Canad. Math. Bull Vol. 62 (1), 2019 pp. 199–208
http://dx.doi.org/10.4153/CMB-2018-014-8

Merge Decompositions, Two-sided Krohn–Rhodes, and Aperiodic Pointlikes

Samuel J. van Gool and Benjamin Steinberg

Abstract. This paper provides short proofs of two fundamental theorems of finite semigroup theory whose previous proofs were significantly longer, namely the two-sided Krohn-Rhodes decomposition theorem and Henckell's aperiodic pointlike theorem. We use a new algebraic technique that we call the merge decomposition. A prototypical application of this technique decomposes a semigroup T into a two-sided semidirect product whose components are built from two subsemigroups T_1, T_2, which together generate T, and the subsemigroup generated by their setwise product T_1T_2. In this sense we decompose T by merging the subsemigroups T_1 and T_2. More generally, our technique merges semigroup homomorphisms from free semigroups.

Introduction

Eilenberg's variety theorem [3] provides a dictionary between formal language theory and finite semigroup theory. In particular, membership problems in certain Boolean algebras of regular languages (languages accepted by finite automata) are equivalent to membership problems in varieties of finite semigroups. Other natural problems in language theory transform into questions about pointlikes with respect to a variety of finite semigroups, a notion introduced by Henckell and Rhodes [5]. An important problem in language theory is the separation problem: given disjoint regular languages, determine whether they can be separated by a language from a given variety of regular languages. The separation problem is equivalent to decidability of pointlike pairs [1], which is strictly stronger than the membership problem [2,12]. Decidability of pointlikes can be used to obtain decidability of membership problems of related varieties. For instance, the second author showed, using the decidability of aperiodic pointlikes and Zelmanov's solution to the restricted Burnside problem, that the join of the variety of aperiodic semigroups with any variety of finite groups of bounded exponent has decidable membership problem, answering a question of Rhodes and Volkov [15].

The first decidability result on pointlikes was Henckell's theorem on the decidability of aperiodic pointlikes [5], which for a long time was considered one of the most difficult results in the subject. Henckell not only provided a decidability algorithm, he also gave an elegant structural description of the aperiodic pointlike sets that we

Received by the editors September 15, 2017.
Published electronically May 18, 2018.
Author S. J. v. G. was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant #655941. Author B. S. was supported by United States–Israel Binational Science Foundation #2012080 and NSA MSP #H98230-16-1-0047.
AMS subject classification: **20M07**, 20M35, 68Q70.
Keywords: Krohn-Rhodes theorem, aperiodic pointlikes.

call Henckell's formula. Henckell's original proof idea is a variation on the holonomy proof [6] of the Krohn–Rhodes theorem [8] for directly decomposing semigroups into wreath products. The difficult part of Henckell's proof is to prove that a certain semigroup is aperiodic, which he does by wreath product embeddings. In [7], Henckell, Rhodes, and the second author provided a direct proof that Henckell's semigroup is aperiodic, leading to a simpler and shorter proof of his main theorem. They also extended the theorem beyond aperiodic pointlikes to the variety of semigroups whose subgroups have prime divisors belonging to a fixed set π of primes (the restriction of this proof to the aperiodic case can be found in [13, Ch. 4]). Although simpler than Henckell's original proof [5], the proof in [7] is still non-trivial. The authors have extended the methods of [5] to compute pointlikes for other varieties determined by groups [4].

Recently, Place and Zeitoun [11] gave a new proof of the decidability of aperiodic pointlikes, which, unlike the previous proofs, is inductive. They use a language theoretic reformulation of the problem of computing pointlike sets and the McNaughton–Schützenberger theorem that the aperiodic languages are precisely the first order definable languages [16]. The Place–Zeitoun approach follows the inductive proof scheme of the Krohn-Rhodes theorem (the so-called '$V \cup T$' argument [9, 13]) later used by Wilke in the logic context [17], but done in the power set of the semigroup.

This paper introduces a new algebraic tool, in Section 2, that we call the *merge decomposition*. In Section 3, we use this tool to give a short proof of the inductive step of the two-sided Krohn-Rhodes decomposition theorem (*cf.* [13, Ch. 5]). Then, in Section 4, we use the merge decomposition in the inductive step of the Place–Zeitoun inductive scheme to give a short algebraic proof of Henckell's formula for the aperiodic pointlikes. We feel that our approach has several advantages over previous approaches [5, 7, 11]. First of all, it leads to a significantly shorter proof than the previous ones. Secondly, we obtain the best known bound on the length of a two-sided Krohn–Rhodes decomposition of the aperiodic semigroup witnessing pointlikes (or, equivalently, quantifier-depth of the first order formula giving separation).

An advantage of our approach is that it is potentially extendable beyond the realm of first order logic on words. For instance, decidability of pointlikes for some larger varieties than aperiodics is obtained in [7]. We leave this to future work.

1 Preliminaries

We assume familiarity with notions from the theory of semigroups, in particular, relational morphisms and divisions, the wreath product (denoted $\wr$), and the two-sided semidirect product of semigroups (denoted $\bowtie$) and of varieties of finite semigroups (denoted $**$); see, *e.g.,* [13, Ch. 1]. Throughout the paper, we call 'variety' what is called '*pseudo*variety' in [13].

Augmented Semigroups

Let T be a finite semigroup. Let T^I be the monoid obtained by adjoining a new identity, I, to T and T^0 the semigroup obtained by adjoining a new zero to T. We denote by **SL** the variety of finite semilattices and by U_1 the two-element semilattice.

https://doi.org/10.4153/CMB-2018-014-8 Published online by Cambridge University Press

Fact 1.1 *If a variety* $\mathbf{V}$ *contains* T *and* $\mathbf{SL}$*, then* $T^0 \in \mathbf{V}$*. If a variety* $\mathbf{V}$ *contains* T*,* $\mathbf{SL}$*, and is generated by monoids, then* $T^I \in \mathbf{V}$*.*

Proof The first statement is true, because T^0 is a homomorphic image of $T \times U_1$ [3, Ex. I.9.2]. For the second statement, we distinguish two cases. If T is a monoid, then T^I embeds in $T \times U_1$, where U_1 denotes the two-element semilattice [3, Ex. I.9.1]. If T is not a monoid, then T divides some monoid $M \in \mathbf{V}$, and since T is not a monoid, it follows that T^I divides the same monoid M. ∎

The semigroup T acts faithfully on T^I by multiplication on the right, and thus T embeds into the semigroup of total functions on T^I; we identify every element $t \in T$ with the corresponding right multiplication map. Further, for every $t \in T^I$, we denote by $t^\sharp$ the function with constant value t. We define $T^\sharp := T \cup \{t^\sharp : t \in T^I\}$, the semigroup consisting of the right multiplication maps and the constant maps. Thus, $T^\sharp$ naturally acts on T on the right.[1] Dually, $T^\flat$ denotes the semigroup consisting of left multiplication maps for every $t \in T$ and constant maps $t^\flat$ for every $t \in T^I$. Note that $T^\flat = ((T^{\mathrm{op}})^\sharp)^{\mathrm{op}}$, and $T^\flat$ acts on T on the left.

Fact 1.2 *For any finite semigroup* T*, let* $\widetilde{T}$ *denote the monoid obtained from* T *by adjoining an identity and a zero and let* M *be any monoid with* $|M| > |T|$*. Then* $T^\flat$ *embeds in* $M \wr \widetilde{T}$*.*

Proof Fix a bijection $t \mapsto m_t$ between T and a subset of $M \setminus \{1_M\}$. We define a function $i\colon T^\flat \to M \wr \widetilde{T}$. For every $t \in T$, define $i(t) := (c_1, t)$, where $c_1 \in M^{\widetilde{T}}$ denotes the function with constant value 1_M, the identity of M, and $i(t^\flat) := (f_t, 0)$, where $f_t \in M^{\widetilde{T}}$ denotes the function defined by $f_t(0) := 1_M$ and $f_t(t') := m_{t't}$ for all $t' \in T^I$. It is straightforward to verify that i is an injective homomorphism. ∎

Applications of the constructions $T \mapsto T^\sharp$ and $T \mapsto T^\flat$ to finite semigroup theory can be found in [10].

Triple Product

Let $(S, +)$ be a (not necessarily commutative) semigroup equipped with two actions on it, a left action of a semigroup $(S_L, \cdot)$ and a right action of a semigroup $(S_R, \cdot)$, which commute. The *triple product*[2] $T = (S_R, S, S_L)$ is the semigroup of triples (s_R, s, s_L), with multiplication defined by

$$(s_R, s, s_L) \cdot (s'_R, s', s'_L) := (s_R s'_R, s s'_R + s_L s', s_L s'_L).$$

Fact 1.3 *If* $S \in \mathbf{V}$ *and* $S_L, S_R \in \mathbf{W}$*, then* $(S_R, S, S_L) \in \mathbf{V} * \mathbf{W}$*.*

[1] Note that our definition of $T^\sharp$ for a semigroup T deviates slightly from the definition of $M^\sharp$ for a monoid M in [13, Subsec. 4.1.2].

[2] We follow the notation of [3, Sec V.9]; note the positions of the semigroups acting on the left and on the right. Also note that the multiplication can be viewed as matrix multiplication, if we represent an element (s_R, s, s_L) by the lower triangular matrix $\left[\begin{smallmatrix} s_R & 0 \\ s & s_L \end{smallmatrix}\right]$.

https://doi.org/10.4153/CMB-2018-014-8 Published online by Cambridge University Press

Proof Define an action of $S_L \times S_R$ on S by $\langle s_L, s_R\rangle s := s_L s$ and $s\langle s_L, s_R\rangle := s s_R$. Then T is isomorphic to the two-sided semidirect product $S \bowtie (S_L \times S_R)$ (*cf., e.g.,* [3, Sec. V.9]). ∎

2 The Merge Decomposition

Throughout this section, we fix the following:

- a finite alphabet A and two disjoint subalphabets A_1, A_2 such that $A = A_1 \cup A_2$;
- two homomorphisms $\psi_1 \colon A_1^+ \to T_1$ and $\psi_2 \colon A_2^+ \to T_2$, with T_1 and T_2 finite;
- a homomorphism $\chi \colon (T_1 \times T_2)^+ \to T_0$.

For any $w_1 \in A_1^+$, $w_2 \in A_2^+$, define $\mu(w_1 w_2) := (\psi_1(w_1), \psi_2(w_2)) \in T_1 \times T_2$. Since the subsemigroup $(A_1^+ A_2^+)^+$ of A^+ is freely generated by the infinite set of generators $A_1^+ A_2^+$, the function μ extends uniquely to a homomorphism $\mu \colon (A_1^+ A_2^+)^+ \to (T_1 \times T_2)^+$. We define $\psi_0 \colon (A_1^+ A_2^+)^+ \to T_0$ to be the composition $\chi \circ \mu$. For $i = 0, 1, 2$, we denote the external identity of T_i^I by I_i, and we also denote by ψ_i the homomorphism from the corresponding free *monoid* to the finite monoid T_i^I; *i.e.,* $\psi_i(\varepsilon) := I_i$.

For any word w in A^+, uniquely write $w = v_2 u v_1$, with $v_2 \in A_2^*$, $u \in (A_1^+ A_2^+)^*$, and $v_1 \in A_1^*$, and define $\tau(w) := (\psi_2(v_2), \psi_0(u), \psi_1(v_1))$. The function $\tau \colon A^+ \to T_2^I \times T_0^I \times T_1^I$ is not a homomorphism in general. The aim in this section is to show that the kernel of τ can be refined to a semigroup congruence of finite index in a well-controlled variety.

To this end, we will define a semigroup T_M and a homomorphism $\psi_M \colon A^+ \to T_M$. Let $S := (T_0^I)^{T_1^I \times T_2^I}$, with the pointwise product of T_0^I, written additively. We define a left action of $T_1^\sharp$ and a right action of $T_2^\flat$ on S. For $s \in S$, $s_L \in T_1^\sharp$, and $s_R \in T_2^\flat$, let $s_L s s_R \in S$ be defined by $[s_L s s_R](t_1, t_2) := s(t_1 s_L, s_R t_2)$ for every $(t_1, t_2) \in T_1^I \times T_2^I$. Let $T_M := (T_2^\flat, S, T_1^\sharp)$ be the triple product; we call T_M the *merge semigroup* associated with ψ_1, ψ_2, and χ.

Fact 2.1 *Let* $\mathbf{V}$ *be a variety, and* $\mathbf{W}$ *a variety generated by monoids and containing* $\mathbf{SL}$. *If* $T_0 \in \mathbf{V}$, $T_1, T_2 \in \mathbf{W}$, *and* T_M *is any triple product of* $T_2^\flat$, $(T_0^I)^{T_1^I \times T_2^I}$, *and* $T_1^\sharp$, *then* $T_M \in \mathbf{V} * (\mathbf{SL} * \mathbf{W})$.

Proof Applying Fact 1.2 with M a semilattice (*e.g.,* a chain) with $|T_2| + 1$ elements and using $\widetilde{T_2} \in \mathbf{W}$ by Fact 1.1 yields $T_2^\flat \in \mathbf{SL} * \mathbf{W}$. Similarly, $T_1^\sharp \in \mathbf{SL} * \mathbf{W}$. Fact 1.3 gives the result. ∎

For any $w_1 \in A_1^+$, we define an element $s_{w_1} \in S$ by $s_{w_1}(t_1, I_2) := I_0$ and $s_{w_1}(t_1, t_2) := \chi(t_1 \psi_1(w_1), t_2)$, for all $t_1 \in T_1^I$ and $t_2 \in T_2$. Now let $\psi_M \colon A^+ \to T_M$ be the unique homomorphism defined by

$$\psi_M(a_1) := (I_2^\flat, s_{a_1}, \psi_1(a_1)) \text{ for } a_1 \in A_1, \quad \psi_M(a_2) := (\psi_2(a_2), i_0, I_1^\sharp) \text{ for } a_2 \in A_2,$$

where i_0 denotes the identity of S, *i.e.,* the function with constant value I_0. We call the homomorphism $\psi_M \colon A^+ \to T_M$ the *merge decomposition* of A^+ along χ, ψ_1, and ψ_2.

The crucial property of the merge decomposition is the following proposition.

Proposition 2.2 *There exists a function* $f \colon T_M \to T_2^I \times T_0^I \times T_1^I$ *such that* $f \circ \psi_M = \tau$.

https://doi.org/10.4153/CMB-2018-014-8 Published online by Cambridge University Press

Proof For any $(t_2, s, t_1) \in T_M$, define $f(t_2, s, t_1) := (t_2 I_2, s(I_1, I_2), I_1 t_1)$. We show $f \circ \psi_M = \tau$.

We first prove, for all $w_1 \in A_1^+$, $\psi_M(w_1) = (I_2^\flat, s_{w_1}, \psi_1(w_1))$. By induction, assume that this holds for all shorter words in A_1^+. Then, writing $w_1 = a_1 w_1'$, the left and right coordinates are clearly as stated, and the middle coordinate of $\psi_M(w_1) = \psi_M(a_1)\psi_M(w_1')$ is $s_{a_1} I_2^\flat + \psi_1(a_1) s_{w_1'}$. From the definition of the right action and of s_{a_1} we get that $s_{a_1} I_2^\flat = i_0$. From the definition of the left action and of $s_{w_1'}$ and s_{w_1}, we get that $\psi_1(a_1) s_{w_1'} = s_{w_1}$. For $w_2 \in A_2^+$, we easily obtain $\psi_M(w_2) = (\psi_2(w_2), i_0, I_1^\sharp)$, since $s_L i_0 s_R = i_0$ for all s_L, s_R, because i_0 is a constant map. Multiplying these two results, for any $w_1 \in A_1^+$ and $w_2 \in A_2^+$, $\psi_M(w_1 w_2) = (I_2^\flat, s_{w_1 w_2}, I_1^\sharp)$, where $s_{w_1 w_2}(I_1, I_2) = s_{w_1}(I_1, \psi_2(w_2)) = \chi(\psi_1(w_1), \psi_2(w_2)) = \psi_0(w_1 w_2)$.

We next prove, by induction on the length of $u \in (A_1^+ A_2^+)^+$ as a word in the free semigroup generated by $A_1^+ A_2^+$, that $\psi_M(u) = (I_2^\flat, s_u, I_1^\sharp)$, where $s_u(I_1, I_2) = \psi_0(u)$. We have already established the base case. If $u = (w_1 w_2) u'$ for some $w_1 \in A_1^+$ and $w_2 \in A_2^+$ with $u' \in (A_1^+ A_2^+)^+$, then, for the middle coordinate s_u of $\psi_M(u) = \psi_M(w_1 w_2)\psi_M(u')$, we have

$$s_u(I_1, I_2) = [s_{w_1 w_2} I_2^\flat + I_1^\sharp s_{u'}](I_1, I_2) = \psi_0(w_1 w_2) \cdot \psi_0(u') = \psi_0(u).$$

Finally, to prove that $f \circ \psi_M = \tau$, let $w \in A^+$. Suppose that $w = v_2 u v_1$ with $u \in (A_1^+ A_2^+)^+$, $v_1 \in A_1^+$ and $v_2 \in A_2^+$. Then, using our previous calculations, we get

$$\psi_M(v_2 u v_1) = \big(\psi_2(v_2), i_0, I_1^\sharp\big) \cdot (I_2^\flat, s_u, I_1^\sharp) \cdot \big(I_2^\flat, s_{v_1}, \psi_1(v_1)\big) = \big(\psi_2(v_2)^\flat, s, \psi_1(v_1)^\sharp\big),$$

where

$$s(I_1, I_2) = \big((i_0 I_2^\flat + I_1^\sharp s_u) I_2^\flat + I_1^\sharp s_{v_1}\big)(I_1, I_2) = I_0 \cdot s_u(I_1, I_2) \cdot I_0 = \psi_0(u).$$

Thus, in this case, $f(\psi_M(w)) = \tau(w)$. If one or more of the factors in the factorization $w = v_2 u v_1$ are empty, then the proof is similar but simpler. ∎

We end with a prototypical application of the technique, to be used in the next section.

Corollary 2.3 *Let S be a finite semigroup and let T_1, T_2 be subsemigroups of S such that $T_1 \cup T_2$ generates S. Denote by $T_0 := \langle T_1 T_2 \rangle$, the subsemigroup generated by $T_1 T_2$. Then the semigroup S divides a triple product of $T_2^\flat$, $(T_0^I)^{T_1^I \times T_2^I}$, and $T_1^\sharp$.*

Proof Let $A_i := T_i \times \{i\}$ for $i = 1, 2$ and $A := A_1 \cup A_2$. Denote by $\psi : A^+ \twoheadrightarrow S$ the surjective homomorphism defined on generators $(t_i, i) \in A$ by $\psi(t_i, i) := t_i$. For $i = 1, 2$, let ψ_i be the restriction of ψ to A_i^+, and let $\chi : (T_1 \times T_2)^+ \to T_0$ be the homomorphism defined by $\chi(t_1, t_2) := t_1 t_2$ for $(t_1, t_2) \in T_1 \times T_2$. Note that ψ_0, as defined above, in this case turns out to be the restriction of ψ to $(A_1^+ A_2^+)^+$. Hence, writing $m : T_2^I \times T_0^I \times T_1^I \to T^I$ for the multiplication map $m(t_2, t_0, t_1) := t_2 t_0 t_1$, we have $\psi = m \circ \tau$. Let $\psi_M : A^+ \to T_M$ be the merge decomposition along χ, ψ_1, and ψ_2. By Proposition 2.2, pick $f : T_M \to T_2^I \times T_0^I \times T_1^I$ such that $\tau = f \circ \psi_M$. Then $\psi = m \circ f \circ \psi_M$, so S divides T_M, since ψ is surjective. ∎

https://doi.org/10.4153/CMB-2018-014-8 Published online by Cambridge University Press

We use $C(S)$ to denote the two-sided complexity of a finite semigroup S; see [13, Def. 5.1.4]. Retaining the notation of Corollary 2.3, it follows that $C(S) \leq C(T_0) + \max\{C(T_1), C(T_2)\}$.

3 Two-sided Krohn–Rhodes Theorem

In this section, we apply the merge decomposition technique of Section 2 to give a short proof of the crucial step in the two-sided Krohn–Rhodes theorem.

For any finite semigroup S, define $\mathbf{V}_S$ to be the smallest variety that is closed under two-sided semidirect products and contains **SL** and all simple groups that divide S.

Theorem 3.1 (Two-sided Krohn-Rhodes) *Let S be a finite semigroup. Then $S \in \mathbf{V}_S$.*

Proof By induction on $|S|$.

Case 1. *S is a group.* Any finite group embeds in an iterated wreath product of its simple group divisors, *cf., e.g.,* [13, Cor. 4.1.6].

Case 2. *S is cyclic.* Any finite cyclic semigroup divides an iterated wreath product of a subgroup and copies of U_1, *cf., e.g.,* [13, Cor. 4.1.28].

Case 3. *S is not a group and S is not cyclic.* Let A be a minimal generating set for S and note that $|A| \geq 2$. Since S is not a group, without loss of generality, S is not right simple (*cf., e.g.,* [13, Lem. A.3.3]). Therefore, there exists $a \in A$ such that $aS \subsetneq S$. Let $A_1 := \{a\}$, $A_2 := A \setminus A_1$, $T_i := \langle A_i \rangle$ for $i = 1, 2$, and $T_0 := \langle T_1 T_2 \rangle$. By minimality of A, T_1 and T_2 are strictly contained in S. By the induction hypothesis, $T_i \in \mathbf{V}_{T_i}$, which is contained in $\mathbf{V}_S$, since any simple group dividing T_i also divides S. Moreover, $T_0 \subseteq aS$, so T_0 is also strictly contained in S. By the induction hypothesis again, $T_0 \in \mathbf{V}_{T_0} \subseteq \mathbf{V}_S$. Since $T_1 \cup T_2$ generates S, by Corollary 2.3, S divides a triple product of $T_2^\flat$, $(T_0^I)^{T_1^I \times T_2^I}$, and $T_1^\sharp$. Hence, by Fact 2.1, $S \in \mathbf{V}_S * * (\mathbf{V}_S * * \mathbf{V}_S) = \mathbf{V}_S$. ∎

4 Henckell's Theorem on Aperiodic Pointlikes

Recall that any element s in a finite semigroup S has a unique *idempotent power*, s^ω. A semigroup S is called *aperiodic* if every subgroup of S is trivial, or, equivalently, $s^\omega s = s^\omega$ for every $s \in S$. For $k \geq 1$, define $\mathbf{SL}^{k+1} := \mathbf{SL} * * \mathbf{SL}^k$. A semigroup S is aperiodic if and only if $S \in \mathbf{SL}^k$ for some k; indeed, the necessity follows from Theorem 3.1.[3]

Fact 4.1 *For any $m, n \geq 1$, $\mathbf{SL}^m * * \mathbf{SL}^n \subseteq \mathbf{SL}^{m+n}$.*

Proof By induction on m. The case $m = 1$ is true by definition. By the lax associativity of double semidirect product [13, Cor. 2.6.26],

$$(\mathbf{SL} * * \mathbf{SL}^{m-1}) * * \mathbf{SL}^n \subseteq \mathbf{SL} * * (\mathbf{SL}^{m-1} * * \mathbf{SL}^n).$$

[3] A finite semigroup S lies in $\mathbf{SL}^k$ if, and only if, every language recognized by S can be defined by a first-order sentence of quantifier depth $\leq k$; this result is contained in [16, Ch. VI], and relates our work in Section 4 to the logical approach of [11].

https://doi.org/10.4153/CMB-2018-014-8 Published online by Cambridge University Press

By the induction hypothesis,

$$\mathbf{SL} * * (\mathbf{SL}^{m-1} * * \mathbf{SL}^{n}) \subseteq \mathbf{SL} * * \mathbf{SL}^{m+n-1} = \mathbf{SL}^{m+n}. \qquad \blacksquare$$

Let $\mathbf{V}$ be a variety. A subset X of a finite semigroup S is called $\mathbf{V}$-*pointlike* if, for any relational morphism $\rho: S \nrightarrow T$ with $T \in \mathbf{V}$, $X \subseteq \rho^{-1}(t)$ for some $t \in T$. Any singleton set is $\mathbf{V}$-pointlike, and the collection of $\mathbf{V}$-pointlike subsets of a semigroup S forms a downward closed subsemigroup, $\mathrm{PL}_{\mathbf{V}}(S)$, of the power semigroup 2^S, partially ordered by inclusion, and with multiplication of subsets of S.

The following observation is specific to the variety $\mathbf{A}$ of aperiodic semigroups: if X is an $\mathbf{A}$-pointlike set in S, then so is the set $X^{\omega+*} := \bigcup_{n\geq 0} X^{\omega}X^{n}$. Indeed, for any $\rho: S \nrightarrow T$ with T aperiodic, $X \subseteq \rho^{-1}(t)$ for some $t \in T$, which gives $X^{m} \subseteq \rho^{-1}(t^{m})$ for all $m \geq 1$. Aperiodicity of T then yields $X^{\omega}X^{n} \subseteq \rho^{-1}(t^{\omega})$ for all $n \geq 0$.

We will call a subset U of 2^S *saturated*, if it is a subsemigroup that is closed downward in the inclusion order and closed under the operation $X \mapsto X^{\omega+*}$. Clearly, any subset U of 2^S is contained in a smallest saturated set, which we call its *saturation*, and denote by $\mathrm{Sat}(U)$.

We will need the following lemma, which was essentially already in [5]; see also [7].

Lemma 4.2 *Let G be a subgroup of 2^S. Then $\bigcup G \in \mathrm{Sat}(G)$.*

Proof Let $C_1, \ldots, C_k$ be an exhaustive list of the cyclic subgroups of G. Note that, for any generator X of C_i, $X^{\omega+*} = \bigcup C_i$, so $\bigcup C_i \in \mathrm{Sat}(G)$ for every i. Also note that $G = C_1 \cdots C_k$. Therefore, since multiplication distributes over union, $\bigcup G = (\bigcup C_1) \cdots (\bigcup C_k) \in \mathrm{Sat}(G)$. $\blacksquare$

We will use the merge decomposition (Section 2) to give a short proof of the following theorem.

Theorem 4.3 (*cf.* [5,7,11]) *Let S be a semigroup. The set $\mathrm{PL}_{\mathbf{A}}(S)$ is the saturation of the set of singletons in 2^S. Moreover, if A is a generating set for S, then $\mathrm{PL}_{\mathbf{A}}(S) = \mathrm{PL}_{\mathbf{SL}^k}(S)$, where $k = (|A|-1)2^{\binom{|S|}{2}} + 2^{|A|} - 1$.*

Proof Throughout the proof, for any finite alphabet A, semigroup S, and homomorphism $\varphi: A^+ \to 2^S$, define $U_\varphi := \mathrm{im}(\varphi)$, $S_\varphi := \bigcup U_\varphi$, and $k(\varphi) := \big(|\varphi(A)|-1\big)2^{\binom{|S_\varphi|}{2}} + 2^{|S_\varphi|} - 1$.

Claim *For any homomorphism $\varphi: A^+ \to 2^S \setminus \{\varnothing\}$, there exists a homomorphism $\psi: A^+ \to T$ with $T \in \mathbf{SL}^{k(\varphi)}$ and $\bigcup \varphi(\psi^{-1}t) \in \mathrm{Sat}(U_\varphi)$ for every $t \in T$.*

Proof of Claim The construction of $\psi: A^+ \to T$ with $T \in \mathbf{SL}^{k(\varphi)}$ is by induction on the parameter $(|S_\varphi|, |\varphi(A)|)$ in $\mathbb{N}^2$, ordered lexicographically.

Case 1. *For every $a \in A$, $\varphi(a)S_\varphi = S_\varphi = S_\varphi\varphi(a)$.*

Let $e = \varphi(w)$ be an idempotent in the minimal ideal of U_φ. Then $G := eU_\varphi e$ is a subgroup of U_φ; see, *e.g.*, [13, App. A]. By Lemma 4.2, $\bigcup G$ lies in $\mathrm{Sat}(eU_\varphi e)$, and hence also in $\mathrm{Sat}(U_\varphi)$, since $eU_\varphi e \subseteq U_\varphi$. Using the assumption in this case and the

https://doi.org/10.4153/CMB-2018-014-8 Published online by Cambridge University Press

fact that multiplication distributes over union, we have

$$S_\varphi = \varphi(w)S_\varphi\varphi(w) = e\Big(\bigcup U_\varphi\Big)e = \bigcup G.$$

Thus, S_φ lies in $\mathrm{Sat}(U_\varphi)$, and we choose ψ to be the trivial homomorphism $A^+ \to \{1\} \in \mathbf{SL}$.

Case 2. $|\varphi(A)| = 1$.

Denote the unique element of $\varphi(A)$ by X. Since U_φ is a finite cyclic semigroup, pick $m \leq |U_\varphi|$ such that X^m is idempotent, *i.e.,* $X^m = X^\omega$. Let $T := \langle x \mid x^m = x^{m+1}\rangle$, the finite aperiodic cyclic semigroup of order m, and let $\psi\colon A^+ \to T$ be the homomorphism defined by $a \mapsto x$ for every letter $a \in A$. Note that $T \in \mathbf{SL}^m$ [13, Lem. 4.1.27], and, since $U_\varphi \subseteq 2^{S_\varphi} \setminus \{\varnothing\}$, we have $m \leq |U_\varphi| \leq 2^{|S_\varphi|} - 1 = k(\varphi)$. From the definitions, note that, for $1 \leq i < m$, $\bigcup \varphi(\psi^{-1}x^i) = X^i$, which lies in U_φ, and for $i \geq m$, $\bigcup \varphi(\psi^{-1}x^i) = X^{\omega+*}$, which lies in $\mathrm{Sat}(U_\varphi)$.

Case 3. $|\varphi(A)| \geq 2$, *and there is* $a_0 \in A$ *such that* $\varphi(a_0)S_\varphi \subsetneq S_\varphi$ *or* $S_\varphi\varphi(a_0) \subsetneq S_\varphi$.

Without loss of generality, we can assume that $\varphi(a_0)S_\varphi \subsetneq S_\varphi$. Let

$$A_1 := \big\{\, a \in A \mid \varphi(a) = \varphi(a_0)\big\} \quad \text{and} \quad A_2 := A \setminus A_1.$$

Note that, since $|\varphi(A)| \geq 2$, $\varphi(A_1)$ and $\varphi(A_2)$ are non-empty proper subsets of $\varphi(A)$. For $i = 1, 2$, denote by φ_i the restriction of φ to A_i^+, and pick $\psi_i\colon A_i^+ \to T_i$ with $T_i \in \mathbf{SL}^{k(\varphi_i)}$ and $\bigcup \varphi(\psi_i^{-1}t) = \bigcup \varphi_i(\psi_i^{-1}t) \in \mathrm{Sat}(U_{\varphi_i}) \subseteq \mathrm{Sat}(U_\varphi)$, for all $t \in T_i$. Without loss of generality, we can assume the ψ_i are surjective.

Let $\varphi_0\colon (T_1 \times T_2)^+ \to 2^S \setminus \{\varnothing\}$ be the unique homomorphism defined, for $(t_1, t_2) \in T_1 \times T_2$, by $\varphi_0(t_1, t_2) := \bigcup \varphi(\psi_1^{-1}t_1 \cdot \psi_2^{-1}t_2)$. Note that $S_{\varphi_0} \subseteq \varphi(a_0)S_\varphi$, since any $w \in \psi_1^{-1}t_1 \cdot \psi_2^{-1}t_2$ starts with a letter from the subalphabet A_1. Since $\varphi(a_0)S_\varphi \subsetneq S_\varphi$ by assumption, $|S_{\varphi_0}| < |S_\varphi|$, so the induction hypothesis applies to φ_0: pick a homomorphism $\chi\colon (T_1 \times T_2)^+ \to T_0$ with $T_0 \in \mathbf{SL}^{k(\varphi_0)}$ such that $\bigcup \varphi_0(\chi^{-1}(t)) \in \mathrm{Sat}(U_{\varphi_0}) \subseteq \mathrm{Sat}(U_\varphi)$, for every $t \in T_0$.

Define $\mu\colon (A_1^+A_2^+)^+ \to (T_1 \times T_2)^+$ and $\psi_0 := \chi \circ \mu$, as in Section 2. Note that, for any $w_1 \in A_1^+$, $w_2 \in A_2^+$, we have $\varphi(w_1w_2) \subseteq \varphi_0(\mu(w_1w_2))$, and, hence, $\varphi(w) \subseteq \varphi_0(\mu(w))$ for all $w \in (A_1^+A_2^+)^+$. Therefore, by the definition of ψ_0, $\bigcup \varphi(\psi_0^{-1}t) \subseteq \bigcup \varphi_0(\chi^{-1}t)$ for all $t \in T_0$, so also $\bigcup \varphi(\psi_0^{-1}t) \in \mathrm{Sat}(U_\varphi)$. Applying the construction of Section 2, let $\psi_M\colon A^+ \to T_M$ be the merge homomorphism, and pick $f\colon T_M \to T_2^I \times T_0^I \times T_1^I$ such that $f \circ \psi_M = \tau$. Let $t \in T_M$, and write $f(t) = (t_2, t_0, t_1) \in T_2^I \times T_0^I \times T_1^I$. If $(t_2, t_0, t_1) \in T_2 \times T_0 \times T_1$, then

$$\bigcup \varphi(\psi_M^{-1}t) \subseteq \bigcup \varphi\big(\tau^{-1}(t_2, t_0, t_1)\big) = \bigcup \varphi(\psi_2^{-1}t_2) \cdot \bigcup \varphi(\psi_0^{-1}t_0) \cdot \bigcup \varphi(\psi_1^{-1}t_1) \in \mathrm{Sat}(U_\varphi),$$

and, if $t_i = I_i$ for one or more $i \in \{0, 1, 2\}$, a similar inclusion holds, omitting the corresponding factors $\bigcup \varphi(\psi_i^{-1}t_i)$ from the final product.

Let us write $m := |S_\varphi|$. Note that, since S_{φ_0} is strictly contained in S_φ and $\varphi_0(T_1 \times T_2)$ is contained in $2^{S_{\varphi_0}} \setminus \{\varnothing\}$, we have

$$k(\varphi_0) \leq (2^{m-1} - 2)2^{\binom{m-1}{2}} + 2^{m-1} - 1 = 2^{\binom{m}{2}} - 2^{\binom{m-1}{2}+1} + 2^{m-1} - 1 \leq 2^{\binom{m}{2}} - 1,$$

using that $\binom{m}{2} = m - 1 + \binom{m-1}{2}$ and $2^{m-1} \leq 2^{\binom{m-1}{2}+1}$.

https://doi.org/10.4153/CMB-2018-014-8 Published online by Cambridge University Press

By Facts 2.1 and 4.1, $T_M \in \mathbf{SL}^k$, where $k = k(\varphi_0) + \max\{k(\varphi_1), k(\varphi_2)\} + 1$. Using that $|\varphi(A_i)| < |\varphi(A)|$, we have

$$k(\varphi_0) + \max\{k(\varphi_1), k(\varphi_2)\} + 1 \leq (2^{\binom{m}{2}} - 1) + \Big((|\varphi(A)| - 2)2^{\binom{m}{2}} + 2^m - 1 \Big) + 1 = k(\varphi). \qquad \blacksquare$$

Now, to prove the theorem, let A be a generating set for S, define $\varphi\colon A^+ \to 2^S$ by $\varphi(a) := \{a\}$ for $a \in A$, and pick $\psi\colon A^+ \to T$ as in the claim. Then U_φ is the set of singletons, $|\varphi(A)| = |A|$, and $S_\varphi = S$, so that $k(\varphi) = (|A| - 1)2^{\binom{|S|}{2}} + 2^{|S|} - 1 =: k$. Define the relational morphism $\rho\colon S \twoheadrightarrow T$ by $\rho^{-1}(t) := \bigcup \varphi(\psi^{-1}t)$. Then, for any $\mathbf{SL}^k$-pointlike $X \subseteq S$, we have $X \subseteq \rho^{-1}(t)$ for some $t \in T$, and therefore, since $\rho^{-1}(t)$ lies in $\mathrm{Sat}(U_\varphi)$ by the claim, so does X. We have proved that $\mathrm{PL}_{\mathbf{SL}^k}(S) \subseteq \mathrm{Sat}(U_\varphi)$, while the remarks at the beginning of this section imply $\mathrm{Sat}(U_\varphi) \subseteq \mathrm{PL}_{\mathbf{A}}(S)$, which is clearly contained in $\mathrm{PL}_{\mathbf{SL}^k}(S)$, since $\mathbf{SL}^k \subseteq \mathbf{A}$. Thus, $\mathrm{PL}_{\mathbf{SL}^k}(S) = \mathrm{Sat}(U_\varphi) = \mathrm{PL}_{\mathbf{A}}(S)$. $\blacksquare$

Acknowledgments In an earlier version of the proof of Theorem 4.3, we proved the claim for

$$k(\varphi) := |\varphi(A)|2^{\binom{|S_\varphi|}{2}}.$$

We acknowledge the help of MathOverflow [14] for guiding us to the slightly better bound given in the paper.

References

[1] J. Almeida, *Some algorithmic problems for pseudovarieties*. Publ. Math. Debrecen **54**(1999), no. suppl., 531–552.
[2] K. Auinger and B. Steinberg, *On the extension problem for partial permutations*. Proc. Amer. Math. Soc. **131**(2003), no. 9, 2693–2703. http://dx.doi.org/10.1090/S0002-9939-03-06860-6
[3] S. Eilenberg, *Automata, languages, and machines. Vol. B*. Pure and Applied Mathematics, 59, Academic Press, New York, 1976.
[4] S. J. v. Gool and B. Steinberg, *Pointlike sets for varieties determined by groups*. 2018. arxiv:1801.04638
[5] K. Henckell, *Pointlike sets: the finest aperiodic cover of a finite semigroup*. J. Pure Appl. Algebra **55**(1988), 85–126. http://dx.doi.org/10.1016/0022-4049(88)90042-4
[6] K. Henckell, S. Lazarus, and J. Rhodes, *Prime decomposition theorem for arbitrary semigroups: general holonomy decomposition and synthesis theorem*. J. Pure Appl. Algebra **55**(1988), no. 1–2, 127–172. http://dx.doi.org/10.1016/0022-4049(88)90043-6
[7] K. Henckell, J. Rhodes, and B. Steinberg, *Aperiodic pointlikes and beyond*. Internat. J. Algebra Comput. **20**(2010), no. 2, 287–305. http://dx.doi.org/10.1142/S0218196710005662
[8] K. Krohn and J. Rhodes, *Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines*. Trans. Amer. Math. Soc. **116**(1965), 450–464. http://dx.doi.org/10.2307/1994127
[9] K. Krohn, J. Rhodes, and B. Tilson, *Algebraic theory of machines, languages, and semigroups*. Academic Press, New York, 1968.
[10] E. W. H. Lee, J. Rhodes, and B. Steinberg, *Join irreducible semigroups*. 2017. arxiv:1702.03753
[11] T. Place and M. Zeitoun, *Separating regular languages with first-order logic*. Log. Methods Comput. Sci. **12**(2016), Paper no. 5. http://dx.doi.org/10.2168/LMCS-12(1:5)2016
[12] J. Rhodes and B. Steinberg, *Pointlike sets, hyperdecidability and the identity problem for finite semigroups*. Internat. J. Algebra Comput. **9**(1999), no. 3–4, 475–481. http://dx.doi.org/10.1142/S021819679900028X
[13] ———, *The q-theory of finite semigroups*. Springer Monographs in Mathematics, Springer, New York, 2009.
[14] B. Steinberg, *A strange two-variable recursion*. MathOverflow question, answered by M. Fischler. https://mathoverflow.net/q/278517

https://doi.org/10.4153/CMB-2018-014-8 Published online by Cambridge University Press

[15] ———, *On pointlike sets and joins of pseudovarieties*. Internat. J. Algebra Comput. **8**(1998), no. 2, 203–234. http://dx.doi.org/10.1142/S0218196798000119
[16] H. Straubing, *Finite automata, formal logic, and circuit complexity*. Progress in Theoretical Computer Science, Birkhäuser Boston Inc., Boston, MA, 1994. http://dx.doi.org/10.1007/978-1-4612-0289-9
[17] T. Wilke, *Classifying discrete temporal properties*. In: STACS'99, Lecture Notes. in Computer Science, 1563, Springer, 1999, pp. 32–46. http://dx.doi.org/10.1007/3-540-49116-3_3

Department of Mathematics, City College of New York, New York, New York 10031, USA
e-mail: samvangool@me.com bsteinberg@ccny.cuny.edu