A COUNTABLE FAMILY OF FINITELY PRESENTED INFINITE CONGRUENCE-FREE MONOIDS

FATMA AL-KHAROUSI, ALAN J. CAIN, VICTOR MALTCEV, AND ABDULLAHI UMAR

Abstract. We prove that the monoids

$$\mathrm{Mon}\langle a, b, c, d : a^n b = 0, ac = 1, db = 1, dc = 1$$
$$dab = 1, da^2 b = 1, \ldots, da^{n-1} b = 1\rangle$$

are congruence-free for all $n \geq 1$. This provides a new countable family of finitely presented congruence-free monoids, bringing us one step closer to understanding the monoid version of the Boone–Higman Conjecture. We also provide examples showing that finitely presented congruence-free monoids may have quadratic Dehn function.

1. Introduction and Main Result

It is a classical theorem of Rabin (see [11]) that every countable group embeds in a finitely generated simple group. Taking a deeper look at this question, Boone and Higman proved in [7] (see also [11]) that a finitely generated group has soluble word problem if and only if it embeds in a simple subgroup of a finitely presented group. This motivated them to raise the question, which is now still an open problem, referred to as the Boone–Higman Conjecture:

Open Problem 1. Does every group with soluble word problem embed in a finitely presented simple group?

Note that the condition of having soluble word problem is crucial, since every finitely presented simple group necessarily has soluble word problem. There are plenty of results regarding finitely presented simple groups, out of which we will mention only the result of Röver [14] that Grigorchuk groups embed in finitely presented simple groups, and a result of Scott [15] that there is a finitely presented simple group with insoluble conjugacy problem. Both results of Röver and Scott rely on the infinite family of finitely presented simple groups found by Higman [9].

Strangely, the analogous questions for semigroups have not been studied so extensively. The natural counterpart of simplicity to consider in semigroup theory is *congruence-freeness*: recall that a semigroup S is congruence-free if it has only two congruences — the identity relation and the relation $S \times S$. First of all, the analogue of Rabin's Theorem does hold, as was shown by Byleen in [8]. Secondly, in a series of papers by Birget [1, 2, 3, 4, 5], it was developed and studied the analogue of Higman's countable family.

Recent work by the third author has exhibited a countable family of finitely presented bisimple $\mathcal{H}$-trivial congruence-free monoids [13], and proved that every finite

2010 *Mathematics Subject Classification.* 20M05 (Primary) 20M10 (Secondary).

Key words and phrases. Boone-Higman Conjecture, congruence-free, finitely presented, rewriting systems.

semigroup embeds in a finitely presented congruence-free monoid [12]. These two papers contained the only known examples of finitely presented infinite congruence-free monoids that are not groups.

The main goal of this note is to further expand the class of known examples of finitely presented infinite congruence-free non-group monoids by proving the following result:

Main Result. *The monoids*

$$M_n = \mathrm{Mon}\langle a, b, c, d : a^n b = 0, ac = 1, db = 1, dc = 1 \\ dab = 1, da^2 b = 1, \ldots, da^{n-1} b = 1\rangle$$

are congruence-free for all $n \geq 1$.

(Strictly, the monoid M_n are defined by presentations within the category of monoids-with-zero. However, these can be converted to standard monoid presentations by adding 0 as a generator and adding defining relations $0x = 0$ and $x0 = 0$ for all $x \in \{a, b, c, d, 0\}$. The resulting presentations are clearly still finite.)

We obtained this family while trying to embed monoids $\mathrm{Mon}\langle a, b : a^n b = 0\rangle$ in finitely presented congruence-free monoids. If one increases the exponent of b by 1, the question of embedding seems to become much harder, and we have been unable to resolve it even for the monoid $\mathrm{Mon}\langle a, b : a^2 b^2 = 0\rangle$. Thus we ask the following questions:

Open Problem 2. Does the monoid $\mathrm{Mon}\langle a, b : a^2 b^2 = 0\rangle$ embed in a finitely presented congruence-free monoid? If 'yes', can one write an explicit presentation for the monoid containing $\mathrm{Mon}\langle a, b : a^2 b^2 = 0\rangle$?

Before we embark on the proof of our theorem, we provide all the ingredients required for the proof.

2. Preliminaries

We will require some information from both semigroup theory and computer science.

The correspondence between normal groups and homomorphisms in group theory is paralleled by the correspondence between congruences and homomorphisms in semigroup theory. For a semigroup S, a binary relation $\rho \subseteq S \times S$ is called a *congruence* if it is an equivalence relation and compatible with multiplication on the left and right: that is, if $x \,\rho\, y$ for some $x, y \in S$, then $zx \,\rho\, zy$ and $xz \,\rho\, yz$ for all $z \in S$. The equivalence classes of S with respect to a congruence ρ on it, form a factor-semigroup denoted by S/ρ. A subset $I \subseteq S$ is called an *ideal* of a semigroup S, if $IS \cup SI \subseteq I$. With every ideal $I \subseteq S$ there is associated the so-called *Rees congruence* $\rho_I = (I \times I) \cup \Delta$, where Δ is the identity relation on S. A semigroup is called *simple* if it has only one ideal, namely the whole semigroup itself. A semigroup S with zero 0 is called 0-*simple* if it has only two ideals, namely the whole semigroup and $\{0\}$. Because of the Rees congruences, one easily sees that every congruence-free semigroup is either simple or 0-simple. For further background on semigroups, see [10].

A *rewriting system* (A, R) comprises a finite alphabet A and a subset $R \subseteq A^* \times A^*$, where A^* stands for the free monoid over A. Every pair (l, r) from R is called a *rule* and normally is written as $l \to r$. For $x, y \in A^*$ we write $x \to y$, if

there exist $\alpha, \beta \in A^*$ and a rule $l \to r$ from R such that $x = \alpha l \beta$ and $y = \alpha r \beta$. Denote by $\to^*$ the transitive reflexive closure of $\to$. A rewriting system (A, R) is:

- *confluent* if for every words $w, x, y \in A^*$ such that $w \to^* x$ and $w \to^* y$, there exists $W \in A^*$ such that $x \to^* W$ and $y \to^* W$;
- *terminating* if every infinite derivation $x_0 \to x_1 \to x_2 \to \cdots$ stabilises.

Confluent terminating systems, which are also called *complete systems*, give a very convenient way of working with finitely generated monoids: if a monoid is presented by $M = \mathrm{Mon}\langle A : l_i = r_i \quad i \in I\rangle$ and it turns that the system $S = (A, \{l_i \to r_i\}_{i \in I})$ is complete, then the elements of M are in bijection with the *normal forms* for S, i.e. those words from A^* which omit the subwords l_i, and for a word $w \in A^*$ to find its normal form with respect to S, we just need to apply $\to$ successively to w as many times as we can (this process must stop by the termination condition) and the result will always be the same word depending only on w. See [6] for more details on rewriting systems.

Our final notation to fix is as follows: if A is a finite generating set for a semigroup S and u and v are words over A, then by $u \equiv v$ we will mean that u and v coincide literally; and by $u = v$ we will mean that u and v represent the same element of the semigroup S.

3. Proof of the Main Result

One easily sees that the presentation for M_n considered as the corresponding rewriting system is complete. Thus we can use the normal forms for M_n with respect to this complete system. Note that if a word in the normal form contains d, then all the letters following this distinguished d are only a's and d's. We will use this fact quite frequently in the proof.

Let us start collecting some information about M_n:

Lemma 3. *M_n is 0-simple.*

Proof. To prove the lemma, it suffices to show that if w is a non-zero word over $\{a, b, c, d\}^*$ in its normal form, then $M_n w M_n = M_n$. We will prove it by induction on the length $|w|$ of w. The base case $|w| = 0$, i.e. $w = 1$, is trivial. Now let us do the transition $(< |w|) \mapsto |w|$.

Let us first assume that w contains letters d. We can take the last letter d, after which by the above remark there can follow only letters a. Hence w is representable as $w \equiv w' d a^k$ for some $k \geq 0$. Then $w c^k a b = w' d a b = w'$ and we may apply induction.

So, let now $w \in \{a, b, c\}^*$. If w starts with b or c, then by premultiplying w with d, we can cancel out that corresponding b or c, and then use induction. So, we may assume that w starts with a. If w is a power of a, then by the relation $ac = 1$ we immediately get $M_n = M_n w M_n$. So, again because of the relation $ac = 1$, we may assume that $w \equiv a^k b w'$ for some $k \geq 1$. Because of the relation $a^n b = 0$, we see that $k < n$. But then $d a^k b = 1$ and so $dw = w'$ and we are done by induction. □

In order to prove that M_n is congruence-free, we proceed by induction on $|u| + |v|$ proving that if ρ is a congruence on M_n and $u \,\rho\, v$ for some distinct normal form words u and v over $\{a, b, c, d\}$, then $\rho = M_n \times M_n$.

Let us first check the base case – without loss we may assume that $|u| = 0$ and $|v| = 1$. Then we have that $u = 1$ and $v \in \{a, b, c, d, 0\}$. Having $1 \,\rho\, 0$ immediately

implies $\rho = M_n \times M_n$. If $1 \,\rho\, a$, then $a^{n-1}b \,\rho\, a^n b = 0$ and so $0 \,\rho\, da^{n-1}b = 1$. If $1 \,\rho\, b$ or $1 \,\rho\, c$, then $1 = db = dc \,\rho\, d$ and so $ab \,\rho\, dab = 1$, implying $0 = a^n b \,\rho\, a^{n-1}$, which yields $0 \,\rho\, a^{n-1}c^{n-1} = 1$. So, in any of the cases we obtain $1 \,\rho\, 0$ and so the base case holds.

Now we do the step $(< |u| + |v|) \mapsto (|u| + |v|)$.

Let us first sort out the case when both u and v contain d, i.e. $u \equiv Uda^p$ and $v \equiv Vda^q$ for some $p, q \geq 0$. If $p = q$, then $U \not\equiv V$ and $U = Uda^p c^{p+1} \,\rho\, Vda^q c^{q+1} = V$ and we may use induction. So, let, say, $p > q$. Then $Uda^{p-q} \,\rho\, Vd$ and so $0 = Uda^{(p-q)+n-1}b \,\rho\, Vda^{n-1}b = V$, hence we may use 0-simplicity to conclude that $0 \,\rho\, 1$ and consequently $\rho = M_n \times M_n$.

Now let us deal with the case when only one of u and v contains d: say $u \equiv Uda^p$ and $v \in \{a, b, c\}^*$ for some $p \geq 0$. Then $Ud = uc^p \,\rho\, vc^p \in \{a, b, c\}^*$. Let v' be the normal form for vc^p. If v' has a as the last letter, then $U = Uda^{n-1}b \,\rho\, v'a^{n-1}b = 0$ and we may use 0-simplicity. So, we may assume that v' does not end with a. Since vc^p does not contain d's and rewriting does not introduce letters d, and in normal forms c cannot follow a, one sees now that if v' contains a's, then each such letter a in v' is a part of a subword $a^k b$ with $1 \leq k \leq n-1$. Using this fact and the relations $dc = 1$ and $da^k b = 1$ for all $1 \leq k \leq n-1$, there exists an appropriate $m \geq 0$ such that $d^m v' = 1$. Then $d^m Ud \,\rho\, 1$. In particular, recalling that $db = 1$, d is invertible in M_n/ρ, and so ab is invertible in M_n/ρ, which yields from $a^n b = 0$ that $a^n = 0$ in M_n/ρ. Then $1 = a^n c^n = 0$ in M_n/ρ and so $\rho = M_n \times M_n$.

So, from now on we may assume that $u, v \in \{a, b, c\}^*$.

Let us first deal with the case when one of u and v is empty, say $v \equiv 1$. Then $u \not\equiv 1$. If u starts with b or c, then, since we already know from the presentation that b and c are left invertible in M_n, respectively b or c is invertible in M_n/ρ, and then d is invertible in M_n/ρ, yielding $1 = 0$ in M_n/ρ as above. So assume, $u \equiv a^k U$, $k \geq 1$ and such that either $U \equiv 1$ or U starts with b. If $U \equiv 1$, then a is invertible in M_n/ρ, which yields $b = 0$ in M_n/ρ and so $1 = db = 0$ in M_n/ρ. So let $U \not\equiv 1$. Then $0 = a^{n-1}u \,\rho\, a^{n-1}$ and so $1 = a^{n-1}c^{n-1} = 0$ in M_n/ρ.

Let now $u \not\equiv 1$ and $v \not\equiv 1$. Assume first that at least one of u and v starts with a, say, $u \equiv a^k U$ for some $k \geq 1$. We may also assume that k is a maximal possible number with $u \equiv a^k U$. Then either $U \equiv 1$, or U starts with b.

- $U \equiv 1$. Then $va^{n-1}b \,\rho\, a^{k+n-1}b = 0$. If $va^{n-1}b \neq 0$, we may use 0-simplicity. If $va^{n-1}b = 0$, then v must end with a. But then $v \equiv Va$ and so $a^{k-1} = uc \,\rho\, vc = V$ and since $a^{k-1} \not\equiv V$, we may use induction.
- $U \equiv bU_1$ for some $U_1 \in \{a, b, c\}^*$. Then $k \leq n-1$ and $u \equiv a^k bU_1 \,\rho\, v$. Then $a^{n-k}v \,\rho\, 0$. Again, if $a^{n-k}v \neq 0$, then we may use 0-simplicity. If $a^{n-k}v = 0$, then v must start with $a^k b$: $v \equiv a^k bV$ and then $U_1 = du \,\rho\, dv = V$ and again since $U_1 \not\equiv V$, we may use induction.

Finally, let neither of u and v start with a. If u and v start with the same letter x (which will be either b or c) and $u \equiv xU$ and $v \equiv xV$, then $U \not\equiv V$ and $U = du \,\rho\, dv = V$ and we may use induction. So, without loss we will assume that $u \equiv bU$ and $v \equiv cV$. Then $U = dbU \,\rho\, dcV = V$, so we may assume that $U \equiv V$ (otherwise use induction). But also $U = dabU \,\rho\, dacV = dV = dU$. We have that $U \neq dU$ and $|U| + |dU| \leq 2|U| + 1 < 2|U| + 2 = |u| + |v|$, and thus may use induction.

4. Dehn function

All the so currently known examples of finitely presented congruence-free monoids – from the Main Result, and from [13] and [12] – admit finite complete length-decreasing rewriting systems, and thus have linear Dehn functions. The following example shows that finitely presented congruence-free monoid may have quadratic Dehn function.

Example 4. The monoid M presented by the finite complete system

$$\begin{aligned} ab &\to ba \\ cbad &\to 1 \\ cb^2 &\to 1 \\ a^2d &\to 1 \\ cad &\to 0 \\ cbd &\to 0 \\ cd &\to 1 \end{aligned}$$

is congruence-free and has quadratic Dehn function.

Proof. That the monoid has quadratic Dehn function is immediate on noting that only the first rewriting rule can be applied to words that contain only symbols a and b, and that rewriting a^nb^n to its b^na^n requires n^2 applications to move each of the n symbols a to the right of each of the n symbols b.

Furthermore, it is routine to check that M is 0-simple.

We proceed by induction on $|u|+|v|$ proving that if u and v are in their normal forms and $u\,\rho\,v$ for some congruence ρ on M, then $\rho = M \times M$. The base case is obvious. Now we do the step $(< |u|+|v|) \mapsto (|u|+|v|)$.

First deal with the case when both u and v contain c. Then u and v decompose as $u \equiv Ucb^pa^q$ and $v \equiv Vcb^ra^s$ where $p,q,r,s \geq 0$. Since a is right cancellative, we may assume that either $q = 0$ or $s = 0$. Without loss we will assume that $s = 0$, i.e. $v \equiv Vcb^r$.

First we consider the case when $q = 0$. If $p = r$, then since $p, r \in \{0,1\}$, by $cd = 1$ and $cbad = 1$, we may use induction. If $p = 1$ and $r = 0$, i.e. $Ucb\,\rho\,Vc$ and so $U = Ucbad\,\rho\,Vcad = 0$ and we may use 0-simplicity. The case when $p = 0$ and $r = 1$ is dealt similarly.

Thus we may assume that $q > 0$. To recall: $Ucb^pa^q\,\rho\,Vcb^r$. We will go through four cases depending whether p and r are 0 or 1:

- $p = r = 0$: $Uca^q\rho Vc$. If $q = 1$, then $Uca\rho Vc$ and so $0 = Ucad\rho Vcd = V$ and we may use 0-simplicity. So, we may assume that $q \geq 2$. Then $Uca^{q-2} = Uca^qd\,\rho\,Vcd = V$ and so we may assume that $V \equiv Uca^{q-2}$. Thus, initially we had $Uca^q\,\rho\,Uca^{q-2}c$. Then $Ua^q = Uca^qb^2\,\rho\,Uca^{q-2}cb^2 = Uca^{q-2}$ and now we may use induction.
- $p = 0$ and $r = 1$: $Uca^q\,\rho\,Vcb$. Then $Ucba^q\,\rho\,V$ and so we may assume that $V \equiv Ucba^q$. Thus initially we had $Uca^q\,\rho Ucba^qcb$, and postmultiplying this with ad, we obtain $Uca^{q-1}\,\rho\,Ucba^q$ and so $Uc\,\rho\,Ucba$ and now we may use induction.
- $p = 1$ and $r = 0$: $Ucba^q\,\rho\,Vc$. Then $Ucba^{q-1} = Ucba^q \cdot ad\,\rho\,Vcad = 0$ and we may use 0-simplicity.

- $p = r = 1$: $Ucba^q \,\rho\, Vcb$. Then $0 \neq Ucba^q d \,\rho\, Vcbd = 0$ and we may use 0-simplicity.

Thus, from now on we may assume that u and v do not both contain c's. Let us deal with the case when one of u and v contain c's. Say, $u \equiv Ucb^p a^q$ and $v \in \{a, b, d\}^*$. Then $Ucb^p = u(ad)^q \,\rho\, v(ad)^q$. Recall that $p \in \{0, 1\}$. Now we have $0 = Ucbd \,\rho\, v(ad)^q b^{1-p} d \neq 0$ and we may use 0-simplicity.

Therefore, we may assume that none of u and v contains c. By symmetry, we may assume that none of u and v contains d. Since $ab = ba$ and a is right cancellative, and b is left cancellative, essentially we are left to deal with two cases:

- $u = b^p$ and $v = a^q$. Without loss we will assume that $q > 0$. Now, $b^{2p} \,\rho\, a^{2q}$ and so $1 \rho c^p a^{2q}$. This means that a is invertible in M/ρ, and so d is invertible in M/ρ. Thus from $cad = 0$, we have that $c = 0$ in M/ρ and so $0 = cb^2 = 1$ in M/ρ.
- $u = b^p a^q$ and $v = 1$. Again without loss we may assume that $q > 0$, hence a is invertible in M/ρ, and as in the previous case we deduce that $0 = 1$ in M/ρ.

□

Open Problem 5. Characterise the Dehn functions of finitely presented congruence-free monoids.

5. Concluding remarks

All the examples of finitely presented congruence-free monoids we have met so far – from this paper and from [13] and [12] – are not only simple or 0-simple, but in fact bisimple or 0-bisimple. We have not managed to find an example of a finitely presented congruence-free but not bisimple monoid and so finish the paper with the following question:

Open Problem 6. Does there exist a finitely presented congruence-free non-bisimple monoid?

Acknowledgements

During the research that led to the this paper, the first author was supported by an FCT Investigador advanced fellowship (IF/01622/2013/CP1161/CT0001). This work was partially supported by FCT through the project UID/MAT/00297/2013 (Centro de Matemática e Aplicações). Some of this research took place during a visit of the first author to Sultan Qaboos University, and we would like to thank SQU for its hospitality.

References

[1] J. C. Birget. Monoid generalizations of the Richard Thompson groups. *J. Pure Appl. Algebra*, 213(2):264–278, 2009.
[2] J. C. Birget. The $\mathcal{R}$- and $\mathcal{L}$-orders of the Thompson-Higman monoid $M_{k,1}$ and their complexity. *Internat. J. Algebra Comput.*, 20(4):489–524, 2010.
[3] J. C. Birget. Bernoulli measure on strings, and Thompson-Higman monoids. *Semigroup Forum*, 83(1):1–32, 2011.
[4] J. C. Birget. Monoids that map onto the Thompson-Higman groups. *Semigroup Forum*, 83(1):33–51, 2011.
[5] J. C. Birget. The Thompson-Higman monoids $M_{k,i}$: the $\mathcal{J}$-order, the $\mathcal{D}$-relation, and their complexity. *Internat. J. Algebra Comput.*, 21(1-2):1–34, 2011.

[6] R. V. Book and F. Otto. *String-Rewriting Systems*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993.
[7] W. W. Boone and G. Higman. An algebraic characterization of groups with soluble word problem. *J. Austral. Math. Soc.*, 18:41–53, 1974. Collection of articles dedicated to the memory of Hanna Neumann, IX.
[8] K. Byleen. Embedding any countable semigroup in a 2-generated congruence-free semigroup. *Semigroup Forum*, 41(2):145–153, 1990.
[9] G. Higman. *Finitely presented infinite simple groups*. Department of Pure Mathematics, Department of Mathematics, I.A.S. Australian National University, Canberra, 1974. Notes on Pure Mathematics, No. 8 (1974).
[10] J. M. Howie. *Fundamentals of Semigroup Theory*, volume 12 of *London Mathematical Society Monographs* (New Series). Clarendon Press, Oxford University Press, New York, 1995.
[11] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory*, volume 89 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 1977.
[12] V. Maltcev. Finite semigroups embed in finitely presented congruence-free monoids. *J. Algebra*, 389:1–5, 2013.
[13] V. Maltcev. A countable series of bisimple $\mathcal{H}$-trivial finitely presented congruence-free monoids. *Semigroup Forum*, 88(1):279–285, 2014.
[14] C. E. Röver. Constructing finitely presented simple groups that contain Grigorchuk groups. *J. Algebra*, 220(1):284–313, 1999.
[15] E. A. Scott. A finitely presented simple group with unsolvable conjugacy problem. *J. Algebra*, 90(2):333–353, 1984.

Department of Mathematics and Statistics, Sultan Qaboos University, Al-Khodh 123, Muscat, Sultanate of Oman
E-mail address: fatma9@squ.edu.om

Centro de Matemática e Aplicações, Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, 2829–516 Caparica, Portugal
E-mail address: a.cain@fct.unl.pt

Department of Mathematics and Statistics, Sultan Qaboos University, Al-Khodh 123, Muscat, Sultanate of Oman
E-mail address: victor.maltcev@gmail.com

Department of Mathematics, Petroleum Institute, Abu Dhabi, U.A.E.
E-mail address: aumar@pi.ac.ae