Star-Free Languages and Local Divisors

Manfred Kufleitner

FMI, University of Stuttgart, Germany*
kufleitner@fmi.uni-stuttgart.de

Abstract. A celebrated result of Schützenberger says that a language is star-free if and only if it is is recognized by a finite aperiodic monoid. We give a new proof for this theorem using local divisors.

1 Introduction

The class of regular languages is built from the finite languages using union, concatenation, and Kleene star. Kleene showed that a language over finite words is definable by a regular expression if and only if it is accepted by some finite automaton [3]. In particular, regular languages are closed under complementation. It is easy to see that a language is accepted by a finite automaton if and only if it is recognized by a finite monoid. As an algebraic counterpart for the minimal automaton of a language, Myhill introduced the *syntactic monoid*, *cf.* [6].

An extended regular expression is a term over finite languages using the operations union, concatenation, complementation, and Kleene star. By Kleene's Theorem, a language is regular if and only if it is definable using an extended regular expression. It is natural to ask whether some given regular language can be defined by an extended regular expression with at most n nested iterations of the Kleene star operation — in which case one says that the language has generalized star height n. The resulting decision problem is called the *generalized star height problem*. Generalized star height zero means that no Kleene star operations are allowed. Consequently, languages with generalized star height zero are called *star-free*. Schützenberger showed that a language is star-free if and only if its syntactic monoid is aperiodic [7]. Since aperiodicity of finite monoids is decidable, this yields a decision procedure for generalized star height zero. To date, it is unknown whether or not all regular languages have generalized star height one.

In this paper, we give a proof of Schützenberger's result based on *local divisors*. In commutative algebra, local divisors have been introduced by Meyberg in 1972, see [2,4]. In finite semigroup theory and formal languages, local divisors were first used by Diekert and Gastin for showing that pure future local temporal logic is expressively complete for free partially commutative monoids [1].

* The author gratefully acknowledges the support by the German Research Foundation (DFG) under grant DI 435/5-1 and the support by ANR 2010 BLAN 0202 FREC.

2 Preliminaries

The set of finite words over an alphabet A is A^*. It is the free monoid generated by A. The empty word is denoted by ε. The *length* $|u|$ of a word $u = a_1 \cdots a_n$ with $a_i \in A$ is n, and the *alphabet* $\mathrm{alph}(u)$ of u is $\{a_1, \ldots, a_n\} \subseteq A$. A language is a subset of A^*. The concatenation of two languages $K, K' \subseteq A^*$ is $K \cdot K' = \{uv \mid u \in K, v \in K'\}$, and the set difference of K by K' is written as $K \setminus K'$. Let A be a finite alphabet. The class of *star-free languages* $\mathrm{SF}(A^*)$ over the alphabet A is defined as follows:

- $A^* \in \mathrm{SF}(A^*)$ and $\{a\} \in \mathrm{SF}(A^*)$ for every $a \in A$.
- If $K, K' \in \mathrm{SF}(A^*)$, then each of $K \cup K'$, $K \setminus K'$, and $K \cdot K'$ is in $\mathrm{SF}(A^*)$.

By Kleene's Theorem, a language is regular if and only if it can be recognized by a deterministic finite automaton [3]. In particular, regular languages are closed under complementation and thus, every star-free language is regular.

Lemma 1. *If $B \subseteq A$, then $\mathrm{SF}(B^*) \subseteq \mathrm{SF}(A^*)$.*

Proof. It suffices to show $B^* \in \mathrm{SF}(A^*)$. We have $B^* = A^* \setminus \bigcup_{b \notin B} A^* b A^*$. □

A monoid M is *aperiodic* if for every $x \in M$ there exists a number $n \in \mathbb{N}$ such that $x^n = x^{n+1}$.

Lemma 2. *Let M be aperiodic. Then $x_1 \cdots x_k = 1$ in M if and only if $x_i = 1$ for all i.*

Proof. If $xy = 1$, then $1 = xy = x^n y^n = x^{n+1} y^n = x \cdot 1 = x$. □

A monoid M *recognizes* a language $L \subseteq A^*$ if there exists a homomorphism $\varphi : A^* \to M$ with $\varphi^{-1}\big(\varphi(L)\big) = L$. A consequence of Kleene's Theorem is that a language is regular if and only if it is recognizable by a finite monoid, see *e.g.* [5]. The class of *aperiodic languages* $\mathrm{AP}(A^*)$ contains all languages $L \subseteq A^*$ which are recognized by some finite aperiodic monoid.

The *syntactic congruence* $\equiv_L$ of a language $L \subseteq A^*$ is defined as follows. For $u, v \in A^*$ we set $u \equiv_L v$ if for all $p, q \in A^*$ we have $puq \in L \Leftrightarrow pvq \in L$. The *syntactic monoid* $\mathrm{Synt}(L)$ of a language $L \subseteq A^*$ is the quotient $A^* / \equiv_L$ consisting of the equivalence classes modulo $\equiv_L$. The *syntactic homomorphism* $\mu_L : A^* \to \mathrm{Synt}(L)$ with $\mu_L(u) = \{v \mid u \equiv_L v\}$ satisfies $\mu_L^{-1}\big(\mu_L(L)\big) = L$. In particular, $\mathrm{Synt}(L)$ recognizes L and it is the unique minimal monoid with this property, see *e.g.* [5].

Let M be a monoid and $c \in M$. We introduce a new multiplication $\circ$ on $cM \cap Mc$. For $xc, cy \in cM \cap Mc$ we let

$$xc \circ cy = xcy.$$

This operation is well-defined since $x'c = xc$ and $cy' = cy$ implies $x'cy' = xcy' = xcy$. For $cx, cy \in Mc$ we have $cx \circ cy = cxy \in Mc$. Thus, $\circ$ is associative and c is the neutral element of the monoid $M_c = (cM \cap Mc, \circ, c)$. Moreover,

$M' = \{x \in M \mid cx \in Mc\}$ is a submonoid of M such that $M' \to cM \cap Mc$ with $x \mapsto cx$ becomes a homomorphism. It is surjective and hence, M_c is a divisor of $(M, \cdot, 1)$ called the *local divisor of M at c*. Note that if $c^2 = c$, then M_c is just the local monoid $(cMc, \cdot, c)$ at the idempotent c.

Lemma 3. *If M is a finite aperiodic monoid and $1 \neq c \in M$, then M_c is aperiodic and $|M_c| < |M|$.*

Proof. If $x^n = x^{n+1}$ in M for $cx \in Mc$, then $(cx)^n = cx^n = cx^{n+1} = (cx)^{n+1}$ where the first and the last power is in M_c. This shows that M_c is aperiodic. By Lemma 2 we have $1 \notin cM \cap Mc$ and thus $|M_c| < |M|$. □

3 Schützenberger's Theorem on star-free languages

The following proposition establishes the more difficult inclusion of Schützenberger's result $\mathrm{SF}(A^*) = \mathrm{AP}(A^*)$. Its proof relies on local divisors.

Proposition 1. *Let $\varphi : A^* \to M$ be a homomorphism to a finite aperiodic monoid M. Then for all $p \in M$ we have $\varphi^{-1}(p) \in \mathrm{SF}(A^*)$.*

Proof. We proceed by induction on $(|M|, |A|)$ with lexicographic order. The claim is obvious for $A = \emptyset$. For $p = 1$ we have $\varphi^{-1}(1) = \{a \in A \mid \varphi(a) = 1\}^*$. Here, the inclusion from left to right follows from Lemma 2 and the other inclusion is trivial. By Lemma 1, we conclude $\varphi^{-1}(1) \in \mathrm{SF}(A^*)$. This also covers both the case $|M| = 1$ and the situation where $\varphi(a) = 1$ for all $a \in A$.

Let now $p \neq 1$ and let $c \in A$ with $\varphi(c) \neq 1$. We set $B = A \setminus \{c\}$ and we let $\varphi_c : B^* \to M$ be the restriction of φ to B^*. We have

$$\varphi^{-1}(p) \;=\; \varphi_c^{-1}(p) \cup \bigcup_{p = p_1 p_2 p_3} \varphi_c^{-1}(p_1) \cdot \left[\varphi^{-1}(p_2) \cap cA^* \cap A^*c\right] \cdot \varphi_c^{-1}(p_3). \qquad (1)$$

The inclusion from right to left is trivial. The other inclusion can be seen as follows: Every word w with $\varphi(w) = p$ either does not contain the letter c or we can factorize $w = w_1 w_2 w_3$ with $c \notin \mathrm{alph}(w_1 w_3)$ and $w_2 \in cA^* \cap A^*c$, *i.e.*, we factorize w at the first and the last occurrence of c. Equation (1) is established by setting $p_i = \varphi(w_i)$. By induction on the size of the alphabet, we have $\varphi_c^{-1}(p_i) \in \mathrm{SF}(B^*)$, and thus $\varphi_c^{-1}(p_i) \in \mathrm{SF}(A^*)$ by Lemma 1.

Since $\mathrm{SF}(A^*)$ is closed under union and concatenation, it remains to show $\varphi^{-1}(p) \cap cA^* \cap A^*c \in \mathrm{SF}(A^*)$ for $p \in \varphi(c)M \cap M\varphi(c)$. Let

$$T = \varphi_c(B^*).$$

The set T is a submonoid of M. In the remainder of this proof, we will use T as a finite alphabet. We define a substitution

$$\begin{aligned} \sigma : \quad (B^*c)^* &\to T^* \\ v_1 c \cdots v_k c &\mapsto \varphi_c(v_1) \cdots \varphi_c(v_k) \end{aligned}$$

for $v_i \in B^*$. In addition, we define a homomorphism $\psi : T^* \to M_c$ with $M_c = (\varphi(c)M \cap M\varphi(c), \circ, \varphi(c))$ by

$$\begin{aligned} \psi : \quad T^* &\to M_c \\ \varphi_c(v) &\mapsto \varphi(cvc) \end{aligned}$$

for $\varphi_c(v) \in T$. Consider a word $w = v_1 c \cdots v_k c$ with $k \geq 0$ and $v_i \in B^*$. Then

$$\begin{aligned} \psi\big(\sigma(w)\big) &= \psi\big(\varphi_c(v_1)\varphi_c(v_2)\cdots\varphi_c(v_k)\big) \\ &= \varphi(cv_1c) \circ \varphi(cv_2c) \circ \cdots \circ \varphi(cv_kc) \\ &= \varphi(cv_1cv_2\cdots cv_kc) = \varphi(cw). \end{aligned} \tag{2}$$

Thus, we have $cw \in \varphi^{-1}(p)$ if and only if $w \in \sigma^{-1}\big(\psi^{-1}(p)\big)$. This shows $\varphi^{-1}(p) \cap cA^* \cap A^*c = c \cdot \sigma^{-1}\big(\psi^{-1}(p)\big)$ for every $p \in \varphi(c)M \cap M\varphi(c)$. In particular, it remains to show $\sigma^{-1}\big(\psi^{-1}(p)\big) \in \mathrm{SF}(A^*)$. By Lemma 3, the monoid M_c is aperiodic and $|M_c| < |M|$. Thus, by induction on the size of the monoid we have $\psi^{-1}(p) \in \mathrm{SF}(T^*)$, and by induction on the size of the alphabet we have $\varphi_c^{-1}(t) \in \mathrm{SF}(B^*) \subseteq \mathrm{SF}(A^*)$ for every $t \in T$. For $t \in T$ and $K, K' \in \mathrm{SF}(T^*)$ we have

$$\begin{aligned} \sigma^{-1}(T^*) &= A^*c \cup \{1\} \\ \sigma^{-1}(t) &= \varphi_c^{-1}(t) \cdot c \\ \sigma^{-1}(K \cup K') &= \sigma^{-1}(K) \cup \sigma^{-1}(K') \\ \sigma^{-1}(K \setminus K') &= \sigma^{-1}(K) \setminus \sigma^{-1}(K') \\ \sigma^{-1}(K \cdot K') &= \sigma^{-1}(K) \cdot \sigma^{-1}(K'). \end{aligned}$$

Only the last equality requires justification. The inclusion from right to left is trivial. For the other inclusion, suppose $w = v_1 c \cdots v_k c \in \sigma^{-1}(K \cdot K')$ for $k \geq 0$ and $v_i \in B^*$. Then $\varphi_c(v_1)\cdots\varphi_c(v_k) \in K \cdot K'$, and thus $\varphi_c(v_1)\cdots\varphi_c(v_i) \in K$ and $\varphi_c(v_{i+1})\cdots\varphi_c(v_k) \in K'$ for some $i \geq 0$. It follows $v_1 c \cdots v_i c \in \sigma^{-1}(K)$ and $v_{i+1} c \cdots v_k c \in K'$. This shows $w \in \sigma^{-1}(K) \cdot \sigma^{-1}(K')$.

We conclude that $\sigma^{-1}(K) \in \mathrm{SF}(A^*)$ for every $K \in \mathrm{SF}(T^*)$. In particular, $\sigma^{-1}\big(\psi^{-1}(p)\big) \in \mathrm{SF}(A^*)$. □

Remark 1. A more algebraic viewpoint of the proof of Proposition 1 is the following. The mapping σ can be seen as a length-preserving homomorphism from a submonoid of A^*—freely generated by the infinite set B^*c—onto T^*; and this homomorphism is defined by $\sigma(vc) = \varphi_c(v)$ for $vc \in B^*c$. The mapping $\tau : M\varphi(c) \cup \{1\} \to M_c$ with $\tau(x) = \varphi(c) \cdot x$ defines a homomorphism. Now, by Equation (2) the following diagram commutes:

$$\begin{array}{ccc} (B^*c)^* & \xrightarrow{\ \sigma\ } & T^* \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ M\varphi(c) \cup \{1\} & \xrightarrow{\ \tau\ } & M_c \end{array}$$

The following lemma gives the remaining inclusion of $\mathrm{SF}(A^*) = \mathrm{AP}(A^*)$. Its proof is standard; it is presented here only to keep this paper self-contained.

Lemma 4. *For every language $L \in \mathrm{SF}(A^*)$ there exists an integer $n(L) \in \mathbb{N}$ such that for all words $p, q, u, v \in A^*$ we have*

$$p\,u^{n(L)}q \in L \;\Leftrightarrow\; p\,u^{n(L)+1}q \in L.$$

Proof. For the languages A^* and $\{a\}$ with $a \in A$ we define $n(A^*) = 0$ and $n(\{a\}) = 2$. Let now $K, K' \in \mathrm{SF}(A^*)$ such that $n(K)$ and $n(K')$ exist. We set

$$n(K \cup K') = n(K \setminus K') = \max\big(n(K), n(K')\big),$$
$$n(K \cdot K') = n(K) + n(K') + 1.$$

The correctness of the first two choices is straightforward. For the last equation, suppose $p\,u^{n(K)+n(K')+2}q \in K \cdot K'$. Then either $p\,u^{n(K)+1}q' \in K$ for some prefix q' of $u^{n(K')+1}q$ or $p'\,u^{n(K')+1}q \in K'$ for some suffix p' of $pu^{n(K)+1}$. By definition of $n(K)$ and $n(K')$ we have $p\,u^{n(K)}q' \in K$ or $p'\,u^{n(K')}q \in K'$, respectively. Thus $p\,u^{n(K)+n(K')+1}q \in K \cdot K'$. The other direction is similar: If $p\,u^{n(K)+n(K')+1}q \in K \cdot K'$, then $p\,u^{n(K)+n(K')+2}q \in K \cdot K'$. This completes the proof. □

Theorem 1 (Schützenberger). *Let A be a finite alphabet and let $L \subseteq A^*$. The following conditions are equivalent:*

1. *L is star-free.*
2. *The syntactic monoid of L is finite and aperiodic.*
3. *L is recognized by a finite aperiodic monoid.*

Proof. "1 ⇒ 2": Every language $L \in \mathrm{SF}(A^*)$ is regular. Thus $\mathrm{Synt}(L)$ is finite, *cf.* [5]. By Lemma 4, we see that $\mathrm{Synt}(L)$ is aperiodic. The implication "2 ⇒ 3" is trivial. If $\varphi^{-1}\big(\varphi(L)\big) = L$, then we can write $L = \bigcup_{p \in \varphi(L)} \varphi^{-1}(p)$. Therefore, "3 ⇒ 1" follows by Proposition 1. □

The syntactic monoid of a regular language (for instance, given by a non-deterministic automaton) is effectively computable. Hence, from the equivalence of conditions "1" and "2" in Theorem 1 it follows that star-freeness is a decidable property of regular languages. The equivalence of "1" and "3" can be written as

$$\mathrm{SF}(A^*) = \mathrm{AP}(A^*).$$

The equivalence of "2" and "3" is rather trivial: The class of finite aperiodic monoids is closed under division, and the syntactic monoid of L divides any monoid that recognizes L, see *e.g.* [5].

Acknowlegdements

The author would like to thank Volker Diekert and Benjamin Steinberg for many interesting discussions on the proof method for Proposition 1.

References

1. V. Diekert and P. Gastin. Pure future local temporal logics are expressively complete for Mazurkiewicz traces. *Information and Computation*, 204:1597–1619, 2006.
2. A. Fernández López and M. Tocón Barroso. The local algebras of an associative algebra and their applications. In J. Misra, editor, *Applicable Mathematics in the Golden Age*, pages 254–275. Narosa, 2002.
3. S. C. Kleene. Representation of events in nerve nets and finite automata. In C. E. Shannon and J. McCarthy, editors, *Automata Studies*, number 34 in Annals of Mathematics Studies, pages 3–40. Princeton University Press, 1956.
4. K. Meyberg. Lectures on algebras and triple systems. Technical report, University of Virginia, Charlottesville, 1972.
5. J.-É. Pin. *Varieties of Formal Languages*. North Oxford Academic, London, 1986.
6. M. O. Rabin and D. Scott. Finite automata and their decision problems. *IBM Journal of Research and Development*, 3:114–125, 1959. Reprinted in E. F. Moore, editor, *Sequential Machines: Selected Papers*, Addison-Wesley, 1964.
7. M. P. Schützenberger. On finite monoids having only trivial subgroups. *Information and Control*, 8:190–194, 1965.