International Journal of Algebra and Computation
Vol. 25, Nos. 1 & 2 (2015) 293–300
© World Scientific Publishing Company
DOI: 10.1142/S0218196715400111

A new proof of the locality of R

Howard Straubing
Computer Science Department, Boston College
Chestnut Hill, Massachusetts 02476, USA
straubin@cs.bc.edu

Received 29 May 2013
Accepted 24 December 2014
Published 2 February 2015

Communicated by J. E. Pin and M. Sapir

We give a simple proof of a wreath product decomposition for locally $\mathcal{R}$-trivial finite categories. As immediate consequences we obtain two classic results of Stiffler on the decomposition of $\mathcal{R}$-trivial monoids and locally $\mathcal{R}$-trivial semigroups. A small modification of the argument provides a new proof of a recent theorem of Bojańczyk, Straubing and Walukiewicz on the decomposition of forest algebras.

Keywords: Finite semigroups; finite categories; forest algebras.

Mathematics Subject Classification: 20M07, 20M35

1. Statement of the Results

We give simple new proofs of two old theorems of Stiffler [6] on the decomposition of finite semigroups.

This section is devoted to a statement of the classic results. In Secs. 2 and 3 we prove the principal theorems. In Sec. 4 we indicate how the same proof idea can be used to obtain a recent result on the wreath product decomposition of forest algebras, originally proved by Bojańczyk, Walukiewicz and Straubing [1].

Most of the notation and terminology concerning wreath products, transformation semigroups, pseudovarieties and products of pseudovarieties are from Eilenberg [4]. See also [8], which employs the same notation and includes the basics of the algebra of finite categories. Much more on finite categories can be found in the original paper of Tilson [9].

If m, m' are elements of a monoid M then we write $m \leq_{\mathcal{R}} m'$ if $m = m'm''$ for some $m'' \in M$. We write $m \equiv_{\mathcal{R}} m'$ if both $m \leq_{\mathcal{R}} m'$ and $m' \leq_{\mathcal{R}} m$. We extend this notion to categories: We write $x \leq_{\mathcal{R}} y$ for two arrows in a category if $x = yz$ for some arrow z. Observe that this requires x and y to be coinitial — that is, x and y to have the same initial object.

We denote by $\mathbf{R}$ the pseudovariety of $\mathcal{R}$-trivial finite monoids; that is, monoids M in which each $\equiv_{\mathcal{R}}$-class has one element. We denote by U_1 the monoid $\{0,1\}$ with the usual multiplication. We also, through a standard abuse of notation, denote by U_1 the transformation monoid $(\{0,1\},\{0,1\})$ defined by the right action of U_1 on itself. We denote by $\circ$ the wreath product of right transformation monoids. If X is a transformation monoid then we denote by $X^{[k]}$ the k-fold wreath product

$$\underbrace{X \circ \cdots \circ X}_{k \text{ times}}.$$

The first theorem of Stiffler is as follows.

Theorem 1.1. *Let M be a finite monoid. Then $M \in \mathbf{R}$ if and only if $M \prec U_1^{[k]}$ for some $k > 0$.*

We note that it is quite easy to prove that $\mathcal{R}$-triviality is preserved under wreath product, so that the "hard" part of Theorem 1.1 is the "only if" direction, that every $\mathcal{R}$-trivial monoid admits such a decomposition.

The second theorem of Stiffler is customarily stated as an equation relating two operations on pseudovarieties:

Theorem 1.2.

$$\mathbf{LR} = \mathbf{R} * \mathbf{D}.$$

Here $\mathbf{LR}$ consists of all finite semigroups S such that for every idempotent $e \in S$, the monoid eSe is $\mathcal{R}$-trivial. $\mathbf{D}$ denotes the pseudovariety of definite semigroups — those finite semigroups S that satisfy $se = e$ for all $s \in S$ and idempotents $e \in S$. The symbol $*$ represents the wreath product operation on pseudovarieties. Once again, one inclusion in the above theorem is easy: any nontrivial pseudovariety $\mathbf{V}$ of finite monoids satisfies $\mathbf{V} * \mathbf{D} \subseteq \mathbf{LV}$. So the real content of Theorem 1.2 is the fact that every semigroup in $\mathbf{LR}$ divides the wreath product of an $\mathcal{R}$-trivial monoid and a definite semigroup.

Stiffler's original motivation was the classification of the smallest wreath product-closed pseudovarieties containing certain "prime", or indecomposable transformation semigroups. Thus $\mathbf{R}$ appears as the wreath product closure of U_1, $\mathbf{D}$ as the wreath product closure of the transformation semigroup $D_1 = (\{a,b\},\{a,b\})$, with $qx = x$ for all $q, x \in \{a,b\}$, and $\mathbf{LR}$ as the wreath product closure of $\{U_1, D_1\}$.

Theorems 1.1 and 1.2 have some important consequences in formal language theory: For instance, they provide characterizations of fragments of linear temporal logic in which only the "future" and "next" operators, but not the "until" operator, are available [3].

Theorem 1.2 follows from (and is in fact equivalent to) a more general result about finite categories. A category $\mathcal{C}$ is said to be *locally* $\mathbf{R}$-trivial if each of the *base monoids* $\mathrm{Hom}_{\mathcal{C}}(c,c)$, $c \in \mathrm{Obj}(\mathcal{C})$ is $\mathcal{R}$-trivial. We denote by $\ell\mathbf{R}$ the family of locally $\mathcal{R}$-trivial finite categories.

We say $\mathcal{C}$ is *globally* $\mathcal{R}$-trivial if $\mathcal{C} \prec M$, where M is $\mathcal{R}$-trivial. This last relation means that for each arrow $x \in \mathrm{Hom}_{\mathcal{C}}(c,d)$ there is a nonempty set $M_x \subseteq M$ of *covers* of x with the following properties:

- $1 \in M_{1_c}$ for each $c \in \mathrm{Obj}(C)$.
- (Injectivity) If x, y are distinct coterminal arrows of $\mathcal{C}$ — that is, if $x, y \in \mathrm{Hom}_{\mathcal{C}}(c,d)$ for some objects c, d — then $M_x \cap M_y = \emptyset$.
- (Multiplicativity) If x, y are consecutive arrows — that is, if $x \in \mathrm{Hom}_{\mathcal{C}}(c,d)$, $y \in \mathrm{Hom}_{\mathcal{C}}(d,e)$ for some objects c, d, e, so that the product $xy \in \mathrm{Hom}_{\mathcal{C}}(c,e)$ is defined — then, $M_x M_y \subseteq M_{xy}$.

The family of globally $\mathcal{R}$-trivial categories is denoted $g\mathbf{R}$.

Theorem 1.3.

$$\ell\mathbf{R} = g\mathbf{R}.$$

Once again, inclusion from right to left holds for arbitrary pseudovarieties and is a trivial consequence of the definition. Theorem 1.2 follows from Theorem 1.3 by a general principle for translating such "local–global" theorems for categories into theorems of the form "$\mathbf{LV} = \mathbf{V} * \mathbf{D}$". (This is the "Delay Theorem"; see [9, 7].)

Stiffler's original proofs are based on a study of ideal structure of the semigroups concerned. Eilenberg [4] proves Theorems 1.1 and 1.2 by a classification of prime transformation semigroups. More recently Steinberg [5] gave proofs of these theorems by generalizing results on ideal structure to the setting of categories. Our approach is quite different, and considerably easier.

2. Proof of Theorem 1.1

Let M be an $\mathcal{R}$-trivial monoid. $\mathcal{R}$-triviality guarantees that we can order the elements of M as

$$M = \{m_1, \ldots, m_n\},$$

where $m_i \leq_{\mathcal{R}} m_j$ implies $i \geq j$. In particular $m_1 = 1$. We encode elements of M as bit strings of length n, which we write sometimes as n-tuples, and sometimes as strings. The encoding is given by

$$\widetilde{m_i} = (1, \ldots, 1, 0, \ldots, 0) = 1^{n-i-1}0^{i-1}.$$

Because we deal with wreath product decompositions of right transformation semigroups, we typically number the components of an n-tuple of bits as $(b_n, \ldots, b_1)$.

Let $m \in M$. We set

$$\widehat{m} = (f_n^{[m]}, \ldots, f_1^{[m]}),$$

where $f_1^{[m]} \in U_1$, and where for $j > 1$,

$$f_j^{[m]} : \{0,1\}^{j-1} \to U_1.$$

The maps f_j are defined as follows: If $j \geq k$, then $f_j^{[m]}(1^{j-k}0^{k-1})$ is the jth component of $\widetilde{m_k m}$. This includes the case where $j = k$, in which case we have $f^{[m]}(0^{j-1}) = 1$ if $m_j m = m_j$ and 0 if $m_j m$ is strictly $<_{\mathcal{R}}$-below m_j. It also includes the case $j = 1$, and gives $f_1^{[m]} = 1$ if and only if $m = 1$. We define the functions $f^{[m]}$ arbitrarily on $(j-1)$-tuples that do not have the form described above.

The n-tuple of functions $\widehat{m}$ is an element of the underlying monoid of the n-fold wreath product $U_1^{[n]}$, and $\widehat{m}$ acts on bit strings $(b_n, \ldots, b_1)$ by

$$(b_n, \ldots, b_1)\widehat{m} = (b_n \cdot f_n^{[m]}(b_{n-1}, \ldots, b_1), \ldots, b_2 \cdot f_2^{[m]}(b_1), b_1 \cdot f_1^{[m]}).$$

We thus prove the desired division (in fact, an embedding of M into the wreath product) by establishing

$$\widetilde{m_k} \cdot \widehat{m} = \widetilde{m_k m}.$$

Let $j \in \{1, \ldots, n\}$. If $j \geq k$ the jth components of $\widetilde{m_k} \cdot \widehat{m}$ and $\widetilde{m_k m}$ are equal by definition of $\widehat{m}$. If $j < k$, then the jth component of $\widetilde{m_k}$ is 0, and thus the jth component of $\widetilde{m_k} \cdot \widehat{m}$ is 0. Since $m_k m = m_r$ for some $r \geq j$, the jth component of $\widetilde{m_k m}$ is 0 as well.

3. Proof of Theorem 1.3

Lemma 3.1. *Let $\mathcal{C} \in \ell\mathbf{R}$. Let $x, y \in \mathrm{Hom}_{\mathcal{C}}$ be coterminal arrows. If $x \equiv_{\mathcal{R}} y$ then $x = y$.*

Proof. If $x \equiv_{\mathcal{R}} y$ then there exist $w, z \in \mathrm{Hom}_{\mathcal{C}}$ such that $y = xw$, $x = yz$. Since x, y are coterminal, w and z are loops at the same object: that is, $w, z \in \mathrm{Hom}_{\mathcal{C}}(c, c)$ for some object c. Since $\mathcal{C} \in \ell\mathbf{R}$, the base monoid at c is $\mathcal{R}$-trivial, and thus for sufficiently large n,

$$(wz)^n w = (wz)^n,$$

so

$$y = x(wz)^n w = x(wz)^n = x. \qquad \square$$

We now turn to the proof of Theorem 1.3 itself. Let $\mathcal{C}$ be a locally $\mathcal{R}$-trivial category. The $\mathcal{R}$-classes $\{R_1, \ldots, R_n\}$ of $\mathcal{C}$ are partially ordered by $\leq_{\mathcal{R}}$. As before, we can impose a total order that extends this, so we can suppose that $R_i \leq_{\mathcal{R}} R_j$ implies $i \geq j$. Let M be the set of *increasing partial right transformations* on $\{1, \ldots, n\}$. That is, M consists of functions f such that $i \cdot f \geq i$ for all $i \in \{1, \ldots, n\}$ provided $i \cdot f$ is defined. M is clearly a monoid under composition with the identity function as the identity element, and is $\mathcal{R}$-trivial.

We cover arrows of $\mathcal{C}$ by elements of M according to the following scheme: Let $x \in \mathrm{Hom}(c, d)$ be an arrow of $\mathcal{C}$. We cover x by the partial transformation f_x, where $i \cdot f_x = j$ if and only if there is an arrow $y \in \mathrm{Hom}(b, c)$ such that $y \in R_i$ and $yx \in R_j$. By Lemma 3.1, there can be at most one arrow in R_i with final object c, so such a

y, if it exists, is unique. Thus f_x is well-defined. In particular, each identity arrow 1_c is covered by the transformation that is the identity on $\mathcal{R}$-classes that contain an arrow with terminal object c, and undefined otherwise. We will also cover each identity arrow 1_c by the identity element 1 of M.

It remains to show that this scheme defines a division of categories. By definition, each 1_c is covered by the identity of M. We show the multiplicative property: Let $x \in \mathrm{Hom}(c, d)$, $y \in \mathrm{Hom}(d, e)$ be consecutive arrows. We first suppose that neither x nor y is an identity arrow. Then the only monoid elements covering x and y are the partial transformations f_x, f_y. We need to show that $f_x f_y$ covers xy. This will follow from

$$f_x f_y = f_{xy}.$$

To verify this identity, suppose $i \cdot f_x f_y = j$. Let $i \cdot f_x = k$. There is thus an arrow $z \in R_i$ such that $zx \in R_k$. Since $k \cdot f_y = j$, there is an arrow $z' \in R_k$ with $z'y \in R_j$. By Lemma 3.1, $z' = zx$, so $z(xy) \in R_j$, and thus $i \cdot f_{xy} = j$. Conversely, if $i \cdot f_{xy} = j$, then there is $z \in R_i$ with $zxy \in R_j$. Letting R_k be the $\mathcal{R}$-class of zx, we find $i \cdot f_x = k$ and $k \cdot f_y = j$. Thus $i \cdot (f_x f_y) = (i \cdot f_x) f_y$ whenever either side of this equation is defined. In the case where x is an identity arrow 1_c, then x is also covered by $1 \in M$, and we have $y = 1_c y$ is covered by $1 \cdot f_y = f_y$, and similarly if y is an identity arrow.

We now show the injectivity property: Suppose $x, y \in \mathrm{Hom}(c, d)$ are both covered by $m \in M$. If neither x nor y is an identity arrow, then this implies $f_x = f_y$. Let R_i be the $\mathcal{R}$-class of 1_c. Since $1_c x = x$, $j = i \cdot f_x$ where R_j is $\mathcal{R}$-class of x. Since $f_x = f_y$, we also have $i \cdot f_y = j$, and thus R_j is the $\mathcal{R}$-class of y. Again by Lemma 3.1, $x = y$. Suppose one of x, y is an identity arrow; without loss of generality we can suppose $x = 1_c$ and $c = d$. Then we might have x covered by 1 because x is an identity arrow, and y covered by 1 because $f_y = 1$. But Lemma 3.1 implies that if $f_y = 1$, then y is a right identity element of the monoid $\mathrm{Hom}(c, c)$, and hence the identity of $\mathrm{Hom}(c, c)$. So $y = 1_c = x$. This completes the proof.

4. Decomposition of Forest Algebras

We can adapt the simple scheme of Theorem 1.1 to settings where there is some additional structure on M, and thereby obtain a new proof of a recent theorem developed to study temporal logics on trees [1].

A *forest algebra* is a transformation monoid (H, V) where H is itself a monoid. We denote the product in H additively, so that its identity is denoted 0. If there is an absorbing element (i.e. a zero) in H, we denote it ∞. We require that right and left addition in H be represented by the action of V on H, that is, for each $h \in H$ there are elements $v_h, {}_h v \in V$ such that for all $g \in H$,

$$g \cdot v_h = g + h, \quad g \cdot {}_h v = h + g.$$

Apart from this, there is no connection presumed between the action of V on H and the operation in H, but the definition of division is required to take the operation on H into account: If $(H, V), (H', V')$ are forest algebras, then

$$(H', V') \prec (H, V)$$

if and only if there is a surjective monoid homomorphism $\Phi : H_1 \to H'$, where H_1 is a submonoid of H, and for all $v \in V'$ there exists an element $\hat{v}$ of V such that for all $h \in H_1$,

$$\Phi(h\hat{v}) = \Phi(h)v.$$

(In particular, $H_1\hat{v} \subseteq H_1$.)

The wreath product of forest algebras is defined exactly as for transformation monoids: the state set $H_2 \times H_1$ of $(H_2, V_2) \circ (H_1, V_1)$ is given the monoid structure of the direct product.

Forest algebras were introduced by Bojańczyk and Walukiewicz [2] as a tool in the study of regular languages of unranked trees and forests. The problem of characterizing many natural-looking logically-defined classes of such languages is equivalent to computing the wreath product closures of certain simple forest algebras [1]. We will not describe this connection to logic here, but instead present our result as a purely algebraic decomposition theorem.

The analogue of the transformation monoid U_1 is

$$\mathcal{U}_1 = (\{0, \infty\}, \{1, 0\}),$$

where 1 is the identity transformation, and $c \cdot 0 = \infty$ for $c \in \{0, \infty\}$. Note that this is *identical* to U_1, except that we have provided an additive structure for the state set.

The following theorem, proved in [1], is the analogue for forest algebras of Theorem 1.1.

Theorem 4.1. *Let (H, V) be a finite forest algebra. The following are equivalent*:

- *H is idempotent and commutative, and for all $h \in H, v \in V$, $hv + h = hv$.*
- *(H, V) divides an iterated wreath product of copies of $\mathcal{U}_1 = (\{0, \infty\}, \{1, 0\})$.*

Proof. That the second condition implies the first is easy, and we have nothing to add to what already appears in [1]. For the converse, we define, for $h, h' \in H$, $h \leq h'$ if $h = h' + g$ for some $g \in H$. Since H is assumed to be idempotent and commutative, this is equivalent to $h + h' = h$, because $h + h' = h' + g + h' = h' + g = h$. The identity $hv + h = hv$ can then be rewritten as $hv \leq h$.

We first encode elements h of H by H-tuples τ^h from $\{0, \infty\}$. If $h' \leq h$, then we set the h'-component of τ^h to 0, otherwise to ∞. We are now in a position to apply our proof scheme: Since H is idempotent and commutative, $\leq$ is a partial order on H, and thus $h \in H$ is completely determined by its encoding τ^h. Since (H, V) satisfies the identity $hv \leq h$, we obtain each component τ^{hv} from the corresponding component of τ^h by the action in $\mathcal{U}_1$. The only additional thing we need to check is that the additive structure is preserved by the encoding.

For this we show $\tau_{h_1+h_2} = \tau_{h_1} + \tau_{h_2}$. If the h-component of $\tau^{h_1+h_2}$ is 0, then $h \le h_1 + h_2$, and we have $h_1 + h_2 \le h_1$, $h_1 + h_2 \le h_2$. Thus the h-components of τ^{h_1} and τ^{h_2} are both 0, and so the h-component of $\tau^{h_1} + \tau^{h_2}$ is 0. Conversely, if the h-component of $\tau^{h_1} + \tau^{h_2}$ is 0, then the h-components of τ^{h_1} and τ^{h_2} are both 0, and thus $h \le h_1$, $h \le h_2$. This implies $h = h + h_1 = h + h_2$, so $h = h + h =$ $h_1 + h_2 + h + h = h_1 + h_2 + h$, and thus $h \le h_1 + h_2$, so the h-component of $\tau^{h_1+h_2}$ is 0.

We thus have a homomorphism, in fact an isomorphism, from $\{\tau^h : h \in H\}$ onto H. We now linearly order the elements of H so that $h \le h'$ implies h' occurs to the right of h. Thus each element τ^h is represented by an ordered H-tuple $(a_k, \ldots, a_1)$, where $k = |H|$. The rest of the proof is essentially identical to that of Theorem 1.1. $\square$

Of course, if (H, V) satisfies the conditions of the theorem, V is an $\mathcal{R}$-trivial monoid. However, this is not sufficient. For example, suppose $H = \{0, \infty\} \times \{0, \infty\}$ and V is generated by transformations a and b, where

$$(0,0)a = (\infty,0)a = (\infty,0), \quad (0,0)b = (\infty,0)b = (0,\infty)a = (0,\infty)b = (0,\infty).$$

It is easy to check that the underlying monoid is $\mathcal{R}$-trivial, and that H is idempotent and commutative. However we have

$$(\infty,0)b + (\infty,0) = (\infty,\infty) \ne (0,\infty) = (\infty,0)b,$$

so the identity $hv + h = hv$ is not satisfied.

Acknowledgments

Thanks to Benjamin Steinberg and Jean-Eric Pin for some helpful discussions and suggestions, and to the anonymous referees for invaluable suggestions.

The author was supported by the National Science Foundation Under Grant No. CCF0915056.

References

[1] M. Bojańczyk, H. Straubing and I. Walukiewicz, Wreath products of forest algebras, with applications to tree logics, *Log. Meth. Comput. Sci.* **8**(3) (2012) 1–39.

[2] M. Bojańczyk and I. Walukiewicz, Forest algebras, in *Logic and Automata*: *History and Perspectives*, eds. E. Grädel, J. Flum and T. Wilke (Amsterdam University Press, 2008), pp. 107–132.

[3] J. Cohen, D. Perrin and J. E. Pin, On the expressive power of temporal logic, *J. Comput. System Sci.* **46**(3) (1993) 271–294.

[4] S. Eilenberg, *Automata, Languages and Machines*, Vol. B (Academic Press, 1974).

[5] B. Steinberg, A modern approach to some results of Stiffler, in *Semigroups and Languages*, eds. I. Araujo, M. Branco, V. Fernandes and G. Gomes (World Scientific, 2004), pp. 240–251.

[6] P. E. Stiffler, Extensions of the fundamental theorem of finite semigroups, *Adv. Math.* **11**(2) (1973) 159–209.

[7] H. Straubing, Finite semigroup varieties of the form $\mathbf{V} * \mathbf{D}$, *J. Pure Appl. Algebra* **36** (1985) 53-94.
[8] H. Straubing, *Finite Automata, Formal Logic and Circuit Complexity* (Birkhäuser, 1994).
[9] B. Tilson, Categories as algebra: An essential ingredient in the theory of monoids, *J. Pure Appl. Algebra* **48** (1987) 83–198.

Copyright of International Journal of Algebra & Computation is the property of World Scientific Publishing Company and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.