

Equations and Dot-Depth One

By: [Francine Blanchet-Sadri](#)

Communicated by: H. Straubing

F. Blanchet-Sadri, "Equations and Dot-Depth One." *Semigroup Forum*, Vo. 47, No. 3, 1993, pp 305-317.

Made available courtesy of Springer Verlag: The original publication is available at <http://www.springerlink.com/>

*****Reprinted with permission. No further reproduction is authorized without written permission from Springer Verlag. This version of the document is not the version of record. Figures and/or pictures may be missing from this format of the document.*****

Abstract:

This paper studies the fine structure of the Straubing hierarchy of star-free languages. Sequences of equations are defined and are shown to be sufficiently strong to characterize completely the monoid varieties of a natural subhierarchy of level one. In a few cases, it is also shown that those sequences of equations are equivalent to finite ones. Extensions to a natural sublevel of level two are discussed.

Article:

1. Introduction

This paper deals with the problem of the decidability of the different levels of the Straubing hierarchy of star-free languages. The problem is a central one in the theory of regular languages. Its study is justified by its recognized connections with logic and the theory of complexity. More specifically, this paper is concerned with the problem of finding equations for Straubing's varieties of monoids.

1.1. Literature review

Let A be a given finite alphabet. The regular languages over A are those subsets of A^* , the free monoid generated by A , constructed from the finite languages over A by the boolean operations, the concatenation product and the star. The star-free languages are those regular languages which can be obtained from the finite languages by the boolean operations and the concatenation product only. According to Schützenberger [14], $L \subseteq A^*$ is star-free if and only if its syntactic monoid $M(L)$ is finite and aperiodic or $M(L)$ contains no nontrivial subgroups). General references on the star-free languages are McNaughton and Papert [12], Eilenberg [8], or Pin [13].

Natural classifications of the star-free languages are obtained based on the alternating use of the boolean operations and the concatenation product. Let $A^+ = A^* - \{1\}$, where 1 denotes the empty word. Let A^+B_0 be the class of finite or cofinite subsets of A^+ , and let A^+B_{k+1} denote the class of subsets of A^+ which are boolean combinations of languages of the form $L_1 \dots L_n$ ($n \geq 1$) with $L_1, \dots, L_n \in A^+B_k$. Only nonempty words over A are considered to define this hierarchy; in particular, the complement operation is applied with respect to A^+ . The language classes A^+B_0, A^+B_1, \dots form the so-called dot-depth hierarchy introduced by Cohen and Brzozowski in [7]. The union of the classes A^+B_0, A^+B_1, \dots is the class of star-free languages.

Our attention is directed toward a closely related and more fundamental hierarchy, this one in A^* , introduced by Straubing in [16]: A^*V_0 consists of the empty set A^* , and A^*V_{k+1} denotes the class of languages over A which are boolean combinations of languages of the form $L_0 a_1 L_1 a_2 \dots a_n L_n$ ($n \geq 0$) with $L_0, \dots, L_n \in A^*V_k$ and $a_1, \dots, a_n \in A$. Let $A^*V = \bigcup_{k \geq 0} A^*V_k$. $L \subseteq A^*$ is star-free if and only if $L \in A^*V_k$ for some $k \geq 0$. The *dot-depth* of L is the smallest such k .

For $k \geq 1$, let us define subhierarchies of A^*V as follows: for all $m \geq 1$, let $A^*V_{k,m}$ denote the class of boolean combinations of languages of the form $L_0a_1L_1a_2\dots a_nL_n$ ($0 \leq n \leq m$) with $L_0, \dots, L_n \in A^*V_{k-1}$ and $a_1, \dots, a_n \in A$. We have $A^*V_k = \bigcup_{m \geq 1} A^*V_{k,m}$. Easily, $A^*V_{k,m} \subseteq A^*V_{k+1,m}$, and $A^*V_{k,m} \subseteq A^*V_{k,m+1}$. Similarly, subhierarchies of $A+B_k$ can be defined. In A^+B_1 several hierarchies and classes of languages have been studied; the most prominent examples are the β -hierarchy [6], also called depth-one finite cofinite hierarchy, and the class of locally testable languages.

The Straubing hierarchy gives examples of $*$ -varieties of languages. One can show that V , V_k and $V_{k,m}$ are $*$ -varieties of languages. According to Eilenberg, there exist varieties of monoids \mathbf{V} , \mathbf{V}_k and $\mathbf{V}_{k,m}$ corresponding to V , V_k and $V_{k,m}$, respectively. \mathbf{V} is the variety of aperiodic monoids. We have that for $L \subseteq A^*$, $L \in A^*V$ if and only if $M(L) \in \mathbf{V}$, for each $k \geq 0$, $L \in A^*V_k$ if and only if $M(L) \in \mathbf{V}_k$, and for $k \geq 1$, $m \geq 1$, $L \in A^*V_{k,m}$ if and only if $M(L) \in \mathbf{V}_{k,m}$.

An outstanding open problem is whether one can decide if a star-free language has dot-depth k , i.e., can we effectively characterize the varieties V_k ? The variety V_0 consists of the trivial monoid alone, V_1 of all finite \mathcal{J} -trivial monoids [15]. Straubing [17] conjectured an effective characterization, based on the syntactic monoid of the language, for V_2 . His characterization, formulated in terms of the novel use of categories in semigroup theory is shown to be necessary in general, and sufficient for an alphabet of two letters.

In the framework of semigroup theory, Brzozowski and Knast [5] showed that the dot-depth hierarchy is infinite. Thomas [19] gave a new proof of this result, which shows also that the Straubing hierarchy is infinite, based on the following version of the Ehrenfeucht-Fraissé game.

First, one regards a word $w \in A^*$ of length $|w|$ as a word model $w = (\{1, \dots, |w|\}, <^w, (Q_a^w)_{a \in A})$ where the universe $\{1, \dots, |w|\}$ represents the set of positions of letters in w , $<^w$ denotes the $<$ -relation in w , and Q_a^w are unary relations over $\{1, \dots, |w|\}$ containing the positions with letter a , for each $a \in A$. For a sequence $\bar{m} = (m_1, \dots, m_k)$ of positive integers, where $k \geq 0$, the game $\mathcal{G}_{\bar{m}}(u, v)$ is played between two players I and II on the word models u and v . A play of the game consists of k moves. In the i th move, player I chooses, in u or in v , a sequence of m_i positions; then player II chooses, in the remaining word, also a sequence of m_i positions. After k moves, by concatenating the position sequences chosen from u and v , two sequences of positions $p_1 \dots p_n$ from u and $q_1 \dots q_n$ from v have been formed where $n = m_1 + \dots + m_k$. Player II has won the play if the two subwords in u and v given by the position sequences $p_1 \dots p_n$, and $q_1 \dots q_n$ coincide. If there is a winning strategy for player II in the game $\mathcal{G}_{\bar{m}}(u, v)$ to win each play we write $u \sim_{\bar{m}} v$. The two players play the game $\mathcal{G}_{\bar{m}}(u, v)$ on a pair of words u and v . Player I tries to demonstrate a difference between them while player II tries to keep the words looking the same. $\sim_{\bar{m}}$ naturally defines a congruence on A^* . Thomas [18, 19] infers that for $k \geq 1$, $M \in V_k$ if and only if for every morphism $\varphi : A^* \rightarrow M$ there exists $\bar{m} = (m_1, \dots, m_k)$ such that $\sim_{\bar{m}}$ refines φ , or, more precisely, for $k \geq 1$, $m \geq 1$, $M \in V_{k,m}$ if and only if for every morphism $\varphi : A^* \rightarrow M$ there exists $\bar{m} = (m, m_2, \dots, m_k)$ such that $\sim_{\bar{m}}$ refines φ . Applications of the characterizations of V_k and $V_{k,m}$ in terms of the $\sim_{\bar{m}}$'s appear in [1,2,3,4].

Eilenberg showed that every variety of monoids is *ultimately defined* by a sequence of equations. For example, the variety \mathbf{V} of aperiodic monoids is ultimately defined by the equations $x^n = x^{n+1}$ ($n > 0$). The variety \mathbf{V}_1 is ultimately defined by the equations $(xy)^m = (yx)^m$ and $x^m = x^{m+1}$ ($m > 0$). This gives a decision procedure for \mathbf{V}_1 , i.e., $M \in \mathbf{V}_1$ if and only if for all $x, y \in M$, $(xy)^m = (yx)^m$ and $x^m = x^{m+1}$ with m the cardinality of M . One can show that every variety of monoids generated by a single monoid is *defined* by a (finite or infinite) sequence of equations. $\mathbf{V}_{1,m}$ being generated by $A^*/\sim_{(m)}$, can we find explicitly a sequence of equations that define $\mathbf{V}_{1,m}$? If so, can we find explicitly a *finite* sequence of equations that define $\mathbf{V}_{1,m}$? An attempt to answer these open problems was made in [2]. There, finite sequences of equations were defined which are satisfied in the $\mathbf{V}_{1,m}$'s (but not necessarily complete for the $\mathbf{V}_{1,m}$'s). It was shown that those sequences of equations are complete for $\mathbf{V}_{1,1}$, $\mathbf{V}_{1,2}$ and $\mathbf{V}_{1,3}$. More precisely, $\mathbf{V}_{1,1}$ is defined by $x = x^2$ and $xy = yx$, $\mathbf{V}_{1,2}$ by $xyzx = yxzx$ and $(xy)^2 = (yx)^2$, and $\mathbf{V}_{1,3}$ by $zyxvxy = xzxyvxy$, $ywvxyzx = ywvxyzx$ and $(xy)^3 = (yx)^3$ (suggested to me by J.-E. Pin to be equivalent to $xyxzx = xyx^2zx$, $xyzx^2uz = xyxzx^2uz$, $zux^2zyx = zux^2zxyx$ and $(xy)^3 = (yx)^3$).

This paper studies the fine structure of the Straubing hierarchy. The results are concerned in particular with sequences of equations for the corresponding varieties of monoids. The question of finding complete sequences of equations which characterize Straubing's varieties is solved for the $V_{1,m}$'s. It is also shown that the sequences of equations which characterize $V_{1,1}$, $V_{1,2}$ and $V_{1,3}$ are equivalent to finite ones. Generalizations to $V_{2,1}$ are discussed. (Knast [9,10] provide an equation system for level one of Brzozowski's dot-depth hierarchy.) The proofs rely on some combinatorial properties of the congruences $\sim_{(m)}$ and $\sim_{(1,m)}$ stated in Section 2.

In the following, notation and basic concepts are introduced.

1.2. Preliminaries

For more information on the matters discussed in this subsection, see the books by Eilenberg [8], Lallement [11] or Pin [13].

Let A be a finite set. $|A|$ denote the *cardinality* of A or the number of elements in A . A^* , the *free monoid* generated by A , is the set of all sequences of length ≥ 0 of elements of A with concatenation being the operation (such sequences are called words). The unique string of length 0, denoted by 1 and called the empty word, acts as the identity. A *language* over A is a subset of A^* . $|w|$ denotes the length of the word w , and wA denotes the set of letters in w . A word u is a *prefix* of w if there exists a word v such that $uv = w$. A word u is a *suffix* of w if there exists a word v such that $vu = w$. A word u is a *factor* (or *segment*) of a word v if there exists words x and y such that $v = xuy$. A word $u = a_1 \dots a_n$ (where a_1, \dots, a_n are letters) is a *subword* of v if there exist words v_0, \dots, v_n such that $v = v_0 a_1 v_1 a_2 \dots a_n v_n$.

An equivalence \sim on A^* is a *congruence* if $x \sim y$ implies $uxv \sim uyv$ for all $u, v, x, y \in A^*$. A congruence \sim is *aperiodic* if there exists $n \geq 0$ such that $x^n \sim x^{n+1}$, for all x . The \sim -class of x is $[x]_{\sim} = \{y \mid x \sim y\}$. The set of all \sim -classes is denoted by A^*/\sim and the *index* of \sim is defined as the cardinality of A^*/\sim . This set becomes a monoid by considering the operation $[x]_{\sim} [y]_{\sim} = [xy]_{\sim}$; $[1]_{\sim}$ acts as the identity. There exists a surjective morphism $\sim: A^* \rightarrow A^*/\sim$, defined by $x \sim = [x]_{\sim}$. Conversely, any morphism $\varphi: A^* \rightarrow M$ induces a congruence on A^* defined by $x\varphi y$ if and only if $x\varphi = y\varphi$. Note that we use the same symbol to denote the congruence and the related morphism. If φ is surjective, there exists an isomorphism between A^*/φ and M . Any monoid can then be represented as a quotient of A^* by a congruence.

If $L \subseteq A^*$ is a union of \sim -classes, we say that L is a \sim -language. For any language L over A , the *syntactic congruence* of L is defined by $x \sim_L y$ if and only if for all $u, v \in A^*$, $uxv \in L$ if and only if $uyv \in L$. \sim_L is the congruence of minimal index with the property that L is a \sim -language, i.e., for any congruence \sim on A^* , L is a \sim -language if and only if $\sim \subseteq \sim_L$. The quotient monoid A^*/\sim_L is denoted by $M(L)$ and is called the *syntactic monoid* of L . If M is a monoid and there exists a morphism $\varphi: A^* \rightarrow M$ such that $L = S\varphi^{-1}$ for some $S \subset M$, we say that M *recognizes* L . A language is said to be *recognizable* if it is recognized by a finite monoid. Kleene's theorem asserts that the regular languages in A^* are exactly those recognized by finite monoids. It is well known that $M(L)$ is the monoid M of minimal cardinality with the property that M recognizes L ; in fact, $M(L) < M$ if and only if M recognizes L . Also L is regular if and only if $M(L)$ is finite.

W is a variety of monoids, or M -variety, if

- it is a class of finite monoids closed under division, i.e., if $M \in W$ and $M' < M$ (or M' is a morphic image of a submonoid of M), then $M' \in W$, and
- it is closed under finite direct product, i.e., if $M, M' \in W$, then $M \times M' \in W$.

For any class C of finite monoids, we denote by $\langle C \rangle_M$ the last M -variety containing C . Clearly, $M \in \langle C \rangle_M$ if and only if there exists a finite sequence M_1, \dots, M_n of monoids of C such that $M < M_1 \times \dots \times M_n$. We call $\langle C \rangle_M$ the M -variety generated by C .

To find the positions which spell the first occurrences of every subword of length $\leq m$ of a word w (or the (m) first position in w), proceed as follows:

- let w_1 denote the smallest prefix of w such that $w_1\alpha = w\alpha$ (call the last position of w_1 , p_1);
- let w_2 denote the smallest prefix of $w(p_1, |w|]$ such that $w_2\alpha = (w(p_1, |w|))\alpha$ (call the last position of w_2 , p_2);
-
-
- and let w_m denote the smallest prefix of $w(p_{m-1}, |w|]$ such that $w_m\alpha = (w(p_{m-1}, |w|))\alpha$ (call the last position of w_m , p_m).

p_1, \dots, p_m are among the positions we are looking for. Then, repeat the process to find the positions which spell the first occurrences of every subword of length $\leq m$ of $w[1, p_1)$ and of length $\leq (m - i + 1)$ of $w(p_{i-1}, p_i)$ for $2 \leq i \leq m$.

A similar statement is valid to find the positions spelling the last occurrences of every subword of length $\leq m$ of w (or the (m) last positions in w).

The (m) first and the (m) last positions in w are called the (m) positions in w .

The following Lemmas are from [4].

Lemma 2.4. *Let $m \geq 1$. Let $u, v \in A^+$ and let p_1, \dots, p_s in u ($p_1 < \dots < p_s$), ($q_1, \dots, q_{s'}$ in v ($q_1 < \dots < q_{s'}$)) be the (m) positions in u (v). $u \sim_{(1,m)} v$ if and only if*

- $s = s'$,
- $Q_a^u p_i$ if and only if $Q_a^v q_i$, $a \in A$ for $1 \leq i \leq s$, and
- $u(p_i, p_{i+1}) \sim_{(1)} v(q_i, q_{i+1})$ for $1 \leq i \leq s - 1$.

Lemma 2.5. *Let $m \geq 1$. Let $u, v \in A^+$ be such that $u \sim_{(1,m)} v$. Then there exists $w \in A^+$ satisfying:*

- $Q_a^u p_i$ if and only if $Q_a^w p_i''$ if and only if $Q_a^v q_i'$, $a \in A$ for $1 \leq i \leq s$,
- $u_i \sim_{(1)} w_i \sim_{(1)} v_i$, for $1 \leq i \leq s - 1$, and
- u_i, v_i are subwords of w_i for $1 \leq i \leq s - 1$,

where p_1, \dots, p_s ($p_1 < \dots < p_s$), p_1', \dots, p_s' ($p_1' < \dots < p_s'$), p_1'', \dots, p_s'' ($p_1'' < \dots < p_s''$) denote the (m) positions in u , v and w , respectively, $u_i = u(p_i, p_{i+1})$, $v_i = v(p_i', p_{i+1}')$, and $w_i = (p_i'', p_{i+1}'')$ for $1 \leq i \leq s - 1$.

Lemma 2.4 and Lemma 2.5 imply that for $m \geq 1$, and $u, v \in A^*$, if $u \sim_{(1,m)} v$, then there exists $w \in A^*$ such that u is a subword of w , v is a subword of w and $u \sim_{(1,m)} w \sim_{(1,m)} v$.

We end this section with a few observations useful in the proof of Theorem 4.3. First, $x^{2m+1} \sim_{(1,m)} x^{2m+2}$ and $2m + 1$ is the smallest positive integer n with the property that $x^n \sim_{(1,m)} x^{n+1}$. Second, consider a nonempty word w over an alphabet of two letters. Let $m \geq 1$ and let p_1, \dots, p_s ($p_2 < \dots < p_s$) be the (m) positions in w . Let $1 \leq i \leq s - 1$. If it is not the case that p_i is the last among the (m) first positions in w and p_{i+1} the first among the (m) last positions in w , then $|(w(p_i, p_{i+1}))\alpha| < 2$.

3. Equations and the V_m 's

In this section, we define sequences of equations and show that they are complete for the V_m 's. Also, in a few cases, we show that those sequences of equations are equivalent to finite ones.

3.1. Complete sequences of equations for the $V_{1,m}$'s

We now define some terminology that will be used in Definition 3.1 and Definition 4.1.

By an i -subset we mean a subset with i elements.

Let $m \geq 1$. A segment of type $r_1(m)$ in the element of $\{x_1\}$ is x_1 ; a segment of type $r_2(m)$ in the elements of $\{x_1, x_2\}$ is $(x_2)^e x_1$ or $(x_1)^e x_2$ for some e , $1 \leq e \leq m$; a segment of type $r_{i+1}(m)$ in the elements of $S_{i+1} = \{x_1, \dots, x_i, x_{i+1}\}$ is the nonempty concatenation of at most m segments of type $r_i(m)$ in the elements of an i -subset of S_{i+1} , say S_i , followed by the concatenation (maybe empty) of at most m segments of type $r_{i-1}(m)$ in the elements of an $i-1$ -subset of S_i , say S_{i-1}, \dots , followed by the concatenation (maybe empty) of at most m segments of type $r_1(m)$ in the element of a 1-subset of S_2 , say S_1 , followed by the element in $S_{i+1} - S_i$. Similarly, a segment of type $l_1(m)$ in the element of $\{x_1\}$ is x_1 ; a segment of type $l_2(m)$ in the elements of $\{x_1, x_2\}$ is $x_1(x_2)^e$ or $x_2(x_1)^e$ for some e , $1 \leq e \leq m$; a segment of type $l_{i+1}(m)$ in the elements of $S_{i+1} = \{x_1, \dots, x_i, x_{i+1}\}$ is the nonempty concatenation of at most m segments of type $l_i(m)$ in the elements of an i -subset of S_{i+1} , say S_i , preceded by the concatenation (maybe empty) of at most m segments of type $l_{i-1}(m)$ in the elements of an $i-1$ -subset of S_i , say S_{i-1}, \dots , preceded by the concatenation (maybe empty) of at most m segments of type $l_1(m)$ in the element of a 1-subset of S_2 say S_1 , preceded by the element in $S_{i+1} - S_i$.

Definition 3.1. Let $m \geq 1$ and let r be a nonnegative integer. $C_{(m)}^r$ is a finite sequence consisting of equations of the form

$$u_r \dots u_0 v_0 \dots v_r = u_r \dots u_0 x v_0 \dots v_r$$

where $u_0 = x^{n_0}$, $v_0 = x^{n'_0}$, where for $1 \leq i \leq r$, u_i is the concatenation of n_i segments of type $l_{i+1}(m)$ in the elements of $\{x, y_1, y_i\}$ is the concatenation of n'_i segments of type $r_{i+1}(m)$ in the elements of $\{x, z_1, \dots, z_i\}$, and where $n_i, n'_i \geq 0$, $0 \leq i \leq r$, and $m = n_0 + \dots + n_r + n'_0 + \dots + n'_r$.

Note that $C_{(m)}^0$ consists of the equation $x^m = x^{m+1}$. We have $C_{(m)}^0 \subseteq C_{(m)}^1 \subseteq C_{(m)}^2 \subseteq C_{(m)}^3 \subseteq \dots$

Theorem 3.3 gives a characterization of $V_{1,m}$ in terms of the $C_{(m)}^r$'s

Lemma 3.2. Let $|A| = r+1$, $r \geq 0$. Let M be a monoid generated by A . Then M belongs to $V_{1,m}$ if and only if M satisfies the equations in $C_{(m)}^r$.

Proof. We have to prove that $M \in V_{1,m}$ if and only if M satisfies the equations in $C_{(m)}^r$, or $M \in V_{1,m}$ if and only if for every morphism $\varphi : A^* \rightarrow M$,

$$(1) u_r \dots u_0 v_0 \dots v_r \varphi = u_r \dots u_0 x v_0 \dots v_r \varphi$$

for every equation $u_r \dots u_0 v_0 \dots v_r = u_r \dots u_0 x v_0 \dots v_r$ in $C_{(m)}^r$. Suppose $M \in V_{1,m}$ and let $\varphi : A^* \rightarrow M$ be a morphism. Then $\sim_{(m)} \subseteq \varphi$. Now, let

$$u_r \dots u_0 v_0 \dots v_r = u_r \dots u_0 x v_0 \dots v_r$$

be an equation in $C_{(m)}^r$ where the u 's and the v 's are as in Definition 3.1 and let $n = n_0 + \dots + n_r$ and $n' = n'_0 + \dots + n'_r$. By Lemma 2.2, $u_r \dots u_0 \sim_{(m)} u_r \dots u_0 x$ and $v_0 \dots v_r \sim_{(n')} x v_0 \dots v_r$. Since $n + n' = m$, Lemma 2.3 implies that

$$u_r \dots u_0 v_0 \dots v_r \sim_{(m)} u_r \dots u_0 x v_0 \dots v_r$$

and hence Equation (1) holds.

Conversely, let $\varphi : A^* \rightarrow M$ be a surjective morphism satisfying all the instances of Equation (1). We want to show that $\sim_{(m)} \subseteq \varphi$. Let $f \sim_{(m)} g$. Lemma 2.1 permits us to consider only the case where f is a subword of g . We observe also that if f is a subword of h and h is a subword of g , we have also $f \sim_{(m)} h$. Hence, we have only to consider the case where $f = uv$ and $g = uav$. So we have $uv \sim_{(m)} uav$. Lemma 2.3 implies the existence of n and n' such that $n + n' \geq m$, $u \sim_{(n)} ua$ and $v \sim_{(n')} av$. Lemma 2.2 implies the existence of $w_1, \dots, w_n \in A^*$, $w'_1, \dots, w'_{n'} \in A^*$ such that $u = w_n \dots w_1$, $v = w'_1 \dots w'_{n'}$, $\{a\} \subseteq w_1 \alpha \subseteq \dots \subseteq w_n \alpha$ and $\{a\} \subseteq w'_1 \alpha \subseteq \dots \subseteq w'_{n'} \alpha$. We can choose w_1 to be the smallest suffix of u to contain a , w_2 the smallest suffix of $u - w_1$ to contain $w_1 \alpha, \dots, w'_1$ the smallest prefix of v to contain a , w'_2 the smallest prefix of $v - w'_1$ to contain $w'_1 \alpha, \dots$. Hence $u = w_n w_{n-1} \dots w_1$, $v = w'_1 \dots w'_{n'} w'$ where $w, w' \in A^*$. There exist nonnegative integers n_0, \dots, n_r such that the n_0 first segments among w_1, \dots, w_n are of type $l_1(m_0)$ in the element of $\{a\}$, the n_1 next segments are of type $l_2(m_1)$ in the elements of $\{a, b_1\}$, \dots , and the last n_r segments are of type $l_{r+1}(m_r)$ in the elements of $\{a, b_1, \dots, b_r\}$. Here, m_0, \dots, m_r are positive integers, a, b_1, \dots, b_r are in A . Similarly, there exist nonnegative integers n'_0, \dots, n'_r such that the n'_0 first segments among $w'_1, \dots, w'_{n'}$ are of type $r_1(m'_0)$ in the element of $\{a\}$, the n'_1 next segments are of type $r_2(m'_1)$ in the elements of $\{a, c_1\}, \dots$, and the last n'_r segments are of type $r_{r+1}(m'_r)$ in the elements of $\{a, c_1, \dots, c_r\}$. Here, m'_0, \dots, m'_r are positive integers and c_1, \dots, c_r are in A . It is possible that some of $m_0, \dots, m_r, m'_0, \dots, m'_r$ be greater than m . If this is the case for some m_i , say, $0 \leq i \leq r$, and w_k ($1 \leq k \leq n$) is of type $l_{i+1}(m_i)$ in the elements of an $i + 1$ -subset of A , one can write $w_k \varphi$ as $new w_k \varphi$ where $new w_k$ is of type $l_{i+1}(m)$ in the elements of that subset of A . This can be done using instances of Equation (1). For example, let $r = 2$ and $A = \{a, b, c\}$. Let

$$u = \overbrace{ababab}^w \overbrace{abc}^{w_4} \overbrace{bacacaaaccacacccccacca}^{w_3} \overbrace{abbb}^{w_2} \overbrace{a}^{w_1}, \text{ and } v = \overbrace{cccca}^{w'_1} \overbrace{cbcba}^{w'_2} \overbrace{bcc}^{w'}$$

$uv \sim_{(5)} uav$ since $u \sim_{(4)} ua$ and $v \sim_{(2)} av$. Here, $m = 5$, $n = 4$ and $n' = 2$. There is $n_0 = 1$ segment in u of type $l_1(m_0) = l_1(1)$ in the element of $\{a\}$, i.e. w_1 ; there is $n_1 = 1$ segment in u of type $l_2(m_1) = l_2(3)$ in the elements of $\{a, b\}$, i.e. w_2 ; and there are $n_2 = 2$ segments in u of type $l_3(m_2) = l_3(7)$ in the elements of $\{a, b, c\}$, i.e. w_3 and w_4 . Also, there is $n'_1 = 0$ segments in v of type $r_1(m'_0) = r_1(1)$ in the element of $\{a\}$; there is $n'_1 = 1$ segment in v of type $r_2(m'_1) = r_2(4)$ in the elements of $\{a, c\}$, i.e. w'_1 ; and there is $n'_2 = 1$ segment in v of type $r_3(m'_2) = r_3(2)$ in the elements of $\{a, b, c\}$; i.e. w'_2 . We have that $m_2 > 5$ and w_3 is of type $l_3(m_2)$ in the elements of $\{a, b, c\}$. By hypothesis, $\varphi : A^* \rightarrow M$ is a surjective morphism satisfying all the instances of Equation (1). In particular, since $v_1 = x v_1$ where v_1 is the concatenation of 5 segments of type $r_2(5)$ in the elements of $\{x, z_1\}$ belongs to $\mathcal{C}_{(5)}^2$, $v_1 \varphi = x v_1 \varphi$. Hence, one can write $w_3 \varphi$ as $new w_3 \varphi$ where $new w_3$ is of type $l_3(5)$ in the elements of $\{a, b, c\}$.

$$\begin{aligned} w_3 \varphi &= ba(ca)(ca)(aac)(ca)(ca)ccccacca\varphi \\ &= bc(ac)(aaac)(ca)(ca)(cccca)cca\varphi \\ &= ba(ca)(aac)(ca)(ca)(cccca)cca\varphi \\ &= bc(aaac)(ca)(ca)(cccca)(cca)\varphi \\ &= baaaccacccccacca\varphi \\ &= new w_3 \varphi \end{aligned}$$

(the segments inside () are of type $r_2(5)$ in the elements of $\{a, c\}$). Similarly, if we have some m'_i greater than m . Hence $w_n \dots w_1 w'_1 \dots w'_{n'} \varphi = w_n \dots w_1 a w'_1 \dots w'_{n'} \varphi$ and $uv \varphi = uav \varphi$ follows.

Theorem 3.3. $V_{1,m}$ is defined by $\bigcup_{r \geq 0} \mathcal{C}_{(m)}^r$.

Proof. By Lemma 3.2.

3.2. Are the complete sequences of equations of the preceding sub-section equivalent to finite ones?

Is $V_{1,m}$ defined by a *finite* sequence of equations, or is $\bigcup_{r \geq 0} C_{(m)}^r$ equivalent to a finite sequence of equations? The answer is positive for $V_{1,1}$, $V_{1,2}$ and $V_{1,3}$ as the next three Theorems show.

Theorem 3.4. $\bigcup_{r \geq 0} C_{(1)}^r$ is equivalent to $C_{(1)}^1$.

Proof. $x = x^2$ is an instance of $xy_1 = xy_1x$. For $r > 0$, $1 \leq i \leq r$, equations of the form $u_i = u_i x$ where $u_i \sim_{(1)} xy_1 \dots y_i$ are easily seen to be deduced from $xy_1 = xy_1x$, and the equations of the form $v_i = xv_i$ where $v_i \sim_{(1)} xz_1 \dots z_i$ are seen to be deduced from $z_1x = xz_1x$. The equations $xy_1 = xy_1x$ and $z_1x = xz_1x$ both belong to $C_{(1)}^1$.

Theorem 3.5. $\bigcup_{r \geq 0} C_{(2)}^r$ is equivalent to $C_{(2)}^1$.

Proof. $x^2 = x^3$ is a special instance of $xy_1z_1x = xy_1xz_1x$. For $r > 0$, $1 \leq k \leq r$, let $u_k \sim_{(1)} xy_1 \dots y_k$ and $v_k \sim_{(1)} xz_1 \dots z_k$. For $1 \leq i, j \leq r$, instances of $u_i x = u_i x^2$, $xv_j = x^2v_j$, and $u_i v_j = u_i x v_j$ are easily seen to be deduced from $xy_1z_1x = xy_1xz_1x$. For $1 \leq i \leq j \leq r$, equations of the form $u_j u_i = u_j u_i x$ and $v_i v_j = xv_i v_j$ can be deduced from $xy_1z_1x = xy_1xz_1x$, $(xy_1)^2 = (xy_1)^2 x$ and $(z_1x)^2 = x(z_1x)^2$ which belong to $C_{(2)}^1$. For instance, $u_j u_i = u_j x u_i x u_i$ (using $xy_1z_1x = xy_1xz_1x$ several times since $(xu_i x)\alpha \subseteq u_i \alpha$ and $(xu_i x)\alpha \subseteq u_j \alpha = u_j x u_i x u_i$ (using $(xy_1)^2 = (xy_1)^2 x = u_j u_i x$ (since $u_j u_i = u_j x u_i x u_i$)).

Theorem 3.6. $\bigcup_{r \geq 0} C_{(3)}^r$ is equivalent to $C_{(3)}^2$.

Proof. The following sequence of equations

$$\begin{aligned} xy_1xz_1x &= xy_1x^2z_1x \\ xy_1z_1x^2z_2z_1 &= xy_1xz_1x^2z_2z_1 \\ y_1y_2x^2y_1z_1x &= y_1y_2x^2y_1xz_1x \\ (xy_1)^3 &= (xy_1)^3x \\ (z_1x)^3 &= x(z_1x)^3 \end{aligned}$$

belongs to $C_{(3)}^2$. For $r > 0$, $1 \leq l \leq r$, let $u_l \sim_{(1)} xy_1 \dots y_l$ and $v_l \sim_{(1)} xz_1 \dots z_l$

$x^3 = x^4$ is an instance of $xy_1xz_1x = xy_1x^2z_1x$. For $1 \leq i, j \leq r$, equations of the form $u_i x^2 = u_i x^3$, $x^2v_j = x^3v_j$, and $u_i xv_j = u_i x^2v_j$ are easily seen to be deduced from $xy_1xz_1x = xy_1x^2z_1x$.

For $1 \leq k \leq r$ and $1 \leq i \leq j \leq r$, we show how to deduce instances of $u_j u_i v_k = u_j u_i x v_k$ from the five equations stated at the beginning of the proof (instances of $u_j u_i x = u_j u_i x^2$, $xv_i v_j = x^2v_i v_j$, and $u_k v_i v_j = u_k x v_i v_j$ are deduced similarly).

$u_j u_i v_k = u_j u_i x v_k$ can be written as $w'xwv''xw''' = w'xwxw''xw'''$ where $w \in \{y_1, \dots, y_i\}^*$, $w' \sim_{(1)} xy_1 \dots y_j$, $w'' \in \{z_1, \dots, z_k\}^*$, $w''' \in \{x, z_1, \dots, z_k\}^*$ and can be deduced as follows: if $w = 1$, then $w'xw''x = w'x^2w''x$ using $xy_1xz_1x = xy_1x^2z_1x$ since x is in w' ; if $w \neq 1$, then $w = w_1 \dots w_n$ and $w'xwxw''x = w'xw_1 \dots w_n xw''x$

$$\begin{aligned} &= w'x^2w_1 \dots w_n xw''x \text{ (using } xy_1xz_1x = xy_1x^2z_1x \text{ since } x \text{ is in } w') \\ &= w'x^2w_1xw_2 \dots w_n xw''x \text{ (using } y_1y_2x^2y_1z_1x = y_1y_2x^2y_1xz_1x \text{ since } w_1 \text{ is in } w') \\ &= w'x^2w_1x^2w_2 \dots w_n xw''x \text{ (using } xy_1xz_1x = xy_1x^2z_1x) \\ &= w'x^2w_1x^2w_2xw_3 \dots w_n xw''x \text{ (using } y_1y_2x^2y_1z_1x = y_1y_2x^2y_1xz_1x \text{ since } w_2 \text{ is in } w') \\ &= w'x^2w_1x^2w_2x^2w_3 \dots w_n xw''x \text{ (using } xy_1xz_1x = xy_1x^2z_1x) \\ &\vdots \\ &= w'x^2w_1x^2w_2x^2w_3x^2 \dots x^2w_n xw''x \\ &= w'x^2w_1x^2w_2x^2w_3x^2 \dots x^2w_n w''x \text{ (using } y_1y_2x^2y_1z_1x = y_1y_2x^2y_1xz_1x \text{ since } w_n \text{ is in } w') \\ &= w'x^2w_1x^2w_2x^2w_3x^2 \dots xw_n w''x \text{ (using } xy_1xz_1x = xy_1x^2z_1x) \\ &= w'x^2w_1x^2w_2x^2w_3x^2 \dots x^2w_{n-1}w_n w''x \text{ (using } y_1y_2x^2y_1z_1x = y_1y_2x^2y_1xz_1x \text{ since } w_{n-1} \text{ is in } w') \\ &= w'x^2w_1x^2w_2x^2w_3x^2 \dots xw_{n-1}w_n w''x \text{ (using } xy_1xz_1x = xy_1x^2z_1x) \\ &\vdots \end{aligned}$$

$$\begin{aligned}
&= w'x^2w_1 \dots w_nw''x \\
&= w'xw_1 \dots w_nw''x \text{ (using } xy_1xz_1x = xy_1x^2z_1x \text{ since } x \text{ is in } w') \\
&= w'xww''x.
\end{aligned}$$

Now, for $1 \leq i \leq j \leq k \leq r$, we show how $u_k u_j u_i = u_k u_j u_i x$ can be deduced (the proof is similar for the equations $v_i v_j v_k = x v_i v_j v_k$). Similarly as above, we can show that $u_k u_j u_i = u_k u_j z u_i$ can be deduced where z is any variable among x, y_1, \dots, y_i . Hence, $u_k u_j u_i = u_k u_j u_i x u_i$ follows. So we get, $u_k u_j u_i = u_k u_j u_i x u_i = u_k u_j u_i x u_i x u_i = u_k u_j u_i x u_i x u_i x u_i = u_k u_j u_i x u_i x u_i x$ (using $(xy_1)^3 = (xy_1)^3 x$) $= u_k u_j u_i x u_i x = u_k u_j u_i x$.

For $m \geq 4$, does there exist r' for which $\bigcup_{r \geq 0} C_{(m)}^r$ is equivalent to $C_{(m)}^{r'}$? A positive answer to this question would provide complete *finite* sequences of equations for all the $V_{1,m}$'s.

4. Equations and $V_{2,1}$

In this section, we give an equational characterization of the monoids in $V_{2,1}$ generated by two letters.

Definition 4.1. Let $m \geq 1$. $C_{(1,m)}$ is a finite sequence consisting of equations of the form $uxyv = uyxv$ where u, v are the concatenation of m segments of type $r_2(2m+1)$ or $l_2(2m+1)$ in the elements of $\{x, y\}$.

$C'_{(1,m)}$ is a finite sequence consisting of equations of the form

$$u'uxvv' = u'ux^2vv'$$

where $u = x^n, v = x^{n'}$, where u' (v') is the concatenation of $m - n$ ($m - n'$) segments of type $r_2(2m+1)$ or $l_2(2m+1)$ in the elements of $\{x, y\}$, and where $0 \leq n, n' \leq m$.

Note that the equations in $C_{(1,m)}$ are of the form $w_1xyw_2 = w_1yxw_2$ and the ones in $C'_{(1,m)}$ of the form $w_3xw_4 = w_3x^2w_4$. Recall from Subsection 1.1 that $xy = yx$ and $x = x^2$ are the defining equations for $V_{1,1}$. The following Lemma is from [4].

Lemma 4.2. Every monoid in $V_{2,1}$ satisfies $C_{(1,m)} \cup C'_{(1,m)}$ for all sufficiently large m .

Lemma 4.3. Let M be a monoid generated by A , an alphabet of two elements. Then M belongs to $V_{2,1}$ if and only if M ultimately satisfies the equations $\bigcup_{m \geq 1} C_{(1,m)} \cup C'_{(1,m)}$.

Proof. We have to prove that $M \in V_{2,1}$ if and only if M satisfies the equations in $C_{(1,m)} \cup C'_{(1,m)}$ for all m sufficiently large. By Lemma 4.2, monoids in $V_{2,1}$ satisfy $C_{(1,m)} \cup C'_{(1,m)}$ for all sufficiently large m .

Conversely, let $\varphi : A^* \rightarrow M$ be a surjective morphism satisfying $w\varphi = w'\varphi$ for every equation $w = w'$ in $\bigcup_{n \geq m} C_{(1,n)} \cup C'_{(1,n)}$ for some $m \geq 1$. Let us show that $M \in V_{2,1}$. It is sufficient to prove that for all f and g in A^* , $f \sim_{(1,m)} g$ implies $f\varphi = g\varphi$. For $f = g = I$, it is certainly true. So assume $f, g \neq I$ and $f \sim_{(1,m)} g$. We want to show that $f\varphi = g\varphi$. Let p_1, \dots, p_s ($p_1 < \dots < p_s$) (q_1, \dots, q_s ($q_1 < \dots < q_s$)) be the (m) positions in f (g). Lemma 2.5 allows us to consider only the case where

- $Q_a^f p_i$ if and only if $Q_a^g q_i, a \in A$ for $1 \leq i \leq s$,
- $f_i \sim_{(1)} g_i$ and
- f_i is a subword of g_i for $1 \leq i \leq s-1$,

where $f_i = f(p_i, p_{i+1}), g_i = g(q_i, q_{i+1})$ for $1 \leq i \leq s-1$. Here

$$\begin{aligned}
f &= a_1 f_1 a_2 f_2 \dots a_{s-1} f_{s-1} a_s, \\
g &= a_1 g_1 a_2 g_2 \dots a_{s-1} g_{s-1} a_s,
\end{aligned}$$

where $Q_{ai}^f p_i$ and $Q_{ai}^g q_i$ for some $a_i \in A$, $1 \leq i \leq s$. The above permits us to consider only the case where $f = a_1 f_1 a_2 f_2 \dots f_{i-1} a_i f_i a_{i+1} f_{i+1} \dots a_{s-1} f_{s-1} a_s$, $g = a_1 f_1 a_2 f_2 \dots f_{i-1} a_i g_i a_{i+1} f_{i+1} \dots a_{s-1} f_{s-1} a_s$, where f_i is a subword of g_i and $f_i \sim_{(1)} g_i$ for some i between 1 and $s-1$. We observe also that if f_i is a subword of h_i and h_i a subword of g_i , we have also $f_i \sim_{(1)} h_i$. Hence we have only to consider the case where $f = a_1 f_1 a_2 f_2 \dots f_{i-1} a_i u v a_{i+1} f_{i+1} \dots a_{s-1} f_{s-1} a_s$, $g = a_1 f_1 a_2 f_2 \dots f_{i-1} a_i u a v a_{i+1} f_{i+1} \dots a_{s-1} f_{s-1} a_s$ for some i between 1 and $s-1$, some a in u or in v . Since $|A| = 2$, we have the following cases.

Case 1: If p_i is the last position among the (m) first positions in f and p_{i+1} the first position among the (m) last positions in g , then using a particular case of $C'_{(1,m)}$ i.e $x^{2m+1} = x^{2m+2}$ enables us to assume that f and g do not contain more than 2^{m+1} consecutive occurrences of a letter. Hence, we are able to write $f\varphi$ and $g\varphi$ as $f\varphi = u_m \dots u_1 u v v_1 \dots v_m \varphi$, $g\varphi = u_m \dots u_1 u a v v_1 \dots v_m \varphi$ where the u 's and the v 's are segments of type $r_2(2m+1)$ or $l_2(2m+1)$ in the elements of $\{a, b\}$ where $a, b \in A$. Then using $C_{(1,m)}$ and $C'_{(1,m)}$ enables us to write $g\varphi$ as $u_m \dots u_1 u v v_1 \dots v_m \varphi = f\varphi$ since a is in u or in v .

Case 2: Otherwise, uv contains only a 's, and a is in u or in v . Assume a is in u , so $uv = u'_0 a u_0 v$ for some $u'_0, u_0 \in A^*$. The proof when a is in v is similar. Using $x^{2m+1} = x^{2m+2}$ enables us as in Case 1 to assume that f and g do not contain more than $2m+1$ consecutive occurrences of a letter. From the choice of the p_i 's, $a_1 f_1 a_2 f_2 \dots f_{i-1} a_i u'_0 \sim_{(m)} a_1 f_1 a_2 f_2 \dots f_{i-1} a_i u'_0 a$ and $u_0 v a_{i+1} f_{i+1} \dots a_{s-1} f_{s-1} a_s \sim_{(m)} a u_0 v a_{i+1} f_{i+1} \dots a_{s-1} f_{s-1} a_s$. Lemma 2.2 hence implies the existence of $u_1, \dots, u_m \in A^*$, $v_1 \dots v_m \in A^*$ such that

$$\begin{aligned} a_1 f_1 a_2 f_2 \dots f_{i-1} a_i u'_0 &= u_m \dots u_1, \\ u_0 v a_{i+1} f_{i+1} \dots a_{s-1} f_{s-1} a_s &= v_1 \dots v_m, \end{aligned}$$

$\{a\} \subseteq u_1 \alpha \subseteq \dots \subseteq u_m \alpha$ and $\{a\} \subseteq v_1 \alpha \subseteq \dots \subseteq v_m \alpha$. Moreover, it is easy to see that if we assume that there exist k and l between 0 and m such that $u_{m-k} = \dots = u_1 = a = v_1 = \dots = v_{m-l}$, and such that the other u 's and v 's are of type $r_2(2m+1)$ or $l_2(2m+1)$ in the elements of $\{a, b\}$, then $u_m \dots u_1$ is a suffix of $a_1 f_1 a_2 f_2 \dots f_{i-1} a_i u'_0$ and $v_1 \dots v_m$ is a prefix of $u_0 v a_{i+1} f_{i+1} \dots a_{s-1} f_{s-1} a_s$. $C'_{(1,m)}$ gives

$$\begin{aligned} u_m \dots u_{m-k+1} a^{2m+1-k-l} v_{m-l+1} \dots v_m \varphi &= \\ u_m \dots u_{m-k+1} a^{2m+2-k-l} v_{m-l+1} \dots v_m \varphi. \end{aligned}$$

The result $f\varphi = g\varphi$ follows.

References

- [1] Blanchet-Sadri, F., "Some Logical Characterizations of the Dot-Depth Hierarchy and Applications," Ph.D. Thesis, McGill University, 1989.
- [2] Blanchet-Sadri, F., *Games, equations and the dot-depth hierarchy*, Computers Math. Applic. 18 (1989), 809-822.
- [3] Blanchet-Sadri, F., *On dot-depth two*, RAIRO Inform. Theor. Applic. 24 (1990), 521-529.
- [4] Blanchet-Sadri, F., *Games, equations and dot-depth two monoids*, Discr Appl. Math. 39 (1992), 99-111.
- [5] Brzozowski, J. A. and R. Knast, *The dot-dept hierarchy of star-free languages is infinite*, J. Comp. Sys. Sci. 16 (1978), 37-55.
- [6] Brzozowski, J. A. and I. Simon, *Characterizations of locally testable events*, Discr. Math. 4 (1973), 243-271.
- [7] Cohen, R. S. and J. A. Brzozowski, *Dot-depth of star-free events*, J. Comp. Sys. Sci. 5 (1971), 1-15.
- [8] Eilenberg, S., "Automata, Languages and Machines B," Academic Press, New York, 1976.
- [9] Knast, R., *A semigroup characterization of dot-depth one languages*, RAIRO Inform. Theor. 17 (1983), 321-330.
- [10] Knast, R., *Some theorems on graph congruences*, RAIRO Inform. Theor. 17 (1983), 331-342.
- [11] Lallement, G., "Semigroups and Combinatorial Applications," Wiley, N. Y., 1979.
- [12] McNaughton, R. and S. Papert, "Counter-free Automata," MIT Press, Cambridge, Mass., 1971.

- [13] Pin, J.-E. "Varieties de Langages Formels," Masson, Paris, 1984.
- [14] Schützenberger, M. P., *On finite monoids having only trivial subgroups*, Inform. Control 8 (1965), 190-194.
- [15] Simon, I., *Piecewise testable events*, In: Proc. Second GI Conf., Lect. Notes in Comp. Sci. 33 (1975), 214-222.
- [16] Straubing, H., *Finite semigroup varieties of the form $V * D$* , Pure Appl. Algebra 36 (1985), 53-94.
- [17] Straubing, H., *Semigroups and languages of dot-depth two*, In: Proc. Thirteenth ICALP, Lect. Notes in Comp. Sci. 226 (1986), 416-423.
- [18] Thomas, W., *Classifying regular events in symbolic logic*, J. Comp. Sys. Sci. 25 (1982), 360-376.
- [19] Thomas, W., *An application of the Ehrenfeucht-Fraïssé game in formal language theory*, Bull. Soc. Math. France 16 (1984), 11-21.