ISRAEL JOURNAL OF MATHEMATICS **TBD** (XXXX), 1–8
DOI: 10.1007/s000000000000000000000000

CORRIGENDUM TO "AUTOMATON SEMIGROUPS AND GROUPS: ON THE UNDECIDABILITY OF PROBLEMS RELATED TO FREENESS AND FINITENESS"

BY

DANIELE D'ANGELI*

Università degli Studi Niccolò Cusano
Via Don Carlo Gnocchi, 3, 00166 Roma, Italy
e-mail: dangeli@math.tugraz.at

AND

EMANUELE RODARO**

Department of Mathematics, Politecnico di Milano
Piazza Leonardo da Vinci 32, 20133 Milano, Italy
e-mail: emanuele.rodaro@polimi.it

AND

JAN PHILIPP WÄCHTER

Institut für Formale Methoden der Informatik (FMI), Universität Stuttgart
Universitätsstraße 38, 70569 Stuttgart, Germany
e-mail: jan-philipp.waechter@fmi.uni-stuttgart.de

The last part of Lemma 3.5[1] about the generated group is stated incorrectly. Independently from that, the argumentation below Corollary 3.8 is flawed. This affects Proposition 3.9, Theorem 3.12, Corollary 3.13 and Corollary 3.14. In particular, the question whether the freeness problem for automaton semigroups is decidable remains open.

* The first author was supported by the Austrian Science Fund project FWF P24028-N18 and FWF P29355-N35.

** The second author thanks the project INDAM-GNSAGA.

Received April 13, 2020 and in revised form July 23, 2020

1 All numeral references refer to the corresponding results of [1].

We first recall Lemma 3.5 for the definition of $\mathcal{T}_{\mathcal{M}}$.

LEMMA 3.5: *Let $\mathcal{M}$ be a finite set of $\mathbb{Z}^{d\times d}$ matrices. Furthermore, for every $M \in \mathcal{M}$, let V_M be the finite set of vectors $\boldsymbol{v} \in \mathbb{Z}^d$ such that all components of $\boldsymbol{v}$ are between $-\|M\|$ and $\|M\| - 1$. Here, $\|M\|$ denotes the norm*

$$\|M\| = \max_{1\leq i\leq d} \sum_{j=1}^{d} |m_{i,j}|$$

where $m_{i,j}$ is the entry in the i^{th} row and j^{th} column of M.

Then, one can compute a complete S-automaton $\mathcal{T}_{\mathcal{M}}$ with state set

$$Q_{\mathcal{M}} = \{m_{M,\boldsymbol{v}} \mid M \in \mathcal{M}, \boldsymbol{v} \in V_M\}$$

such that the homomorphism $\varphi : \mathscr{S}(\mathcal{T}_{\mathcal{M}}) \to \mathrm{SAff}_d(\mathbb{Z})$ induced by

$$\varphi(m_{M,\boldsymbol{v}}) = M_{\boldsymbol{v}}$$

for $M \in \mathcal{M}$ and $\boldsymbol{v} \in V_M$ is a well-defined isomorphism from $\mathscr{S}(\mathcal{T}_{\mathcal{M}})$ into the subsemigroup of $\mathrm{SAff}_d(\mathbb{Z})$ generated by $\{M_{\boldsymbol{v}} \mid M \in \mathcal{M}, \boldsymbol{v} \in V_M\}$.

If all matrices in $\mathcal{M}$ are invertible, then $\mathcal{T}_{\mathcal{M}}$ is inverse-deterministic and φ extends to a well-defined isomorphism from $\mathscr{G}(\mathcal{T})$ into the subgroup of $\mathrm{Aff}_d(\mathbb{Z})$ generated by $\{M_{\boldsymbol{v}} \mid M \in \mathcal{M}, \boldsymbol{v} \in V_M\}$.

The last part of Lemma 3.5 states that the group generated by the automaton $\mathcal{T}_{\mathcal{M}}$ is isomorphic to a subgroup of $\mathrm{Aff}_d(\mathbb{Z})$. However, in general, the inverse over $\mathbb{Z}_n$ of a matrix with entries from $\mathbb{Z}$ is not from $\mathbb{Z}^{d\times d}$. In fact, this only holds for matrices with determinant -1 or 1. Thus, the group generated by $\mathcal{T}_{\mathcal{M}}$ is only isomorphic to a subgroup of $\mathrm{Aff}_d(\mathbb{Z}_n)$.

THE GROUP CASE. Generally, the problem is that not every relation in $\mathcal{T}_{\mathcal{M}}$ yields a relation in the linear (semi)group generated by some finite set of matrices $\mathcal{M}$ (where $\mathcal{T}_{\mathcal{M}}$ is the automaton from Lemma 3.5). A relation of the form

$$m_{M_\ell,\boldsymbol{v}_\ell} \cdots m_{M_1,\boldsymbol{v}_1} \circ = m_{M_\ell,\boldsymbol{v}'_\ell} \cdots m_{M_1,\boldsymbol{v}'_1} \circ$$

with $\ell \geq 1$, $M_1, \ldots, M_\ell \in \mathcal{M}$ and $\boldsymbol{v}_i, \boldsymbol{v}'_i \in V_{M_i}$ for all $1 \leq i \leq \ell$ can exist for $\mathcal{T}_{\mathcal{M}}$. It is a proper relation if there is some $1 \leq i \leq \ell$ with $\boldsymbol{v}_i \neq \boldsymbol{v}'_i$. Such a proper relation implies

$$M_\ell \cdots M_1 = M_\ell \cdots M_1$$

in the linear semigroup by Lemma 3.6; however, this is not a proper relation.

Concerning Proposition 3.9, we can prove that, in fact, the group generated by $\mathcal{T}_{\mathcal{M}}$ is never free (except for trivial cases):

PROPOSITION A: *Let $d \geq 2$ and $\mathcal{M}$ be a finite set of $\mathbb{Z}^{d\times d}$ matrices with non-zero determinant. Then, $\mathscr{G}(\mathcal{T}_{\mathcal{M}})$ is not free (where $\mathcal{T}_{\mathcal{M}}$ is the G-automaton from Lemma 3.5).*

Proof. The group generated by $\mathcal{T}_{\mathcal{M}}$ is isomorphic to the subgroup G of $\operatorname{Aff}_d(\mathbb{Z}_n)$ generated by $\{M_{\boldsymbol{v}} \mid M \in \mathcal{M}, \boldsymbol{v} \in V_M\}$. We will show that this affine subgroup is not free. Instead of $M_{\boldsymbol{v}}$, we will use the semidirect product notation $(\boldsymbol{v}, M)$ for elements of G.

First, observe that the linear group L generated by $\mathcal{M}$ is a subgroup of G. If it is trivial, then $\mathcal{M}$ can only contain the identity matrix and, by [5, Lemma 4.1], we have $G \simeq \mathbb{Z}^d \rtimes L$. Since we have $d \geq 2$, this contains the non-cyclic, abelian subgroup $\mathbb{Z}^d$ and, thus, cannot be free.

Therefore, assume that L is non-trivial and let $1 \neq M \in L$. The group G cannot be free if L is not free and there is nothing to show in this case. Thus, we assume that L is free, which implies that all (non-identity) matrices in $\mathcal{M}$ have infinite order (as elements of the general linear group). Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be two different vectors from V_M (note that such vectors always exist) and consider the subgroup H of G generated by $(\boldsymbol{u}, M)$ and $(\boldsymbol{v}, M)$. We will show that this subgroup is solvable but not cyclic and, therefore, not free.

First, assume that H is cylic. Then, there is some $(\boldsymbol{w}, N)$ such that

$$(\boldsymbol{u}, M) = (\boldsymbol{w}, N)^i$$

and

$$(\boldsymbol{v}, M) = (\boldsymbol{w}, N)^j$$

for some $i, j \in \mathbb{Z}$. From the second components, we obtain $N^i = M = N^j$. Since M is not the identity matrix, N cannot be the identity matrix either and must, therefore, have infinite order. This implies $i = j$, which is not possible, however, as we have $\boldsymbol{u} \neq \boldsymbol{v}$.

To show that H is solvable, we show that the commutator subgroup $[H, H]$ is abelian. To see this, consider a commutator $[(\boldsymbol{w}_1, M), (\boldsymbol{w}_2, M)]$ of elements $(\boldsymbol{w}_1, M), (\boldsymbol{w}_2, M) \in H$. We have

$$[(\boldsymbol{w}_1, M), (\boldsymbol{w}_2, M)] = (\boldsymbol{w}_2, M)^{-1}(\boldsymbol{w}_1, M)^{-1}(\boldsymbol{w}_2, M)(\boldsymbol{w}_1, M) = (\boldsymbol{w}', 1)$$

for some vector $\boldsymbol{w}'$. Thus, all such transformations commute. ∎

As a consequence, Proposition 3.9 can only be stated as follows.

Proposition 3.9: *IICP is reducible to the problem Free Subgroup Presentation*

Input:	*a* G*-automaton* $\mathcal{T} = (Q, \Sigma, \delta)$ *and* *a finite subset* $\boldsymbol{P} \subseteq Q^+$
Question:	*does the subgroup generated by* $\boldsymbol{P}$ *in* $\mathscr{G}(\mathcal{T})$ *admit a relation over* $\boldsymbol{P}$*?*

However, Gillibert already showed that the order problem for automaton groups

Input:	a G-automaton $\mathcal{T} = (Q, \Sigma, \delta)$ and some $\boldsymbol{q} \in Q^*$
Question:	has $\boldsymbol{q}$ finite order in $\mathscr{G}(\mathcal{T})$?

is undecidable [3]. It is a special case of Free Subgroup Presentation and, therefore, the undecidability of Free Subgroup Presentation follows directly (and independently from the undecidability of IICP) from Gillibert's result.

The Semigroup Case. The same problem also affects the semigroup case in Theorem 3.12 and Corollary 3.13. Accordingly, the statement that "by Lemma 3.6, the semigroup generated by $\mathcal{T}_{\mathcal{M}}$ is free if and only if so is the linear semigroup generated by $\mathcal{M}$" made in the original proof of Theorem 3.12 is incorrect. In fact, we obtain—similar to the group case—that the semigroup generated by $\mathcal{T}_{\mathcal{M}}$ is never free.

Proposition B: *Let* $\mathcal{M}$ *be a non-empty, finite set of matrices from* $\mathbb{Z}^{d\times d}$*. Then,* $\mathscr{S}(\mathcal{T}_{\mathcal{M}})$ *is not a free semigroup (where* $\mathcal{T}_{\mathcal{M}}$ *is the* S*-automaton from Lemma 3.5).*

To prove Proposition B, we show something more general and derive Proposition B from that. However, we first need to introduce some semigroup concepts. To every semigroup S, we can adjoin a new neutral element 1 to obtain the monoid S^1. Clearly, S is a free semigroup if and only if S^1 is a free monoid.

A **proper length** function for some monoid M is a homomorphism λ from M to the free monoid of rank one $(\mathbb{N}, +)$ such that $\lambda(s) = 0$ implies $s = 1$. A monoid M is **equidivisible** if, for all $s_1, s_2, s_1', s_2' \in M$ with $s_1 s_2 = s_1' s_2'$, there is some $x \in M$ with $s_1 = s_1' x$ and $x s_2 = s_2'$ or with $s_1 x = s_1'$ and $s_2 = x s_2'$. Free monoids are equidivisable by Levi's Lemma [4, Proposition 7.1.2] and, obviously, admit a proper length function; the converse holds as well [4, Proposition 7.1.8], which yields the following characterization.

Fact C: *A monoid M is free if and only if it admits a proper length function and is equidivisable.*

If T is a subsemigroup of a free semigroup S, then T^1 is a submonoid of S^1 and inherits the proper length function of S^1. Accordingly, T is free if (and only if) T^1 is equidivisable.

A (**left**) **action** of a semigroup S on a monoid M is a homomorphism $\alpha : S \to \operatorname{End}(M)$ where $\operatorname{End}(M)$ is the monoid of monoid endomorphisms of M. In particular, we require $\alpha_s(1_M) = 1_M$ for all $\alpha_s = \alpha(s)$ (with $s \in S$). We will also write ${}^s m$ for $\alpha_s(m)$ if the action is clear from the context.

If the semigroup S acts on the left on some monoid M, we can define the **semidirect product** $M \rtimes S$: it is the semigroup whose elements are in $M \times S$ and whose multiplication is given by $(m, s)(n, t) = (m \, {}^s n, st)$. We can consider S as a subsemigroup of $M \rtimes S$ by identifying s with $(1, s)$.[2]

In general, not every subsemigroup of a free semigroup is free; quite to the contrary, every (non-empty) free semigroup contains a non-free subsemigroup (see, e.g., [4, p. 243]). However, for certain subsemigroups of a semidirect product, we still have a connection concerning their freeness.

Lemma D: *Let M be a monoid, S a semigroup and let T be a subsemigroup of $M \rtimes S$ containing S as a subsemigroup. Then, S is a free semigroup if T is one.*

Proof. Assume that T is a free semigroup or, equivalently, that T^1 is a free monoid. Then, T^1 is equidivisable and has a proper length function. We will show that both these properties are inherited by S^1 and that, thus, S is a free semigroup.

For the proper length function, we set the length of 1 to 0 and the length of s to that of $(1, s)$, which is in T because S is a subsemigroup of T. To show that S^1 is equidivisable, let $s_1 s_2 = s_1' s_2'$ for $s_1, s_2, s_1', s_2' \in S^1$. We need some $x \in S^1$ with $s_1 = s_1' x$ and $x s_2 = s_2'$ or with $s_1 x = s_1'$ and $s_2 = x s_2'$. If we have $s_1 = 1$, we can set $x = s_1'$ to obtain $s_1 x = s_1'$ and $s_2 = 1 s_2 = s_1' s_2' = x s_2'$. The cases $s_2 = 1$, $s_1' = 1$ or $s_2' = 1$ are symmetric. In the case $s_1, s_2, s_1', s_2' \neq 1$, we have $(1, s_1)(1, s_2) = (1, s_1')(1, s_2')$ in T^1 and, because T^1 is equidivisable, there is some $y \in T^1$ with $(1, s_1) = (1, s_1')y$ and $y(1, s_2) = (1, s_2')$ or with $(1, s_1)y = (1, s_1')$ and $(1, s_2) = y(1, s_2')$. If $y = 1$, we obtain $s_1 = s_1'$ and $s_2 = s_2'$

[2] This is possible because we have ${}^s 1 = 1$.

and we choose $x = 1$. Otherwise, $y \in T^1 \setminus \{1\} = T \subseteq M \rtimes S$ is of the form $y = (m, x) \in M \times S$ and, from the second components of the equations in the two cases, we see that $x \in S$ is indeed the sought element, which concludes the proof that S^1 is equidivisable. ∎

The above connection allows us to show a general statement that certain subsemigroups of semidirect products are not free, from which we will finally derive Proposition B.

PROPOSITION E: *Let M be a monoid and S a semigroup. Furthermore, let T be a subsemigroup of $M \rtimes S$ such that S is a proper subsemigroup of T. Let $(\hat{m}, \hat{s}) \in T \setminus S$ (i.e., we have $M \ni \hat{m} \neq 1_M$ and $\hat{s} \in S$).*

If $({}^{\hat{s}}\hat{m}, \hat{s})$ is in T, then T cannot be a free semigroup.

Proof. We show the statement by contradiction. Thus, assume that T is a free semigroup. Then, S is also a free semigroup by Lemma D and T^1 and S^1 are both free monoids.

Since S is a subsemigroup of T, we have $(1, \hat{s}) \in T$ and

$$(1, \hat{s})(\hat{m}, \hat{s}) = (1\, {}^{\hat{s}}\hat{m}, \hat{s}^2) = ({}^{\hat{s}}\hat{m}\, 1, \hat{s}^2) = ({}^{\hat{s}}\hat{m}, \hat{s})(1, \hat{s})$$

because the action of S on the monoid M fixes the neutral element. By assumption, we have $({}^{\hat{s}}\hat{m}, \hat{s}) \in T$ and, because T^1 as a free monoid is equidivisable, there is some $y \in T^1$ with $y(\hat{m}, \hat{s}) = (1, \hat{s})$ or with $(\hat{m}, \hat{s}) = y(1, \hat{s})$. Since we have $\hat{m} \neq 1$, we obtain $y \neq 1$ in both cases. Thus, $y = (m, x) \in T^1 \setminus \{1\} = T \subseteq M \times S$ and we obtain $(m, x)(\hat{m}, \hat{s}) = (1, \hat{s})$ in the first and $(\hat{m}, \hat{s}) = (m, x)(1, \hat{s})$ in the second case. In both cases, we have $x\hat{s} = \hat{s}$ in the free semigroup S, which is not possible. ∎

Proof of Proposition B. By Lemma 3.5, the semigroup generated by $\mathcal{T}_{\mathcal{M}}$ is isomorphic to the subsemigroup T of $\mathrm{SAff}_d(\mathbb{Z})$ generated by $\{M_{\boldsymbol{v}} \mid M \in \mathcal{M}, \boldsymbol{v} \in V_M\}$. In other words, T is a subsemigroup of the semidirect product $\mathbb{Z}^d \rtimes S$ where S is the linear semigroup generated by $\mathcal{M}$ and the action of S on the (additive) monoid $\mathbb{Z}^d$ is given by the normal matrix multiplication.

If $\mathcal{M}$ only contains the zero matrix $0 \in \mathbb{Z}^{d \times d}$, then T consists only of $0_{\mathbf{0}}$, i.e., T is the trivial monoid and, thus, not a free semigroup. If $\mathcal{M}$ contains a non-zero matrix M, then we must have $\|M\| \geq 1$. We will show that there is some $\boldsymbol{v} \in V_M \setminus \{\mathbf{0}\}$ with $M\boldsymbol{v} \in V_M$. This way, we have $M_{\boldsymbol{v}} \in T \setminus S$ as well as $M_{M\boldsymbol{v}} \in T$ and can apply Proposition E to obtain that T is not free.

As the vector $\boldsymbol{v}$, we choose $-\boldsymbol{e}_1$ where $\boldsymbol{e}_1$ is the 1^{st} d-dimensional unit vector. We have $\|M\| \geq 1$ and, thus, $-\|M\| \leq -1$, which implies $\boldsymbol{v} = -\boldsymbol{e}_1 \in V_M$. On the other hand, we have that the i^{th} component of $\boldsymbol{w} = M\boldsymbol{v}$ is $-m_{i,1}$ where $m_{i,1}$ is the entry of M in the i^{th} row and 1^{st} column. Since we have $m_{i,1} \leq \|M\|$ and, thus, $-m_{i,1} \geq -\|M\|$, we obtain $\boldsymbol{w} = M\boldsymbol{v} \in V_M$ as well. ∎

As a result of the flaw in the argumentation, Theorem 3.12 and Corollary 3.13 have to be re-formulated as follows; in particular, the question whether the freeness problem for automaton semigroups is decidable remains open.

THEOREM 3.12: *The problem*

Input:	*a G-automaton $\mathcal{T} = (Q, \Sigma, \delta)$ and*
	a finite subset $\boldsymbol{P} \subseteq Q^+$
Question:	*is the subsemigroup generated by $\boldsymbol{P}$ in $\mathscr{S}(\mathcal{T})$ free?*

is undecidable.

COROLLARY 3.13: *The freeness problem for subsemigroups of automaton semigroups*

Input:	*a finitely generated subsemigroup T of an automaton semigroup*
Question:	*is T free?*

is undecidable.

The corrected version of Theorem 3.12 can be proved by reducing Matrix Semigroup Freeness to the problem. Here, we map $\mathcal{M}$ to $\mathcal{T}_{\mathcal{M}}$ and use

$$\boldsymbol{P} = \{m_{M,\mathbf{0}} \mid M \in \mathcal{M}\}$$

as the generators of the subsemigroup (where $\mathbf{0}$ is the d-dimensional zero vector). The corrected version of Corollary 3.13 immediately follows from the corrected version of Theorem 3.12.

Again, the corrected version of Theorem 3.12 also follows from the undecidability of the order problem for automaton groups [3] (and the corrected version of Corollary 3.13 even follows from the undecidability of the order/torsion problem for automaton semigroups implied by [2, Lemma 3.11 and 3.12]).

Finally, the reduction in the proof of Corollary 3.14 is still correct. However, we do not have that G-Semigroup Freeness is undecidable anymore. Therefore, the statement of the corollary does not follow.

References

[1] D. D'Angeli, E. Rodaro and J. Ph. Wächter, *Automaton semigroups and groups: On the undecidability of problems related to freeness and finiteness*, Israel Journal of Mathematics **237** (2020), 15–52.

[2] P. Gillibert, *The finiteness problem for automaton semigroups is undecidable*, International Journal of Algebra and Computation **24** (2014), 1–9.

[3] P. Gillibert, *An automaton group with undecidable order and Engel problems*, Journal of Algebra **497** (2018), 363–392.

[4] J. M. Howie, *Fundamentals of Semigroup Theory*, London Mathematical Society Monographs, Vol. 12, Clarendon Press, Oxford, 1995.

[5] Z. Šunić and E. Ventura, *The conjugacy problem in automaton groups is not solvable*, Journal of Algebra **364** (2012), 148–154.