Zero-One Law for Regular Languages
and Semigroups with Zero

Ryoma Sin’ya
Tokyo Institute of Technology
shinya.r.aa@m.titech.ac.jp
École Nationale Supérieure des Télécommunications
rshinya@enst.fr

Keywords: zero-one laws, syntactic monoids with zero, zero automata, finite model theory, equational theory, synchronisation words

Abstract. A regular language has the zero-one law if its asymptotic density converges to either zero or one. We prove that the class of all zero-one languages is closed under Boolean operations and quotients. Moreover, we prove that a regular language has the zero-one law if and only if its syntactic monoid has a zero element. Our proof gives both algebraic and automata characterisation of the zero-one law for regular languages, and it leads the following two corollaries: (i) There is an \(O(n \log n)\) algorithm for testing whether a given regular language has the zero-one law. (ii) The Boolean closure of existential first-order logic over finite words has the zero-one law.

1 Introduction

Let \(L\) be a regular language over a finite alphabet \(A\). Recall that the counting function \(\gamma_n(L)\) of \(L\) counts the number of different words of length \(n\) in \(L\):

\[
\gamma_n(L) = |L \cap A^n|
\]

The density function \(\mu_n(L)\) of \(L\) is the fraction defined by

\[
\mu_n(L) = \frac{\gamma_n(L)}{\gamma_n(A^*)} = \frac{|L \cap A^n|}{|A^n|}
\]

where \(A^n\) is the set of all words of length \(n\) over \(A\). The asymptotic density \(\mu(L)\) of \(L\) is defined by \(\mu(L) = \lim_{n \to \infty} \mu_n(L)\), if the limit exists. We can regard \(\mu_n(L)\) as the probability that a randomly chosen word of length \(n\) is in \(L\), and \(\mu(L)\) as its asymptotic probability. The following class is our main target of this paper.

**Definition 1.** A regular language \(L\) **has the zero-one law**, or is **zero-one** for short, if its asymptotic density \(\mu(L)\) is either zero or one. We denote by \(ZO\) the class of all regular zero-one languages.

The notion zero-one law comes from finite model theory. It states that properties expressible in many logics (e.g., first-order logic, logic with a fixed point operator, finite variable infinitary logic and certain fragments of second-order logic) are almost surely true or almost surely false; either they hold for almost all finite structures, or they fail for almost all finite structures (cf. [1]).
**Equational theory of regular languages and languages with zero.**

A *variety of languages* is a class of regular languages closed under Boolean operations, inverses of morphisms and left and right quotients by words. Eilenberg’s variety theorem [2] states that varieties of languages are in one-to-one correspondence with *varieties of finite monoids*, that is, classes of finite monoids closed under taking submonoids, quotient monoids and finite direct products. Reiterman [3] proved that any variety of finite monoids can be characterised by a set of *profinite identities*. A profinite identity is an identity between two *profinite words*. The profinite words on an alphabet $A$ is the completion of $A^*$ by a certain metric defined by monoids and denoted by $\hat{A}^*$. We do not intend to explain in detail the notion of profinite words in this paper, we refer to a book written by Pin [4] for more information on this subject.

Since the work of Eilenberg and Reiterman, the theory have been extended several times over the last thirty years by relaxing the definition of a variety of languages. In particular, Gehrke et al. have introduced *equational theory* of regular languages in their ICALP paper [5], and they proved the following equational description of a *Boolean quotenting algebra*; i.e., a class of languages closed under Boolean operations and quotients.

**Proposition 1 (Proposition 7.4 in [5]).** A set of regular languages of $A^*$ is a Boolean quotenting algebra if and only if it can be defined by a set of semigroup equations of the form $u = v$, where $u, v$ in $\hat{A}^*$.

In addition, Gehrke et al. showed that the class of all regular languages whose syntactic monoid has a zero can be defined by a *profinite equation* with a certain profinite word $\rho_A$ as follows.

**Definition 2.** A regular language $L$ has a zero, or $L$ is a language with zero, if its syntactic monoid has a zero element. We denote by $Z$ the class of all regular languages with zero.

**Proposition 2 (Proposition 9.1 in [5]).** A regular language of $A^*$ has a zero if and only if it satisfies the equations $x\rho_A = \rho_A = \rho_Ax$ for all $x$ in $\hat{A}^*$.

Proposition 2 shows us an equational characterisation of $Z$. However, it is still unknown whether there exists combinatorial characterisation or syntactic characterisation of $Z$.

**Our results.** In this paper, we first prove that $ZO$ the class of all zero-one languages is closed under Boolean operations and quotients.

**Theorem 1.** $ZO$ is a Boolean quotenting algebra.

According to Theorem 1 and Proposition 1, $ZO$ must have an equational definition. However, how to find it? We completely answer this question by proving the following theorem, which characterises $ZO$ and $Z$ by means of a transparent condition for their minimal automata: *zero automata* which will be described later. That is, $ZO$ and $Z$ are equivalent and hence they has the same equational definition $x\rho_A = \rho_A = \rho_Ax$ from Proposition 2.
Theorem 2. Let $L$ be a regular language. The following three conditions are equivalent.

1. $L$ has a zero.
2. $L$ has the zero-one law.
3. Its minimal automaton is zero.

This is surprising because these two notion seem completely different from each other; $ZO$ is defined by the asymptotic behavior of its density, while $Z$ is defined by the existence of a zero of its syntactic monoid. Theorem 2 gives us the both algebraic and automata characterisation of the zero-one law for regular languages, and this leads the two following corollaries.

First, the automata characterisation of zero-one languages in Theorem 2 gives us an efficient algorithm testing for the zero-one law as the following corollary. Note that Hopcroft’s automaton minimisation algorithm has $O(n \log n)$ complexity and Tarjan’s strongly connected components algorithm has complexity $O(n + n|A|)$ complexity where $n$ and $n|A|$ denote the number of states and the number of transitions of a given deterministic automaton respectively.

Corollary 1. There is an $O(n \log n)$ algorithm for testing whether a given regular language has the zero-one law, if it is given by an $n$-states deterministic finite automaton.

Second, the algebraic characterisation of zero-one languages in Theorem 2 tells us that certain logics over finite words have the zero-one law. We say that a logic $L$ has the zero-one law if, every language definable in $L$ has the zero-one law (cf. [1]). A language is called piecewise testable if, it is a finite Boolean combination of languages of the form $A^*a_1A^*a_2\cdots a_kA^*$ for each $a_i$ in $A$. Simon’s theorem [6] characterises piecewise testable languages by so-called $J$-trivial monoids, and it is also known that the Boolean closure of existential first-order logic captures precisely piecewise testable languages (cf. [7]). In addition, since every $J$-trivial syntactic monoid has a zero element (cf. [4]), Theorem 2 leads the following corollary.

Corollary 2. The Boolean closure of existential first-order logic over finite words has the zero-one law.

Related works. General theorems of correspondence between combinatorial properties of class of languages and algebraic structures of monoids have been investigated (cf. Table 1). One of the most old, famous and beautiful result is Schützenberger’s theorem [8] characterising star-free languages as corresponding to aperiodic monoids. Schützenberger also characterised the class of monoids so-called DA by unambiguous polynomials which are particular regular languages. The other well known algebraic characterisation of languages is Simon’s theorem [6] described above.
| Languages            | Monoids          |
|---------------------|------------------|
| star-free           | aperiodic        |
| unambiguous polynomials | DA              |
| piecewise testable  | $J$-trivial      |
| zero-one            | with zero (also called null) |

(Schützenberger, 1965 [8])
(Schützenberger, 1976 [9])
(Simon, 1975 [6])
(Theorem 2)

| Languages            | Equations (with the precondition $xA = xA$ for all $x$ in $A^*$) |
|----------------------|---------------------------------------------------------------|
| zero-one             | $T$ (Theorem 2)                                               |
| sparse or cosparse   | $\forall x, y \in A^+, i(x) \neq i(y) \Rightarrow (x^\omega y^\omega)^\omega = xA$ (Theorem 9.6 in [5]) |
| slender or coslender | $\forall x, y \in A^+, u \in A^+, i(uy) \neq i(x) \Rightarrow x^\omega uy^\omega = xA$ (Theorem 9.4 in [5]) |

There exist other classes of languages related to zero. We call the language $A^*$ full. If $\mu_n(L) = O(1)$ with respect to $n$, then $L$ is called a slender language. A language is sparse if it has a polynomial density, that is, $\mu_n(L) = O(n^k)$ for some $k > 0$. Finally, a language $L$ is called coslender if its complement is slender, and a language $L$ is called cosparse if its complement is sparse. Let us denote by $i(w)$ the first letter of a word $w$. Gehrke et al. [5] proved that both the class of all sparse or cosparse languages and the class of all slender or coslender languages are Boolean quotienting algebras, and showed these equational definition as in Table 2 with a certain profinite word $x^\omega$: the idempotent element generated by $x$ in $\hat{A}^*$. Details of these results can be found in a book written by Pin [4].

In contrast to the class of monoids with zero, its natural corresponding class zero automata has not been given much attention. Only few studies (e.g., [10]) have investigated zero automata in the context of the theory of synchronising word for Černý’s conjecture as far as we know. Thus, we describe the detailed definition and properties of zero automata in Section 3.

The notion of density $\mu_n$ presented in this paper was firstly studied by Berstel [11] in 1973, by Salomaa and Soittola [12] in 1978 in the context of the theory of formal power series and they showed that $\mu_n(L)$ has finitely many accumulation points and each accumulation point is rational. Another approach, based on Markov chains theory, was presented by Bodirsky et al. [13], and they introduced an $O(n^3)$ algorithm whether a given language $L$ satisfies $\mu(L) = 1$ (and hence whether $L$ has the zero-one law), if $L$ is given by an $n$-states deterministic finite automaton. Corollary 1 gives us a more efficient algorithm.

**Paper outline.** We first give the necessary definitions and terminology for languages, monoids, and automata in Section 2. In Section 3 we give the definition of zero automata, and we describe its properties which we will use to prove Theorem 2. Then we prove Theorem 1 in Section 4, and finally we prove Theorem 2 in Section 5.
2 Preliminaries

In this paper, all considered automata are deterministic finite, complete and accessible. We refer the reader to the book by Sakarovitch [14] for background material.

Languages and Monoids. We denote by $A^*$ [$A^n$] the set of all words [of length $n$] over a finite alphabet $A$, and denote $|w|$ by the length of a word $w$ in $A^*$, i.e., $|w| = k \Leftrightarrow w \in A^k$. The empty word is denoted by $\varepsilon$. That is, $A^*$ is the free monoid over $A$ with the identity element $\varepsilon$. We can easily verify that

$$\mu_{n+k}(A^k L) = \frac{|A^k L \cap A^{n+k}|}{|A^{n+k}|} = \frac{|A^k (L \cap A^n)|}{|A^k A^n|} = \frac{|L \cap A^n|}{|A^n|} = \mu_n(L)$$

holds for any language $L$ of $A^*$ and $k \geq 0$, thus $\mu(A^k L) = \mu(L)$ if it exists. If two languages $L$ and $K$ of $A^*$ are mutually disjoint ($L \cap K = \emptyset$), then clearly $\mu(L \cup K) = \mu(L) + \mu(K)$ holds if both $\mu(L)$ and $\mu(K)$ exist. We write $v \circ w$ [$v \not\subset w$] for a pair of words $v, w$ in $A^*$ if $w$ contains $v$ (does not contain) $v$ as a subword; which means that there exists $x, y$ in $A^*$ such that $x y = w$. Let $L$ be a language of $A^*$ and let $u$ be a word of $A^*$. The left [right] quotient $u^{-1} L [L u^{-1}]$ of $L$ by $u$ is defined by:

$$u^{-1} L = \{ v \in A^* \mid u v \in L \} \quad \text{and} \quad L u^{-1} = \{ v \in A^* \mid v u \in L \}.$$  

We denote by $\overline{L} = A^* \setminus L$ the complement of $L$. Given a language $L$ of $A^*$, the syntactic congruence of $L$ in $A^*$ is the relation $\sim_L$ defined on $A^*$ by $u \sim_L v$ if and only if, $x y \in L \Leftrightarrow x y v \in L$ holds for all $x, y$ in $A^*$. The quotient $A^*/\sim_L$ is the syntactic monoid of $L$ and the natural morphism $\phi_L : A^* \rightarrow A^*/\sim_L$ is the syntactic morphism of $L$. If $M$ is a monoid, an element $0$ in $M$ is said to be a zero if, $0 m = m 0 = 0$ holds for all $m$ in $M$.

Automata. An (complete deterministic finite) automaton over a finite alphabet $A$ is a quintuple $A = (Q, A, \cdot, q_0, F)$ where

- $Q$ is a finite set of states;
- $\cdot : Q \times A \rightarrow Q$ is a transition function, which can be extended to a mapping $\cdot : Q \times A^* \rightarrow Q$ by $q \cdot \varepsilon = q$ and $q \cdot a w = (q \cdot a) \cdot w$ where $q \in Q, a \in A, w \in A^*$;
- $q_0 \in Q$ is an initial state, and $F \subseteq Q$ is a set of final states.

The set of all acceptable words of $A$, or language of $A$, is denoted by $L(A) = \{ w \in A^* \mid q_0 \cdot w \in F \}$. We say $A$ recognises $L$ if $L = L(A)$. It is a basic fact that, for any regular language $L$, there exists a unique automaton recognises $L$ that has the minimum number of states: the minimal automaton of $L$ and we denote it by $A_L$. Each word $w$ in $A^*$ defines a transformation $w : q \mapsto q \cdot w$ on $Q$, the transition monoid of $A$ is equal to the transformation monoid generated by the generators $A$. It is a well known that the syntactic monoid of a regular language is equal to the transition monoid of its minimal automaton (cf. [14]).
For any subset \( P \) of \( Q \), the past of \( P \) is the language denoted by \( \text{Past}(P) \) and defined by:

\[
\text{Past}(P) = \{ w \in A^* \mid q_0 \cdot w \in P \}.
\]

One can easily verify that \( \text{Past}(P) \) is the language recognised by an automaton \( \langle Q, A, \cdot, q_0, P \rangle \) and \( \text{Past}(F) = L(A) \) by the definition. In Section 5, we will use the following fundamental lemma from variety theory.

**Lemma 1** (cf. [15]). Let \( A_L = \langle Q, A, \cdot, q_0, F \rangle \) be the minimal automaton of a language \( L \). Then for any subset \( P \) of \( Q \), its past \( \text{Past}(P) \) can be expressed as a finite Boolean combination of languages of the form \( Lw^{-1} \).

### 3 Zero automata

In this section, we describe the definition of zero automata and its properties.

Let \( \mathcal{A} \) be an automaton \( \langle Q, A, \cdot, q_0, F \rangle \). For each pair of state \( p, q \) in \( Q \), we say that \( q \) is reachable from \( p \) if there exists a word \( w \) such that \( p \cdot w = q \). \( \mathcal{A} \) is called accessible if every state \( q \) in \( Q \) is reachable from the initial state \( q_0 \). A subset \( P \) of \( Q \) is called strongly connected component, if for every pair \( p, q \) in \( P \) are reachable from each other. We say a subset \( P \) of \( Q \) is closed if there is no transition from any state \( p \) in \( P \) to a state which does not in \( P \). That is, \( Q \setminus P \) are not reachable from \( P \). Note that, every (complete) automaton has at least one closed strongly connected component. A strongly connected component \( P \) is trivial if it consists of a single state \( P = \{ p \} \). We call a state \( q \) in \( Q \) is zero if \( q \cdot w = q \) holds for every word \( w \) in \( A^* \). We shall identify a singleton \( \{ p \} \) with its unique element \( p \). If a strongly connected component is both closed and trivial, then it clearly consists of a single zero state. A word \( w \) is a synchronising word of \( \mathcal{A} \) if there exists a certain state \( q \) in \( Q \), \( p \cdot w = q \) holds for every state \( p \) in \( Q \). That is, \( w \) is the constant map from \( Q \) to \( q \).

We call an automaton synchronising if it has a synchronising word. Note that any synchronising automaton has at most one zero state. As we will prove in Section 5, the following class of automata captures precisely \( ZO \) and \( Z \).

**Definition 3.** An automaton is zero if it is synchronising and has a zero state.

**Example 1.** Consider two automata \( \mathcal{A}_0 \) and \( \mathcal{A}_1 \) illustrated in Figure 1. \( \mathcal{A}_0 \) is a zero automaton but \( \mathcal{A}_1 \) is not, though both automata have a zero state \( q_5 \). The only difference between \( \mathcal{A}_0 \) and \( \mathcal{A}_1 \) is the transition \( q_4 \cdot a \); which equals to \( q_5 \) in \( \mathcal{A}_0 \), while which equals to \( q_3 \) in \( \mathcal{A}_1 \). We can easily verify that, \( \mathcal{A}_0 \) has the unique closed strongly connected component \( q_5 \), while \( \mathcal{A}_1 \) has the two closed strongly connected components \( \{ q_3, q_4 \} \) and \( q_5 \).

We can rephrase Definition 3 by using the uniqueness of strongly connected component as follows.

**Lemma 2.** Let \( \mathcal{A} = \langle Q, A, \cdot, q_0, F \rangle \) be an automaton. Then \( \mathcal{A} \) is zero if and only if \( \mathcal{A} \) has a unique closed strongly connected component and it is trivial.
Fig. 1. Zero and non-zero automata

Fig. 2. Synchronising word $v_{n-1} = w_0 \cdots w_{n-1}$ in the proof of Lemma 2

**Proof.** First we assume $A$ is zero with a zero state $p$. Then there exists a synchronising word $w$ and it clearly satisfies $q \cdot w = p$ for each $q$ in $Q$ since $p$ is zero. This shows that there is no closed strongly connected component in $Q \setminus p$.

Now we prove the converse direction, we assume $A$ has a unique closed strongly connected component and it is trivial $p$. We can verify that for every state $q$ in $Q$, there exists a word $w$ in $A^*$, such that $q \cdot w = p$. Indeed, if there does not exist such word $w$ for some $q$, then the set of all reachable states from $q : \{r \in Q \mid \exists w \in A^*, q \cdot w = r\}$ must contains at least one closed strongly connected component which does not contain $p$. This contradicts with the uniqueness of the closed strongly connected component $p$ in $A$. Then the existence of a synchronising word $w$ is guaranteed because we can concretely construct it. Let $n$ be the number of states $n = |Q|$ and let $Q = \{q_0, \cdots, q_{n-1} = p\}$. We define a word sequence $w_i$ inductively by $w_0 = u_{q_0}$ and $w_i = u_{(q_i \cdot v_{i-1})}$ where each $u_{q_i}$ is a shortest word satisfies $q_i \cdot u_{q_i} = p$, and $v_{i-1}$ is the word of the form $w_0 \cdots w_{i-1}$. As shown in Figure 2, we can easily verify that the word $v_{n-1} = w_0 \cdots w_{n-1}$ is a synchronising word satisfies $q \cdot v_{n-1} = p$ for each $q$ in $Q$.

For example, consider the zero automaton $A_0$ in Figure 1. Then each $u_{q_i}$, $w_{q_i}$ and $v_{q_i}$ are defined as follows.
| $q_i$ | $u_{q_i}$ | $w_{q_i}$ | $v_{q_i}$ |
|-------|----------|----------|----------|
| $q_0$ | aab      | aab      | aab      |
| $q_1$ | ab       | b        | aabb     |
| $q_2$ | b        | $\varepsilon$ | aabb |
| $q_3$ | aa       | $\varepsilon$ | aabb |
| $q_4$ | a        | $\varepsilon$ | aabb |
| $q_5$ | $\varepsilon$ | $\varepsilon$ | aabb |

The obtained word $v_{q_4} = aabb$ is a synchronising word which satisfies $q_i \cdot aabb = q_5$ for all $q_i$ in $A_0$. It is clear that the non-zero automaton $A_1$ in Figure 1 does not have a synchronising word since it has two closed strongly connected components.

4 \( ZO \) is a Boolean quotienting algebra

Before proving Theorem 1, we introduce the following lemma.

**Lemma 3.** Let $L$ be a language of $A^*$ and $w$ be a word in $A^k$. Then the asymptotic density of $L$ exists if and only if the asymptotic density of the languages $wL$ and $Lw$ exists. Moreover, these density satisfies $\mu(wL) = \mu(Lw) = |A|^{-k}\mu(L)$.

**Proof.** Since $wL$ and $Lw$ clearly have the same counting function, we only have to prove the case of $wL$. For every $u, v$ in $A^k$ and $u \neq v$, the language $uL$ and $vL$ are obviously mutually disjoint and these counting functions satisfies

$$
\gamma_n(uL) = \gamma_n(vL) = \begin{cases} 0 & n < k, \\ \gamma_{n-k}(L) & n \geq k. \end{cases}
$$

This shows that $uL$ and $vL$ have the same counting function and thus have the same asymptotic density if its exists. We can easily verify that

$$
\mu(L) = \mu(A^kL) = \sum_{u \in A^k} \mu(uL) = |A|^k\mu(wL)
$$

holds for any $w$ in $A^k$. \(\square\)

Now we prove Theorem 1.

**Proof (Theorem 1).** We first prove that $ZO$ is closed under Boolean operations, and then prove that $ZO$ is closed under quotients.

**ZO is closed under Boolean operations.** Let $L, K$ be two languages in $ZO$. It is obvious that $ZO$ is closed under complement since $\mu(\overline{L}) = 1 - \mu(L) \in \{0, 1\}$, and we can easily verify that the following equations holds.

- $\mu(L \cup K) = 0$ if $\mu(L) = 0$ and $\mu(K) = 0$;
- $\mu(L \cap K) = 0$ if either $\mu(L) = 0$ or $\mu(K) = 0$;
- $\mu(L \cup K) = 1$ if either $\mu(L) = 1$ or $\mu(K) = 1$;
- $\mu(L \cap K) = 1$ if $\mu(L) = 1$ and $\mu(K) = 1$. 
ZO is closed under quotients. We first prove that ZO is closed under left quotients. Let $L$ be a regular language in ZO and we can assume that $L$ does not contain $\varepsilon$ without loss of generality. First we assume $\mu(L) = 0$. By the definition of left quotients, one can easily verify that

$$L = \bigcup_{a \in A} aa^{-1}L$$

holds (since $\varepsilon \notin L$) and all these sets $aa^{-1}L$ are mutually disjoint. It follows that the following equation holds.

$$\mu(L) = \lim_{n \to \infty} \frac{|L \cap A^n|}{|A^n|} = \lim_{n \to \infty} \frac{|\bigcup_{a \in A} aa^{-1}L \cap A^n|}{|A^n|} = \lim_{n \to \infty} \frac{|\bigcup_{a \in A} aa^{-1}L \cap A^n|}{|A^n|} = \lim_{n \to \infty} \frac{\sum_{a \in A} |aa^{-1}L \cap A^n|}{|A^n|} = \sum_{a \in A} \mu(aa^{-1}L) = 0.$$ 

This leads, for each $a$ in $A$, the asymptotic density $\mu(aa^{-1}L)$ equals to zero since its summation equals zero. In addition, $\mu(aa^{-1}L)$ coincides with $\mu(a^{-1}L)$ for any $a$ in $A$, because $\mu(aa^{-1}L) = |A|^{-1}\mu(a^{-1}L) = 0$ by Lemma 3 whence $\mu(a^{-1}L) = 0$.

Next we assume $\mu(L) = 1$. Then $\mu(TL) = 0$ and

$$a^{-1}T = \{w \in A^* | aw \in T\} = \{w \in A^* | aw \notin L\} = a^{-1}L$$

holds. We therefore obtain:

$$\mu(a^{-1}L) = 1 - \mu(a^{-1}L) = 1 - \mu(a^{-1}T) = 1 - 0 = 1.$$ 

We can prove that ZO is closed under right quotients by the same manner.  

\[5\] Equivalence of ZO and Z

To prove Theorem 2, we will use the following lemma which is a direct consequence of Lemma 1 and Theorem 1.

**Lemma 4.** Let $L$ be a regular language in ZO, $A_L = \langle Q, A, \cdot, q_0, F \rangle$ be its minimal automaton. Then, for any subset $P$ of $Q$ in $A_L$, its past $\text{Past}(P)$ also has the zero-one law. That is, $\text{Past}(P)$ is in ZO for any $P$.

**Proof.** By Lemma 1, for any subset $P$ of $Q$, its past $\text{Past}(P)$ can be expressed as a finite Boolean combination of languages of the form $Lw^{-1}$. It follows that $\text{Past}(P)$ has the zero-one law, since $L$ has the zero-one law and ZO is closed under Boolean operations and quotients by Theorem 1.

Lemma 4 will be used in proving the direction $2 \Rightarrow 3$. Now we give the proof of Theorem 2.
Proof (Theorem 2). We show the implications 3 → 1 → 2 → 3.

The direction 3 → 1 (\(A_L\) is zero ⇒ \(L\) has a zero). Let \(A_L = \langle Q, A, \cdot, q_0, F \rangle\) be the minimal automaton of \(L\) and it is zero with a zero state \(p\). Let \(M\) be the transition monoid of \(A_L\), let \(\phi: A^* \rightarrow M\) be the syntactic morphism of \(L\). Then we can verify that \(M\) has a zero element \(\mathbf{0}\) as the transformation \(\mathbf{0}: q \mapsto \mathbf{p}\) for all \(q \in Q\), that is, \(\mathbf{0}\) is the constant map from \(Q\) to \(q\). The existence of \(\mathbf{0}\) is guaranteed since \(A_L\) is synchronising. Indeed, for any synchronising word \(w\), \(\phi(w) = \mathbf{0}\) holds. One can easily verify that \(m\mathbf{0} = \mathbf{0}m = \mathbf{0}\) for all \(m \in M\). This proves that \(M\) the syntactic monoid of \(L\) has the zero.

The direction 1 ⇒ 2 (\(L\) has a zero ⇒ \(L\) has the zero-one law). Let \(L\) be a regular language in \(\mathcal{Z}\), \(M\) be its syntactic monoid with a zero element \(\mathbf{0}\) and \(\phi: A^* \rightarrow M\) be its syntactic morphism. We choose a word \(w_0\) from the preimage of \(\mathbf{0}\): \(w_0 \in \phi^{-1}(\mathbf{0})\).

Now we prove \(\mu(L) = 1\) if \(w_0\) in \(L\). By the definition of zero, we have:

\[
\phi(xw_0y) = \phi(x)\phi(w_0)\phi(y) = \phi(x)\mathbf{0}\phi(y) = \mathbf{0}
\]

for any words \(x, y \in A^*\). That is, if \(w\) contains \(w_0\) as a subword, then \(\phi(w) = \phi(w_0) = \mathbf{0}\) holds and hence \(w\) also in \(L\). Let \(L_{w_0} = \{w \in A^* \mid w_0 \triangleleft w\}\) be the set of all words that contain \(w_0\) as a subword. Then clearly \(L_{w_0}\) is contained in \(L\) from which we get \(\mu_n(L_{w_0}) \leq \mu_n(L)\) for all \(n\). The density \(\mu_n(L_{w_0})\) is nothing but the probability that a randomly chosen word of length \(n\) contains \(w_0\) as a subword. The following well known theorem, sometimes called Borge’s theorem (cf. Note I.35 in [16]), ensures that \(\mu_n(L_{w_0})\) tends to one if \(n\) tends to infinity. This shows \(\mu(L) = \mu(L_{w_0}) = 1\).

Borge’s theorem. Take any fixed finite set \(\Pi\) of words in \(A^*\). A random word in \(A^*\) of length \(n\) contains all the words of the set \(\Pi\) as subwords with probability tending to one exponentially fast as \(n\) tends to infinity.

Indeed, for any \(w\) in \(A^*\), we can calculate the exact probability by using autocorrelation polynomial (cf. [16]). We can prove \(\mu(L) = 0\) if \(w_0\) not in \(L\) by the same manner.

The direction 2 ⇒ 3 (\(L\) has the zero-one law ⇒ \(A_L\) is zero). Let \(L\) be a regular language in \(\mathcal{Z}\) and \(A_L = \langle Q, A, \cdot, q_0, F \rangle\) be its minimal automaton, let \(\{P_1, \cdots, P_k\}; P_i \subseteq Q\) be the closed strongly connected components of \(A_L\), and \(P = \bigcup_{i=1}^k P_i\) be its union. Our goal is to prove that \(A_L\) has a unique closed strongly connected component and it is trivial; i.e., \(k = 1\) and \(P = P_1 = p\) for a unique zero state \(p\) in \(Q\). It follows that \(A_L\) is zero by Lemma 2.

For any closed strongly connected component \(P_i\), there exists a word \(w_i\) such that \(q_0w_i\) in \(P_i\) since \(A_L\) is accessible. The closeness of \(P_i\) leads that the language \(w_iA^*\) is contained in \(\text{Past}(P_i)\) from which we get the following inequality

\[
0 < \mu(w_iA^*) = |A|^{-|w_i|}\mu(A^*) = |A|^{-|w_i|} \leq \mu(\text{Past}(P_i)) \tag{1}
\]
holds for each $P_i$ by Lemma 3. Lemma 4 and Equation (1) leads that the asymptotic density $\mu(\text{Past}(P_i))$ surely exists and satisfies

$$\mu(\text{Past}(P_i)) = 1$$

for every closed strongly connected component $P_i$.

Now we prove $k = 1$. By Equation (2), we can easily verify that

$$\mu \left( \bigcup_{i=1}^{k} \text{Past}(P_i) \right) = \sum_{i=1}^{k} \mu(\text{Past}(P_i)) = k$$

holds because $A_L$ is deterministic whence all $\text{Past}(P_i)$ are mutually disjoint. Note that, every automaton has at least one closed strongly connected component whence $k \geq 1$. This clearly shows $k = 1$, that is, $A_L$ has the unique closed strongly connected component $P = P_1$.

Next we let $P = \{p_1, \ldots, p_n\}$ and prove $n = 1$. Since $P$ satisfies $\mu(\text{Past}(P)) = 1$ by Equation (2), there exists exactly one state $p$ in $P$ satisfies $\mu(\text{Past}(p)) = 1$ by Lemma 4. Further, because $P$ is strongly connected, for every state $p_i$ in $P$, there exists a word $w_i$ such that $p \cdot w_i = p_i$. It follows that Past$(p)w_i \subseteq$ Past$(p_i)$ and thus

$$0 < \mu(\text{Past}(p)w_i) = |A|^{-|w_i|} \mu(\text{Past}(p)) = |A|^{-|w_i|} \leq \mu(\text{Past}(p_i)) = 1$$

(3)

holds for every state $p_i$ in $P$ by Lemma 3 and Lemma 4. Equation (2) and Equation (3) leads that the following equation

$$\mu(\text{Past}(P)) = \sum_{i=1}^{n} \mu(\text{Past}(p_i)) = \sum_{i=1}^{n} 1 = n = 1$$

holds because $A_L$ is deterministic whence all $\text{Past}(p_i)$ are mutually disjoint. We now obtain $n = 1$, that is, $P$ is the singleton $P = p_1 = p$. This ends of the proof of Theorem 2.

Remark 1. It is interesting that, though we use Borge’s theorem to prove the direction $1 \Rightarrow 2$, Theorem 2 is a vast generalization of Borge’s theorem, since any language of the form $A^* K A^*$ where $K$ is regular is always recognised by a zero automaton (but the converse is not true). To state Theorem 2 more precisely, by the proof above we can easily verify that, a regular language $L$ satisfies $\mu(L) = 1$ if and only if its minimal automaton $A_L$ is zero and the zero state of $A_L$ is a final state.
Acknowledgement. I am grateful to Prof. Sakarovitch whose comments and suggestions (and his excellent book [14]) were innumerable valuable throughout the course of my study. Special thanks also go to Prof. Minamide whose meticulous comments were an enormous help to me. This work was supported by JSPS KAKENHI Grant Number 26·11962.

References

1. Libkin, L.: Elements of Finite Model Theory. SpringerVerlag (2004)
2. Eilenberg, S., Tilson, B.: Automata, languages and machines. Volume B. Pure and applied mathematics. Academic Press, New-York, San Francisco, London (1976)
3. Reiterman, J.: The Birkhoff theorem for finite algebras. Algebra Universalis 14 (1982) 1–10
4. Pin, J.E.: Mathematical foundations of automata theory. http://www.liafa.jussieu.fr/~jep/MPRI/MPRI.html.
5. Gehrke, M., Grigorieff, S., Pin, J.E.: Duality and equational theory of regular languages. In: Proceedings of the 35th International Colloquium on Automata, Languages and Programming, Part II. ICALP ’08, Berlin, Heidelberg, Springer-Verlag (2008) 246–257
6. Simon, I.: Piecewise testable events. In: Proceedings of the 2nd GI Conference on Automata Theory and Formal Languages, London, UK, UK, Springer-Verlag (1975) 214–222
7. Diekert, V., Gastin, P., Kufleitner, M.: A survey on small fragments of first-order logic over finite words. International Journal of Foundations of Computer Science 19(3) (June 2008) 513–548
8. Schützenberger, M.: On finite monoids having only trivial subgroups. Information and Control 8(2) (1965) 190 – 194
9. Schützenberger, M.: Sur le produit de concatenation non ambigu. Semigroup Forum 13(1) (1976) 47–75
10. Rystsov, I.K.: Reset words for commutative and solvable automata. Theoretical Computer Science 172 (1997) 273–279
11. Berstel, J.: Sur la densité asymptotique de langages formels. In: International Colloquium on Automata, Languages and Programming (ICALP, 1972), France, North-Holland (1973) 345–358
12. Salomaa, A., Soittola, M.: Automata: Theoretic Aspects of Formal Power Series. Springer-Verlag New York, Inc., Secaucus, NJ, USA (1978)
13. Bodirsky, M., Grtner, T., von Oertzen, T., Schwinghammer, J.: Efficiently computing the density of regular languages. In Farach-Colton, M., ed.: LATIN 2004: Theoretical Informatics, Volume 2976 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2004) 262–270
14. Sakarovitch, J.: Elements of Automata Theory. Cambridge University Press, New York, NY, USA (2009)
15. Klíma, O.: On varieties of automata enriched with an algebraic structure (extended abstract). In: Proceedings 14th International Conference on Automata and Formal Languages, Szeged, Hungary, May 27-29, 2014. Volume 151 of Electronic Proceedings in Theoretical Computer Science., Open Publishing Association (2014) 49–54
16. Flajolet, P., Sedgewick, R.: Analytic Combinatorics. 1 edn. Cambridge University Press, New York, NY, USA (2009)
17. Lawson, M.V.: Finite Automata. Birkhuser (2005)
Appendix: proof of Lemma 1

Let \( A \) be an automaton \( A = \langle Q, A, \cdot, q_0, F \rangle \). For any subset \( P \) of \( Q \) in \( A \), the future of \( P \) is the language denoted by \( \text{Fut}(P) \) and defined by:

\[
\text{Fut}(P) = \{ w \in A^* \mid \exists p \in P, p \cdot w \in F \}.
\]

It is well known that, an (accessible) automaton \( A \) is minimal if and only if

\[
p = q \iff \text{Fut}(p) = \text{Fut}(q)
\]

holds for every pair of states \( p, q \) in \( Q \). The well known Myhill-Nerode theorem states that every regular language has only a finite number of left and right quotients (cf. [14]). Here we give the proof of Lemma 1 to make this paper self-contained. While the Lemma 1 is folklore, one of variant of a fundamental lemma in variety theory, we can not find any literature that proves Lemma 1 explicitly. The proof we gave here is essentially based on the proof of Lemma 12.1.8 in a book written by Lawson [17].

**Lemma 1.** Let \( A_L = \langle Q, A, \cdot, q_0, F \rangle \) be the minimal automaton of a regular language \( L \), then for any subset \( P \) of \( Q \), its past \( \text{Past}(P) \) can be expressed as a (finite) Boolean combination of languages of the form \( L w^{-1} \).

**Proof.** We only have to prove that, for any state \( q \) in \( Q \), its past \( \text{Past}(q) \) can be expressed as a Boolean combination of languages of the form \( L w^{-1} \). Our goal is to prove the following equation with the usual conventions \( \bigcap_{w \in \emptyset} L w^{-1} = A^* \) and \( \bigcup_{w \in \emptyset} L w^{-1} = \emptyset \):

\[
\text{Past}(q) = \left( \bigcap_{w \in \text{Fut}(q)} L w^{-1} \right) \setminus \left( \bigcup_{w \notin \text{Fut}(q)} L w^{-1} \right).
\]

(5)

The finiteness of this Boolean combination follows from Myhill-Nerode theorem.

We prove first that the left hand side is contained in the right hand side in Equation (5). Let \( v \) be a word in \( \text{Past}(q) \). If a word \( w \) in \( \text{Fut}(q) \), then \( vw \) in \( L \) by the definition, and hence \( v \) in \( L w^{-1} \). If a word \( w \) not in \( \text{Fut}(q) \), then \( vw \) not in \( L \) by the definition, and hence \( v \) not in \( L w^{-1} \). It follows that the left hand side is contained in the right hand side in Equation (5).

Then we prove that the right hand side is contained in the left hand side in Equation (5). Let \( v \) be a word in right hand side in Equation (5). Let \( p \) be the state satisfies \( q_0 \cdot v = p \), that is, \( v \) is a word in \( \text{Past}(p) \). For any \( w \) in \( \text{Fut}(q) \), by the form of Equation (5), \( v \) is in \( L w^{-1} \) from which we get \( vw \) in \( L \) whence \( p \cdot w \) in \( F \). That is, \( w \) also belongs to \( \text{Fut}(p) \). Conversely, for any \( w \) not in \( \text{Fut}(q) \), \( vw \) is not in \( L \) and thus \( v \) not in \( L w^{-1} \). That is, \( w \) not belongs to \( \text{Fut}(p) \). It follows that \( p \) and \( q \) have the same future \( \text{Fut}(p) = \text{Fut}(q) \) from which we get \( p = q \) by Condition (4) of the minimality of \( A_L \). Hence we obtain \( v \) in \( \text{Past}(q) \) and thus the right hand side is contained in the left hand side in Equation (5). \( \square \)