The polycyclic monoids P_n and the Thompson groups $V_{n,1}$

Mark V. Lawson
Department of Mathematics
and the
Maxwell Institute for Mathematical Sciences
Heriot-Watt University
Riccarton
Edinburgh EH14 4AS
Scotland
M.V.Lawson@ma.hw.ac.uk

December 21, 2006

Abstract

We construct what we call the strong orthogonal completion C_n of the polycyclic monoid P_n on n generators. The inverse monoid C_n is congruence free and its group of units is the Thompson group $V_{n,1}$. Copies of C_n can be constructed from partitions of sets into n blocks each block having the same cardinality as the underlying set.

2000 AMS Subject Classification: 20M18, 20E32.

1 Introduction

The goal of this paper is to describe the precise algebraic connection between the polycyclic inverse monoid P_n and the Thompson group $V_{n,1}$. The polycyclic monoids were introduced by Nivat and Perrot [14] as generalisations of the bicyclic monoid. They have numerous applications including to the study of context-free languages [6, 7], the construction of the Cuntz C^*-algebras [15, 16], and in the definition of amenability given in [5]. They are discussed in detail in Chapter 9 of my book [8], and I outline their properties below. Prior knowledge of these semigroups is not necessary to read this paper

In a previous paper [12], I showed how to construct the orthogonal completion D_n of the polycyclic monoid P_n. In this paper, I shall construct a quotient of this completion, called the strong completion C_n. The group of units of C_n will turn out to be the Thompson group $V_{n,1}$. Birget [3] described one connection between the Thompson group $V = V_{2,1}$ and the polycyclic monoid on two generators: he proved that the group is a subgroup of a quotient algebra of the monoid. Our approach owes a lot to Birget's but is different. Birget works with semigroup algebras and as a result he obtains a representation of the Thompson group as a subgroup. A particular case of our result on V can be found in [1].

2 Orthogonal completions of inverse semigroups

In this section, I shall recall some results from [12].

Throughout this paper, we shall be dealing with inverse semigroups with zero. *We shall always require that homomorphisms between such semigroups map zero to zero.* Multiplication in semigroups will usually be denoted by concatenation, but occasionally I shall use $\cdot$ for clarity. Inverse semigroups come equipped with their own order, called the *natural partial order*, and this will always be the order used. We write $\mathbf{d}(s) = s^{-1}s$ and $\mathbf{r}(s) = ss^{-1}$ for each element s in the inverse semigroup S. A pair of elements $s, t \in S$ is said to be *orthogonal* if

$$s^{-1}t = 0 = st^{-1}.$$

Observe that s and t are orthogonal iff $\mathbf{d}(s)\mathbf{d}(t) = 0$ and $\mathbf{r}(s)\mathbf{r}(t) = 0$. A subset of S is said to be *orthogonal* iff each pair of distinct elements in it is orthogonal. We denote by $s + t$ the join of orthogonal elements s and t if it exists. More generally, we denote by $\sum A$ the join of the orthogonal subset A if it exists. In these cases, we talk about *orthogonal joins*. Let $D(S)$ denote the set of finite orthogonal subsets of the inverse semigroup S that contain zero. Then $D(S)$ is an inverse semigroup under multiplication of subsets, and an inverse monoid if S is an inverse monoid. An inverse semigroup with zero S will be said to be *orthogonally complete* if it satisfies the following two axioms:

(DC1) S has all joins of finite orthogonal subsets.

(DC2) Multiplication distributes over finite orthogonal joins.

The semigroup $D(S)$ is orthogonally complete as is the symmetric inverse monoid $I(X)$ on the set X.

Lemma 2.1 *Let S be orthogonally complete.*

(i) *If $\sum_{i=1}^{n} a_i$ exists, then $\sum_{i=1}^{n} a_i^{-1}$ exists and*

$$(\sum_{i=1}^{n} a_i)^{-1} = \sum_{i=1}^{n} a_i^{-1}.$$

(ii) *If $\sum_{i=1}^{n} a_i$ exists, then both $\sum_{i=1}^{n} \mathbf{d}(a_i)$ and $\sum_{i=1}^{n} \mathbf{r}(a_i)$ exist and*

$$\mathbf{d}(\sum_{i=1}^{n} a_i) = \sum_{i=1}^{n} \mathbf{d}(a_i) \text{ and } \mathbf{r}(\sum_{i=1}^{n} a_i) = \sum_{i=1}^{n} \mathbf{r}(a_i).$$

■

Homomorphisms between inverse semigroups with zero map finite orthogonal subsets to finite orthogonal subsets. If the orthogonal joins are preserved then we say that the homomorphism is *orthogonal join preserving*. Define the function $\iota\colon S \to D(S)$ by $s \mapsto \{0, s\}$. This is an injective homomorphism.

Theorem 2.2 *Let S be an inverse semigroup with zero, and let $\theta\colon S \to T$ be a homomorphism to an orthogonally complete inverse semigroup T. Then there is a unique orthogonal join preserving homomorphism $\phi\colon D(S) \to T$ such that $\phi\iota = \theta$.* ■

The inverse monoid $D(S)$ is called the *orthogonal completion of S*.

Put $A_n = \{a_1, \ldots, a_n\}$. A string in A_n^*, the free monoid generated by A_n, will be called *positive*. If $u = vw$ are strings, then v is called a *prefix* of u, and a *proper prefix* if w is not the empty string. A pair of elements of A_n^* is said to be *prefix-comparable* if one is a prefix of the other. If x and y are prefix-comparable we define

$$x \wedge y = \begin{cases} x & \text{if } y \text{ is a prefix of } x \\ y & \text{if } x \text{ is a prefix of } y \end{cases}$$

The polycyclic monoid P_n, where $n \geq 2$, is defined as a monoid with zero by the following presentation

$$P_n = \langle a_1, \ldots, a_n, a_1^{-1}, \ldots, a_n^{-1} \colon a_i^{-1}a_i = 1 \,\text{and}\, a_i^{-1}a_j = 0, i \neq j \rangle.$$

Intuitively, think of $a_1, \ldots, a_n$ as partial bijections of a set X and $a_1^{-1}, \ldots, a_n^{-1}$ as their respective partial inverses. The first relation says that each partial bijection a_i has domain the whole of X and the second says that the ranges of distinct a_i are disjoint. As a concrete example of P_2, one can take as a_1 and a_2 the two maps that shrink the Cantor set to its lefthand and righthand sides, respectively. Every non-zero element of P_n is of the form yx^{-1} where $x, y \in A_n^*$, and where we identify the identity with the element $1 = \varepsilon\varepsilon^{-1}$. The product of two elements yx^{-1} and vu^{-1} is zero unless x and v are prefix-comparable. If they are prefix-comparable then

$$yx^{-1} \cdot vu^{-1} = \begin{cases} yzu^{-1} & \text{if } v = xz \text{ for some string } z \\ y(uz)^{-1} & \text{if } x = vz \text{ for some string } z \end{cases}$$

The non-zero idempotents in P_n are the elements of the form xx^{-1}, where x is positive, and the natural partial order is given by $yx^{-1} \leq vu^{-1}$ iff $(y, x) = (v, u)p$ for some positive string p. Observe that an element lying above a non-zero idempotent in a polycyclic monoid is itself a non-zero idempotent. Inverse semigroups with this property are said to be *E^*-unitary*.

Lemma 2.3 *Let xx^{-1} and yy^{-1} be non-zero idempotents. Then $xx^{-1} \cdot yy^{-1} \neq 0$ if and only if either $xx^{-1} \leq yy^{-1}$ or $yy^{-1} \leq xx^{-1}$. When non-zero $xx^{-1} \cdot yy^{-1}$ is equal to $(x \wedge y)(x \wedge y)^{-1}$.* ■

Remark Suppose that in the polycyclic monoid

$$xy^{-1} \leq uv^{-1}, wz^{-1}.$$

Then either $uv^{-1} = wz^{-1}$, $uv^{-1} \leq wz^{-1}$ or $uv^{-1} \geq wz^{-1}$.

A *prefix code* in A_n^* is a non-empty subset C with the property that no element of C is a proper prefix of any other element of C. A prefix code is *maximal* if it is not contained in any other prefix code. The following is essentially Proposition II.4.7 of [2].

Lemma 2.4 *Let $C \subseteq A_n^*$ be a maximal prefix code such that $C \neq \{\varepsilon\}$. Then there exists a string u such that $ua_1, \ldots, ua_n \in C$ and*

$$C' = C \setminus \{ua_1, \ldots, ua_n\} \cup \{u\}$$

is a maximal prefix code. ■

The following result was inspired by [3] and is crucial to our work.

Lemma 2.5 *A subset*

$$\{y_1 x_1^{-1}, \ldots, y_m x_m^{-1}\}$$

of P_n is orthogonal iff $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_m\}$ are both prefix codes. ■

If $A = \{x_1 x_1^{-1}, \ldots, x_n x_n^{-1}\} \cup \{0\}$ is an orthogonal subset of P_n, then $Z_A = \{x_1, \ldots, x_n\}$ is the *associated prefix code*.

Theorem 2.6 *The orthogonal completion of the polycyclic monoid P_n is isomorphic to the inverse monoid R_n consisting of right ideal isomorphisms between the finitely generated right ideals of the free monoid on n generators.* ■

An idempotent e of S is called *essential* if for each non-zero idempotent $f \in S$ we have that $ef \neq 0$.

Lemma 2.7 *The following are equivalent in $D(P_n)$:*

(i) *A is an essential idempotent.*

(ii) *AB is non-zero for all non-zero idempotents B.*

(iii) *Z_A is a maximal prefix code.* ■

Lemma 2.8 *Let S be an inverse monoid with zero. Let S^e denote the set of elements s such that both $\mathbf{d}(s)$ and $\mathbf{r}(s)$ are essential idempotents. Then S^e is an inverse submonoid of S.* ■

By Lemma 2.7, the essential idempotents in $D(P_n)$ are those whose associated prefix codes are maximal. By Lemmas 2.5 and 2.7, the elements of $D^e(P_n)$ are those in which the domains and ranges correspond to maximal prefix codes.

Proposition 2.9 *The inverse semigroup $D^e(P_n)$ is isomorphic to the inverse monoid of right ideal isomorphisms between the finitely generated* essential *right ideals of the free monoid on n generators.* ■

From Birget [3] and Scott [17] the following is now immediate.

Corollary 2.10 *The maximum group homomorphic image of $D^e(P_n)$ is the Thompson group $V_{n,1}$.* ■

Notation and a convention We write $D_n = D(P_n)$. The elements of D_n are finite orthogonal sets containing zero. Because the zero is always there, I shall almost always ignore it in what follows. Except when I am specifically interested in the zero element $\{0\}$, it will always be the non-zero elements which are of interest.

To conclude this section, we shall examine in more detail the properties of the set of idempotents of the inverse semigroup D_n. Unproved statements follow from results in [12]. The set of idempotents of D_n is in bijective correspondence with the set of finite prefix codes in A_n^*, and the set of essential idempotents in D_n is in bijective correspondence with the set of finite maximal prefix codes in A_n^*. The set of idempotents in D_n forms a semilattice with respect to the natural partial order. There is therefore a corresponding semilattice structure on the finite prefix codes. To describe it, we shall use the following. We say that the string x is an *extension* of the string y if $x = yz$ for some string z. We define $x \wedge y$ to be the *shortest extension* of x and y if it is defined (which will be the case only when x and y are prefix-comparable). Given two prefix codes X and Y we define $X \leq Y$ iff each element of X is an extension of an element of Y. For arbitrary prefix codes X and Y, the prefix code $X \circ Y$ is either empty or consists of the set of shortest extensions of all pairs of elements one from X and one from Y. In the case X and Y are both maximal prefix codes then $X \circ Y$ is always non-empty and a maximal prefix code; in this case, the maximal prefix code is obtained by 'overlaying' the two codes and taking the result as their meet. If $E(D_n)$ is the semilattice of idempotents of D_n and $\mathcal{PC}_n$ the semilattice of finite prefix codes in A_n^*, then the function $E \mapsto Z_E$ is an isomorphism of semilattices.

There are a number of unary operations which can also be defined on $\mathcal{PC}_n$ which then have algebraic correlates in $E(D_n)$:

- Let E correspond to a (maximal) prefix code Z_E. Conjugates of the form $y^{-1}Ey$ also correspond to (maximal) prefix codes: the corresponding (maximal) prefix code is $y^{-1}Z_E$ where here $y^{-1}x$ means remove the prefix y from x if y is a prefix of x and is undefined otherwise; in terms of trees, $y^{-1}Z_E$ is the portion of the (maximal) prefix code which starts at y and so is itself a (maximal) prefix code.

- Conjugates of the form yEy^{-1} correspond to prefix codes: the corresponding code is yZ_E; in terms of trees we are attaching the prefix code Z_E to the 'stalk y'.

Lemma 2.11

(i) *Let E and F be idempotents in D_n such that Z_E and Z_F are maximal prefix codes. Then Z_{EF} is a maximal prefix code.*

(ii) *Let E be an idempotent such that Z_E is a maximal prefix code. Then for all $A \in D_n$, we have that $EA = \{0\}$ iff $A = \{0\}$, and dually.*

(iii) *Let $F = \{xx^{-1}$: finite number of x's$\}$ and E_x, where $xx^{-1} \in F$, be idempotents in D_n such that Z_{E_x} and Z_F are maximal prefix codes. Then*

$$G = \bigcup_{xx^{-1} \in F} xE_x x^{-1}$$

is such that Z_G is a maximal prefix code. This result can be described in terms of trees: we take the tree corresponding to the maximal prefix code Z_F and glue to each leaf x the tree corresponding to the maximal prefix code E_x. The tree we get clearly corresponds to a maximal prefix code.

(iv) *Let $F = \{xx^{-1}$: finite number of x's$\}$, E_x, where $xx^{-1} \in F$, and*

$$G = \bigcup_{xx^{-1} \in F} xE_x x^{-1}$$

be idempotents in D_n where Z_G and Z_{E_x} are maximal prefix codes. Then F is a maximal prefix code. This result can be described in terms of trees: we take the tree corresponding to a maximal prefix code and erase a subtree tree which corresponds to a maximal prefix code. The tree we get clearly corresponds to a maximal prefix code.

Proof The proofs of (i) and (ii) follow from Lemmas 2.7 and 2.8. The proof of (i) follows from the fact that the product of two essential idempotents is an essential idempotent. To prove (ii), let e be an essential idempotent and a an arbitrary element. Then $ea = 0$ iff $eaa^{-1} = 0$, but this occurs iff $aa^{-1} = 0$, because e is essential. This in turn occurs iff $a = 0$. The proof of (iii) can either be done directly from the definitions or it is essentially Proposition II.4.1(1) of [2]. The proof of (iv) can either be done directly or is essentially Proposition II.4.1(3) of [2]. ■

3 Strong orthogonal completions of polycyclic monoids

To explain the motivation of this paper, I need to return to the definition of P_n. The idempotents $a_1a_1^{-1}, \ldots, a_na_n^{-1}$ are pairwise orthogonal, and so their orthogonal join is an idempotent in D_n. We would like to force this orthogonal join to be the identity. To do this, I shall define a congruence $\equiv$ on D_n which will force this to happen in the most efficient way. The quotient monoid $C_n = D_n/\equiv$ will still be orthogonally complete but the orthogonal join of (the images of) the idempotents $a_ia_i^{-1}$ will now be the identity. It will transpire that the congruence $\equiv$ restricted to D_n^e, will be the minimum group congruence. Consequently, the group of units of C_n will then be the Thompson group $V_{n,1}$ by Corollary 2.10. Most of this section will be taken up with defining the congruence $\equiv$ and determining its properties.

Let $A, B \in D_n$ where $A = \{x_iy_i^{-1} \colon 1 \leq i \leq p\}$ and $B = \{u_jv_j^{-1} \colon 1 \leq j \leq q\}$. Define $A \preceq B$ iff we can write

$$A = \bigcup_{j=1}^{q} u_jE_jv_j^{-1}$$

where E_j is an idempotent in D_n and Z_{E_j} is a maximal prefix code. I shall write $A \preceq_e B$ iff $A = B \setminus \{u_jv_j^{-1}\} \cup u_j\{a_1a_1^{-1}, \ldots, a_na_n^{-1}\}v_j^{-1}$. I shall write $A \preceq_e^* B$ if $A = A_1 \preceq_e A_2 \preceq_e \ldots \preceq_e A_n = B$ for some n.

Remarks

(i) If $A \preceq B$ then each element in A lies beneath an element of B, and each non-zero element of B lies above a non-zero element of B.

(ii) Define $A_j = u_jE_jv_j^{-1}$. Then with slight abuse of notation, we have that $A_j \preceq u_jv_j^{-1}$. The A_j are orthogonal.

Lemma 3.1

(i) *If $A \preceq B$ then $A \leq B$.*

(ii) *The relation $\preceq$ is a partial order D_n.*

(iii) *If $A \preceq B$ then $A = \{0\}$ iff $B = \{0\}$.*

(iv) *If $A \preceq B$ then A is an idempotent iff B is an idempotent.*

(v) *If* $A \preceq B$ *then* $A^{-1} \preceq B^{-1}$.

(vi) *Let* A *and* B *be non-zero. If* $A \preceq B$ *then* $AC = \{0\}$ *iff* $BC = \{0\}$*, and dually.*

(vii) *If* $A \preceq B$ *then* $AC \preceq BC$*, and dually.*

(viii) $A \preceq B$ *iff* $A^{-1}A \preceq B^{-1}B$ *and* $A \leq B$.

(ix) *Let* A, B, C *all be non-zero, and* $A, B \preceq C$*. Then there exists a non-zero* D *such that* $D \preceq A, B$.

(x) $A \preceq B$ *iff* $A \preceq_e^* B$.

Proof (i) By Lemma 2.3(i) [12], $A \leq B$ if each element of A lies beneath an element of B with respect to the natural partial order. The result is therefore immediate from the definition.

(ii) Reflexivity follows from the fact that $\{\varepsilon\}$ is a maximal prefix code. Antisymmetry follows from (i), above. We now prove transitivity. Let $A = \{x_i y_i^{-1}\}$, $B = \{u_j v_j^{-1}\}$, and $C = \{w_k z_k^{-1}\}$ be such that $A \preceq B \preceq C$. We prove that $A \preceq C$. Let $A = \sum_j u_j E_j v_j^{-1}$ where the Z_{E_j} are maximal prefix codes, and let $B = \sum_k w_k F_k z_k^{-1}$ where the Z_{F_k} are maximal prefix codes. The element $w_k z_k^{-1}$ lies above the set of elements of A given by

$$w_k \Big(\bigcup_{rr^{-1} \in F_k} r E_j r^{-1} \Big) z_k^{-1}$$

for some j. The fact that the expression within the brackets is associated with a maximal prefix code follows by Lemma 2.11. Thus $A \preceq C$, as required.

(iii) This is immediate from the definition.

(iv) This follows by Remarks (i), the fact that idempotents in an inverse semigroup form an order ideal, and the fact that P_n is E^*-unitary.

(v) Suppose that $A \preceq B$. Then $A = \sum_{j=1}^{n} u_j E_j v_j^{-1}$. Taking inverse of both sides gives the result.

(vi) This is immediate from the definition.

(vii) By (vi), we may assume that both products are non-zero. The result follows by multiplying out and using Lemma 2.11 when necessary.

(viii) Suppose $A \preceq B$. Then from (v) and (vii), we have that $A^{-1}A \preceq B^{-1}B$, and from (i), we have that $A \leq B$. To prove the converse, suppose that $A^{-1}A \preceq B^{-1}B$ and $A \leq B$. Then $A = BA^{-1}A$. By (vii), we have that $BA^{-1}A \preceq BB^{-1}B$, and so $A \preceq B$, as required.

(ix) Let $C = \{x_i y_i^{-1}\}$, $A = \{u_j v_j^{-1}\}$, $B = \{w_k z_k^{-1}\}$ where $A, B \preceq C$. Thus $A = \cup_i x_i E_i y_i^{-1}$ and $B = \cup_i x_i F_i y_i^{-1}$ where E_i and F_i are associated with maximal prefix codes. Define $D = \cup_i x_i E_i F_i y_i^{-1}$. To show that $D \preceq A$, choose a typical element of A: namely, $x_i pp^{-1} y_i^{-1}$ where $pp^{-1} \in E_i$. A subset of D is $x_i pp^{-1} F_i y_i^{-1}$, which can be rewritten as $(x_i p)(p^{-1} F_i p)(y_i p)^{-1}$ where $p^{-1} F_i p$ is a maximal prefix code by Lemma 2.11. It follows that $D \preceq A$, and a similar argument shows that $D \preceq B$.

(x) One direction is immediate by the transitivity proved in (ii). We prove that $A \preceq B$ implies $A \preceq_e^* B$. Observe that it is enough to prove that $A \preceq uv^{-1}$ implies that $A \preceq_e^* uv^{-1}$. By Lemma 2.4, $C \neq \{\varepsilon\}$ is a maximal prefix code iff there exists u such that $uA_n \subseteq C$ and $C' = C \setminus \{ua_1, \ldots, ua_n\} \cup \{u\}$ is a maximal prefix code. Observe that $|C'| < |C|$. Let E be such that $Z_E = C$, and let E' be such that $Z_{E'} = C'$. Then $E \preceq_e E'$. By induction we get that $E \preceq_e^* \{0, 1\}$. It follows that Z_E is a maximal prefix code iff $E \preceq_e^* \{0, 1\}$. Observing that $A' \preceq_e B'$ implies that $uA'v^{-1} \preceq_e uB'v^{-1}$, the result follows. ■

Remark Lemma 3.1 shows that the partial order $\preceq$ refines the natural partial order on D_n. At the same time it shares a number of important properties with the natural partial order: namely, (v) and (viii).

A congruence ρ on an inverse semigroup S is said to be *0-restricted* if the only element of S which is ρ-related to zero is zero. It is said to be *idempotent pure* if the only elements of S which are ρ-related to idempotents are themselves idempotents.

Define $\equiv$ on D_n as follows. We require $\{0\} \equiv \{0\}$, and if A and B are both non-zero, then $A \equiv B$ iff there exists a non-zero C such that $C \preceq A, B$.

Proposition 3.2 *With the above definition we have the following.*

(i) *The relation $\equiv$ is a 0-restricted, idempotent pure congruence on D_n.*

(ii) *The congruence $\equiv$ restricted to D_n^e is the minimum group congruence.*

(iii) *The congruence $\equiv$ restricted to the image of P_n in D_n is equality.*

(iv) *The congruence $\equiv$ is the smallest congruence on D_n in which all the essential idempotents are identified.*

(v) *Let $A_i \equiv B_i$ where the A_i (respectively the B_i) are orthogonal. Then $\sum A_i \equiv \sum B_i$.*

Proof (i) We show first that $\equiv$ is an equivalence relation. Reflexivity: $\{0\} \equiv \{0\}$ by fiat; and $A \equiv A$ for all non-zero A since $\preceq$ is a partial order by Lemma 3.1(ii). Symmetry: this is immediate from the definition. Transitivity: this follows by Lemma 3.1(ix). The fact that $\equiv$ is a congruence follows from Lemma 3.1(vi) and (vii). The fact that $\equiv$ is 0-restricted follows from Lemma 3.1(iii). Idempotent purity follows by Lemma 3.1(iv).

(ii) By Lemma 3.1(viii), it is enough to prove the claim for idempotents. We prove that $E \leq F$ implies $E \preceq F$ when Z_E and Z_F are maximal prefix codes. Because Z_E is a maximal prefix code, it is easy to check that each element of F lies above an element of E. Fix $bb^{-1} \in F$ and let A be the set of all elements of E that lie beneath bb^{-1}. Each element of A is of the form $bww^{-1}b^{-1}$ for some string w. Thus $A = bGb^{-1}$ where G is an idempotent and Z_G is a prefix code; it remains to show that it is a maximal prefix code. Let xx^{-1} be any non-zero idempotent. The string bx must be prefix comparable with a string $bw \in Z_E$

since Z_E is a maximal prefix code and $E \leq F$. Observe that $w \in Z_G$. Thus $bw(bw)^{-1} \cdot bx(bx)^{-1} \neq 0$ from which it follows that $ww^{-1} \cdot xx^{-1} \neq 0$. Thus G is an essential idempotent and so Z_G is a maximal prefix code.

(iii) Let xy^{-1} and uv^{-1} be such that $xy^{-1} \equiv uv^{-1}$. There are therefore idempotents E and F associated with maximal prefix codes such that $xEy^{-1} = uFv^{-1}$. Observe that $xEx^{-1} = uFu^{-1}$ and $yEy^{-1} = vFv^{-1}$. Now $Z_{xEx^{-1}} = xZ_E$ and $Z_{uFu^{-1}} = uZ_F$. Suppose $u = xz$. Then $Z_E = zZ_F$. But Z_E is a maximal prefix code and so z is the empty string. There is a similar dual argument. Thus $u = x$. Similarly $v = y$.

(iv) Let $\simeq$ be any congruence on D_n which identifies the essential idempotents. Let $A \equiv B$. Then there exists $C \preceq A, B$. Thus we can write

$$C = \sum x_i E_i y_i^{-1} = \sum u_j F_j v_j^{-1}$$

where $A = \{x_i y_i^{-1}\}$ and $B = \{u_j v_j^{-1}\}$ and E_i and F_j correspond to maximal prefix codes. By assumption, $C \simeq A$ and $C \simeq B$ and so $A \simeq B$, as required.

(v) This is immediate from the definition. ■

Proposition 3.3 *The congruence $\equiv$ is the unique congruence defined on D_n which is 0-restricted, idempotent pure, and identifies all the essential idempotents.*

Proof Let $\simeq$ be a 0-restricted idempotent pure congruence which identifies all the essential idempotents. By Proposition 3.2(iv), we have that $\equiv$ is contained in $\simeq$. We prove that the reverse inclusion holds.

We show first that it is enough to prove the result for idempotents. Suppose that for E and F idempotents, we have that $E \simeq F$ implies $E \equiv F$. We prove that $\simeq$ is contained in $\equiv$. Let $A \simeq B$. Then $A^{-1}A \simeq A^{-1}B$. Now $\simeq$ is idempotent pure and so since $A^{-1}A$ is an idempotent, we have that $A^{-1}B$ is an idempotent. Without loss of generality we can assume that it is non-zero. By assumption, $A^{-1}A \equiv A^{-1}B$. But then $A \equiv AA^{-1}B$. Now $AA^{-1} \simeq BB^{-1}$ implies $AA^{-1} \equiv BB^{-1}$. Thus $AA^{-1}B \equiv B$. It follows that $A \equiv B$. Thus the theorem will be proved if we can prove it for idempotents.

Next we prove a slightly more general result. Let S be an inverse monoid with zero. Let $\simeq$ be a 0-restricted, idempotent pure congruence that identifies all the essential idempotents. Then $a \simeq 1$ iff a is an essential idempotent. There is only one direction to prove. Suppose $a \simeq 1$. Then a is an idempotent because $\simeq$ is idempotent pure. Let f be any non-zero idempotent. Then $fa \simeq f$. Now $\simeq$ is 0-restricted and so fa is non-zero. It follows that a is an essential idempotent. Thus $\simeq$ identifies with the identity element all and only the essential idempotents.

Now we return to the particular case we are interested in. We look first at a special case. Let $E = \{u_i u_i^{-1} \colon 1 \leq i \leq p\}$ be a non-zero idempotent. Suppose that $E \simeq xx^{-1}$. Then for each i we have that $u_i u_i^{-1} \simeq u_i u_i^{-1} xx^{-1}$. Because $\simeq$ is 0-restricted, we have that $u_i u_i^{-1} xx^{-1} \neq 0$. Thus by Lemma 2.3, we have for each i that either $u_iu_i^{-1} \leq xx^{-1}$ or $xx^{-1} \leq u_iu_i^{-1}$. Now $x^{-1}Ex \simeq 1$, and so $F = x^{-1}Ex$ is an essential idempotent by our general result above. Thus Z_F is a maximal prefix code. If $xx^{-1} \leq u_iu_i^{-1}$ for some i, then because $\simeq$ is 0-restricted, it follows that E contains exactly one (non-zero) element: $u_iu_i^{-1}$. But then F contains only one element and, since it is associated with a maximal prefix code, that element must be the identity. It follows that $x = u_i$ and so $E \equiv xx^{-1}$. Thus we may assume that $u_iu_i^{-1} \leq xx^{-1}$ for all i. Thus $E = xFx^{-1}$ where F is associated with a maximal prefix code. It follows that $E \preceq xx^{-1}$ and so $E \equiv xx^{-1}$.

Now let $E = \{u_iu_i^{-1}\colon 1 \leq i \leq p\} \simeq F = \{x_jx_j^{-1}\colon 1 \leq j \leq q\}$. Then $Ex_jx_j^{-1} \simeq x_jx_j^{-1}$. Thus $Ex_jx_j^{-1} \preceq x_jx_j^{-1}$ for all j by the preceding result. Put $D = \{u_iu_i^{-1}x_jx_j^{-1}\colon 1 \leq i \leq p, 1 \leq j \leq q\}$. The fact that $\simeq$ is 0-restricted implies that D is not zero. By symmetry and Proposition 3.2(v), we have that $D \preceq E, F$. Thus $E \equiv F$. ∎

Lemma 3.4 *Let S be an orthogonally complete inverse semigroup, and let $\equiv$ be a 0-restricted congruence on S such that if $s_1 \equiv t_1$ and $s_2 \equiv t_2$ and s_1 and s_2 are orthogonal, and t_1 and t_2 are orthogonal then $s_1 + s_2 \equiv t_1 + t_2$. Then $S/\equiv$ is orthogonally complete.*

Proof Denote the $\equiv$-class containing s by $[s]$. By induction, we can prove that if $s_i \equiv t_i$ for $1 \leq i \leq p$ and the s_i are orthogonal and the t_i are orthogonal then $\sum s_i \equiv \sum t_i$.

Let $[s_i]$ be a finite orthogonal subset of $S/\equiv$. Because the congruence is 0-restricted, the set s_i is orthogonal and so $s = \sum s_i$ exists in S. Clearly $[s_i] \leq [s]$. Suppose that $[s_i] \leq [t]$ for all i. Then $[s_i] = [t\mathbf{d}(s_i)]$ and so $s_i \equiv t\mathbf{d}(s_i)$. It is easy to check that the $t\mathbf{d}(s_i)$ are orthogonal and so, by assumption, $\sum s_i \equiv \sum t\mathbf{d}(s_i)$. By Lemma 2.1, we know that $\mathbf{d}(\sum s_i) = \sum \mathbf{d}(s_i)$. Thus $\sum t\mathbf{d}(s_i) = t \sum \mathbf{d}(s_i) = t\mathbf{d}(s)$. Hence $[s] \leq [t]$. It follows that $\sum [s_i]$ exists. We have proved that $S/\equiv$ has orthogonal joins. In fact, we have shown that $[\sum s_i] = \sum [s_i]$.

The fact that multiplication distributes over finite orthogonal joins follows from the existence of orthogonal joins and distributivity in S, and our result above. ∎

Put $C_n = D(P_n)/\equiv$. By Proposition 3.2 and Lemma 3.4, C_n is orthogonally complete and contains an isomorphic copy of P_n and every element of C_n is the join of a finite orthogonal subset of P_n and all essential idempotents are identified.

More generally, let S be an inverse monoid with zero containing P_n as an inverse submonoid such that S is orthogonally complete, every element of S is the join of a finite orthogonal subset of P_n, and such that $\sum_i a_ia_i^{-1} = 1$. Then S is called a *strong orthogonal completion of P_n*.

Theorem 3.5 *Any two strong orthogonal completions of P_n are isomorphic.*

Proof Let S be a strong orthogonal completion of P_n. Let $A, B \in D(P_n)$. We begin by proving in four steps that $\sum A = \sum B$ in S iff $A \equiv B$ in D_n.

1. *Let $A = \{y_i x_i^{-1}\colon 1 \leq i \leq m\}$ be an orthogonal subset of P_n. Then $\sum A = 1$ iff the elements of A are idempotents and $\{x_i\colon 1 \leq i \leq m\}$ is a maximal prefix code.*
Suppose first that $\sum A = 1$. Since each element of A lies beneath 1 in the natural partial order, it follows that each element of A is an idempotent. Thus $y_i = x_i$ for each $1 \leq i \leq m$. By Lemma 2.5, since A is an orthogonal set, it follows that $\{x_i\colon 1 \leq i \leq m\}$ is a prefix code. We prove that it is a maximal prefix code. Suppose not. Then there is a string y such that

$$\{x_i\colon 1 \leq i \leq m\} \cup \{y\}$$

is a prefix code. Thus $yy^{-1} \cdot x_i x_i^{-1} = 0$ for $1 \leq i \leq m$. But from distributivity in S we get that

$$yy^{-1} = yy^{-1}1 = \sum_{i=1}^{m} yy^{-1} \cdot x_i x_i^{-1},$$

but this implies that not all $yy^{-1} \cdot x_i x_i^{-1}$ can be zero. We therefore get a contradiction. It follows that A is a maximal prefix code, as claimed.

Conversely, suppose that $A = \{x_i x_i^{-1}\colon 1 \leq i \leq m\}$ is such that the x_i form a maximal prefix code. We prove that $\sum A = 1$. Put $C = \{x_i\colon 1 \leq i \leq m\}$. If $C = \{\varepsilon\}$ then the result is trivially true. By Lemma 2.4, there is a string u such that $ua_i \in C$ and $C' = C \setminus \{ua_i\colon 1 \leq i \leq m\} \cup \{u\}$ is a maximal prefix code. Observe that $|C'| < |C|$. Put $A' = \{vv^{-1}\colon v \in C'\}$. Thus $|A'| < |A|$. Then it is easy to check that $\sum A = \sum A'$ using our assumptions about S. This process can be iterated with A' replacing A above. The process will terminate when A' contains only the empty string at which point we will get that the union is the identity, as claimed.

2. *Let $A = \{u_i u_i\colon 1 \leq i \leq m\}$ be an orthogonal set of idempotents of P_n. Then $xx^{-1} = \sum A$ iff $A \preceq xx^{-1}$.*
Suppose first that $A \preceq xx^{-1}$. Then there is an element E of $D(P_n)$ such that Z_E is a maximal prefix code and $A = xEx^{-1}$. But then $\sum A = \sum xEx^{-1} = x(\sum E)x^{-1} = xx^{-1}$, using (1).

Conversely suppose that

$$xx^{-1} = \sum_{i=1}^{m} u_i u_i^{-1}.$$

Then $u_i u_i^{-1} \leq xx$ for each i. Hence $u_i = xw_i$ for some unique string w_i. Thus

$$xx^{-1} = \sum_{i=1}^{m} xw_i w_i^{-1} x^{-1}.$$

Now multiply on the left by x^{-1} and on the right by x and use the distributivity law to get

$$1 = \sum_{i=1}^{m} w_i w_i^{-1}.$$

Hence by (1), we have that $\{w_i \colon 1 \leq i \leq m\}$ is a maximal prefix code. ■

3. *Let $A = \{x_i y_i^{-1} \colon 1 \leq i \leq m\}$ be an orthogonal subset of P_n. Then $uv^{-1} = \sum x_i y_i^{-1}$ iff $A \preceq uv^{-1}$.*
From $A \preceq uv^{-1}$ and (1), we easily deduce that $\sum A = uv^{-1}$. Conversely, suppose that $\sum A = uv^{-1}$. Then $vv^{-1} = \sum y_i y_i^{-1}$. Thus by (2) there is a maximal prefix code Z_E such that $\{y_i y_i^{-1}\} = vEv^{-1}$. Elementary inverse semigroup theory gives $\{x_i y_i^{-1}\} = uEv^{-1}$ and so $A \preceq uv^{-1}$.

4. *Let $A = \{x_i y_i^{-1}\}$ and $B = \{u_j v_j^{-1}\}$. Then $\sum A = \sum B$ iff $A \equiv B$.*
The proof that $A \equiv B$ implies $\sum A = \sum B$ is straightforward and uses (1). We prove the converse. Suppose that $\sum A = \sum B$. Then $\sum A = \sum B \cdot A^{-1}A$. Put $C = B \cdot A^{-1}A$. For each i, we have that $x_i y_i^{-1} = \sum_j u_j v_j^{-1} \cdot y_i y_i^{-1}$. Thus by (3), we have that $C \preceq A$. For each j, we have that $u_j v_j^{-1} = \sum_i u_j v_j^{-1} \cdot y_i y_i^{-1}$. Thus by (3), we have that $C \preceq B$. Hence $A \equiv B$, as required.

We can now prove that S is isomorphic to C_n. Each element $s \in S$ can be written $s = \sum A$ for some finite orthogonal subset of P_n. Map s to $[A \cup \{0\}]$, the $\equiv$-equivalence class; this is unambiguous because $s = \sum B$ implies that $A \equiv B$. In this way we get a surjective function from S to C_n which is injective by what we have proved above. It is straightforward to check that we have a homomorphism and so an isomorphism. ■

We have proved that the polycyclic monoid P_n possesses a *unique* strong orthogonal completion C_n. The next lemma will lead to a simple way of calculating in C_n.

Lemma 3.6 *If $A \preceq B, C$ then there exists D such that $B, C \preceq D$.*

Proof Let $A = \{x_i y_i^{-1}\}$, $B = \{u_j v_j^{-1}\}$ and $C = \{w_k z_k^{-1}\}$. Then $A \preceq B$ implies that $A = \cup_j u_j E_j v_j^{-1}$ where the E_j correspond to maximal prefix codes, and $A \preceq C$ implies that $A = \cup_k w_k F_k z_k^{-1}$ where the F_k correspond to maximal prefix codes.

Observe that by Lemma 3.1 (v) and (vii), we have that $A^{-1}A \preceq B^{-1}C$ and $AA^{-1} \preceq BC^{-1}$. By Lemma 3.1(iv), it follows that $B^{-1}C$ and BC^{-1} are idempotents. Define

$$D = \max\{u_j v_j^{-1}, w_k z_k^{-1}\} \cup \{0\},$$

where 'max' means 'pick the maximal elements of'. Using our observation, and the Remark following Lemma 2.3, we deduce that D is a finite orthogonal subset of P_n.

I shall prove that $B \preceq D$; a similar argument proves that $C \preceq D$. To do this, it will be enough to prove the following. Let $w_k z_k^{-1} \in C$. Let B_k denote all the elements of B that lie beneath $w_k z_k^{-1}$. I shall prove that $B_k = w_k G_k z_k^{-1}$, where G_k corresponds to a maximal prefix code. We have that

$$F_k = \cup_j w_k^{-1} u_j E_j v_j^{-1} z_k.$$

Now $w_k^{-1} u_j = 0$ unless w_k and u_j are prefix-comparable, and $v_j^{-1} z_k = 0$ unless z_k and v_j are prefix comparable. If both are non-zero, then $(w_k z_k^{-1})^{-1} u_j v_j^{-1}$ and $w_k z_k^{-1}(u_j v_j^{-1})^{-1}$ are both non-zero idempotents. It follows that the elements are comparable — but $w_k z_k^{-1}$ is maximal. Thus the terms are only non-zero when $u_j v_j^{-1} \leq w_k z_k^{-1}$. Let $(u_j, v_j) = (w_k, z_k) p_j$. Then $G_k = \{p_j p_j^{-1}\}$ and $F_k = \cup_j p_j E_j p_j^{-1}$. The fact that G_k is associated with a maximal prefix code now follows from Lemma 2.11. ■

Calculations in C_n can be carried out in the following way. If $A \preceq B$ and $A \neq B$ then $|B| < |A|$. It follows that an increasing sequence $A_1 \preceq A_2 \preceq A_3 \ldots$ must stabilise in a finite number of steps. I shall call $\preceq$-maximal elements *irreducible*. Thus for each A there is an irreducible element B such that $A \preceq B$. By Lemma 3.6, this irreducible element is unique. It follows that $A \equiv B$ iff $A' = B'$, where $A \equiv A'$ and $B \equiv B'$, and A' and B' are irreducible. Elements of C_n can be written as formal finite sums $\sum_{i=1}^{m} x_i y_i^{-1}$ when $x_i y_i^{-1} \neq x_j y_j^{-1}$ implies that the elements are orthogonal. We require that the sum is commutative and idempotent and that left and right distributivity laws hold, and that $0 + xy^{-1} = xy^{-1} = xy^{-1} + 0$ for all $xy^{-1} \in P_n$. In addition, we require that $\sum_{i=1}^{n} a_i a_i^{-1} \equiv 1$. To determine whether two elements are $\equiv$-equivalent we carry out reductions using $\preceq_e$. Thus the sorts of calculations that Birget carries out, for example on page 602 of [3], can also be carried out in this formalism but extended to the whole of C_n.

4 Algebraic properties of C_n

In this section, I shall examine the semigroup-theoretic properties of the inverse monoid C_n.

In [12], we proved that the orthogonal completion of the polycyclic monoid on n generators, D_n, was isomorphic to the inverse monoid R_n of right ideal isomorphisms between the finitely generated right ideals of the free monoid on n generators. In this section, we shall prove an analogous result for the strong orthogonal completion C_n.

Let $A = A_n = \{a_1, \ldots, a_n\}$ and denote by A^ω the set of all (right) infinite strings over A. If X is a subset of A^* then XA^ω consists of all those infinite strings that have a finite prefix from X. I shall call such sets *right ideals* of A^ω. I shall say that they are *finitely generated* if X is finite. A bijection $f\colon XA^\omega \to YA^\omega$ between finitely generated right ideals is called a *right ideal* *isomorphism* if X and Y are finite prefix codes and there is a bijection $f_1 \colon X \to Y$ such that

$$f(xw) = f_1(x)w$$

for all $x \in X$ and $w \in A^\omega$. We denote by S_n the set of all right ideal isomorphisms between finitely generated right ideals of A^ω together with the empty function.

Remark Let X and Y be two finite prefix codes and let f_1 be a bijection from X to Y. Define f from XA^ω to YA^ω by $f(xw) = f_1(x)w$. Then f is a well-defined right ideal isomorphism.

Lemma 4.1 *The set S_n satisfies the following conditions:*

(i) *S_n is a groupoid under the restricted product.*

(ii) *If $f \in S_n$, where f: $XA^\omega \to YA^\omega$ and $X'A^\omega \subseteq XA^\omega$, then f restricted to $X'A^\omega$ also belongs to S_n.*

(iii) *The set of finitely generated right ideals is closed under intersection.*

We deduce that S_n is an inverse monoid.

Proof (i) Let f: $XA^\omega \to YA^\omega$ be an element of S_n. We show that f^{-1} is an element of S_n. Define g: $YA^\omega \to XA^\omega$ by $g(yw) = f_1^{-1}(y)w$. This is a well-defined element of S_n and it is easy to check that it is the inverse of f. Let g: $YA^\omega \to ZA^\omega$ be an element of S_n. Then it is easy to check that gf is also an element of S_n.

(ii) We show first that we may assume without loss of generality that each element of X' has as a prefix an element of X. From $X'A^\omega \subseteq XA^\omega$ we deduce that each element of X' is comparable with an element of X. Let $x' \in X'$. Then either x' is a prefix of some element of X, or some element of X is a prefix of x'. Suppose that there is no element $x \in X$ which is a prefix of x'. Then there are elements of X of which x' is a proper prefix. Let Z be the set of all strings such that $x'Z \subseteq X$. Then Z is a prefix code; we claim that Z is a *maximal* prefix code. Suppose not. Then there exists a string u such that u is not comparable with any element of Z. Thus $x'u$ cannot be comparable with any element of $x'Z$. Now $x'uw \in XA^\omega$ for any infinite string w. Thus $x'u$ is comparable with some element $x \in X$. By assumption, x cannot be a prefix of x'. Suppose that x is a prefix of $x'u$. Then $u = u'u''$ where $x = x'u'$. Thus $u' \in Z$ and u' is a prefix of u, which is a contradiction. Suppose that $x'u$ is a prefix of x. Then $x = x'uv$ for some v. Thus $uv \in Z$ and u is a prefix of uv, a contradiction. We have therefore proved that Z is a maximal prefix code.

Put $X'' = X' \setminus \{x'\} \cup x'Z$. For all maximal prefix codes Z, we have that $ZA^\omega = A^\omega$. Thus $X'A^\omega = X''A^\omega$. The element x' has been removed, and replaced by elements all of which live in X. Observe that X'' is also a prefix code. Continuing in this way, we can assume that each element of X' is either in X or has an element of X as a prefix (which is unique because X is a prefix code).

Under our assumption, let $x' \in X'$. Then $x' = xu$ for a unique $x \in X$ and string $u \in A^*$. Let Y' consist of the elements $f_1(x)u$. It is a prefix code, because X and Y are prefix codes. It is immediate that the image of $X'A^\omega$ under f is contained in $Y'A^\omega$ and that it is in fact equal to $Y'A^\omega$. The function g_1 from X' to Y' that takes $x' = xu$ to $f_1(x)u$ is injective and so surjective. Thus the function g: $X'A^\omega \to Y'A^\omega$ defined by $g(x'w) = g_1(x')w$ is the restriction of f to $X'A^\omega$.

(iii) Observe that $xA^\omega \cap yA^\omega$ is either empty or one is contained in the other. From this the result follows.

The final claim follows from the theory of inductive groupoids [8], but can also be seen directly from the observation that

$$fg = (f|E)(g^{-1}|E)^{-1},$$

where the product on the righthand side is a groupoid product, and where E is the intersection of the domain of f and the image of g. ■

Theorem 4.2 *The inverse monoids C_n and S_n are isomorphic.*

Proof Recall the definition of R_n from Theorem 2.6. Define a function θ: $R_n \to S_n$ which maps f: $XA^* \to YA^*$ to $\bar{f}$: $XA^\omega \to YA^\omega$ where $\bar{f}_1 = f$ restricted to X, and maps the empty function to the empty function. This is a surjective function which is easily seen to be a homomorphism. By construction it is 0-restricted, idempotent pure and identifies all essential idempotents. Thus by Proposition 3.3, the kernel of θ is $\equiv$ and so C_n is isomorphic to S_n, as required.■

Remark An alternative proof of the above theorem follows from Theorem 3.5: the inverse monoid S_n is easily seen to be a strong orthogonal completion of P_n.

Lemma 4.3 *Let X and Y be finite prefix codes. Then a necessary and sufficient condition for $XA^\omega = YA^\omega$ is that for all finite strings z we have that z is not prefix-comparable with any element of X iff z is not prefix-comparable with any element of Y.*

Proof Suppose first that $XA^\omega = YA^\omega$. Let z be a finite string that is not prefix-comparable with any element of X. Suppose that z is prefix-comparable with some element y of Y. Then $zu = yv$ for some finite strings u and v. There are now two possibilities: either $z = yq$ or $y = zq$ for some finite string q. Suppose the former. Then for all infinite strings w we have that $zw = yqw$. Thus $zA^\omega \subseteq YA^\omega$ and so $zA^\omega \subseteq XA^\omega$, which implies that z is prefix-comparable with some element of X which is a contradiction. Thus we must have that $y = zq$. But then $yA^\omega = zqA^\omega \subseteq XA^\omega$ and so z is comparable with an element of X, which is a contradiction. It follows that z is not prefix-comparable with any element of Y. The converse is proved similarly.

Suppose now that for all finite strings z we have that z is not prefix-comparable with any element of X iff z is not prefix-comparable with any element of Y. We shall prove that $XA^\omega = YA^\omega$. In fact, we shall prove that if for all finite strings z we have that z is not prefix-comparable with any element of $X \Rightarrow z$ is not prefix-comparable with any element of Y then $YA^\omega \subseteq XA^\omega$. Let $y \in Y$. Suppose that y is not prefix-comparable with any element of X. Then it cannot be prefix-comparable with any element of Y: a contradiction. Thus y is prefix-comparable with some element $x \in X$. Hence $yu = xv$ for some finite strings u and v. It follows that $y = xp$ or $x = yp$ for some finite string p. Suppose the former. Then $yA^\omega = xpA^\omega \subseteq xA^\omega \subseteq XA^\omega$ (which is heading in the right direction). Suppose the latter: $x = yp$ where p is not the empty string. Let Z be the set of all finite strings such that $yZ \subseteq X$. By assumption, Z is non-empty. Since X is a prefix code, so is Z. We prove that Z is a maximal prefix code. Suppose not. Then there exists a string d such that d is not prefix-comparable with any element of Z. Thus yd is not prefix-comparable with any element of X. By our hypothesis, it follows that yd is not prefix-comparable with any element of Y: a contradiction. Hence Z is a maximal prefix code. But $yA^\omega = yZA^\omega \subseteq XA^\omega$. We have proved that for all y, we have that $yA^\omega \subseteq XA^\omega$. Thus $YA^\omega \subseteq XA^\omega$, as required. ■

We say that the set of idempotents of an inverse semigroup S is 0-*disjunctive* if for all non-zero idempotents e and f where $e \neq f$ there is an idempotent g such that either $eg \neq 0$ and $fg = 0$ or $eg = 0$ and $fg \neq 0$.

Lemma 4.4 *The set of idempotents of the inverse semigroup C_n is 0-disjunctive.*

Proof We use the isomorphic copy S_n. Idempotents in S_n are identity functions on subsets of the form XA^ω. Suppose that $XA^\omega \neq YA^\omega$. Then by Lemma 4.3, there is a finite string z such that z is not prefix-comparable with any element of X but is prefix-comparable with some elements of Y or z is not prefix-comparable with any element of Y but is prefix-comparable with some elements of X. Suppose the former. Then $zA^\omega \cap XA^\omega = \emptyset$, but $zA^\omega \cap YA^\omega \neq \emptyset$. The result now follows. ■

Fundamental inverse semigroups are discussed in Section 5.2 of [8]. Our proof below uses the result that an inverse semigroup is fundamental iff the only centralisers of the idempotents are themselves idempotents; see Proposition 5.2.5 of [8].

Lemma 4.5 *The inverse monoid C_n is fundamental.*

Proof We shall prove that S_n is fundamental. Let $f \colon XA^\omega \to YA^\omega$ be an element of S_n which is not an idempotent. Thus there exists an element $xw \in XA^\omega$ such that $f(xw) \neq xw$. Since $f(xw) = f_1(x)w$ we have that $f_1(x) \neq x$. We may therefore find a $z \in A^*$ such that either (1) $x \in zA^*$ and $f_1(x) \notin zA^*$ or (2)$x \notin zA^*$ and $f_1(x) \in zA^*$. Let i be the identity function defined on zA^ω. This is an element of S_n. If (1) holds then if is defined but fi is empty, whereas if (2) holds then if is empty and fi is defined. In both cases, $if \neq fi$. Hence the only centralisers of the idempotents are idempotents, from which it follows that S_n is fundamental. ∎

Remark The above argument is a special case of a more general way of characterising fundamental inverse semigroups in topological terms due to Wagner; see Proposition 5.2.10 of [8].

Lemma 4.6 *The inverse monoid C_n is 0-simple*

Proof Observe that for any finite prefix code X and finite string z, we have that X and zX are both prefix codes having the same cardinality. Next observe that if Y is any prefix code and $y \in Y$ then $yXA^\omega \subseteq YA^\omega$. Thus the identity on XA^ω is isomorphic to the identity on yXA^ω which is contained in YA^ω. Thus C_n is 0-simple by Proposition 3.1.10 of [8]. ∎

Lemma 4.7 *The inverse monoid C_n has n $\mathcal{D}$-classes.*

Proof If $Z \subseteq A_n^*$ is a maximal prefix code, then $|Z| \equiv 1 \,(\operatorname{mod} n-1)$. Furthermore, for every $s \equiv 1 \,(\operatorname{mod} n-1)$ there is a finite maximal prefix code such that $s = |Z|$. Let Z be a finite maximal prefix code with s elements, and let r be such that $1 \leq r \leq n-2$, then $X_{r,s} = \{a_1, \ldots, a_r\} \cup a_n Z$ is a prefix code with $s + r$ elements.

Let X be any finite prefix code containing t elements. If $t \equiv 1 \,(\operatorname{mod} n-1)$ then there is a finite maximal prefix code Z with t elements. There is therefore a right ideal isomorphism from XA^ω to $ZA^\omega = A^\omega$. If on the other hand $t \equiv r' \,(\operatorname{mod} n-1)$ where $2 \leq r' \leq n-1$, then there is a finite prefix code $X' = X_{r'-1,s}$ having $t = s + (r'-1)$ elements, for some $s \equiv 1 \,(\operatorname{mod} n-1)$. Thus there is a right ideal isomorphism from XA^ω to $X'A^\omega = \{a_1, \ldots, a_{r'-1}, a_n\}A^\omega$. The distinct partial identities defined on the following sets A^ω, $\{a_1, a_n\}A^\omega$, ..., $\{a_1, \ldots, a_{n-2}, a_n\}A^\omega$ therefore form a transversal of the non-zero $\mathcal{D}$-classes. ∎

By Lemmas 4.4, 4.5, 4.6, 4.7 and [13], we have proved the following.

Theorem 4.8 *The inverse monoid C_n is congruence-free. In addition, C_2 is 0-bisimple, whereas for $n \geq 3$, C_n is 0-simple, but not 0-bisimple.* ∎

5 Representations

The goal of this section is to show how a class of representations of P_n can be used to construct isomorphic copies of C_n. We shall be interested in homomorphisms from P_n to $I(X)$, where X is a non-empty set, which are monoid homomorphisms and map the zero of P_n to the zero of $I(X)$. Such a homomorphism θ is an injection because P_n is congruence-free, and the image under θ is non-trivial because the zero and the identity are mapped to distinct elements. We call θ a *representation* of P_n in $I(X)$. We say that a representation is *strong* iff

$$1_X = \sum_{i=1}^{n} \theta(a_i a_i^{-1}).$$

Proposition 5.1 *With each strong representation $\theta\colon P_n \to I(X)$ we can associate a strong orthogonal completion C_n^{θ} of P_n.*

Proof The image P_n' of θ is an inverse submonoid of $I(X)$ isomorphic to P_n. Let C_n^{θ} be the disjoint union of the finite orthogonal subsets of P_n'. It is easy to check that this is an inverse submonoid of $I(X)$ and because θ is a strong representation it is a strong orthogonal completion of P_n'. ■

We now show how to construct strong representations of P_n. Let X be a set. The notation $\sqcup_1^n X$ means the disjoint union of n copies of the set X. Specifically, define

$$\sqcup_1^n X = \cup_{i=1}^{n} X \times \{i\}.$$

There are injective functions $\kappa_i\colon X \to \sqcup_1^n X$ given by $x \mapsto (x, i)$.

Proposition 5.2 *Let X be a non-empty set.*

(i) *Let $f_1, \ldots, f_n$ be n injective functions from X to itself whose images are disjoint. Map a_i to f_i and extend this in the obvious way to a map $\theta\colon P_n \to I(X)$. Then θ is a representation of P_n and every representation is obtained in this way.*

(ii) *The strong representations correspond to the case where the images of the f_i defined in (i) form a partition of X.*

(iii) *Let $X = \bigcup_{i=1}^{n} X_i$ be a partition of X into n disjoint non-empty subsets each having the same cardinality as X. For each choice $f_i\colon X \to X_i$ of bijections, we get a strong representation of P_n. Every strong representation of P_n arises in this way.*

(iv) *Every bijection from $\sqcup_1^n X$ to X determines and is determined by n injective functions $f_1, \ldots, f_n$ from X to itself whose images form a partition of X.*

Proof (i) Suppose we are given the functions f_i satisfying the stated properties. Define θ to map a_i to f_i. Then there is a unique extension of θ to a monoid homomorphism from the free monoid A_n^* to $I(X)$. We now extend θ to P_n by mapping xy^{-1} to $\theta(x)\theta(y)^{-1}$. The fact that θ is a homomorphism follows from the assumptions placed on the functions f_i. Conversely, given a representation $\theta\colon P_n \to I(X)$, and defining $f_i = \theta(a_i)$, we get functions satisfying the stated conditions and they clearly determine θ.

(ii) This is immediate.

(iii) This is just a reformulation of (ii).

(iv) Let $f\colon \sqcup_1^n X \to X$ be a bijection. Define $f_i\colon X \to X$ by $f_i = f\kappa_i$. These are injections. The images of the f_i are disjoint and their union is X. Now let f_i be n injections from X to X whose images are disjoint and their union is X. Define $f\colon \sqcup_1^n X \to X$ by $f(x,i) = f_i(x)$. It is easy to check that f is a bijection. These two processes are clearly mutually inverse. ■

We may summarise by saying that given an equivalence relation with n equivalence classes on a set X with the property that each equivalence class has the same cardinality as X then we can construct a strong representation of P_n in $I(X)$.

Example 5.3 We explore the above result in the case of $V = V_{2,1}$. Let $I = [0,1]$. Define

$$p^{-1}\colon [0, \frac{1}{2}] \to [0,1] \text{ by } x \mapsto 2x$$

and

$$q^{-1}\colon [\frac{1}{2}, 1] \to [0,1] \text{ by } x \mapsto 2x - 1.$$

This is almost, but not quite, a strong representation of P_2, when we map a_1 to p and a_2 to q. We shall now construct from this a genuine strong representation. A *dyadic rational* in I is a rational number that can be written in the form $\frac{a}{2^b}$ for some natural numbers a and b. Let I' be the unit interval with the dyadic rationals removed. The maps p and q and their inverses map dyadic rationals to dyadic rationals. We may therefore define

$$p'^{-1}\colon [0, \frac{1}{2}]' \to [0,1]' \text{ by } x \mapsto 2x$$

and

$$q'^{-1}\colon [\frac{1}{2}, 1]' \to [0,1]' \text{ by } x \mapsto 2x - 1$$

where the primes on the intervals mean that dyadic rationals have been removed. It follows that we get a strong representation of P_2 on I'.

Consider the following two elements of the strong orthogonal completion of P_2 constructed from the above strong representation

$$\alpha' = p'^2 p'^{-1} + p'q'(q'p')^{-1} + q'q'^{-2}$$

and

$$\beta' = p'p'^{-1} + q'p'^2(q'p')^{-1} + q'p'q'(q'^2p')^{-1} + q'^2q'^{-3}.$$

The maps α' and β' are bijections defined on I'. Define now functions A and B on I as follows (computed from the representations of α' and β' above):

$$A(x) = \begin{cases} \frac{x}{2} & \text{for } 0 \le x \le \frac{1}{2} \\ x - \frac{1}{4} & \text{for } \frac{1}{2} \le x \le \frac{3}{4} \\ 2x - 1 & \text{for } \frac{3}{4} \le x \le 1 \end{cases}$$

and

$$B(x) = \begin{cases} x & \text{for } 0 \le x \le \frac{1}{2} \\ \frac{x}{2} + \frac{1}{4} & \text{for } \frac{1}{2} \le x \le \frac{3}{4} \\ x - \frac{1}{8} & \text{for } \frac{3}{4} \le x \le \frac{7}{8} \\ 2x - 1 & \text{for } \frac{7}{8} \le x \le 1 \end{cases}$$

It can be checked that A restricted to I' is α', and B restricted to I' is β'.

In fact, α' and β' generate the subgroup F of the Thompson group V, and the maps A and B of I are one of the common ways of defining this subgroup [4]. We can see that they arise naturally from a specific and simple strong representation of P_2. ■

Acknowledgements I am grateful to the referee for spotting a couple of errors and a lacuna in a proof in the first version of this paper.

References

[1] L. Bartholdi, R. Grigorchuk, V. Nekrashevych, From fractal groups to fractal sets, *Fractals in Graz* (eds P. Grabner, W. Woess) Trends in Mathematics, Birkhäuser Verlag, 2003, 25–118.

[2] J. Berstel, D. Perrin, *Theory of codes*, Academic Press, 1985.

[3] J.-C. Birget, The groups of Richard Thompson and complexity, *Inter. J. Alg. and Comput.* **14** (2004), 569–626.

[4] J. W. Cannon, W. J. Floyd, W. R. Parry, Introductory notes on Richard Thompson's groups, *Enseign. Math.* (2) **42** (1996), 215–256.

[5] T. Ceccherini-Silberstein, R. Grigorchuk, P. de la Harpe, Amenability and paradoxical decompositions for pseudogroups and for discrete metric spaces, *Tr. Mat. Inst. Steklova* **224** (1999), 68–111.

[6] S. Eilenberg, *Automata, languages and machines* volume A, Academic Press, New York, 1974.

[7] R. H. Gilman, Formal languages and infinite groups, *DIMACS Series in Discrete Mathematics and Theoretical Computer Science* **25** (1996), 27–51.

[8] M. V. Lawson, *Inverse semigroups: the theory of partial symmetries*, World Scientific, 1998.

[9] M. V. Lawson, Constructing inverse semigroups from category actions, *J. Pure and Applied Alg.* **137** (1999), 57–101.

[10] M. V. Lawson, A correspondence between balanced varieties and inverse monoids, *Inter. J. Alg. and Comput.* **16** (2006), 887–924.

[11] M. V. Lawson, A class of subgroups of the Thompson group V, accepted by *Semigroup Forum*.

[12] M. V. Lawson, Orthogonal completions of the polycyclic monoids, accepted by *Communications in Algebra*.

[13] W. D. Munn, Congruence-free inverse semigroups, *Quart. J. Math. Oxford* (2) **25** (1974), 463–484.

[14] M. Nivat, J.-F. Perrot, Une généralisation du monoïde bicyclique, *Comptes Rendus de l'Académie des Sciences de Paris* **271** (1970), 824-827.

[15] A. L. T. Paterson, *Groupoids, inverse semigroups, and their operator algebras*, Birkhäuser, 1999.

[16] J. Renault, *A groupoid approach to C^*-algebras*, Lecture Notes in Mathematics 793, Springer-Verlag, 1980.

[17] E. A. Scott, A construction which can be used to produce finitely presented infinite simple groups, *J. Alg.* **90** (1984), 294–322.