J. Austral. Math. Soc. (*Series A*) **54** (1993), 236–253

CONGRUENCES ON FREE MONOIDS AND SUBMONOIDS OF POLYCYCLIC MONOIDS

JOHN MEAKIN and MARK SAPIR

(Received 20 August 1990)

Communicated by P. G. Trotter

Abstract

We establish a one-to-one "group-like" correspondence between congruences on a free monoid X^* and so-called positively self-conjugate inverse submonoids of the polycyclic monoid $P(X)$. This enables us to translate many concepts in semigroup theory into the language of inverse semigroups.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 20 M 8, 20 M 10.

1. Introduction

For basic background on semigroups we refer the reader to Clifford and Preston [2] or Lyapin [3]: standard information about inverse semigroups may be found in Petrich [8]. Of particular concern to us in the present paper is the *polycyclic monoid* $P(X)$ on a set X, introduced into the literature by Nivat and Perrot [7]. The monoid $P(X)$ may be defined as the inverse hull of the free monoid X^* on the non-empty set X: it arises naturally as the syntactic monoid of the restricted Dyck language on a set of cardinality $|X|$ and also in connection with the operation of a push-down automaton, which may be realized by a rational transducer with values in $P(X)$. We refer the reader to the papers [6, 7, 9], for further details and applications of the polycyclic monoid in formal language theory. For the reader's convenience, we briefly

The research of the first author was partially supported by NSF grant DMS-8702019.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

indicate below a few elementary facts about the polycyclic monoid which we shall use in the present paper.

If X is a non-empty set and X^{-1} a disjoint set in one-one correspondence with X (by means of the mapping $x \to x^{-1}$, $x \in X$) then $P(X)$ may be viewed as the monoid presented by the set $X \cup X^{-1}$ of generators and relations of the form $xx^{-1} = 1$, $xy^{-1} = 0$, $x \neq y$, $x, y \in X$. If $|X| = 1$, then $P(X)$ is just the bicyclic monoid (Clifford and Preston [2]). As usual, with every word $w = x_1 \dots x_n \in (X \cup X^{-1})^*$ we associate a word $w^{-1} = x_n^{-1} \dots x_1^{-1}$. From the presentation of $P(X)$ it follows that each element of $P(X)$ may be written uniquely in the form $u^{-1}v$ for some words $u, v \in X^*$. The multiplication in $P(X)$ is described as follows:

$$(u_1^{-1}v_1)(u_2^{-1}v_2) = \begin{cases} u_1^{-1}wv_2 & \text{if } v_1 = wu_2, \text{ some } w \in X^* \\ u_1^{-1}w^{-1}v_2 & \text{if } u_2 = wv_1, \text{ some } w \in X^* \\ 0 & \text{otherwise} \end{cases}$$

Idempotents of $P(X)$ are of the form $u^{-1}u$ $(u \in X^*)$ and the semilattice of idempotents of $P(X)$ is just the usual partially ordered set of X^* (with a 0 adjoined if $|X| > 1$).

Of course $P(X)$ is an inverse monoid: we show in this paper that every monoid is coded by an inverse submonoid of an appropriate polycyclic monoid.

2. The semigroups P_X, Q_X, I_X

Let X be a finite non-empty set and let $X^{\mathbf{Z}}$ be the set of doubly infinite words (sequences) over X. An element $\underline{x}$ of $X^{\mathbf{Z}}$ will usually be denoted by $\underline{x} = (\dots, x_{-2}, x_{-1}, x_0, x_1, x_2, \dots)$ or $\underline{x} = (x_n)_{n \in \mathbf{Z}}$: here x_n denotes the entry in position $n (n \in \mathbb{Z})$ of the doubly infinite word $\underline{x}$ and $\mathbb{Z}$ denotes the set of integers. It may be convenient for the reader to view the word $\underline{x}$ as being printed on a doubly infinite tape and to consider position 0 of the tape as being located by means of a fixed reading head that scans x_0. Let $Y = X$ if $|X| > 1$ and $Y = X \cup \{t\}$ where $t \notin X$ if $|X| = 1$. We define $|X| + 1$ (partial) mappings from $Y^{\mathbf{Z}}$ to $Y^{\mathbf{Z}}$.

The first mapping is the shift T that shifts each sequence one space to the right. More precisely, if $\underline{x} = (x_n)_{n \in \mathbf{Z}}$, then T maps $\underline{x}$ to $\underline{y} = (y_n)_{n \in \mathbf{Z}}$ where $y_n = x_{n-1}$ (for $n \in \mathbb{Z}$). Note that if we view $\underline{x}$ as being printed on a doubly infinite tape with fixed reading head then T has the effect of shifting the tape one space to the right, so that the symbol scanned by the reading head becomes x_{-1}, instead of x_0. Clearly T is a permutation of $Y^{\mathbf{Z}}$ (with

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

domain all of $Y^{\mathbf{Z}}$ and inverse T^{-1}, the map that shifts each sequence one space to the left).

For each letter $x \in X$ we denote by α_x the mapping that deletes x_1 from $(x_n)_{n\in\mathbf{Z}}$ if $x_1 = x$. Thus α_x is a partial mapping from $Y^{\mathbf{Z}}$ to $Y^{\mathbf{Z}}$ with domain being set of all sequences $(x_n)_{n\in\mathbf{Z}}$ for which $x_1 = x$: the mapping α_x maps $(x_n)_{n\in\mathbf{Z}}$ to $(y_n)_{n\in\mathbf{Z}}$ where

$$y_n = \begin{cases} x_n & \text{if } n \leq 0 \\ x_{n+1} & \text{if } n \geq 1. \end{cases}$$

It is clear that $\alpha_x (x \in X)$ is a partial one-one mapping of $Y^{\mathbf{Z}}$ to $Y^{\mathbf{Z}}$ with inverse map α_x^{-1}, the map that inserts the letter x in $(x_n)_{n\in\mathbf{Z}}$ between x_0 and x_1, thus creating the new sequence $(z_n)_{n\in\mathbf{Z}}$ with

$$z_n = \begin{cases} x_n & \text{for } n \leq 0 \\ x & \text{for } n = 1 \\ x_{n-1} & \text{for } n > 1. \end{cases}$$

Since T and $\alpha_x (x \in X)$ are partial one-one maps of $Y^{\mathbf{Z}}$ to $Y^{\mathbf{Z}}$, we may view them as elements of the symmetric inverse monoid $\mathrm{SIM}(Y^{\mathbf{Z}})$ on the set $Y^{\mathbf{Z}}$ (see Clifford and Preston [2] or Petrich [8] for background on the symmetric inverse monoid). We now define three submonoids P_X, I_X and Q_X of $\mathrm{SIM}(Y^{\mathbf{Z}})$. We use the notation $\langle U\rangle$ to denote the inverse submonoid of $\mathrm{SIM}(Y^{\mathbf{Z}})$ generated by the subset $U \subseteq \mathrm{SIM}(Y^{\mathbf{Z}})$: define

$$P_X = \langle\{\alpha_x : x \in X\}\rangle,$$
$$I_X = \langle\{\alpha_x : x \in X\} \cup \{T\}\rangle,$$

and let Q_X be the set of elements of I_X that can be written as a product of (positive and negative) powers of T and the $\alpha_x (x \in X)$ for which the sum of powers of T involved is zero.

Remark. We shall see later that no element of Q_X can be written as a product of powers of T and the $\alpha_x (x \in X)$ in such a way that the sum of powers of T involved is non-zero.

Note that I_X is a finitely generated inverse monoid and that Q_X is a finitely generated algebra of type $\langle \cdot, ^{-1}, T\rangle$ where T is an isomorphism $a \mapsto T^{-1} a T$.

For every word $u \in X^*$, it is convenient to fix the notation α_u for the mapping from $Y^{\mathbf{Z}}$ to $Y^{\mathbf{Z}}$ that deletes the word u from a sequence $(x_n)_{n\in\mathbf{Z}}$ if $u = x_1 x_2 \ldots x_k$. Clearly α_u is a partial one-one map of $Y^{\mathbf{Z}}$ to $Y^{\mathbf{Z}}$ with domain the set of sequences $(x_n)_{n\in\mathbf{Z}}$ for which $u = x_1 x_2 \ldots x_k$; also α_u is the product $\alpha_u = \alpha_{x_1}\alpha_{x_2}\ldots\alpha_{x_k} \in P_X$. We establish a number of basic properties and facts concerning the monoids P_X, I_X, and Q_X.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

LEMMA 2.1. *The monoid P_{X} is isomorphic to the polycyclic monoid $P(\mathrm{X})$.*

PROOF. Note that for every $x, y \in \mathrm{X}$, $\alpha_x^{-1}\alpha_x = 1$ (identity map of $\mathrm{SIM}(\mathrm{Y}^{\mathbf{Z}})$) and $\alpha_x^{-1}\alpha_y = 0$ if $x \neq y$. It follows that every element of P_{X} is expressible in the form $\alpha_u\alpha_v^{-1}$ for some $u, v \in \mathrm{X}^*$. The element $\alpha_u\alpha_v^{-1}$ of P_{X} has as domain the set of all sequences $(x_n)_{n\in\mathbf{Z}}$ with $x_1 \dots x_k = u$ (some k) and has the effect of replacing the subword $x_1 \dots x_k = u$ of such a sequence by the subword v. It follows that if $u, v, s, t \in \mathrm{X}^*$ then $\alpha_u\alpha_v^{-1} = \alpha_s\alpha_t^{-1}$ iff $u = s$ and $v = t$. Hence every element of P_{X} is uniquely expressible in the form $\alpha_u\alpha_v^{-1}$ for some $u, v, \in \mathrm{X}^*$. From the description of the polycyclic monoid $P(\mathrm{X})$ given in section 1 it is now clear that the map $u^{-1}v \mapsto \alpha_{r(u)}\alpha_{r(u)}^{-1}$ is an isomorphism from $P(\mathrm{X})$ onto P_{X}. (Here $r(u)$ denotes the reverse of the word u: that is, if $u = x_1x_2 \dots x_k$ then $r(u) = x_k \dots x_2x_1$.)

Denote the set of idempotents of I_{X}, Q_{X} and P_{X} by EI_{X}, EQ_{X} and EP_{X} respectively. Note that EI_{X} and EP_{X} are semilattices and EQ_{X} is a semilattice and subalgebra of Q_{X} (since every automorphism preserves idempotents).

LEMMA 2.2. (a) *The semilattice* EP_{X} *consists of zero and all elements of the form* $\alpha_u\alpha_u^{-1}$ *for some* $u \in \mathrm{X}^*$; (b) *the semilattice* EI_{X} *is generated by the set* $\{\mathrm{T}^{-k}\alpha_x\alpha_x^{-1}\mathrm{T}^k : x \in \mathrm{X},\ k \in \mathbb{Z}\} \cup \{1\}$; (c) *the subalgebra* EQ_{X} *coincides with* EI_{X} *and is generated by the set* $\{\alpha_x\alpha_x^{-1} : x \in \mathrm{X}\} \cup \{1\}$.

PROOF. Part (a) is obvious from the description given in section 1 of the semilattice of idempotents of the polycyclic monoid. To prove part (b), suppose first that α is any element of I_{X} with $\alpha \neq 0$ and $\alpha \neq 1$. Then α must be expressible as a finite product of elements of the form $\mathrm{T}, \mathrm{T}^{-1}, \alpha_x$ and α_x^{-1} for $x \in \mathrm{X}$. Now $\mathrm{T}, \mathrm{T}^{-1}$ and α_x^{-1} all have domain $\mathrm{X}^{\mathbf{Z}}$ and α_x has domain consisting of all sequences $(x_n)_{n\in\mathbf{Z}}$ with $x_1 = x$. It follows that there must exist integers $i_1 < i_2 < \dots < i_k \in \mathbb{Z}$ and fixed elements $a_1, a_2, \dots, a_k \in \mathrm{X}$ such that $(x_n)_{n\in\mathbf{Z}}$ is in the domain of α if and only if $x_{i_t} = a_t$ for $1 \leq t \leq k$. Now if α is an idempotent of I_{X} then α must be the restriction of the identity map on $\mathrm{X}^{\mathbf{Z}}$ to its domain, so $\alpha = \beta_{i_1}\beta_{i_2} \dots \beta_{i_k}$ where β_{i_t} is the identity map on the set of sequences $(x_n)_{n\in\mathbf{Z}}$ with $x_{i_t} = a_t$ (for $1 \leq t \leq k$). Since $\beta_{i_t} = \mathrm{T}^{-i_t+1}\alpha_{a_t}\alpha_{a_t}^{-1}\mathrm{T}^{i_t-1}$ the result of part (b) follows. From part (b) it follows that $\mathrm{EI}_{\mathrm{X}} \subseteq \mathrm{EQ}_{\mathrm{X}}$: since the converse is

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

obvious it follows immediately that $\mathrm{EQ_X}$ is generated (as an algebra) by $\{\alpha_x\alpha_x^{-1} : x \in \mathrm{X}\} \cup \{1\}$.

LEMMA 2.3. *For all words* $u, v, s, t \in \mathrm{X}^*$, *all* $k \in \mathbb{Z}$ *and all integers* $l \geq 0$ *we have*

$$\alpha_u \mathrm{T}^{-l} \alpha_s\alpha_t^{-1} \mathrm{T}^l = \mathrm{T}^{-(l+|u|)} \alpha_s\alpha_t^{-1} \mathrm{T}^{(1+|u|)} \alpha_u \tag{1}$$

and hence

$$\begin{aligned}(\mathrm{T}^{-k} \alpha_u\alpha_v^{-1} \mathrm{T}^k)(\mathrm{T})^{(k+|v|+l)}\alpha_s\alpha_t^{-1} \mathrm{T}^{(k+|v|+l)}) \\ = (\mathrm{T}^{-(k+|u|+l)} \alpha_s\alpha_t^{-1} \mathrm{T}^{(k+|u|+l)})(\mathrm{T}^{-k} \alpha_u\alpha_v^{-1} \mathrm{T}^k).\end{aligned} \tag{2}$$

In particular,

$$\alpha_u\alpha_s\alpha_t^{-1} = \mathrm{T}^{-|u|} \alpha_s\alpha_t^{-1} \mathrm{T}^{|u|} \alpha_u. \tag{3}$$

PROOF. Let α (respectively β) denote the mapping on the left side (respectively right side) of equation (1). A sequence $(x_n)_{n\in\mathbf{Z}}$ is in the domain of α if and only if $x_1 \dots x_{|u|} = u$ and $x_{|u|+l+1} \cdots x_{|u|+l+|s|} = s$: similarly one checks that β has this domain. The effect of α when applied to such a sequence is to first erase the segment $x_1 \dots x_{|u|}$ and then replace the segment $x_{|u|+l+1} \cdots x_{|u|+l+|s|}$ by t, while β had the same effect, but in the opposite order. Hence $\alpha = \beta$. Clearly (3) follows from (1) with $l = 0$. To see that (2) also follows from (1) note first that, on replacing u by v and s by t in (1) and taking inverses, we have

$$\alpha_v^{-1} \mathrm{T}^{-(l+|v|)} \alpha_s\alpha_t \mathrm{T}^{(l+|v|)} = \mathrm{T}^{-l} \alpha_s\alpha_t^{-1} \mathrm{T}^l \alpha_v^{-1},$$

so

$$\begin{aligned}\alpha_u\alpha_v^{-1} \mathrm{T}^{-(l+|v|)} \alpha_s\alpha_t^{-1} \mathrm{T}^{(l+|v|)} &= \alpha_u \mathrm{T}^{-l} \alpha_s\alpha_t^{-1} \mathrm{T}^l \alpha_v^{-1} \\ &= \mathrm{T}^{-(l+|u|)} \alpha_s\alpha_t^{-1} \mathrm{T}^{(l+|u|)} \alpha_u\alpha_v^{-1}, \quad \text{by (1)}.\end{aligned}$$

Equation (2) follows immediately from this by premultiplying by T^{-k}, postmultiplying by T^k and noting that $\mathrm{T}^k\mathrm{T}^{-k} = 1$.

LEMMA 2.4. *For all words* $u, v, w \in \mathrm{X}^*$ *with* $|w| \geq 1$ *and for every positive integer* $k \leq |w|$ *we have*

$$\mathrm{T}^{-k} \alpha_u\alpha_v^{-1} \mathrm{T}^k \alpha_w = \alpha_{w(k)u}\alpha_{w(k)v}^{-1}\alpha_w; \tag{4}$$

$$\alpha_w^{-1} \mathrm{T}^{-k} \alpha_u\alpha_v^{-1} \mathrm{T}^k = \alpha_w^{-1}\alpha_{w(k)u}\alpha_{w(k)v}^{-1}, \tag{5}$$

where $w(k)$ *is the prefix of* w *of length* k.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

PROOF. Write w in the form $w = w(k)s$ for some $s \in X^*$. By Lemma 2.3, (3) we have

$$\begin{aligned} T^{-k}\alpha_u\alpha_v^{-1}T^k\alpha_{w(k)} &= \alpha_{w(k)}\alpha_u\alpha_v^{-1} \\ &= \alpha_{w(k)u}\alpha_v^{-1}. \end{aligned}$$

Hence

$$\begin{aligned} T^{-k}\alpha_u\alpha_v^{-1}T^k\alpha_w &= T^{-k}\alpha_u\alpha_v^{-1}T^k\alpha_{w(k)}\alpha_s \\ &= \alpha_{w(k)u}\alpha_v^{-1}\alpha_s \\ &= \alpha_{w(k)u}\alpha_v^{-1}\alpha_{w(k)}^{-1}\alpha_{w(k)}\alpha_s \\ &= \alpha_{w(k)u}\alpha_{w(k)v}^{-1}\alpha_w, \end{aligned}$$

so equality (4) is established. Of course equality (5) follows from equality (4) by interchanging u and v and taking inverses of both sides of the resulting equality.

If $p = \alpha_u\alpha_v^{-1} \in P_X$ for some words $u, v \in X^*$, it is convenient to denote $|v|$ by $|p|$ and $|u| - |v|$ by $d(p)$. We also use the notation $A + B$ to denote the join of A and B in the lattice of inverse submonoids of I_X. If $w = \dots x_{-1}x_0x_1\dots$ is an infinite word and k, l are integers, $k \le l$, then $w[k, l]$ will denote the word $x_k \dots x_l$.

LEMMA 2.5. (a) *Every element $q \in Q_X$ may be uniquely represented in the form*

$$q = T^{-k_1}p_1T^{k_1}T^{-k_2}p_2T^{k_2}\dots T^{-k_n}p_nT^{k_n} \tag{6}$$

for some integers $k_1, k_2, \dots, k_n$ and elements $p_1, \dots, p_n \in P_X\backslash\{1\}$ with $k_2 \ge k_1 + |p_1|$, $k_3 \ge k_2 + |p_2|, \dots, k_n \ge k_{n-1} + |p_{n-1}|$;

(b) *if an element q is represented in the form* (6) *then the domain of q consists of all infinite words w such that*

$$w[k_1 + m_1,\ k_1 + m_1 + |u_1|] = u_1, \quad w[k_2 + m_2,\ k_2 + m_2 + |u_2|] = u_2, \dots, \\ w[k_n + m_n,\ k_n + m_n + |u_n|] = u_n,$$

where m_n may be defined inductively by:

$$m_1 = 1, \dots, m_i = m_{i-1} + d(p_{i-1}), \quad i > 1, \tag{7}$$

and the effect of applying q to such a word is to replace each segment $w[k_i + m_i,\ k_i + m_i + |u_i|]$ by v_i for $i = 1, \dots, n$.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

(c) *if* $p_i = \alpha_{u_i}\alpha_{v_i}^{-1}$ *for some words* u_i, v_i $(i = 1, \dots, k)$, *then* $(\langle p_i : i = 1, 2, \dots, k\rangle + \langle T\rangle) \cap Q_X$ *consists of elements of the type*

$$\text{(8)} \qquad T^{-k_1} q_1 T^{k_1} T^{-k_2} q_2 T^{k_2} \dots T^{-k_n} q_n T^{k_n}$$

where each q_i *is a product of elements of the form* $\alpha_{wu}\alpha_{wv}^{-1}$ *or* $\alpha_{wv}\alpha_{wu}^{-1}$ *for some words* $u, v, w \in X^*$ *with* $(u, v) \in \{(u_j, v_j) : j = 1, \dots, k\}$ *and some integers* k_i *with* $k_{i+1} > k_i + |q_i|$ *for* $i = 1, \dots, n-1$.

PROOF. Using the definition of Q_X and the fact that $TT^{-1} = T^{-1}T = 1$, it is easy to see that every element $q \in Q_X$ may be written in the form $q = T^{-k_1} p_1 T^{k_1} T^{-k_2} p_2 T^{k_2} \dots T^{-k_n} p_n T^{k_n}$ for some integers k_i and elements p_i of P_X. Successive application of equalities (2) of Lemma 2.3 and (4) of Lemma 2.4 then enables us to rewrite the product for q above in such a way that we may assume that $k_1 < k_2 < \cdots < k_n$. Now write $p_i = \alpha_{u_i}\alpha_{v_i}^{-1}$ for some words $u_i, v_i \in X^*$ and let $l_i = k_{i+1} - k_i$ (so that each $l_i > 0$). Thus

$$q = T^{-k_1} \alpha_{u_1}\alpha_{v_1}^{-1} T^{-l_1} \alpha_{u_2}\alpha_{v_2}^{-1} T^{-l_2} \alpha_{u_3}\alpha_{v_3}^{-1} \dots T^{-l_{n-1}} \alpha_{u_n}\alpha_{v_n}^{-1} T^{k_n}.$$

If $l_1 \le |v_1| = |p_1|$ we may rewrite this as

$$q = T^{-k_1} \alpha_{u_1}\alpha_{v_1}^{-1} T^{-l_1} \alpha_{u_2}\alpha_{v_2}^{-1} T^{-(l_1+l_2)} \alpha_{u_3}\alpha_{v_3}^{-1} \dots \alpha_{u_n}\alpha_{v_n}^{-1} T^{k_n}$$

and we may apply equality (5) (Lemma 2.4) to obtain

$$q = T^{-k_1} \alpha_{u_1}\alpha_{v_1}^{-1} \alpha_{v_1(l_1)u_2}\alpha_{v_1(l_1)v_2}^{-1} T^{-(l_1+l_2)} \alpha_{u_3}\alpha_{v_3}^{-1} \dots \alpha_{u_n}\alpha_{v_n}^{-1} T^{k_n}.$$

Similar reductions occur if $l_i \le |v_i| = |p_i|$ (for $1 < i < n$). Then by induction on n we obtain (6). Equality (8) also follows from the above proof.

Condition (b) is an immediate consequence of the definition of the semigroup I_X. Notice that the replacements that are described in condition (b) are independent. Indeed by (6) we have

$$\begin{aligned}(k_{i+1} + m_{i+1}) - (k_i + m_i + |u_i|) &= k_{i+1} - k_i + m_{i+1} - m_i - |u_i| \\ &= k_{i+1} - k_i - |v_i| > 0.\end{aligned}$$

This means that each replacement does not change the segment we obtain as a result of any other replacement. This gives us the uniqueness of the representation (6).

The preceding results enable us to give a presentation for the semigroup I_X. We denote by $\mathrm{Inv}\langle X : R\rangle$ the *inverse* monoid presented by a set X of generators and a set R of relations. Thus we may think of R as a subset of $(X \cup X^{-1})^* \times (X \cup X^{-1})^*$ where X^{-1} is a set in one-one correspondence

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

with X (and disjoint from X) and $\mathrm{Inv}\langle X : R\rangle = (X \cup X^{-1})^*/\tau$, where τ is the congruence on $(X \cup X^{-1})^*$ generated by $\rho \cup R$. (Here ρ is the Vagner congruence on $(X \cup X^{-1})^*$ – see Petrich [8].) Presentations of inverse monoids have received considerable recent attention in the literature - see for example the papers of Stephen [10] and Margolis and Meakin [4].

THEOREM 2.6. (a) *The semigroup* P_X *admits a presentation of the form* $P_X = \mathrm{Inv}\langle \tilde{X} : R_1\rangle$ *where* $\tilde{X} = \{\alpha_x : x \in X\}$ *and* R_1 *consists of the relations* $\alpha_x^{-1}\alpha_x = 1$, $\alpha_x^{-1}\alpha_y = 0$ *for* $x, y \in X$, $x \neq y$.

(b) *The semigroup* I_X *is a semidirect product of* Q_X *and* $\mathbf{Z}$ (*the group of integers*).

(c) *The semigroup* I_X *admits a presentation of the form* $I_X = \mathrm{Inv}\langle \tilde{X} \cup \{T\} : R_2\rangle$ *where* $R_2 = R_1 \cup R_T \cup R_C$, $R_T = \{(TT^{-1}, 1), (T^{-1}T, 1)\}$ *and* R_C *consists of all relations listed in equation* (1), (*Lemma* 2.3).

PROOF. Part (a) was already established in Lemma 2.1. To prove part (b) note first that application of the relations $TT^{-1} = T^{-1}T = 1$ easily enables us to represent every element $y \in I_X$ in the form $y = qT^k$ for some $q \in Q_X$, $k \in \mathbf{Z}$. If $q_1T^{k_1} = q_2T^{k_2}$ for some $q_1, q_2 \in Q_X$ and $k_1, k_2 \in \mathbf{Z}$ then $q_1T^{k_1-k_2} = q_2$. We prove that $q_1 = q_2$ and $k_1 = k_2$. This will in particular provide a justification for the remark made immediately after the definition of Q_X, namely that an element y of I_X is in Q_X only if the sum of powers of T involved in the expression for y, as a product of powers of T and the $\alpha_x (x \in X)$, is zero. Represent q_1 and q_2 in the forms

$$q_1 = T^{-k_1}\alpha_{u_1}\alpha_{v_1}^{-1}T^{k_1}\dots T^{-k_n}\alpha_{u_n}\alpha_{v_n}^{-1}T^{k_n}$$

and

$$q_2 = T^{-l_1}\alpha_{s_1}\alpha_{t_1}^{-1}T^{l_1}\dots T^{-l_m}\alpha_{s_m}\alpha_{t_m}^{-1}T^{l_m}$$

as in equation (6). Then q_1, q_2 and $q_1T^{k_1-k_2}$ all have the same domains, so $m = n$, $k_i = l_i$ and $u_i = s_i$ for all i. The effect of applying q_1 (respectively q_2) to a sequence $\underline{x} = (x_n)_{n\in\mathbf{Z}}$ in this domain is to replace various segments of $\underline{x}$ as specified in Lemma 2.5(b), while $T^{k_1-k_2}$ translates $\underline{x}q_i$ by $(k_1 - k_2)$ spaces to the right. Since $q_1T^{k_1-k_2} = q_2$, this forces $k_1 - k_2 = 0$, so $k_1 = k_2$, whence $q_1 = q_2$ and the representation of $y \in I_X$ in the form qT^k is unique. It is now easy to see that I_X is isomorphic to the semidirect product of Q_X and $\langle T\rangle \cong \mathbf{Z}$ defined by the action $T^k \cdot q = T^k q T^{-k}$ of $\langle T\rangle$ on Q_X.

To prove part (c), let $Y = \tilde{X} \cup \{T\}$ and let τ_1 be the congruence on $(Y \cup Y^{-1})^*$ generated by $\rho \cup R_2$. Then $\mathrm{Inv}\langle \tilde{X} \cup \{T\} : R_2\rangle = (Y \cup Y^{-1})^*/\tau_1$,

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

and since I_X satisfies all the relations in R_2 we may write $I_X \cong (Y \cup Y^{-1})^*/\tau_2$ for some congruence τ_2 on $(Y \cup Y^{-1})^*$ with $\tau_1 \subseteq \tau_2$. If q is a word in $(Y \cup Y^{-1})^*$ for which the sum of powers of T occurring in q is zero, then the proofs of Lemmas 2.3, 2.4 and 2.5 show that application of the relations R_2 alone reduces q to a form as represented in the right-hand side of equation (6). Thus every element $y \in (Y \cup Y^{-1})^*$ is τ_1-related to a word of the form qT^k where q is represented as in the right-hand side of equation (6). If $(q_1 T^{k_1})\tau_1(q_2 T^{k_2})$, then $(q_1 T^{k_1})\tau_2(q_2 T^{k_2})$ so by the proof of part (b) of the present theorem and part (a) of Lemma 2.5 we see that $k_1 = k_2$ and $q_1 = q_2$, so each τ_1-class has a unique representative of the form qT^k (with q represented as in the right-hand side of (6)). Since each τ_2-class has a unique representative of the same form it easily follows that $\tau_1 = \tau_2$. Hence $I_X \cong \mathrm{Inv}\langle \tilde{X} \cup \{T\} : R_2 \rangle$.

We close this section by recording another structural property of the semigroups P_X, I_X and Q_X. We define an inverse semigroup S with zero 0 to be *0-E-unitary* if $E(S) - \{0\}$ is a unitary subset of S: that is if $e^2 = e$, $ex \neq 0$ and $(ex)^2 = ex$ for some e, $x \in S$, then $x^2 = x$. (Here, as usual, $E(S)$ denotes the semilattice of idempotents of S).

PROPOSITION 2.7. *The semigroups P_X, I_X and Q_X are 0-E-unitary inverse monoids.*

PROOF. This result is well-known (and easy to prove) for the polycyclic monoid, and hence for P_X. Let $\alpha = \alpha^2 \in I_X$ and $\gamma \in I_X$. From (the proofs of) Lemmas 2.2 and 2.6 we may write

$$\gamma = T^{-k_1} \alpha_{u_1} \alpha_{v_1}^{-1} T^{k_1} T^{-k_2} \alpha_{u_2} \alpha_{v_2}^{-1} T^{k_2} \ldots T^{-k_m} \alpha_{u_m} \alpha_{v_m}^{-1} T^{k_m} T^k$$

(where the k_i satisfy the constraints of equality (6)) and $\alpha = \beta_{i_1} \beta_{i_2} \ldots \beta_{i_k}$ where β_{i_t} is the identity map on the set of sequences $(x_n)_{n \in \mathbf{Z}}$ with $x_{i_t} = a_t$ (a fixed element of X) for each t. Now $\alpha\gamma$ is the restriction of γ to the intersection of the domain of α with the domain of γ, so by Lemma 2.5(b), its domain consists of all those sequences w with $w[k_i + m_i, k_i + m_i + |u_i|] = u_i$, $x_{i_t} = a_t$ (for $i = 1, \ldots, m$ and $t = 1, \ldots, k$). If $\alpha\gamma$ is a non-zero idempotent of I_X then $\alpha\gamma$ must be the identity map on its domain so $v_i = u_i$ for $i = 1, \ldots, m$ and so γ is also an idempotent of I_X. Hence I_X is 0-E-unitary. From this and the fact that $EI_X = EQ_X$ it follows that Q_X is 0-E-unitary.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

3. Correspondence between semigroups and inverse semigroups

For every relation $\Sigma = \{(u_i, v_i) : i \in I\} \subseteq \mathrm{X}^* \times \mathrm{X}^*$ on the free monoid X^* define

$$\begin{aligned} I(\Sigma) &= \langle \alpha_{u_i}\alpha_{v_i}^{-1}, \mathrm{T} : i \in I\rangle + \mathrm{E}I_{\mathrm{X}} \leq I_{\mathrm{X}}; \\ P(\Sigma) &= I(\Sigma) \cap P_{\mathrm{X}}; \\ Q(\Sigma) &= I(\Sigma) \cap Q_{\mathrm{X}}. \end{aligned}$$

Thus $I(\Sigma)$, $P(\Sigma)$ and $Q(\Sigma)$ are all inverse submonoids of I_{X}. (Here, as before, $+$ denotes join in the lattice of inverse submonoids of I_{X}). In the present section we show that the map $\Sigma \to P(\Sigma)$ sets up an isomorphism from the lattice of congruences on X^* onto a certain sublattice of the lattice of inverse submonoids of P_{X}. We first need one preliminary concept.

The set $P_{\mathrm{X}}^+ = \{\alpha_u : u \in \mathrm{X}^*\}$ is a submonoid of P_{X} isomorphic to the free monoid X^*: elements of P_{X}^+ will be called *positive* elements of P_{X} in this paper (although some readers may prefer to label such elements "negative" in view of the isomorphism developed in Lemma 2.1 between P_{X} and the polycyclic monoid). An inverse submonoid R of P_{X} will be called a *positively self-conjugate* (PSC) submonoid of P_{X} if $p\mathrm{R}p^{-1} \subseteq \mathrm{R}$ for every positive element $p \in P_{\mathrm{X}}^+$.

LEMMA 3.1. *Let* R *be a* PSC *submonoid of* P_{X}. *Then*

(a) R *is a full inverse submonoid of* P_{X} (*that is* $\mathrm{E}P_{\mathrm{X}} \subseteq \mathrm{R}$);

(b) *if* $\alpha_u\alpha_v^{-1} \in \mathrm{R}$ *and* $w \in \mathrm{X}^*$ *then* $\alpha_{wu}\alpha_{wv}^{-1}, \alpha_{uw}\alpha_{vw}^{-1} \in \mathrm{R}$.

PROOF. To prove part (a) note that since $1 \in \mathrm{R}$ we have $\alpha_u\alpha_u^{-1} = \alpha_u 1 \alpha_u^{-1} \in \mathrm{R}$ for all $u \in \mathrm{X}^*$, so the result follows from Lemma 2.2(a). To prove part (b) note first that $\alpha_{wu}\alpha_{wv}^{-1} = \alpha_w\alpha_u\alpha_v^{-1}\alpha_w^{-1} \in \mathrm{R}$ by the definition of PSC submonoid, while

$$\begin{aligned} \alpha_{uw}\alpha_{vw}^{-1} = \alpha_u\alpha_w\alpha_w^{-1}\alpha_v^{-1} &= \alpha_u\alpha_w\alpha_w^{-1}\alpha_v^{-1}\alpha_v\alpha_v^{-1} \\ &= \alpha_u\alpha_v^{-1}\alpha_v\alpha_w\alpha_w^{-1}\alpha_v^{-1} \\ &= \alpha_u\alpha_v^{-1}\alpha_{vw}\alpha_{vw}^{-1} \in \mathrm{R} \quad \text{by part (a)}. \end{aligned}$$

LEMMA 3.2. *If* R *is a* PSC *submonoid of* P_{X} *then in* I_{X} *we have* $\mathrm{R} = (\mathrm{R} + \langle\mathrm{T}\rangle + \mathrm{E}I_{\mathrm{X}}) \cap P_{\mathrm{X}}$.

PROOF. We need only prove that $(\mathrm{R} + \langle\mathrm{T}\rangle + \mathrm{E}I_{\mathrm{X}}) \cap P_{\mathrm{X}} \subseteq \mathrm{R}$. Notice first that $\mathrm{E}P_{\mathrm{X}} \subseteq \mathrm{R}$ by Lemma 3.1. From Lemma 2.2 it is clear that $\mathrm{E}I_{\mathrm{X}} \subseteq$

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

$\mathrm{EP_X} + \langle \mathrm{T} \rangle$, so it suffices to prove that $\mathrm{R} = (\mathrm{R} + \langle \mathrm{T} \rangle) \cap P_{\mathrm{X}}$. By Lemma 2.5(b) and Lemma 3.1(b), every element of $(\mathrm{R} + \langle \mathrm{T} \rangle) \cap Q_{\mathrm{X}}$ can be represented in the form $\mathrm{T}^{-k_1} q_1 \mathrm{T}^{k_1} \mathrm{T}^{-k_2} q_2 \mathrm{T}^{k_2} \ldots \mathrm{T}^{-k_m} q_m \mathrm{T}^{k_m}$ where $k_{i+1} > k_i + |q_i|$ for $i = 1, \ldots, m-1$ and $q_i \in \mathrm{R}$. By the uniqueness of this representation, such an element is in P_{X} if and only if $k_1 = 0$ and $m = 1$. Thus, if such an element belongs to P_{X} it also belongs to R.

PROPOSITION 3.3. *If Σ is a relation on the free monoid X^* then $P(\Sigma)$ is a* PSC *submonoid of P_{X}. Conversely, if* R *is a* PSC *submonoid of P_{X} then there is some relation Σ on X^* (in fact, some congruence Σ on X^*) such that* $\mathrm{R} = P(\Sigma)$.

PROOF. Let $\Sigma = \{(u_i, v_i) : i \in I\}$ be a relation on X^*. Note that equation (3) (Lemma 2.3) implies that $\alpha_u p \alpha_u^{-1} = \mathrm{T}^{-|u|} p \mathrm{T}^{|u|} \alpha_u \alpha_u^{-1}$ for all words $u \in \mathrm{X}^*$ and all $p \in P_{\mathrm{X}}$. If $p \in P(\Sigma)$ then p is a product of elements in $\mathrm{EI_X}$ and elements in $I(\Sigma)$, each of which is a product of powers of T and elements of the form $\alpha_{u_i} \alpha_{v_i}^{-1}$, $i \in I$. It follows that $\mathrm{T}^{-|u|} p \mathrm{T}^{|u|}$ is of the same form and hence $\alpha_u p \alpha_u^{-1} \in I(\Sigma) \cap P_{\mathrm{X}} = P(\Sigma)$. So $P(\Sigma)$ is a PSC submonoid of P_{X}.

Conversely, let R be a PSC submonoid of P_{X}. Define a relation Σ' on X^* by

$$(8) \qquad (u, v) \in \Sigma' \quad \text{if and only if } \alpha_u \alpha_v^{-1} \in \mathrm{R}.$$

It is clear from Lemma 3.1 that Σ' is a congruence on X^*. Now $I(\Sigma') = \langle \{\alpha_u \alpha_v^{-1} : (u, v) \in \Sigma'\} \rangle + \mathrm{EI_X} + \langle \mathrm{T} \rangle = \mathrm{R} + \langle \mathrm{T} \rangle$, so $P(\Sigma') = (\mathrm{R} + \langle \mathrm{T} \rangle) \cap P_{\mathrm{X}} = \mathrm{R}$, by Lemma 3.2.

The main result of the paper is the following.

THEOREM 3.4. *Let Σ be a relation on the free monoid X^* and let Σ^c denote the congruence on X^* generated by Σ. Then*

(a) *for all $u, v \in \mathrm{X}^*$ we have $(u, v) \in \Sigma^c$ if and only if $\alpha_u \alpha_v^{-1} \in P(\Sigma)$;*

(b) $P(\Sigma) = P(\Sigma^c)$;

(c) *the correspondence $\Sigma^c \to P(\Sigma)$ is an isomorphism between the lattice of congruences on X^* and the lattice of* PSC *submonoids of P_{X}.*

PROOF. To prove part (a), suppose first that $(s, t) \in \Sigma$ and $w = psq$,

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

$z = ptq$ for some $p, q \in \mathrm{X}^*$. Then

$$\begin{aligned}\alpha_w\alpha_z^{-1} &= \alpha_{psq}\alpha_{ptq}^{-1} = \alpha_p\alpha_s\alpha_q\alpha_q^{-1}\alpha_t^{-1}\alpha_p^{-1} \\ &= \mathrm{T}^{-|ps|}\alpha_q\alpha_q^{-1}\mathrm{T}^{|ps|}\alpha_p\alpha_s\alpha_t^{-1}\alpha_p^{-1} \quad \text{(by equation (3))} \\ &= \mathrm{T}^{-|ps|}\alpha_q\alpha_q^{-1}\mathrm{T}^{|ps|}\mathrm{T}^{-|p|}\alpha_s\alpha_t^{-1}\mathrm{T}^{|p|}\alpha_p\alpha_p^{-1} \quad \text{(by equation (3))} \\ &\in I(\Sigma).\end{aligned}$$

Also, $\alpha_w\alpha_z^{-1} \in P_{\mathrm{X}}$, so $\alpha_w\alpha_z^{-1} \in P(\Sigma)$. Suppose now that $u = v$ is a consequence of the relations Σ (that is, $(u, v) \in \Sigma^c$). Then there exists a sequence of words $u = w_1, w_2, \dots, w_n = v$ such that $w_i = p_is_iq_i$ and $w_{i+1} = p_it_iq_i$ for some words p_i, s_i, q_i, t_i with $(s_i, t_i) \in \Sigma$ and $i = 1, \dots, n-1$. Then by what was just proved, $\alpha_{w_i}\alpha_{w_{i+1}}^{-1} \in P(\Sigma)$ for $i = 1, \dots, n-1$. It follows that

$$\alpha_u\alpha_v^{-1} = \alpha_{w_1}\alpha_{w_2}^{-1}\alpha_{w_2}\alpha_{w_3}^{-1}\dots\alpha_{w_{n-1}}\alpha_{w_n}^{-1} \in P(\Sigma).$$

Suppose conversely that $\alpha_u\alpha_v^{-1} \in P(\Sigma)$. Then $\alpha_u\alpha_v^{-1} \in Q(\Sigma) + \mathrm{EQ}_{\mathrm{X}}$, so $\alpha_u\alpha_v^{-1}$ can be written as a product of elements in $Q(\Sigma)$ and idempotents of I_{X}. Using Lemma 2.2(b) and the fact that $Q(\Sigma) = (\langle\{\alpha_s\alpha_t^{-1} : (s, t) \in \Sigma\}\rangle + \langle\mathrm{T}\rangle + \mathrm{EI}_{\mathrm{X}}) \cap Q_{\mathrm{X}}$, we may write $\alpha_u\alpha_v^{-1}$ (not necessarily uniquely) as a product of the form $\alpha_u\alpha_v^{-1} = q_1q_2\dots q_m$ where $q_i = \mathrm{T}^{-k_i}\alpha_{s_i}\alpha_{t_i}^{-1}\mathrm{T}^{k_i}$ for some $k_i \in \mathbf{Z}$ and $(s_it_i) \in \Sigma \cup \Sigma^{-1} \cup \{i_{\mathrm{X}}\}$. (Here i_{X} denotes the identity map on X and $\Sigma^{-1} = \{(s, t) : (t, s) \in \Sigma\}$.) Now $\mathrm{Dom}(q_i)$ consists of those sequences $(x_n)_{n\in\mathbf{Z}}$ with $x_{k_i+1}\dots x_{k_i+|s_i|} = s_i$ and $\mathrm{Dom}(\alpha_u\alpha_v^{-1})$ consists of those sequences within $x_1\dots x_{|u|} = u$. Since $\alpha_u\alpha_v^{-1} = q_1(q_2\dots q_m)$ and $\mathrm{Dom}(q_1\dots q_m) \subseteq \mathrm{Dom}\, q_1$ we must have $u = a_1s_1b_1$ for some $a_1, b_1 \in \mathrm{X}^*$. The effect of applying q_1 to a sequence in its domain is to replace $x_1\dots x_{|u|} = a_1s_1b_1$ by $a_1t_1b_1$. Again, since $\mathrm{Dom}(q_1q_2\dots q_m) \subseteq \mathrm{Dom}(q_1q_2)$ we must have $a_1t_1b_1 = a_2s_2b_2$ for some $a_2, b_2 \in \mathrm{X}^*$. Continuing in this manner (by induction on m) and using the fact that $q_1q_2\dots q_m = \alpha_u\alpha_v^{-1}$, we obtain $u = a_1s_1b_1$, $a_1t_1b_1 = a_2s_2b_2$, $a_2t_2b_2 = a_3s_3b_3, \dots, a_{m-1}t_{m-1}b_{m-1} = a_mt_mb_m = v$, for some $a_i, b_i \in \mathrm{X}^*$. It follows that $(u, v) \in \Sigma^c$ (that is, $u = v$ is a consequence of the relations Σ). This proves part (a). Note also that $\Sigma^c = \Sigma'$, the congruence defined by equality (8) with $\mathrm{R} = P(\Sigma)$. It is clear that $P(\Sigma) \subseteq P(\Sigma^c)$ since $\Sigma \subseteq \Sigma^c$. Conversely, if $\alpha_u\alpha_v^{-1} \in P(\Sigma^c)$ then $(u, v) \in (\Sigma^c)^c = \Sigma^c$, so by part (a), $\alpha_u\alpha_v^{-1} \in P(\Sigma)$. Hence $P(\Sigma^c) \subseteq P(\Sigma)$ and part (b) is proved.

Suppose now that $P(\Sigma_1) = P(\Sigma_2)$ for some congruences Σ_1, Σ_2 on X^*. Then if $(u, v) \in \Sigma_1$ we have $\alpha_u\alpha_v^{-1} \in P(\Sigma_1) = P(\Sigma_2)$ by part (a), so $(u, v) \in$

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

Σ_2, again by part (a). Hence $\Sigma_1 \subseteq \Sigma_2$ and dually $\Sigma_2 \subseteq \Sigma_1$. It follows by Proposition 3.3 that the map $\Sigma \to P(\Sigma)$ is a one-one map from the lattice of congruences on X^* onto the lattice of PSC submonoids of P_X. Again, a routine argument using part (a) shows that, for all congruences Σ_1, Σ_2 on X^*, $P(\Sigma_1 \cap \Sigma_2) = P(\Sigma_1) \cap P(\Sigma_2)$ and $P(\Sigma_1 + \Sigma_2) = P(\Sigma_1) + P(\Sigma_2)$, so the map $\Sigma \to P(\Sigma)$ above is a lattice isomorphism. This proves part (c).

The following result was obtained by the authors for free monoids. Francis Pastijn noticed that it is true for arbitrary finitely generated monoids.

Corollary 3.5. *The congruence lattice of every finitely generated monoid is isomorphic to a subalgebra lattice of some finitely generated algebra of finite type.*

Proof. If M is a finitely generated monoid, then $M = X^*/\Sigma$, for some finite set X and some congruence Σ on X^*. The congruence lattice on M is isomorphic to the lattice of congruences on X^* containing Σ. By Theorem 3.4 this lattice is isomorphic to the lattice of PSC submonoids of P_X containing $P(\Sigma)$. We shall introduce the following new unary operations on the inverse monoid P_X:

(i) the unary operations $\overline{\alpha}_x$, $x \in X$, where $\overline{\alpha}_x(p) = \alpha_x p \alpha_x^{-1}$ for all $p \in P_X$;

(ii) the unary operation α, such that $\alpha: p \to \alpha(p)$ is a permutation of P_X whose only nontrivial orbit is $P(\Sigma)$;

(iii) the unary operation β, such that $\beta: p \to \beta(p)$ is the inverse of α.

We observe that 1 belongs to every subalgebra of P_X and that $P(\Sigma)$ is the least subalgebra of P_X. In fact, the subalgebras of P_X are precisely the PSC submonoids containing $P(\Sigma)$. Thus the lattice of congruences of M is isomorphic to the lattice of submonoids of the monoid P_X with additional unary operations.

Remark 3.6. From an old result of Hanf (see [11] for an exposition of this) it follows that the congruence lattice of any finitely generated algebra A with finitely many operations is isomorphic to a subalgebra lattice of some finitely generated Moufang loop. This result is more general than Corollary 3.5. Nevertheless we included Corollary 3.5 in our paper because in order to construct the loop in Hanf's proof one needs the lattice of congruences of A, whereas one needs only the defining relations of A to construct our algebra P_X. Among the new operations of $P(\Sigma)$ only one is not polynomial. Notice that in the group case the lattice of congruences of every finitely generated group $A = \langle X \rangle$ is isomorphic to the lattice of subalgebras of the group A with

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

additional unary operations α_x which provide conjugations by x, $x \in \mathrm{X}$. This observation allows us to formulate the following.

Problem 3.7. Is it possible to associate with every finitely generated monoid $\mathrm{A} = \langle \mathrm{X} \rangle$ an inverse monoid $\mathrm{B} = \langle \mathrm{X} \rangle$ in such a way that the congruence lattice of A is isomorphic to a subalgebra lattice of the monoid B with additional unary operations α_x which provide conjugations by x, $x \in \mathrm{X}$?

Theorem 3.4 presents a solution to this problem in the case of free monoids.

4. Connections with other problems

Theorem 3.4 enables us to translate many important decision problems and properties of arbitrary monoids into equivalent problems and properties of inverse submonoids of the polycyclic monoid. In this section we provide a few remarks and observations along these lines. We first indicate how several standard properties of monoids may be reformulated. The notation is as in Section 3.

Proposition 4.1. *The monoid $I(\Sigma)$ (respectively $Q(\Sigma)$) is finitely generated if and only if all relations in Σ are consequences of a finite subset of the relations in Σ (that is, $\Sigma^c = \Sigma_1^c$ for some finite set $\Sigma_1 \subseteq \Sigma$).*

Proof. Suppose first that $I(\Sigma) = \langle\{\alpha_u\alpha_v^{-1} : (u, v) \in \Sigma\}\rangle + \langle \mathrm{T} \rangle$ is finitely generated. Then there is a finite set $\{q_1, q_2, \dots, q_n\}$ of generators for $I(\Sigma)$, each of which is a product of a (finite) number of powers of T and elements of the form $\alpha_s\alpha_t^{-1}$ for some $(s, t) \in \Sigma \cap \Sigma^{-1}$. So there is a finite set $\Sigma_1 \subseteq \Sigma$ such that $I(\Sigma) = \langle\{\alpha_s\alpha_t^{-1} : (s, t) \in \Sigma_1\}\rangle + \mathrm{EI}_{\mathrm{X}} + \langle \mathrm{T} \rangle = I(\Sigma_1)$. It follows that $P(\Sigma) = P(\Sigma_1)$ and hence by Theorem 3.4 that $\Sigma^c = \Sigma_1^c$.

Conversely suppose that $\Sigma^c = \Sigma_1^c$ for some finite set $\Sigma_1 \subseteq \Sigma$. By Theorem 3.4 we have $P(\Sigma) = P(\Sigma_1)$, whence $I(\Sigma) \cap P_{\mathrm{X}} = I(\Sigma_1) \cap P_{\mathrm{X}}$. Thus if $(u, v) \in \Sigma$ then $\alpha_u\alpha_v^{-1} \in I(\Sigma) \cap P_{\mathrm{X}}$, so $\alpha_u\alpha_v^{-1} \in I(\Sigma_1)$. It follows that $I(\Sigma) = \langle\alpha_u\alpha_v^{-1} : (u, v) \in \Sigma\}\rangle + \mathrm{EI}_{\mathrm{X}} + \langle \mathrm{T} \rangle \subseteq I(\Sigma_1)$, whence $I(\Sigma) = I(\Sigma_1)$, and $I(\Sigma)$ is finitely generated.

The statements about the semigroup $Q(\Sigma)$ follow from those about $I(\Sigma)$. Indeed, if $Q(\Sigma)$ is finitely generated (as an inverse monoid with additional unary operation T) then $I(\Sigma)$ is finitely generated as an inverse semigroup and so $\Sigma^c = \Sigma_1^c$ for some finite subset Σ_1 of Σ. Conversely, if $\Sigma^c = \Sigma_1^c$ with finite $\Sigma_1 \subseteq \Sigma$, then $I(\Sigma) = I(\Sigma_1)$ and so $Q(\Sigma) = I(\Sigma) \cap Q_{\mathrm{X}} = I(\Sigma_1) \cap Q_{\mathrm{X}} = Q(\Sigma)$.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

Remark 4.2. Theorem 3.4 provides us with an analogue, for arbitrary congruences on the free monoid X^*, of the classical coset decomposition of a group relative to a subgroup. Let Σ be a relation on X^* and $P(\Sigma)$ the associated PSC submonoid of P_X. A subset of P_X^+ of the form $P(\Sigma)\alpha_u \cap P_X^+$ for some $u \in X^*$ will be called a (*right*) coset of $P(\Sigma)$ in P_X^+. From Theorem 3.4 it is clear that if u and v are any words in X^* then $(u, v) \in \Sigma^c$ iff $\alpha_u\alpha_v^{-1} \in P(\Sigma)$ iff $P(\Sigma)\alpha_u = P(\Sigma)\alpha_v$ and that the Σ^c-class $[u]$ containing u is given by $[u] = \{v \in X^* : \alpha_v \in P(\Sigma)\alpha_u\}$. It follows that P_X^+ decomposes as a disjoint union of right cosets of $P(\Sigma)$ in the usual way. The map $[u] \to P(\Sigma)\alpha_u \cap P_X^+$ is a well-defined bijection from the set of Σ^c-classes of X^* onto the set of right cosets of $P(\Sigma)$ in P_X^+. Since $P(\Sigma)$ is a PSC-submonoid of P_X, $\alpha_u P(\Sigma)\alpha_u^{-1} \subseteq P(\Sigma)$ and so $\alpha_u P(\Sigma) \subseteq P(\Sigma)\alpha_u$ for all $u \in X^*$. It follows that $P(\Sigma)\alpha_u P(\Sigma)\alpha_v \subseteq P(\Sigma)P(\Sigma)\alpha_u\alpha_v = P(\Sigma)\alpha_u\alpha_v$ for all $u, v \in X^*$, so the right cosets of $P(\Sigma)$ in P_X^+ form a monoid in the obvious way and the map $[u] \to P(\Sigma)\alpha_u \cap P_X^+$ is an isomorphism of $M_\Sigma = \mathrm{Mon}\langle X : \Sigma\rangle$ onto the monoid of right cosets of $P(\Sigma)$ in P_X^+. The cardinality of the set of right cosets of $P(\Sigma)$ in P_X^+ will be called the *index* of $P(\Sigma)$ in P_X^+. It is clear from the above that $M_\Sigma = \mathrm{Mon}\langle X : \Sigma\rangle$ is finite if and only if $P(\Sigma)$ has finite index in P_X^+.

Proposition 4.3. *Let* Σ *be a relation on* X^* *and* $M_\Sigma = \mathrm{Mon}\langle X : \Sigma\rangle$. *Then*

(a) M_Σ *is left cancellative if and only if* $pP(\Sigma)p^{-1} \subseteq P(\Sigma)$ *for all* $p \in P_X$;
(b) M_Σ *is right cancellative if and only if* $P(\Sigma) - \{0\}$ *is a unitary subset of* P_X.

Proof. By Theorem 3.4 it follows that M_Σ is left cancellative if

$$\alpha_u\alpha_s\alpha_t^{-1}\alpha_u^{-1} \in P(\Sigma) \quad \text{implies } \alpha_s\alpha_t^{-1} \in P(\Sigma).$$

Since $\alpha_u^{-1}\alpha_u = 1$, it is clear that this implication holds if $pP(\Sigma)p^{-1} \subseteq P(\Sigma)$ for all $p \in P_X$. Suppose on the other hand that M_Σ is left cancellative, $\alpha_s\alpha_t^{-1} \in P(\Sigma)$ and $v \in X^*$. In order to show that $pP(\Sigma)p^{-1} \subseteq P(\Sigma)$ for all $p \in P_X$, it clearly suffices to show that $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v \in P(\Sigma)$, since $P(\Sigma)$ is a PSC submonoid of P_X. It is clear that $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v \in P(\Sigma)$ if $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v = 0$, so suppose that $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v \neq 0$. There are several cases to consider. If $|v| \leq |s|$ and $|v| \leq |t|$, then $s = vw$ and $t = vu$ for some $w, u \in X^*$, so $\alpha_s\alpha_t^{-1} = \alpha_v\alpha_w\alpha_u^{-1}\alpha_v^{-1} \in P(\Sigma)$, and $(vw, vu) \in \Sigma^c$, and hence $(w, u) \in \Sigma^c$ by left cancellation, that is, $\alpha_w\alpha_u^{-1} \in P(\Sigma)$. Thus in this case, $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v = \alpha_w\alpha_u^{-1} \in P(\Sigma)$, as required. If $|v| \geq |s|$ and $|v| \geq |t|$, then $v = sw = tu$

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

for some w, $u \in X^*$, so $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v = \alpha_w^{-1}\alpha_u \neq 0$. Hence we must have either $u = wp$ or $w = up$ for some $p \in X^*$. Suppose that $u = wp$, some $p \in X^*$, so that $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v = \alpha_p$. Now $v = sw = twp$, so $(sw, twp) \in \Sigma^c$. Also, $(s, t) \in \Sigma^c$, so $(sw, tw) \in \Sigma^c$. Since M_Σ is left cancellative this implies that $(1, p) \in \Sigma^c$, so $\alpha_p \in P(\Sigma)$. The case $w = up$ is similar. Hence $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v \in P(\Sigma)$ in this case as well. Suppose next that $|v| \leq |s|$ and $|v| \geq |t|$, so that $s = vw$ and $v = tu$ for some $u, w \in X^*$. Then $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v = \alpha_w\alpha_u$. Since $(s, t) = \Sigma^c$ we have $(tuw, t) \in \Sigma^c$, so $(uw, 1) \in \Sigma$, by left cancellativity of M_Σ. Thus $(wuwu, wu) \in \Sigma^c$ and so $(wu, 1) \in \Sigma^c$, again by left cancellation. This implies that $\alpha_w\alpha_u \in P(\Sigma)$, so again, $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v \in P(\Sigma)$ in this case. The final case ($|v| \geq |s|$, $|v| \leq |t|$) is handled in a similar fashion, so $\alpha_v^{-1}\alpha_s\alpha_t^{-1}\alpha_v \in P(\Sigma)$ in all cases. This establishes part (a).

To prove (b), suppose first that $P(\Sigma) - \{0\}$ is unitary in P_X and that $(su, tu) \in \Sigma^c$ for some $u, s, t \in X^*$. Then

$$\alpha_s\alpha_u\alpha_u^{-1}\alpha_t^{-1} = \alpha_s\alpha_t^{-1}(\alpha_t\alpha_u\alpha_u^{-1}\alpha_t^{-1}) \in P(\Sigma) - \{0\}.$$

Also $\alpha_{tu}\alpha_{tu}^{-1} \in P(\Sigma) - \{0\}$, so it follows that $\alpha_s\alpha_t^{-1} \in P(\Sigma)$ since $P(\Sigma) - \{0\}$ is unitary. Hence M_Σ is right cancellative. Suppose conversely that M_Σ is right cancellative. Suppose also that $\alpha_s\alpha_t^{-1}\alpha_u\alpha_v^{-1} \in P(\Sigma) - \{0\}$ and $\alpha_u\alpha_v^{-1} \in P(\Sigma)$ for some $s, t, u, v \in X^*$. Then $\alpha_v\alpha_u^{-1} \in P(\Sigma)$ and so $\alpha_s\alpha_t^{-1}\alpha_u\alpha_v^{-1}\alpha_v\alpha_u^{-1} = \alpha_s\alpha_t^{-1}\alpha_u\alpha_u^{-1} \in P(\Sigma) - \{0\}$. We must have either $t = uw$ or $u = tw$ for some $w \in X^*$. In the former case, $\alpha_s\alpha_t^{-1}\alpha_u\alpha_u^{-1} = \alpha_s\alpha_w^{-1}\alpha_u^{-1} \in P(\Sigma)$, so $(s, uw) \in \Sigma^c$, and $(s, t) \in \Sigma^c$: in the latter case, $\alpha_s\alpha_t^{-1}\alpha_u\alpha_u^{-1} = \alpha_s\alpha_w\alpha_w^{-1}\alpha_t^{-1} \in P(\Sigma)$, so $(sw, tw) \in \Sigma^c$, whence $(s, t) \in \Sigma^c$ since M_Σ is right cancellative. Hence in both cases $\alpha_s\alpha_t^{-1} \in P(\Sigma)$, so $P(\Sigma) - \{0\}$ is right unitary in P_X. Since $P(\Sigma)$ is an inverse submonoid of the inverse monoid P_X, $P(\Sigma) - \{0\}$ is left unitary in P_X if and only if it is right unitary in P_X. Hence $P(\Sigma) - \{0\}$ is a unitary subset of P_X, as required.

We close the paper by reformulating a few of the basic decision problems about monoids into equivalent problems about the polycyclic monoid.

Remark 4.4. Let Σ be a relation on X^*. Then the word problem for the monoid $M_\Sigma = \mathrm{Mon}\langle X : \Sigma\rangle$ is equivalent to the membership problem for the submonoid $P(\Sigma)$ of P_X (that is, the problem of deciding, for words $u, v \in X^*$, whether $\alpha_u\alpha_v^{-1} \in P(\Sigma)$ or not.)

Proof. This is obvious from Theorem 3.4 since $(u, v) \in \Sigma^c$ if and only if $\alpha_u\alpha_v^{-1} \in P(\Sigma)$.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

On the one hand, this remark points out the complex nature of PSC submonoids of the polycyclic monoid. For example, if $M_\Sigma = \mathrm{Mon}\langle X : \Sigma\rangle$ is a finitely presented monoid with undecidable word problem, then the membership problem for the corresponding PSC submonoid $P(\Sigma)$ of P_X is also undecidable. Note that $P(\Sigma)$ is the PSC submonoid of P_X generated by $\{\alpha_u\alpha_v^{-1} : (u, v) \in \Sigma\}$; that is, $P(\Sigma)$ is the smallest full inverse submonoid of P_X containing $\{\alpha_u\alpha_v^{-1} : (u, v) \in \Sigma\}$ and satisfying the condition $\alpha_s\alpha_t^{-1} \in P(\Sigma)$ implies $\alpha_{ws}\alpha_{wt}^{-1} \in P(\Sigma)$ for all $w \in X^*$. Hence

REMARK 4.5. If X is a set with at least two elements then there exists a finite set R of elements of I_X such that the membership problem for the subsemigroup of I_X generated by R is undecidable.

PROOF. This follows easily from the existence of a semigroup with two generators and undecidable word problem [5] (and Theorem 3.4).

On the other hand, several classical decision problems for semigroups may be translated into a rather appealing equivalent form by use of Remark 4.3 (that is, Theorem 3.4). For example, as far as the authors are aware, it is not known whether the word problem for one-relation semigroups of the form $M = \mathrm{Mon}\langle X : u = v\rangle$ (u, v fixed words in X^*) is decidable or not. (A positive solution, due to Adian [1], is known, for example, in the case $v = 1$.) The corresponding PSC-submonoid of P_X is generated (as a PSC-submonoid of P_X) by the single element $\alpha_u\alpha_v^{-1}$. Thus we have

REMARK 4.6. The word problem for one-relation semigroups is equivalent to the membership problem for one-generator PSC submonoids of the polycyclic monoid.

Other well-known problems may be reformulated along these lines. The authors believe that progress on some of these problems may result from a detailed examination of the PSC submonoids of the polycyclic monoid.

Acknowledgements

Joint work on this paper commenced when the authors met at a workshop on semigroups organized by John Rhodes in Berkeley in July 1989 and continued when the authors met again at the Mal′cev algebra conference in Novosibirsk in August 1989. Part of the work was completed while the first author was visiting the L.I.T.P., University of Paris VI in October-November 1989 and later Monash University in the first half of 1990. The authors would like to thank Francis Pastijn for several comments and in particular for providing the proof of Corollary 3.5, which is more general than their original result.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press

References

[1] S. I. Adian, 'Defining relations and algorithmic problems for groups and semigroups', *Trudy Mat. Inst. Steklov* **85** (in Russian) Am. Math. Soc. translation 152, 1967.

[2] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Math. Surveys Monographs 7, vol. 1, vol. 2 (Amer. Math. Soc., Providence, 1961–1967).

[3] E. S. Lyapin, *Semigroups* (Moscow, 1960) (in Russian).

[4] S. Margolis and J. Meakin, 'Inverse monoids, trees and context-free languages', *Trans. Amer. Math. Soc.* (to appear).

[5] Yu. V. Matiyasevich, 'Investigation on some algorithmic problems in algebra and number theory', *Trudy MIAN SSSR*, **168** (1984), 218–235.

[6] M. Nivat, 'Sur les automates a memoire pile', in: *Proceedings of the International Computing Symposium, Bonn, 1970* (ed. W. Itzeld), (North Holland, Amsterdam, 1970) pp. 655–663.

[7] M. Nivat and J. F. Perrot, 'Une generalisation du monoide bicyclique', *C.R. Acad. Sci. Paris Sér. I Math.* **A 271** (1970), 824–827.

[8] M. Petrich, *Inverse semigroups*, (Wiley, New York, 1984).

[9] J. Sakarovitch, *Syntaxe des langages de Chomsky*, (Th. Sc. Math., Univ. Paris 7, 1979).

[10] J. Stephen, 'Presentations of inverse monoids', *J. Pure and Applied Algebra* **63** (1990), 81–112.

[11] Th. P. Whaley, *Algebras satisfying the descending chain condition for subalgebras*, (Ph.D. Thesis, Vanderbilt University, 1968).

Department of Mathematics and Statistics
University of Nebraska-Lincoln
Lincoln, Nebraska 68588-0323
U.S.A.

https://doi.org/10.1017/S1446788700037149 Published online by Cambridge University Press