_u^{-9}\delta_t$
$\delta_u\delta_t^{-1}\delta_u^{10}\delta_t^2\delta_u^{-10}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{10}(\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u)^2$
$\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$(\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u)^{-2}\delta_u^{-1}\delta_t^{-1}\delta_u\delta_t\delta_u\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u^{-1}\delta_t^{-1}\delta_u^{-9}\delta_t$
$\delta_u\delta_t^{-1}\delta_u^{10}\delta_t^2\delta_u^{-10}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{10}(\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u)^3$
$\delta_t^{-2}\delta_u^{-6}\delta_t\delta_u\delta_t^{-1}\delta_u^6\delta_t^2\delta_u^{-6}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^5$

S_{19}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^9\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^3\delta_t^2\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^3\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^{2}\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8}$
$\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

S_{20}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{9}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{2}$
$\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^{4}\delta_t^{2}\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{4}\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^{2}\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8}\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}$
$\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^{2}\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^{4}\delta_t^{2}\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{4}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{2}\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

S_{21}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{9}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{3}$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}\delta_t^{-2}\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{2}\delta_t^{2}\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{2}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{2}\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{2}$
$\delta_t^{-2}\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{2}\delta_t^{2}\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{2}\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{3}\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

S_{22}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{9}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{4}$
$\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^{4}\delta_t^{2}\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{4}\delta_t^{-2}\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{2}\delta_t^{2}\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{2}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{3}\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{3}$
$\delta_t^{-2}\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{2}\delta_t^{2}\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{2}\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^{4}\delta_t^{2}\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{4}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{4}\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

S_{23}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{9}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{5}$
$\delta_t^{-2}\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^{5}\delta_t^{2}\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{5}\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}$
$\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^{2}\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{4}$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{4}$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}\delta_t^{-2}\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^{5}\delta_t^{2}\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{5}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{5}\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

S_{24}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{9}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{6}$
$\delta_t^{-2}\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^{5}\delta_t^{2}\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{5}\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^{4}\delta_t^{2}\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{4}$
$\delta_t^{-2}\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{2}\delta_t^{2}\delta_u^{-2}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{2}(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{5}$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{5}$
$\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^{4}\delta_t^{2}\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{4}\delta_t^{-2}\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^{5}\delta_t^{2}\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{5}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{6}\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

S_{25}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{9}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{7}$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^{4}\delta_t^{2}\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{4}$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}\delta_t^{-2}\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^{5}\delta_t^{2}\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{5}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{6}\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{6}$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^{4}\delta_t^{2}\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{4}$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}\delta_t^{-2}\delta_u^{-5}\delta_t\delta_u\delta_t^{-1}\delta_u^{5}\delta_t^{2}\delta_u^{-5}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{5}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{7}\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

S_{26}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{9}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{8}$
$(\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u^{2}\delta_t^{2}\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{2})^{3}(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{7}$
$\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}$
$\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{7}$
$\delta_t^{-2}\delta_u^{-3}\delta_t\delta_u\delta_t^{-1}\delta_u^{3}\delta_t^{2}\delta_u^{-3}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{3}(\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^{2}\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u)^{3}$
$(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^{8}\delta_t^{2}\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{8})^{8}\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u$

S_{27}: $(\delta_u^{-2}\delta_t\delta_u\delta_t^{-1}\delta_u^{9}\delta_t^{2}\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{9}(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^{7}\delta_t^{2}\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^{7})^{9}$

$$
\begin{aligned}
&(\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u^2\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^2)^3(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8)^8\\
&\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t)^{-1}\\
&\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7(\delta_t^{-2}\delta_u^{-7}\delta_t\delta_u\delta_t^{-1}\delta_u^7\delta_t^2\delta_u^{-7}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^7)^8\\
&\delta_t^{-2}\delta_u^{-4}\delta_t\delta_u\delta_t^{-1}\delta_u^4\delta_t^2\delta_u^{-4}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^4(\delta_t^{-2}\delta_u^{-1}\delta_t\delta_u\delta_t^{-1}\delta_u\delta_t^2\delta_u^{-1}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u)^3\\
&(\delta_t^{-2}\delta_u^{-8}\delta_t\delta_u\delta_t^{-1}\delta_u^8\delta_t^2\delta_u^{-8}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u^8)^9\delta_t^{-2}\delta_u^{-9}\delta_t\delta_u\delta_t^{-1}\delta_u^9\delta_t^2\delta_u^{-9}\delta_t^{-1}\delta_u^{-1}\delta_t\delta_u
\end{aligned}
$$

References

[1] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography. Math. Res. Lett. 6(1999), 287-291.

[2] I. Anshel, M. Anshel, B. FISHER, New key agreement protocols in braid group cryptography, in NACCACHE D. (ED.): Topics in CryptologyCCT-RSA, San Francisco, CA, USA, 8C12 April 2001, (LNCS, 2020), 13C27.

[3] I. Anshel, M. Anshel, D. Goldfeld, Non-abelian key agreement protocols, Discrete Appl. Math., 130(2003), 3C12.

[4] W. W. Boone, The word problem, Annals of Mathematics, 70(2)(1959), 207-265.

[5] O. Bogopolski, and E. Ventura, A recursive presentation for Mihailova's subgroup, Groups, Geometry, and Dynamics, 4(3)(2010), 407-417.

[6] V.V. Borisov, Simple examples of groups with unsolvable word problems, Math. Notes, 6(1969), 768-775 (Mat. Zametki, 6(1969), 521-532, in Russian).

[7] G.S. CIJTIN, An associative calculus with an insoluble problem of equivalence, Trudy Mat. Inst. Steklov, 52 (1957), 172-189.

[8] J. C. Cha, K.H. Ko, S. Lee, J.W. Han, J.H. Cheon, An efficient implementation of braid groups, in BOYD C. (ED.): Advances in Cryptology, ASIACRYPT 2001, Gold Coast, Australia, 9-13 December 2001, (LNCS, 2248), 144-156.

[9] J. H. Cheon and B. Jun, A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem, in BONEH D. (ED.): Advances in Cryptology-CRYPTO 2003, Santa Barbara, CA, USA, 17-21 August 2003, (LNCS, 2729), 212-225.

[10] M. Chiswell, D.J. Collins and J. Huebschmann, Aspherical group presentation, Math. Z., 178 (1981), 1-36.

[11] D. J. Collins, A simple presentation of a group with unsolvable word problem, Illnois J. Math., 30(2)(1986), 230-234.

[12] D. J. Collins, Relations among the squares of the generators of the braid group, Invent. Math., 117(1994), 525-530.

[13] P Dehornoy, Using shifted conjugacy in braid-based cryptography, Arxiv ePrint Archive, Report 0609091v1, http://arxiv.org/abs/cs/0609091.

[14] N. Franco and J. Gonzales-Meneses, Conjugacy problem for braid groups and Garside groups, J. Algebra, 266(2003), 112-132.

[15] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne, Probabilistic solutions of equations in the braid group, Advances in Applied Mathematics 35(2005), 323-334.

[16] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne, Length-based conjugacy search in the Braid group, Contemp. Math., Amer. Math. Soc. 418(2006), 75-87.

[17] V. Gebhardt, A new approach to the conjugacy problem in Garside groups, J. Algebra, 292(1)(2005), 282-302.

[18] F.J. Grunewald, On some groups which cannot be finitely presented, J. London Math. Soc., 17(2)(1978), 427-436.

[19] A. Groch, D. Hofheinz, R. Steinwandt, A practical attack on the root problem in braid groups, Contemp. Math., 418(2006), 121-132.

[20] G. Higman, B. H. Neumann and H. Neumann, Embedding theorems for groups, J. London Math. Sco., 24(1949), 247-254.

[21] D. Hofheinz, R. Steinwandt, A practical attack on some braid group based cryptographic primitives, in Public Key Cryptography, 6th International Workshop on Practice and Theory in Public Key Cryptography, in: PKC 2003 (Y. G. Desmedt, ed.), Lecture Notes Comp. Sc. 2567(2002), 187-198.

[22] J. Hughes, A linear algebraic attack on the AAFG1 braid group cryptosystem, in BATTEN L.M., SEBERRY J. (EDS.): Information Security and Privacy, 7th Australian Conf.-ACISP 2002, Melbourne, Australia, July 2002, (LNCS, 2384), 176-189.

[23] J. Hughes, A. Tannenbaum, Length-based attacks for certain group based encryption rewriting systems, Inst. for Mathematics and its applic. (Minneapolis MN) 2000, http://www.ima.umn.edu/preprints/apr2000/1696.pdf, or http://arxiv.org/abs/cs/0306032.

[24] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park, New public-key cryptosystem using braid groups, Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), 166-183, Lecture Notes in Comput. Sci. 1880, Springer, Berlin, 2000.

[25] K. H. Ko, D. H. Choi, M. S. Cho, J. W. Lee, A new signature scheme using conjugacy problem, Cryptology ePrint Archive, Report 2002/168, http://eprint.iacr.org/2002/168.

[26] A. G. Kallka, Representation attacks on the braid Diffie-Hellman public key encryption, Appl. Algebra Eng. Commun. Comput., 17(3-4)(2006), 257-266.

[27] S. La, A. Chaturvedi, Authentication schemes using braid groups, Arxiv ePrint Archive, Report 0507066v1, http://arxiv.org/abs/cs/0507066.

[28] S. J. Lee, E. Lee, Potential Weaknesses of the Commutator Key Agreement protocol Based on Braid Groups. In: Advances in cryptology-Eurocrypt 2002, 14-28 (Lecture Notes Comp. Sc., vol. 2332) Berlin Heidelberg New York Tokyo: Springer 2002.

[29] E. Lee, and J. H. Park, Cryptanalysis of the public-key encryption based on braid groups, in BIHAM E. (ED.): Advances in Cryptology, EUROCRYPT 2003, Warsaw, Poland, 4-8 May 2003, (LNCS, 2656), 477-490.

[30] J. Longrigg and A. Ushakov, Cryptanalysis of shifted conjugacy authentication protocol, Arxiv ePrint Archive, Report 0708.1768, http://arxiv.org/abs/0708n1768

[31] S. Maffre, A Weak Key Test for Braid Based Cryptography, Designs, Codes and Cryptography, 39(3)(2006), 347-373.

[32] K. A. Mihailova, *The occurence problem for direct products of groups*, Dokl. Akad, Nauk SSSR 119,1958,1103-1105.Mat. Sb. (N.S.), 70(112:2)(1966), 241C251.

[33] C. F. Miller III, Decision problems for groups: survey and reflections, in Algorithms and Classification in Combinatorial Group Theory (eds. G Baumslag and C. F. Miller III), MSRI Publications, Springer-Verlag, 23(1992), 1-59.

[34] A. D. Myasnikov, A. Ushakov, Length based attack in braid groups, in PKC 2007, Lecture Notes in Computer Science, 4450(2007), 76-88.

[35] P. S. Novikov, On the algorithmic unsolvability of the word problem in group theory, Trudy Mat. Ins. Steklov, 44(1955), 143 pages, Translation in Amer. math. Soc. Transl, 9(2)(1958), 1-122.

[36] D. Ruinskiy, A. Shamir, B. Tsaban, Cryptanalysis of group-based key agreement protocols using subgroup distance functions, in PKC 2007, Lecture Notes Comp. Sc., 4450(2007), 61-75.

[37] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput., , 26:5(1997): 1484-1509

[38] V. Shpilrain, A. Ushakov, An authentication scheme based on the twisted conjugacy problem,Proceeding ACNS'08 Proceedings of the 6th international conference on Applied cryptography and network security, Springer-Verlag, 2008, 366-372.

[39] V. Shiplrain, A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient, Appl. Alg. in Eng., Communi. and Comp., 17(3-4)(2006), 285-289.

[40] V. Shpilrain and G. Zapata, Combinatorial group theory and public key cryptography, Appl. Algebra Engrg. Comm. Comput. 17(2006), 291-302.

[41] V. Shpilrain and G. Zapata, Using the subgroup membership search problem in public key cryptography, Con- temp. Math., Amer. Math. Soc., 418(2006), 169-179.

[42] H. Sibert, P. Dehornoy, M. Girault, Entity authentication schemes using braid word reduction, Discrete Applied Math. 154(2)(2006), 420-436.

[43] H. Tietze, $\ddot{U}$ber die topologischen invarianten mehrdimensionaler mannigfaltigkeiten, Monatsh, Math. Phys., 19(1908), 1-118.

[44] B. Tsaban, On an authentication scheme based on the root problem in the braid group, lanl.arXiv.org ePrint Archive, September 2005, Online available at http://arxiv.org/ps/cs.CR/0509059.

[45] B.C. Wang, Y.-P. Hu, Signature scheme based on the root extraction problem over braid groups, IET Inf. Secur., 3(2)(2009), 53C59.

Xiaofeng Wang
School of Mathematics and Computational Science
Shenzhen University
Shenzhen City 518060, China wangxf@szu.edu.cn

Guo Li
School of Mathematics and Computational Science
Shenzhen University
Shenzhen City 518060, China guoli@szu.edu.cn