On Ore's Theorem and Universal Words for Permutations and Injections of Infinite Sets

Dedicated to the memory of Rüdiger Göbel

Manfred Droste

Universität Leipzig, Institut für Informatik,
04109 Leipzig, Germany
droste@informatik.uni-leipzig.de

Abstract. We give a simple proof that any injective self-mapping of an infinite set M can be written as a product of an injection and a permutation of M both having infinitely many infinite orbits (and no others). This implies Ore's influential theorem that each permutation of M is a commutator, a similar result due to Mesyan for the injections of M, and a result on which injections f of M can be written in the form $f = x^m \cdot y^n$.

1 Introduction

For words $w = w(x_1, \cdots, x_n)$ in free variables $x_1, \cdots, x_n$, it often leads to difficult problems to describe groups G for which each element $g \in G$ is expressible in the form $g = w(g_1, \cdots, g_n)$ for some $g_1, \cdots, g_n \in G$. In the case of commutators $w = x_1^{-1} \cdot x_2^{-1} \cdot x_1 \cdot x_2$, this is known to be true for all finite and infinite alternating groups [12], all semi-simple complex Lie groups [13], all semi-simple connected algebraic groups [14], and many others; recently, it was established for all finite non-abelian simple groups [6], thereby confirming Ore's conjecture.

Ore [12] showed that, in contrast to the finite symmetric groups S_n somewhat surprisingly, each element of the infinite symmetric groups $S(M)$ of all permutations of an infinite set M is a commutator. His proof involved a non-trivial case analysis of cycle types. Here, we wish to provide a simple geometric proof of an extension of this result. We will consider the monoids $\mathrm{Inj}(M)$ of all injections of an infinite set M. An Ore-type result for these monoids $\mathrm{Inj}(M)$ was recently established in Mesyan [8]; see [9, 3] for consequences and descriptions of the normal subsemigroups of $\mathrm{Inj}(M)$. Our main result will be a simple proof showing that each injection $f \in \mathrm{Inj}(M)$ can be written as a product $f = g \cdot h$ with an injection $g \in \mathrm{Inj}(M)$ and a permutation $h \in S(M)$ each having infinitely many infinite orbits (and no others). This result itself also follows from a general result given in [8] which, however, involves a more complicated case analysis of possible orbits and previous results for $S(M)$. Our idea is to take as underlying set $M = \mathbb{Z} \times \mathbb{Z}$ (for the crucial case that M is countable) and to represent f in a suitable form. This idea was also used for the symmetric group $S(M)$ in [2] and in [4] with applications for extension results on coverings of surfaces. As an immediate consequence of the above result we obtain an Ore-type result for $\mathrm{Inj}(M)$, Ore's result for $S(M)$, and a description of all elements f of $\mathrm{Inj}(M)$ which can be written in the form $f = x^m \cdot y^n$ with $x, y \in \mathrm{Inj}(M)$.

2 Background

Here we summarize the notation and background results, as needed subsequently.

Let M be an infinite set, $\mathrm{Inj}(M)$ the monoid of all injective maps of M and $S(M)$ the symmetric group of all permutations of M. Let $f \in \mathrm{Inj}(M)$. If $x \in M$, the set $\{y \in M \mid xf^i = y \text{ or } yf^i = x \text{ for some } i \geq 0\}$ is called the f-*orbit* of x, or an *orbit* of f. We call an orbit a *forward orbit*, if it is the f-orbit of some x such that $x \notin Mf$. Note that then this orbit equals $\{xf^i \mid i \geq 0\}$ and is infinite. This gives a bijection between $M \backslash Mf$ and the set of forward orbits of f. We have the following important observation.

Proposition 2.1. *Let* $f, g \in \mathrm{Inj}(M)$. *Then*

$$|M \backslash Mfg| = |M \backslash Mf| + |M \backslash Mg|.$$

Proof. We have

$$M \backslash Mfg = (M \backslash Mf)g \,\dot{\cup}\, (M \backslash Mg).$$

□

As usual, for $g \in \mathrm{Inj}(M)$ and $h \in S(M)$, we let $g^h = h^{-1}gh$. We say that two injections $f, g \in \mathrm{Inj}(M)$ are *conjugate* if $f = g^h$ for some $h \in S(M)$. We let $g^{S(M)} = \{g^h \mid h \in S(M)\}$, the set of conjugates of f. Next we wish to describe when two elements of $\mathrm{Inj}(M)$ are conjugate.

We let $\mathbb{N}$ denote the set of positive integers, and $\mathbb{N}_\infty = \mathbb{N} \cup \{\infty\}$. Given $f \in \mathrm{Inj}(M)$, we call any orbit U of f with $U \subseteq Mf$, i.e., which is not a forward orbit, a *closed orbit*; then clearly $f\restriction_U \in S(U)$. We define $\bar{f}$ to be the map from $\mathbb{N}_\infty$ to the cardinals by letting $\bar{f}(n)$ be the number of closed orbits of size n of f, for each $n \in \mathbb{N}_\infty$. Recall that $|M \backslash Mf|$ is the number of forward orbits of f.

The following result, which is well-known for permutations, describes that two elements of $S(M)$ resp. $\mathrm{Inj}(M)$ are conjugate if and only if they have the same "orbit structure".

Proposition 2.2. *(a) Let* $f, g \in S(M)$. *Then* f *and* g *are conjugate if and only if* $\bar{f} = \bar{g}$.
(b) (Mesyan [8]) *Let* $f, g \in \mathrm{Inj}(M)$. *Then* f *and* g *are conjugate if and only if* $\bar{f} = \bar{g}$ *and* $|M \backslash Mf| = |M \backslash Mg|$.

Proof. Note that (a) is a special case of (b). We indicate the proof of (b) for the convenience of the reader. If $f = g^h$ for some $h \in S(M)$, then h maps the orbits of g onto the orbits (of the same length) of f. Hence $\bar{f} = \bar{g}$ and $|M \backslash Mf| = |M \backslash Mg|$.

Conversely, given a length-preserving and forwardness-preserving bijection π from the orbits of g onto the orbits of f, for each orbit U of g, choose elements $x_U \in U$, $y_U \in U\pi$ (and such that $x_U \notin Mg$, $y_U \notin Mf$ in case U is a forward orbit), put $x_U h = y_U$ and extend h uniquely to a permutation of M satisfying $hf = gh$. □

3 The main result

In this section we will provide a simple proof for the following result.

Theorem 3.1. *Let M be an infinite set. Then every injection $f \in \mathrm{Inj}(M)$ is a product $f = g \cdot h$ of an injection $g \in \mathrm{Inj}(M)$ and a permutation $h \in S(M)$ both having infinitely many infinite orbits (and no others). We also have $f = h \cdot g$ with $g \in \mathrm{Inj}(M)$, $h \in S(M)$ as described before.*

We note that Theorem 3.1 is a special case of the main result of Mesyan [8] whose proof, however, involves a detailed analysis of the orbit structure of elements of $\mathrm{Inj}(M)$ and uses previous results on $S(M)$.

For our proof of Theorem 3.1, if M is countable, we take $M = \mathbb{Z} \times \mathbb{Z}$, the integer plane. We will show that for any $f \in \mathrm{Inj}(M)$ there is a conjugate f' of f which moves each element of M at most one unit up or down. For this, we construct f' with the same "orbit structure" as f by employing a Cantor-like enumeration of $\mathbb{Z} \times \mathbb{Z}$ or of suitable subsets (like half-planes). For the case that $f \in S(M)$, this is also described in [2] and [4] (see sections 3-5).

Lemma 3.2. *Let $M = \mathbb{Z} \times \mathbb{Z}$. Then for each $f \in \mathrm{Inj}(M)$ there is $f' \in \mathrm{Inj}(M)$ such that $\bar{f} = \bar{f}'$, $|M \backslash Mf| = |M \backslash Mf'|$ and $(i, j)f' \in \mathbb{Z} \times \{j-1, j, j+1\}$ for each $(i, j) \in M$.*

Proof. If f has infinitely many orbits, it is easy to construct such an injection f' satisfying even $(i, j)f' \in \mathbb{Z} \times \{j\}$ for each $(i, j) \in M$, i.e., the orbits of f' are all contained in the horizontal lines of $M = \mathbb{Z} \times \mathbb{Z}$. Therefore now let f have only finitely many orbits. Consequently, f has at least one infinite orbit.

First, let f have only one forward orbit (and no others). Then consider the "infinite spiral"

$$(0,0) \to (1,0) \to (1,1) \to (0,1) \to (-1,1) \to (-1,0) \to (-1,-1) \to$$
$$(0,-1) \to (1,-1) \to (2,-1) \to (2,0) \to \cdots$$

which gives f'.

This construction leaves a lot of freedom for changes enabling us to deal with the other cases. For instance, assume that $f \in S(M)$ has precisely one infinite closed orbit (and no others). Then let $f' \in S(M)$ act on the upper half plane $\mathbb{Z} \times \mathbb{N}_0$, where $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, similarly as above, like

$$(0,0) \to (1,0) \to (1,1) \to (0,1) \to (-1,1) \to (-1,0) \to (-2,0) \to$$

$$(-2,1) \to (-2,2) \to (-1,2) \to (0,2) \to \cdots .$$

By a similar enumeration of the lower half plane $\mathbb{Z} \times \{-n \mid n > 0\}$, we define the pre-images of $(0,0)$ under f'.

Now if f has $k+1$ infinite orbits ($k > 0$), we can define f' such that it has each half-line $\mathbb{N} \times \{i\}$ ($i = 1, \cdots, k$) as an infinite orbit and has the set $M \setminus \bigcup_{i=1}^{k} \mathbb{N} \times \{i\}$ as the remaining infinite orbit, in each case realizing forwardness or closedness as necessary.

Finally, for the finite orbits of f (note that by our assumption, f has only finitely many orbits), we can take a suitably large interval in $\mathbb{N} \times \{0\}$ to realize the corresponding orbits of f', and use the complement of this interval for the infinite orbits of f'. $\square$

Now we can show Theorem 3.1.

Proof of Theorem 3.1. It suffices to consider the case that M is countable. Indeed, if M is uncountable and $f \in \mathrm{Inj}(M)$, by a standard argument we can split $\dot{\bigcup}_{i \in I} M_i$ into pairwise disjoint f-invariant countable sets M_i, so $f\restriction_{M_i} \in \mathrm{Inj}(M_i)$. Then by the result of the countable case, for each $i \in I$ write $f\restriction_{M_i} = g_i \cdot h_i$ with an injection $g_i \in \mathrm{Inj}(M_i)$ and a permutation $h_i \in S(M_i)$ both having infinitely many infinite orbits (and no others). Then $g = \bigcup_{i \in I} g_i \in \mathrm{Inj}(M)$ and $h = \bigcup_{i \in I} h_i \in S(M)$ satisfy $f = g \cdot h$ as claimed.

So, let M be countable. We may assume that $M = \mathbb{Z} \times \mathbb{Z}$. Let $f \in \mathrm{Inj}(M)$. By Lemma 3.2, there is $f' \in \mathrm{Inj}\, M$ moving each point $x \in M$ at most one unit up or down such that $\bar{f} = \bar{f}'$ and $|M \setminus Mf| = |M \setminus Mf'|$. Then, $f \in f'^{S(M)}$ by Proposition 2.2.

Now define $h : M \to M$ by letting $(i,j)h = (i, j+2)$ for each $(i,j) \in M$. So $h \in S(M)$ has infinitely many infinite orbits (and no others). Now consider $g = f' \cdot h \in \mathrm{Inj}(M)$. Since f' moves each point $x = (i,j) \in M$ at most one unit up or down and h moves each point two units up, we obtain $xg \in \mathbb{Z} \times \{j+1, j+2, j+3\}$, so g moves each point at least one unit up. Hence g has only infinite orbits, and all elements $(i,0)$, $i \in \mathbb{Z}$, lie in different orbits of g, thus g has infinitely many infinite orbits. So $f' = g \cdot h^{-1}$ as claimed, and the first statement of the result follows.

For the second statement, write $f = g \cdot h = h \cdot (h^{-1}gh)$; then $g^h \in \mathrm{Inj}(M)$ as claimed. $\square$

Let C_∞ be the conjugacy class in $S(M)$ comprising all permutations of M with infinitely many infinite orbits (and no others). Note that if in Theorem 3.1 $f \in S(M)$ is a permutation, by the proof of Theorem 3.1 (or by Proposition 2.1) we obtain $f = g \cdot h$ with permutations $g, h \in S(M)$. Hence, as an immediate consequence of Theorem 3.1 we have:

Corollary 3.3. (Gray [5]). *Let M be an infinite set. Then $S(M) = C_\infty^2$.*

By subsequent work of Bertram, Göbel and the author, the author, and Moran, culminating in Moran [10], all conjugacy classes C in $S(M)$ were described satisfying $S(M) = C^2$.

4 Ores's theorem and universal words

Here we will derive Ore's theorem and results on universal words for $S(M)$ and $\mathrm{Inj}(M)$ as immediate consequences of Theorem 3.1. First we have:

Corollary 4.1. (Ore [12]). *Let M be an infinite set. Then each element $f \in S(M)$ is a commutator $f = [g, h]$.*

Proof. By Theorem 3.1 (or Corollary 3.3), write $f = g^{-1} \cdot k$ with $g, k \in C_\infty$. Then $k = h^{-1}gh$ for some $h \in S(M)$ and $f = [g, h]$. □

Mesyan [8] gave a general result describing when an arbitrary injection $f \in \mathrm{Inj}(M)$ can be written as a product of two injections $g, h \in \mathrm{Inj}(M)$ both having at least one infinite orbit. As an immediate consequence, he obtained the subsequent Ore-type result for $\mathrm{Inj}(M)$ which we wish here to deduce from Theorem 3.1.

Corollary 4.2. (Mesyan [8]). *Let M be an infinite set and $f \in \mathrm{Inj}(M)$. Then f can be written in the form $f = g^a \cdot g^b$ for some $g \in \mathrm{Inj}(M)$ and $a, b \in S(M)$ if and only if $|M \backslash Mf|$ is either an even integer or infinite.*

Proof. Clearly, if $f = g^a \cdot g^b$ is of the form described, by Proposition 2.1 we have $|M \backslash Mf| = 2 \cdot |M \backslash Mg|$ as claimed.

Now let $|M \backslash Mf|$ be even or infinite. If $f \in S(M)$, the result is immediate by Corollary 3.3. Hence assume $f \in \mathrm{Inj}(M) \backslash S(M)$, so f has at least two infinite forward orbits. Split $M = M_1 \dot\cup M_2$ in such a way that $|M_1| = |M_2|$, both M_1 and M_2 are f-invariant, and M_1 and M_2 contain the same number of infinite forward orbits of f. By Theorem 3.1, write $f{\restriction_{M_1}} = g_1 \cdot h_1$ and $f{\restriction_{M_2}} = h_2 \cdot g_2$ with injections $g_i \in \mathrm{Inj}(M_i)$ and permutations $h_i \in S(M_i)$ such that $|M_i \backslash M_i f| = |M_i \backslash M_i g_i|$, and g_i, h_i have infinitely many infinite orbits (and no others), for $i = 1, 2$. Let $g = g_1 \cup h_2$ and $g' = h_1 \cup g_2$. Then $g, g' \in \mathrm{Inj}(M)$ satisfy

$$|M \backslash Mg| = |M_1 \backslash M_1 g_1| = |M_1 \backslash M_1 f| = |M_2 \backslash M_2 f| = |M_2 \backslash M_2 g_2| = |M \backslash Mg'|$$

and g, g' each have infinitely many infinite closed orbits (and no other closed orbits). Hence $f = g \cdot g' = g \cdot g^b$ for some $b \in S(M)$ as claimed. □

Let G be a group and $w = w(x_1, \cdots, x_n)$ a word in the free group over $x_1, \cdots, x_n$. Then w is said to be *G-universal*, if for each $g \in G$ there are $g_1, \cdots, g_n \in G$ such that $g = w(g_1, \cdots, g_n)$. By Corollary 4.1, the commutator word $w = [x, y]$ is $S(M)$-universal for infinite sets M. Clearly, no power $w = x^n$ $(n \geq 2)$ is $S(M)$-universal. As a further immediate consequence of Corollary 3.3, we have:

Corollary 4.3. (Silberger [15]). *Let M be an infinite set and $w = x^m \cdot y^n$ with $m, n \neq 0$. Then w is $S(M)$-universal.*

Proof. Let $f \in S(M)$. Write $f = g \cdot h$ with $g, h \in C_\infty$. Since $g^m, h^n \in C_\infty$, they are conjugate to g and h and the result follows. □

We note that we could also obtain Corollary 4.3 as follows. First, write $f \in S(M)$ as a product $f = g \cdot h$ of two involutions $g, h \in S(M)$ each having infinitely many 2-orbits. Note that the m-th power of a cycle of length $2m$ consists of m disjoint 2-cycles. Hence we can write $g = a^m$ with $a \in S(M)$ having only orbits of length $2m$ and, possibly, fixed points. Similarly, $h = b^n$ with $b \in S(M)$ having only orbits of length $2n$, and, possibly, fixed points. In the above proof of Corollary 4.3, we have obtained that $f = a^m \cdot b^n$ with $a, b \in C_\infty$. Extensions of this result are contained in [2]. Mycielski [11] and Lyndon [7], cf. [1], showed that each word $w = w(x_1, \cdots, x_n)$ which does not reduce to a power is $S(M)$-universal.

Now consider a semigroup S and a word $w = w(x_1, \cdots, x_n)$ in the free semigroup over $x_1, \cdots, x_n$. We say that $g \in S$ is a *w-element*, if there are $g_1, \cdots, g_n \in S$ such that $g = w(g_1, \cdots, g_n)$. Given a free semigroup word $w(x_1, \cdots, x_n)$, let $e(x_i)$ be the sum of the exponents of x_i in w, for $i = 1, \cdots, n$. Clearly, by Proposition 2.1, if $f \in \mathrm{Inj}(M)$ is a w-element, then either $M \backslash Mf$ is infinite or $|M \backslash Mf| \in \langle e(x_1), \cdots, e(x_n) \rangle$, the subsemigroup of $(\mathbb{N}, +)$ generated by $e(x_1), \cdots, e(x_n)$. Now we show that for products of powers, we also have the converse.

Corollary 4.4. *Let M be an infinite set, $m, n \geq 1$, and $f \in \mathrm{Inj}(M)$. Then f is a $x^m \cdot y^n$-element if and only if $M \backslash Mf$ is infinite or $|M \backslash Mf| \in \langle m, n \rangle$.*

Proof. As noted before, if $f = g^m \cdot h^n$ with $g, h \in \mathrm{Inj}(M)$, by Proposition 2.1 we have

$$|M \backslash Mf| = m \cdot |M \backslash Mg| + n \cdot |M \backslash Mh|$$

which is infinite or in $\langle m, n \rangle$. Conversely, assume that $|M \backslash Mf| = k \cdot m + \ell \cdot n$ for some $k, \ell \geq 0$. First assume that $k, \ell > 0$. We include the case that $M \backslash Mf$ is infinite here by letting $k = \ell = \infty$. We split $M = M_1 \dot{\cup} M_2$ into two disjoint f-invariant subsets M_1 and M_2 such that M_1 (resp. M_2) contains $k \cdot m$ (resp. $\ell \cdot n$) infinite forward orbits of f. By Theorem 3.1, we can write $f{\restriction}_{M_1} = g_1' \cdot h_1'$ and $f{\restriction}_{M_2} = h_2' \cdot g_2'$ with injections $g_i' \in \mathrm{Inj}(M_i)$ and permutations $h_i' \in S(M_i)$ each having infinitely many infinite orbits (and no others), for $i = 1, 2$. In particular,

$$|M_1 \backslash M_1 g_1'| = |M_1 \backslash M_1 f| = k \cdot m$$

and

$$|M_2 \backslash M_2 g_2'| = |M_2 \backslash M_2 f| = \ell \cdot n.$$

Consequently, $g_1' \cup h_2' \in \mathrm{Inj}(M)$ has $k \cdot m$ forward orbits, infinitely many infinite closed orbits and no others. Choose any $g' \in \mathrm{Inj}(M)$ which has k forward orbits if $M \backslash Mf$ is finite, infinitely many forward orbits if $M \backslash Mf$ is infinite, and in any case infinitely many infinite closed orbits and no others. Then $g_1' \cup h_2'$ is conjugate to g'^m. Therefore, $g_1' \cup h_2' = g^m$ for some $g \in \mathrm{Inj}(M)$. Similarly, we have $h_1' \cup g_2' = h^n$ for some $h \in \mathrm{Inj}(M)$. Hence $f = g^m \cdot h^n$.

If $k = 0$ or $\ell = 0$ (but not both), we can apply a similar (but simpler) argument, using Theorem 3.1 directly for M. Finally, if $k = \ell = 0$, i.e., $f \in S(M)$, the result is immediate by Corollary 4.3. □

In view of Corollary 4.4 and the results of Mycielski and Lyndon for $S(M)$ the following question arises.

Let $w = w(x_1, \cdots, x_n)$ be a free semigroup word, $n \geq 2$, and let $f \in \mathrm{Inj}(M)$ satisfy $|M \backslash Mf| \in \langle e(x_1), \cdots, e(x_n)) \rangle$. Does it follow that f is a w-element?

References

[1] R. Dougherty, J. Mycielski: Representations of infinite permutations by words (II). Proc. Amer. Math. Soc. 127, No. 8 (1999), 2233-2243.

[2] M. Droste: Classes of universal words for the infinite symmetric groups, Algebra Universalis 20 (1985), 205 - 216.

[3] M. Droste, R. Göbel: The normal subsemigroups of the monoid of injective maps. Semigroup Forum 87 (2013), 298-312.

[4] M. Droste, I. Rivin: On extension of coverings. Bull. London Math. Soc. 42 (2010), 1044-1054.

[5] A. B. Gray: Infinite symmetric and monomial groups. Ph.D. Thesis, New Mexico State University, Las Cruces, NM, 1960.

[6] M. Liebeck, E. A. O'Brian: A. Shalev and P. H. Tiep; The Ore Conjecture. Journal of the Europ. Math. Soc. 12 (2010), 939-1008.

[7] R. Lyndon: Words and infinite permutations. Mots, Lang. Raison Calc., Hermès, Paris (1990), 143-152.

[8] Z. Mesyan: Conjugations of injections by permutations. Semigroup Forum 81 (2010), 297-324.

[9] Z. Mesyan: Monoids of injective maps closed under conjugation by permutations. Israel. J. Math. 189 (2012), 287-305.

[10] G. Moran: Conjugacy classes whose squares are infinite symmetric groups. Trans. Amer. Math. Soc. 316 (1989), 439-521.

[11] J. Mycielski: Representations of infinite permutations by words. Proc. Amer. Math. Soc. 100 (1987), 237-241.

[12] O. Ore: Some remarks on commutators. Proc. Amer. Math. Soc. 2 (1951), 307-314.

[13] S. Pasiencier, H. C. Wang: Commutators in a semi-simple Lie group. Proc. Amer. Math. Soc. 13 (1962), 907-913.

[14] R. Ree: Commutators in semi-simple algebraic groups. Proc. Amer. Math. Soc. 15 (1964), 457-460.

[15] D. Silberger: Are primitive words universal for infinite symmetric groups? Trans. Amer. Math. Soc. 276, No. 2 (1983), 841-852.