A Burnside Approach to the Termination of Mohri's Algorithm for Polynomially Ambiguous Min-Plus-Automata*

Daniel Kirsten
Universität Leipzig,
Institut für Informatik,
Postfach 10 09 20,
04009 Leipzig, Germany
http://www.informatik.uni-leipzig.de/~kirsten/

January 16, 2008

Abstract

We show that the termination of Mohri's algorithm is decidable for polynomially ambiguous weighted finite automata over the tropical semiring which gives a partial answer to a question by Mohri [29]. The proof relies on an improvement of the notion of the twins property and a Burnside type characterization for the finiteness of the set of states produced by Mohri's algorithm.

*An extended abstract was presented at Journées Montoises d'Informatique Théorique 2006.

Contents

1 Introduction

Weighted finite automata over the tropical semiring (for short WFA) are of great theoretical and practical interest in computer science. They play a crucial role in the structure theory of recognizable languages in free monoids and trace monoids [9, 18, 28]. However, they have also practical applications in speech recognition, image compression, and database theory [3, 6, 7, 8, 16, 17, 29]. Consequently, weighted finite automata over the tropical semiring and the more particular class of distance automata have been extensively studied by many researchers, e.g., [10, 11, 20, 21, 24, 27, 31, 34, 35, 36].

To achieve efficient implementations, one is interested in utilizing subsequential (deterministic) WFA [29]. In contrast to unweighted automata, there are WFA which do not admit a subsequential equivalent. MOHRI developed an algorithm which determinizes WFA [29][1]. which is implemented within the AT&T FSM Library™. This algorithm is not perfect, e.g., there are WFA on which MOHRI's algorithm does not terminate despite there are subsequential equivalents. Nevertheless, his algorithm is very successful on WFA which occur in speech recognition.

MOHRI raised the question whether it is decidable whether his algorithm terminates on a given WFA [1, 29]. For trim, unambiguous WFA, he gave a decidable characterization of the WFA on which his algorithm terminates [29]. This characterization is based on the so-called twins property. In general, MOHRI's question remains open.

A WFA is called *polynomially ambiguous* if the number of accepting paths (computations) for some word w is polynomially bounded in the length of w. We present a polynomially ambiguous WFA which does not admit an equivalent, finitely ambiguous one. As a main result of this paper, we show that it is decidable whether MOHRI's algorithm terminates on a given trim, polynomially ambiguous WFA.

We will consider some examples of WFA to explain the inadequacy of the notion of the twins property for WFA over the tropical semiring, and we will develop a more appropriate notion which will be called the *clones property*. The main result of the paper states that the clones property is a decidable, sufficient, and necessary condition for the termination of MOHRI's algorithm on trim, polynomially ambiguous WFA (Theorem 3.4, Corollary 3.7). To prove that the clones property is sufficient, we need involved tools as SIMON's factorization forest theorem and we develop a Burnside type characterization. This Burnside type characterization says that MOHRI's algorithm terminates on trim, polynomially ambiguous WFA iff it terminates on every sequence of the form $(vw^k)_{k\geq 1}$. We also provide an example which shows that our Burnside type characterization does not hold for arbitrary WFA.

For trim, finitely ambiguous WFA, the clones property coincides with the twins property. Hence, we can generalize a characterization by MOHRI from unambiguous to finitely ambiguous WFA (Theorem 3.6). We also show that if MOHRI's algorithm terminates on some WFA $\mathcal{A}$, then it terminates on the trim part of $\mathcal{A}$.

The paper is organized as follows. In Section 2, we explain our notation. Section 3, gives an overview. In Section 3.1, we introduce the concept of weighted finite automata over the tropical semiring and give some historical background. In Section 3.2, we give an example of a polynomially ambiguous WFA and prove that it does not admit an equivalent, finitely ambiguous WFA. In Section 3.3, we present MOHRI's algorithm. In Section 3.4, we explain and discuss the notion of the twins property. We present out main results in Section 3.5, and in Section 3.6, we try to evaluate our contribution and state some open problems. To keep Section 3 as a lucid survey, the main proofs are shifted to Section 4.

[1] There is an electronic version of [29] on MOHRI's homepage which contains several corrections

2 Notations

Let $\mathbb{N} = \{0, 1, \dots\}$. For finite sets M, we denote by $|M|$ the number of elements in M.

A *semigroup* $(S, \cdot)$ consists of a set together with a binary associative operation $\cdot$ which is often denoted by juxtaposition. Some $e \in S$ is called *idempotent* if $ee = e$. The set of all idempotents of S is denoted by $\mathsf{E}(S)$. A *monoid* $(M, \cdot, 1)$ consists of a semigroup $(M, \cdot)$ and some element $1 \in M$ which is an identity for $\cdot$.

A *semiring* $(\mathbb{K}, +, \cdot, 1, 0)$ consists of a set $\mathbb{K}$ together with two binary operations $+$, and $\cdot$ such that $+$ is commutative, $(\mathbb{K}, +, 0)$ is a monoid, $(\mathbb{K}, \cdot, 1)$ is a monoid which distributes over $(\mathbb{K}, +)$, and 0 acts as a zero for all elements.

Let $(\mathbb{K}, +, \cdot, 1, 0)$ and $(\mathbb{K}', +, \cdot, 1', 0')$ be two semirings. A mapping $\varphi : \mathbb{K} \to \mathbb{K}'$ is called a *homomorphism* if φ preserves the operations $+$ and $\cdot$ and $\varphi(1) = 1'$ and $\varphi(0) = 0'$. Homomorphisms between semigroups and between monoids are defined similarly.

We denote algebraic structures as semigroups, monoids or semirings just by their set as long as no confusion arises.

The *Boolean semiring* $(\mathbb{B}, \vee, \wedge, 1, 0)$ consists of the set $\mathbb{B} = \{1, 0\}$ whereas the operations are forced by the definition of a semiring.

Let $\mathbb{Z} := \{\dots, -1, 0, 1, \dots, \infty\}$. We extend the ordering $\leq$ and the addition of integers to $\mathbb{Z}$ by setting for every $z \in \mathbb{Z}$, $z \leq \infty$ and $z + \infty = \infty + z := \infty$. Then, $(\mathbb{Z}, \min, +, 0, \infty)$ is a semiring which is called the *tropical semiring*. In the same way, one defines a semiring $(\mathbb{Z}_{\max}, \max, +, 0, -\infty)$ whereas $\mathbb{Z}_{\max} = \{-\infty, \dots, -1, 0, 1, \dots\}$. The mapping which maps every $z \in \mathbb{Z}$ to $-z$ is an isomorphism (bijective homomorphism) between $\mathbb{Z}$ and $\mathbb{Z}_{\max}$.

The mapping $\alpha : \mathbb{Z} \to \mathbb{B}$ defined by $\alpha(\infty) = 0$ and $\alpha(z) = 1$ for $z \in \mathbb{Z} \setminus \{\infty\}$ is a homomorphism.

Let Q be a finite set and $\mathbb{K}$ be a semiring. We denote by $\mathbb{K}^{Q \times Q}$ the set of all $Q \times Q$-matrices over $\mathbb{K}$. For $A \in K^{Q \times Q}$ and $i, j \in Q$, we denote the entry in the i-the row and j-th column by $A[i, j]$. The set $\mathbb{K}^{Q \times Q}$ equipped with matrix multiplication is a monoid. We extend the homomorphism α componentwise to matrices.

Let $B, B' \in \mathbb{K}^Q$ and $A \in \mathbb{K}^{Q \times Q}$. We understand the product BA as a product of a $1 \times Q$-matrix (row matrix) and a $Q \times Q$-matrix. We understand the product AB' as a product of a $Q \times Q$-matrix and a $Q \times 1$-matrix (column matrix). In the same way, the product BAB' yields a member of $\mathbb{K}$.

We identify the members of $\mathbb{B}^Q$ with subsets of Q. For example, for $C \subseteq Q$ and $A \in \mathbb{B}^{Q \times Q}$, we can write CA, and we can regard the result of the product CA as a subset of Q but also as a member of $\mathbb{B}^Q$.

We have to explain our notations concerning matrix multiplication in the tropical semiring. Although the multiplication in the tropical semiring is denoted by $+$, the multiplication of matrices over $\mathbb{Z}$ is denoted by juxtaposition. We define a product $\oplus : \mathbb{Z} \times \mathbb{Z}^Q \to \mathbb{Z}^Q$ by setting for every $z \in \mathbb{Z}$, $B \in \mathbb{Z}^Q$, $i \in Q$, $(z \oplus B)[i] := z + B[i]$. Essentially, $\oplus$ is the multiplication of a 1×1-matrix and a $1 \times Q$-matrix. Hence, we have for every $z, z' \in \mathbb{Z}$, $B \in \mathbb{Z}^Q$, $A \in \mathbb{Z}^{Q \times Q}$, $(z \oplus B)A = z \oplus (BA)$ and $z \oplus (z' \oplus B) = (z + z') \oplus B$ which allows us to shorten notations to $z \oplus BA$ resp. $z \oplus z' \oplus B$. We do not write $\oplus$ by juxtaposition, because it yields misleading notations like $z(z'B) = (z + z')B$.

Let Σ be a finite set of symbols within the entire paper. We denote by Σ^* the free monoid over Σ, i.e., Σ^* consists of all *words* over Σ with concatenation as operation. We denote the empty word by ε. We denote by Σ^+ the free semigroup over Σ, i.e., $\Sigma^+ := \Sigma^* \setminus \varepsilon$. For every $w \in \Sigma^*$, we denote by $|w|$ the length of w. We call a word u a *factor* (resp. *prefix*) of a word w if $w \in \Sigma^* u \Sigma^*$ (resp. $w \in u\Sigma^*$).

3 Overview

3.1 Weighted Finite Automata

A *weighted finite automaton over* $\mathbb{Z}$ (for short *WFA over* $\mathbb{Z}$ *or WFA*) is a tuple $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ whereas

1. Q is a non-empty, finite set of *states*,
2. $\theta : \Sigma^* \to \mathbb{Z}^{Q \times Q}$ is a homomorphism, and
3. $\lambda, \varrho \in \mathbb{Z}^Q$, whereas we consider λ (resp. ϱ) as a $1 \times Q$-matrix (resp. $Q \times 1$-matrix).

Let $\mathcal{A}$ be a WFA over $\mathbb{Z}$. It computes a mapping $|\mathcal{A}| : \Sigma^* \to \mathbb{Z}$ by $|\mathcal{A}|(w) := \lambda\theta(w)\varrho$ for $w \in \Sigma^*$. The mappings computed by WFA are often called *recognizable formal power series*. For an overview on formal power series, the reader is referred to [2, 22, 23, 30].

In the literature, one often considers WFA over $\mathbb{Z}_{\max}$. Since, $\mathbb{Z}_{\max}$ and $\mathbb{Z}$ are isomorphic, one can easily carry over results from $\mathbb{Z}_{\max}$ to $\mathbb{Z}$ and vice versa.

We call two WFA $\mathcal{A}_1$ and $\mathcal{A}_2$ over $\mathbb{Z}$ *equivalent* iff they compute the same mapping.

We call a state $q \in Q$ *accessible* if there are words $u, v \in \Sigma^*$ such that $(\lambda\theta(u))[q] \neq \infty$ and $(\theta(v)\varrho)[q] \neq \infty$. We call $\mathcal{A}$ *trim* if every $q \in Q$ is accessible.

It is well-known that for every WFA one can construct in polynomial time an equivalent trim WFA. We need to recall this construction in Section 4.7.

Let $I := \{\, q \in Q \mid \lambda[q] \neq \infty \,\}$ and $F := \{\, q \in Q \mid \varrho[q] \neq \infty \,\}$. We call the states in I resp. F the *initial states* resp. *accepting states* of $\mathcal{A}$.

Let $p, q \in Q$ and $a \in \Sigma$. If $\theta(a)[p, q] \neq \infty$, then we call $\big(p,\, a,\, \theta(a)[p, q],\, q\big)$ a *transition* in $\mathcal{A}$. Let $m \geq 0$ and $\pi = (q_0, a_1, k_1, q_1)(q_1, a_2, k_2, q_2) \dots (q_{m-1}, a_m, k_m, q_m)$ be a sequence of transitions in $\mathcal{A}$. We call π a *path from* q_0 *to* q_m or for short a *path*. We call $a_1 \dots a_m$ the *label of* π. We call π *accepting* if $q_0 \in I$ and $q_m \in F$.

Let $p, q \in Q$ and $w \in \Sigma^*$. We denote by $p \overset{w}{\rightsquigarrow} q$ the set of all paths from p to q which are labeled by w. For $R, R' \subseteq Q$, we denote by $R \overset{w}{\rightsquigarrow} R'$ the union of $r \overset{w}{\rightsquigarrow} r'$ for every $r \in R$, $r' \in R'$.

Let $k \geq 1$. If for every $w \in \Sigma^*$, there are at most k paths in $I \overset{w}{\rightsquigarrow} F$, then we call $\mathcal{A}$ *k-ambiguous*. If $\mathcal{A}$ is 1-ambiguous, then we call $\mathcal{A}$ *unambiguous*. If $\mathcal{A}$ is k-ambiguous for some $k \geq 1$, then we call $\mathcal{A}$ *finitely ambiguous*.

The classes of mappings which are computable by k-ambiguous WFA for $k = 1, 2, \dots$ form a strict hierarchy. Obviously, this hierarchy exhausts the class of mappings which are computable by finitely ambiguous WFA. The latter class is a proper subclass of the class of all recognizable formal power series over $\mathbb{Z}$. For the strictness of these inclusions and other interesting subclasses of WFA the reader is referred to the excellent survey [20].

Let $P : \mathbb{N} \to \mathbb{N}$ be some polynomial. If for every $w \in \Sigma^*$, there are at most $P(|w|)$ paths in $I \overset{w}{\rightsquigarrow} F$, then we call $\mathcal{A}$ *polynomially ambiguous*.

Polynomially ambiguous (unweighted) automata have been studied by various authors, e.g., [14, 15, 25]. The following characterization is shown implicitly in [14, 15] (cf. Proof of Theorem 3.1 in [15] or Lemma 4.3 in [14]). Although [14, 15] deal with unweighted automata, the construction carries over to WFA over $\mathbb{Z}$ in a straightforward way.

Theorem 3.1. *Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a trim WFA over $\mathbb{Z}$. The following assertions are equivalent.*

1. *The WFA $\mathcal{A}$ is polynomially ambiguous.*

2. For every $q \in Q$ and every $w \in \Sigma^*$, there is at most one path in $q \overset{w}{\rightsquigarrow} q$.

A WFA which satisfies condition (2) in Theorem 3.1 is called *cycle-unambiguous* in [1].

It is undecidable whether two given WFA over $\mathbb{Z}$ are equivalent [21]. Using Theorem 3.1 one can deduce from [21] that the same problem is undecidable for polynomially ambiguous WFA over $\mathbb{Z}$. However, the equivalence of finitely ambiguous WFA is decidable [12].

A *subsequential WFA* is a tuple $\mathcal{A} = [Q, \delta, \sigma, q_0, k_0, \varrho]$ such that:

- Q is a finite set of states,
- $\delta : Q \times \Sigma \to Q$ and $\sigma : Q \times \Sigma \to \mathbb{Z}$,
- $q_0 \in Q$, $k_0 \in \mathbb{Z}$, and
- $\varrho : Q \to \mathbb{Z}$ is a mapping.

We extend δ and σ to words $w \in \Sigma^*$ as follows: for every $q \in Q$, we set $\delta(q, \varepsilon) := q$ and $\sigma(q, \varepsilon) := 0$. For $q \in Q$, $w \in \Sigma^*$, and $a \in \Sigma$, we set $\delta(q, wa) := \delta(\delta(q, w), a)$ and $\sigma(q, wa) := \sigma(q, w) + \sigma(\delta(q, w), a)$.

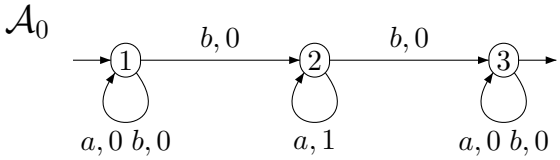
A subsequential WFA defines a mapping $|\mathcal{A}| : \Sigma^* \to \mathbb{Z}$ by $|\mathcal{A}|(w) := k_0 + \sigma(q_0, w) + \varrho(\delta(q_0, w))$. The mappings of subsequential WFA are called *subsequential formal power series*. They are a strict subclass of the mappings of unambiguous WFA [19, 20].

In the literature, one often allows in the definition of a subsequential WFA that δ and σ are partial mappings. However, this does not really extend our definition, since one can achieve totally defined mappings δ and σ by introducing a sink state.

3.2 An Example of a Polynomially Ambiguous WFA

It raises the question whether there are meaningful examples of polynomially ambiguous WFA over $\mathbb{Z}$, or whether the class of mappings which are computable by polynomially ambiguous WFA coincides with the class of mappings of some well-known class of WFA. The largest subclass of polynomially ambiguous WFA found in the literature are the finitely unambiguous WFA [12, 20, 36].

Let $\Sigma = \{a, b\}$. We consider the WFA $\mathcal{A}_0 = [Q_0, \theta_0, \lambda_0, \varrho_0]$ whereas $\lambda_0 = (0, \infty, \infty, \infty)$ and $\varrho_0 = (\infty, \infty, \infty, 0)$.



The drawings should be understood as follows. The arrow in $\mathcal{A}_0$ from state 1 to state 2 with the label $b, 0$ means $\theta_0(b)[1, 2] = 0$. The absence of some arrow $\mathcal{A}_1$ from 1 to 2 with some label a means $\theta_0(a)[1, 2] = \infty$. The incoming unlabeled arrow at state 1 means $\lambda_0[1] = 0$. Similarly, the outgoing unlabeled arrow at 3 means $\varrho_0[3] = 0$.

For every $w \in \Sigma^*$, $q \in Q_0$, every path in $q \overset{w}{\rightsquigarrow} q$ visits only the state q. Hence, there is exactly one path in $q \overset{w}{\rightsquigarrow} q$. By Theorem 3.1, $\mathcal{A}_0$ is polynomially ambiguous.

For every $w \in \Sigma^*$, $|\mathcal{A}_0|(w)$ is the least $\ell \geq 0$ such that $ba^\ell b$ is a factor of w. If w does not admit a factor of the form ba^*b, then $|\mathcal{A}_0|(w) = \infty$.

Proposition 3.2. *There is a polynomially ambiguous WFA over $\mathbb{Z}$ which does not admit an equivalent, finitely ambiguous WFA.*

Proof. It remains to show that $\mathcal{A}_0$, above, does not admit an equivalent, finitely ambiguous WFA. By contradiction, let $k \geq 1$ and $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a k-ambiguous WFA satisfying $|\mathcal{A}| = |\mathcal{A}_0|$.

To derive a contradiction by showing $|\mathcal{A}| \neq |\mathcal{A}_0|$, we introduce an equivalent way to define the semantics of $\mathcal{A}$. Let $m \geq 0$ and $\pi = (q_0, a_1, k_1, q_1)(q_1, a_2, k_2, q_2) \dots (q_{m-1}, a_m, k_m, q_m)$ be a path in $\mathcal{A}$. We define $\sigma_0(\pi) := \sum_{i=1,\dots,m} k_i$ and $\bar{\sigma}(\pi) := \lambda[q_0] + \sigma(\pi) + \varrho[q_m]$. By an induction on the length of w, we can show for every $p, q \in Q$, $w \in \Sigma^*$,

$$\theta(w)[p,q] \;=\; \min_{\pi \in p \overset{w}{\rightsquigarrow} q} \sigma(\pi) \qquad \text{and} \qquad |\mathcal{A}|(w) \;=\; \min_{\pi \in I \overset{w}{\rightsquigarrow} F} \bar{\sigma}(\pi).$$

Let $n := |Q|$ and $L := \left(ba^{n^k}a^*\right)^{k+1}b$. Let k' be the maximum of the number of accepting paths in $\mathcal{A}$ for some word in L and let $w \in L$ such that there are exactly k' accepting paths for w.

Let $\pi_1, \dots, \pi_{k'}$ the accepting paths of w. We factorize w into $w = u_0 v_1 u_1 \dots v_{k+1} u_{k+1}$ whereas $u_0, \dots, u_{k+1} \in a^*ba^*$ and $v_1, \dots, v_{k+1} \in a^+$.

We factorize $\pi_1, \dots, \pi_{k'}$ into paths which are labeled by $u_0, v_1, u_1, \dots, v_{k+1}, u_{k+1}$, respectively. For every $1 \leq m \leq k'$, there are paths $\xi_{m,0}, \dots, \xi_{m,k+1}$ and $\nu_{m,1}, \dots, \nu_{m,k+1}$ such that $\pi_m = \xi_{m,0}\nu_{m,1}\xi_{m,1} \dots \nu_{m,k+1}\xi_{m,k+1}$ and $\xi_{m,0}, \dots, \xi_{m,k+1}$ and $\nu_{m,1}, \dots, \nu_{m,k+1}$ are labelled with $u_0, \dots, u_{k+1}$ and $v_1, \dots, v_{k+1}$, respectively.

By a counting argument, we can assume that for every $1 \leq m \leq k$, $1 \leq i \leq k+1$, the path $\nu_{m,i}$ is a cycle. If there are some $1 \leq m \leq k'$, $1 \leq i \leq k+1$ such that $\sigma(\nu_{m,i}) < 0$, then we can iterate $\nu_{m,i}$ in π_m and construct an accepting path π' such that $\sigma(\bar{\pi}') < 0$ which is a contradiction.

For every $1 \leq m \leq k'$, there is some $1 \leq i \leq k+1$ such that $\sigma(\nu_{m,i}) > 0$. Just assume the contrary. By iterating the cycles $\sigma(\nu_{m,i})$ in π_m, we can construct for every $w' \in u_0 v_1^+ u_1 \dots v_{k+1}^+ u_{k+1}$ an accepting path π' such that $\bar{\sigma}(\pi') = \bar{\sigma}(\pi_m)$, i.e., $|\mathcal{A}|(w') \leq \sigma'(\pi_m)$, which is a contradiction.

Let $I \subsetneq \{1, \dots, k+1\}$ such that for every $1 \leq m \leq k'$, there is some $i \in I$ such that $\sigma(\nu_{m,i}) > 0$.

Let $1 \leq j \leq k+1$, $j \notin I$. Let ℓ such that $ba^\ell b$ is a factor of $u_{j-1}v_j u_j$.

For every $1 \leq i \leq k+1$ let $v_i' := v_i^{\ell+1}$ if $i \in I$ and let $v_i' := v_i$, otherwise. Let $w' := u_0 v_1' u_1 \dots v_{k+1}' u_{k+1}$.

Let $1 \leq m \leq k'$. By iterating for $i \in I$ the cycles $\pi_{m,i}$ in π_m $\ell + 1$ times, we obtain some accepting path π_m' which is labeled with w' and $\bar{\sigma}(\pi_m') \geq \bar{\sigma}(\pi_m) + \ell > \ell$. In this way, we can construct k' distinct accepting paths $\pi_1', \dots, \pi_{k'}'$ which are labeled with w' and $\bar{\sigma}(\pi_m') > \ell$ for $1 \leq m \leq k'$. Since, $w' \in L$ and by the choice of k', there are no other accepting paths beside $\pi_1', \dots, \pi_{k'}'$. Hence, $|\mathcal{A}|(w') > \ell$. However, since $ba^\ell b$ is a factor of w', we have $|\mathcal{A}_0|(w') \leq \ell$. This contradicts $|\mathcal{A}| = |\mathcal{A}_0|$. □

3.3 MOHRI's algorithm

In practical applications as speech processing, the implementation of subsequential WFA is more efficient than the implementation of arbitrary WFA [29]. Hence, one is interested in an algorithm which transforms a given WFA over $\mathbb{Z}$ into an equivalent subsequential WFA if an equivalent subsequential WFA exists. In [29], MOHRI presented the following algorithm. We explain his algorithm just in the tropical semiring. Let $\mathcal{A} = [Q, E, \lambda, \varrho]$ be a WFA over $\mathbb{Z}$. Let $n := |Q|$ and assume $Q = \{1, \dots, n\}$.

We want to construct an equivalent, subsequential WFA $\mathcal{A}' = [Q', \delta, \sigma, q_0, k_0, \varrho']$. The states Q' are a subset of $\mathbb{Z}^n$.

For every tuple $B \in \mathbb{Z}^n$, let $\min(B) := \min_{1 \leq i \leq n} B[i]$. For every $B \in \mathbb{Z}^n \setminus \{(\infty, \dots, \infty)\}$, let $\mathsf{nf}(B) \in \mathbb{Z}^n$ be defined by $\mathsf{nf}(B) := (-\min(B)) \oplus B$, and let $\mathsf{nf}\big((\infty, \dots, \infty)\big) = (\infty, \dots, \infty)$.

We show some basic properties of the mapping nf before we explain the algorithm.
For every $B \in \mathbb{Z}^n$, we have $B = \min(B) \oplus \mathsf{nf}(B)$.
Let $k \in \mathbb{Z}$ and $B \in \mathbb{Z}^n$. We have $\min(k \oplus B) = k + \min(B)$.
For $k \neq \infty$ and $B \in \mathbb{Z}^n$, can easily show

$$\mathsf{nf}(k \oplus B) = \mathsf{nf}(B). \tag{3.1}$$

Indeed, if $B \neq (\infty, \ldots, \infty)$, then $\mathsf{nf}(k \oplus B) = (-\min(k \oplus B)) \oplus (k \oplus B) = \big(-k - \min(B)\big) \oplus (k \oplus B) = (-\min(B)) \oplus B = \mathsf{nf}(B)$. If $B = (\infty, \ldots, \infty)$, then $B = k \oplus B$, and hence, $\mathsf{nf}(B) = \mathsf{nf}(k \oplus B)$.

Let $B \in \mathbb{Z}^n$ and $A \in \mathbb{Z}^{n \times n}$. If $B \neq (\infty, \ldots, \infty)$, then $\mathsf{nf}\big(\mathsf{nf}(B)A\big) = \mathsf{nf}\big((-\min(B)) \oplus B\, A\big) = \mathsf{nf}(BA)$. If $B = (\infty, \ldots, \infty)$, then $\mathsf{nf}(B) = B$, and hence, $\mathsf{nf}\big(\mathsf{nf}(B)A\big) = \mathsf{nf}(BA)$. Consequently, we have for every $B \in \mathbb{Z}^n$, $A \in \mathbb{Z}^{n \times n}$,

$$\mathsf{nf}\big(\mathsf{nf}(B)A\big) = \mathsf{nf}(BA). \tag{3.2}$$

We construct $\mathcal{A}'$. For every $B \in \mathbb{Z}^n$ and every $a \in \Sigma$, we define

- $\delta(B, a) := \mathsf{nf}\big(B\theta(a)\big)$ and
- $\sigma(B, a) := \min\big(B\theta(a)\big)$.

We show that for every $B \in \mathbb{Z}^n$, $w \in \Sigma^+$, we have

$$\delta(B, w) \;=\; \mathsf{nf}(B\theta(w)). \tag{3.3}$$

For $w \in \Sigma$, (3.3) is the definition of δ. Let $w \in \Sigma^+$, $a \in \Sigma$ and assume by induction that (3.3) is true for w (for every $B \in \mathbb{Z}^n$). We obtain $\delta(B, wa) \;=\; \delta\big(\delta(B, w), a\big) \;=$

$$= \mathsf{nf}\big(\delta(B, w)\theta(a)\big) \;=\; \mathsf{nf}\big(\mathsf{nf}(B\theta(w))\theta(a)\big) \overset{(3.2)}{=} \mathsf{nf}\big(B\theta(w)\theta(a)\big) \;=\; \mathsf{nf}(B\theta(wa)).$$

For every $B \in \mathbb{Z}^n$, $a \in \Sigma$, we have $\sigma(B, a) \oplus \delta(B, a) \;=\; B\theta(a)$. We generalize this equation by an induction to words, i.e., we show for every $w \in \Sigma^*$ and $B \in \mathbb{Z}^n$

$$\sigma(B, w) \oplus \delta(B, w) \;=\; B\theta(w). \tag{3.4}$$

We have $\sigma(B, \varepsilon) \oplus \delta(B, \varepsilon) \;=\; 0 \oplus B \;=\; B\theta(\varepsilon)$. For $w \in \Sigma^*$, $a \in \Sigma$, and $B \in \mathbb{Z}^n$, we get

$$\sigma(B, wa) \oplus \delta(B, wa) \;=\; \Big(\sigma(B, w) + \sigma\big(\delta(B, w), a\big)\Big) \oplus \delta\big(\delta(B, w), a\big) \;=$$

$$= \sigma(B, w) \oplus \Big(\sigma\big(\delta(B, w), a\big) \oplus \delta\big(\delta(B, w), a\big)\Big) \;=\; \sigma(B, w) \oplus \big(\delta(B, w)\theta(a)\big) \;=$$

$$= \big(\sigma(B, w) \oplus \delta(B, w)\big)\theta(a) \;=\; \big(B\theta(w)\big)\theta(a) \;=\; B\theta(wa).$$

We set $k_0 := \min(\lambda)$, $q_0 := \mathsf{nf}(\lambda)$, and $\varrho'(B) = B\varrho$ for $B \in \mathbb{Z}^n$. As a conclusion from (3.4), we get for every $w \in \Sigma^*$

$$k_0 + \sigma(q_0, w) + \varrho'\big(\delta(q_0, w)\big) \;=\; k_0 + \sigma(q_0, w) + \delta(q_0, w)\varrho \;=\; k_0 + \big(\sigma(q_0, w) \oplus \delta(q_0, w)\big)\varrho \;=$$

$$= k_0 + q_0\theta(w)\varrho \;=\; \min(\lambda) + \mathsf{nf}(\lambda)\theta(w)\varrho \;=\; \big(\min(\lambda) \oplus \mathsf{nf}(\lambda)\big)\theta(w)\varrho \;=\; \lambda\theta(w)\varrho \;=\; |\mathcal{A}|(w). \tag{3.5}$$

Let $Q' := \big\{\delta(q_0, w) \;\big|\; w \in \Sigma^*\big\}$. Clearly, Q' is the least subset of $\mathbb{Z}^n$ which contains q_0 and is closed under δ, i.e., for every $B \in Q'$ and every $a \in \Sigma$, we have $\delta(B, a) \in Q'$.

The set Q' is not necessarily finite, even if there is some subsequential WFA which is equivalent to T. If Q' is finite, then we define $\mathcal{A}' = \big[Q', \delta|_{Q'\times\Sigma}, \sigma|_{Q'\times\Sigma}, q_0, k_0, \varrho'|_{Q'}\big]$.

By equation (3.5), $\mathcal{A}$ and $\mathcal{A}'$ are equivalent. In [29], MOHRI gives an algorithm which computes the WFA $\mathcal{A}'$. This algorithm terminates iff Q' is finite.

We say that MOHRI's *algorithm terminates on* $\mathcal{A}$ if the Q' is finite.

Let $(w_k)_{k\geq 1}$ be some sequence of words in Σ^*. We say that MOHRI's *algorithm terminates on* $(w_k)_{k\geq 1}$ *on* $\mathcal{A}$ if the set $\big\{\delta(q_0, w_k) \,\big|\, k \geq 1\big\}$ is finite.

3.4 On the Twins Property

The twins property was introduced by CHOFFRUT in 1977 [5] in the framework of string-to-string transducers. In 1997 [29, 1], MOHRI generalized the twins property to WFA over the tropical semiring as follows.

Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a WFA over $\mathbb{Z}$. Two states $q, q' \in Q$ are called *siblings* if there exists some $u \in \Sigma^*$ such that $\lambda\theta(u)[q] \neq \infty$ and $\lambda\theta(u)[q'] \neq \infty$. Two siblings $q, q' \in Q$ are called *twins* if they satisfy the following condition (TW):

TW. For every $v \in \Sigma^*$ satisfying $\theta(v)[q, q] \neq \infty$ and $\theta(v)[q', q'] \neq \infty$, we have

$$\theta(v)[q, q] = \theta(v)[q', q'].$$

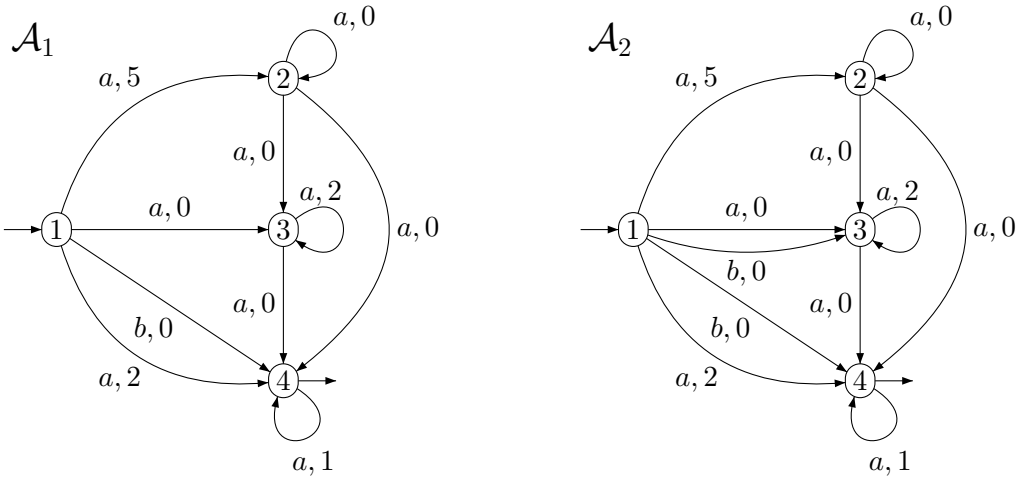
The WFA $\mathcal{A}$ has the *twins property* iff every siblings are twins.

In [29], it is shown that the twins property is a sufficient condition for the termination of MOHRI's algorithm. Moreover, we have the following theorem:

Theorem 3.3 ([29, Theorem 12])**.** *Let $\mathcal{A}$ be a trim, unambiguous WFA over the tropical semiring.* MOHRI*'s algorithm terminates on $\mathcal{A}$ iff $\mathcal{A}$ satisfies the twins property.*

The main weakness of the concept of the twins property is that the twins property is not necessary for the termination of MOHRI's algorithm.

Example 3.1. Let $\Sigma = \{a, b\}$. We consider the WFA $\mathcal{A}_1 = [Q, \theta_1, \lambda, \varrho]$ (left) and $\mathcal{A}_2 = [Q, \theta_2, \lambda, \varrho]$ (right) whereas $\lambda = (0, \infty, \infty, \infty)$ and $\varrho = (\infty, \infty, \infty, 0)$.



Note that $\mathcal{A}_2$ was constructed by inserting a transition $(1, b, 3)$ into $\mathcal{A}_1$.

Let $w \in \Sigma^*$ and $q \in Q$. Every path in $q \overset{w}{\rightsquigarrow} q$ does only visit the state q. Hence, there is at most one path in $q \overset{w}{\rightsquigarrow} q$. By Theorem 3.1, both $\mathcal{A}_1$ and $\mathcal{A}_2$ are polynomially ambiguous.

We apply MOHRI's algorithm to $\mathcal{A}_1$. We get $q_0 = \mathsf{nf}(\lambda) = \lambda$. We examine the set $Q_1' = \{\delta_1(q_0, w) \,|\, w \in \Sigma^*\}$. It is easy to see that for every word $w \in \Sigma^+ b\Sigma^*$, we have $\lambda\theta_1(w) = (\infty, \infty, \infty, \infty)$, and hence, $\delta_1(q_0, w) = (\infty, \infty, \infty, \infty)$. Let $k \in \mathbb{N}$ and $w = ba^k$. We obtain $\lambda\theta_1(w) = (\infty, \infty, \infty, k)$, and by equation (3.3), $\delta_1(q_0, w) = (\infty, \infty, \infty, 0)$. Finally, we calculate $\delta_1(q_0, a^k)$ for $k = 1, 2, \ldots$ We obtain $\delta_1(q_0, a) = (\infty, 5, 0, 2)$, i.e., $(\infty, 5, 0, 2)$ belongs to Q_1'. By continuing for $k = 2, 3, \ldots$, we figure out that $(\infty, 5, 2, 0)$, $(\infty, 4, 4, 0)$, $(\infty, 3, 3, 0)$, $(\infty, 2, 2, 0)$, $(\infty, 1, 1, 0)$, $(\infty, 0, 0, 0)$ belong to Q_1'. For $k \geq 7$, we obtain $\delta_1\big(q_0, a^k\big) = (\infty, 0, 0, 0)$. To sum up, Q_1' consists of 10 states, i.e, MOHRI's algorithm terminates on $\mathcal{A}_1$.

Now, we apply MOHRI's algorithm to $\mathcal{A}_2$. For every $k \geq 0$, we get $\lambda\theta_2(ba^k) = (\infty, \infty, 2k, k)$, and thus, $\delta_2(q_0, ba^k) = (\infty, \infty, k, 0)$. Thus, Q_2' is infinite, i.e., MOHRI's algorithm does not terminate on $\mathcal{A}_2$.

Both $\mathcal{A}_1$ and $\mathcal{A}_2$ have the same siblings: $(1, 1)$ and $\{2, 3, 4\} \times \{2, 3, 4\}$. Both $\mathcal{A}_1$ and $\mathcal{A}_2$ do not satisfy the twins property, e.g., we have $\theta_i(a)[2, 2] = 0 \neq 2 = \theta_i(a)[3, 3]$ for $i \in \{1, 2\}$.

The key question is how to define a variant of the twins property which allows to distinguish between $\mathcal{A}_1$ and $\mathcal{A}_2$. Let us try an approach which relies on some comparison of siblings, i.e., we try to establish some condition (TW') which is similar to the above condition (TW), and we define that some WFA satisfies the (TW')-twins property if every siblings satisfy (TW').

Now, consider the siblings $(2, 3)$ in $\mathcal{A}_1$ and $\mathcal{A}_2$. For every $p \in Q$ and every $w \in \Sigma^*$, we have $\theta_1(w)[2, p] = \theta_2(w)[2, p]$ and $\theta_1(w)[3, p] = \theta_2(w)[3, p]$. Consequently, if (TW') is somehow defined by a comparison of siblings, then $(2, 3)$ satisfies (TW') in $\mathcal{A}_1$ iff $(2, 3)$ satisfies (TW') in $\mathcal{A}_2$. Henceforth, (TW') cannot distinguish between $(2, 3)$ in $\mathcal{A}_1$ and $(2, 3)$ in $\mathcal{A}_2$.

Unfortunately, the same effect happens for every pair of siblings in $\{2, 3, 4\} \times \{2, 3, 4\}$. There is still one more pair of siblings: $(1, 1)$. If (TW') is somehow defined by a comparison of siblings, then (TW') should be satisfied for sibling pairs of the form (q, q) since it means to compare a state to itself.

As a conclusion, it seems to be impossible to define (TW') in way that $\mathcal{A}_1$ satisfies the (TW')-twins property but $\mathcal{A}_2$ does not. □

3.5 Main Results

Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a WFA over $\mathbb{Z}$. Set $n := |Q|$ and assume $Q = \{1, \ldots, n\}$.

We call some set $C \subseteq Q$ a *clone* if there is some word $w \in \Sigma^*$ such that

$$C = \big\{q \in Q \,\big|\, \lambda\theta(w)[q] \neq \infty\big\}.$$

We denote the set of all clones of $\mathcal{A}$ by $\mathsf{Clones}(\mathcal{A}) \subseteq 2^Q$.

Let $p, q \in Q$. Clearly, p and q are siblings iff there exists some $C \in \mathsf{Clones}(\mathcal{A})$ such that $p, q \in C$.

Let $C \subseteq Q$ and $A \in \mathbb{Z}^{n \times n}$, and assume $\alpha(A) \in \mathsf{E}(\mathbb{B}^{n \times n})$. We say that C is *stable* on A if $C\alpha(A) = C$. Assume that C is stable on A. Let $q \in C$. We say that q *has a minimal cycle in* C *and* A if $A[q, q] = \min\big\{A[p, p] \,\big|\, p \in C\big\}$. We say that C and A have the *clones property* if for every $p \in C$ satisfying $A[p, p] \neq \infty$, there is some $q \in C$ such that q has a minimal cycle in C and $A[q, p] \neq \infty$.

If $C = \emptyset$, then C and A satisfy the clones property by definition.

We say that $\mathcal{A}$ has the *clones property* if for every $C \in \mathsf{Clones}(\mathcal{A})$ and every $w \in \Sigma^*$, C and $\theta(w)$ have the clones property, provided that $\alpha(\theta(w)) \in \mathsf{E}(\mathbb{B}^{n \times n})$ and $\theta(w)$ is stable on C.

Our main result is the following equivalence:

Theorem 3.4. *Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a trim, polynomially ambiguous WFA over $\mathbb{Z}$. The following assertions are equivalent:*

1. MOHRI*'s algorithm terminates on $\mathcal{A}$.*
2. *For every $v, w \in \Sigma^*$,* MOHRI*'s algorithm terminates on the sequence $(vw^k)_{k\geq 1}$ on $\mathcal{A}$.*
3. *The WFA $\mathcal{A}$ satisfies the clones property.*

Note that (1) $\Rightarrow$ (2) in Theorem 3.4 is obvious.

To show (2) $\Rightarrow$ (3), we assume that (3) is false. There are $C \in \mathsf{Clones}(\mathcal{A})$ and $w \in \Sigma^*$ such that C and $\theta(w)$ do not satisfy the clones property. Let $v \in \Sigma^*$ such that $C = \{q \in Q \mid \lambda\theta(v)[q] \neq \infty\}$. We can then show that MOHRI's algorithm does not terminate on the sequence $(vw^k)_{k\geq 1}$ which disproves (2) in Theorem 3.4 (Section 4.3).

The proof of (3) $\Rightarrow$ (1) in Theorem 3.4 leads us to a Burnside type problem which requires ambitious algebraic tools as SIMON's factorization forest theorem (Section 4.4 and 4.5).

Example 3.1 (continued). We continue the examination of $\mathcal{A}_1$ and $\mathcal{A}_2$ from Section 3.4. We have $\mathsf{Clones}(\mathcal{A}_1) = \{\emptyset, \{1\}, \{4\}, \{2,3,4\}\}$ and $\mathsf{Clones}(\mathcal{A}_2) = \{\emptyset, \{1\}, \{3,4\}, \{2,3,4\}\}$. Thus, $\mathcal{A}_1$ and $\mathcal{A}_2$ have different sets of clones, although they have the same siblings.

In Section 3.4, we have seen that MOHRI's algorithm does not terminate on the sequence $(ba^k)_{k\geq 1}$ on $\mathcal{A}_2$. We utilize this sequence to show that $\mathcal{A}_2$ does not satisfy the clones property. We consider the clone $C := \{q \in Q \mid \lambda\theta_2(b)[q] \neq \infty\} = \{3,4\}$ and $\theta_2(a)$. It is easy to see that $\alpha(\theta_2(a)) \in \mathsf{E}(\mathbb{B}^{4\times 4})$. If $\mathcal{A}_2$ reads a starting in some state in C, then it can change the state to 3 or 4. Hence, C is stable on $\theta_2(a)$.

Since, $\theta_2(a)[3,3] = 2$ and $\theta_2(a)[4,4] = 1$, the state 4 has a minimal cycle in C and $\theta_2(a)$. The state 3 has not a minimal cycle in C and $\theta_2(a)$. We have $\theta_2(a)[4,3] = \infty$. Consequently, C and $\theta_2(a)$ do not have the clones property, and hence, $\mathcal{A}_2$ does not satisfy the clones property.

In Section 3.4, we have seen that MOHRI's algorithm terminates on $\mathcal{A}_1$. By Theorem 3.4, $\mathcal{A}_1$ satisfies the clones property. □

We show some connections between the clones property and the twins property.

Theorem 3.5. *Let $\mathcal{A}$ be a WFA over $\mathbb{Z}$. If $\mathcal{A}$ has the twins property, then $\mathcal{A}$ has the clones property.*

Proof. Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$. Let $C \in \mathsf{Clones}(\mathcal{A})$ and $w \in \Sigma^*$ such that $\alpha(\theta(w)) \in \mathsf{E}(\mathbb{B}^{n\times n})$ and $\alpha(\theta(w))$ is stable on C. We show that C and $\theta(w)$ have the clones property. If $C = \emptyset$, then we are done. Assume $C \neq \emptyset$. Let $C' := \{q \in C \mid \theta(w)[q,q] \neq \infty\}$. Since, $\mathcal{A}$ has the twins property, we have $\theta(w)[p,p] = \theta(w)[q,q]$ for every $p, q \in C'$. Hence, every $q \in C'$ has a minimal cycle in C and $\theta(w)$. Let $p \in C'$ be arbitrary. We have to show some $q \in C'$ such that q has a minimal cycle in C and $\theta(w)$ and $\theta(w)[q,p] \neq \infty$. We can set $q := p$. □

For finitely ambiguous WFA, we have a stronger property.

Theorem 3.6. *Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a trim, finitely ambiguous WFA over $\mathbb{Z}$. The following assertions are equivalent:*

1. *The WFA $\mathcal{A}$ satisfies the clones property.*
2. *The WFA $\mathcal{A}$ satisfies the twins property.*

3. MOHRI*'s algorithm terminates on* $\mathcal{A}$*.*

Note that (1) $\Leftrightarrow$ (3) follows from directly from Theorem 3.4 and (2) $\Rightarrow$ (1) follows from Theorem 3.5. Moreover, (2) $\Rightarrow$ (3) follows from a result by MOHRI in [29] as seen in Section 3.4.

From Theorem 3.4, we get the following result:

Corollary 3.7. *There is an algorithm which decides whether* MOHRI*'s algorithm terminates on a given trim, polynomially ambiguous WFA over* $\mathbb{Z}$*.*

Proof. The algorithm consists of two simultaneous processes. The first process generates Q'. It terminates iff Q' is finite.

The second process generates the set $\mathsf{Clones}(\mathcal{A})$ and checks for every word $w \in \Sigma^*$ whether $\alpha(\theta(w) \in \mathsf{E}(\mathbb{B}^{n\times n})$ and whether C is stable on $\alpha(\theta(w))$. If so, it checks whether C and $\theta(w)$ satisfy the clones property. It terminates iff C and $\theta(w)$ do not satisfy the clones property. Hence, the second process terminates iff $\mathcal{A}$ does not satisfy the clones property.

By Theorem 3.4(1)$\Leftrightarrow$(3), exactly one of the processes terminates, and MOHRI's algorithm terminates on $\mathcal{A}$ iff the first process terminates. □

Our main results are restricted to trim, polynomially ambiguous WFA over $\mathbb{Z}$. It raises the question whether one generalize our results to other WFA over $\mathbb{Z}$. We prove the following result in Section 4.7.

Theorem 3.8. *Let* $\mathcal{A} = [Q, \theta, \lambda, \varrho]$*. If* MOHRI*'s algorithm terminates on* $\mathcal{A}$*, then* MOHRI*'s algorithm terminates on the trim part of* $\mathcal{A}$*.*

If we are interested in applying MOHRI's algorithm to some WFA $\mathcal{A}$, then we rather apply MOHRI's algorithm to the trim part of $\mathcal{A}$. We can construct the trim part of $\mathcal{A}$ in polynomial time. The trim part has less or as many states as $\mathcal{A}$. If $\mathcal{A}$ is polynomially ambiguous, then so is the trim part of $\mathcal{A}$. Moreover, if MOHRI's algorithm terminates on $\mathcal{A}$, then it terminates on the trim part of $\mathcal{A}$. Henceforth, the restriction to trim WFA is not really a restriction.

3.6 Conclusions and Open Questions

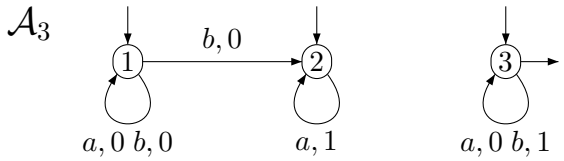
We can decide whether MOHRI's algorithm terminates on a given polynomially ambiguous WFA. It is quite interesting to have a decidability result for a class of WFA for which the equivalence problem is undecidable [21].

In the tropical semiring, the twins property was a suitable concept just for unambiguous WFA. By introducing the clones property, we came over the disadvantages of the twins property for the class of polynomially ambiguous WFA. Remarkably, the twins and the clones property coincide for finitely ambiguous WFA.

The equivalence (2) $\Leftrightarrow$ (3) in Theorem 3.6 generalizes Theorem 3.3 by MOHRI from unambiguous WFA to finitely unambiguous WFA.

It raises the question whether one can generalize Theorem 3.4 and Corollary 3.7 to trim WFA which are not necessarily polynomially ambiguous. Let us consider an example.

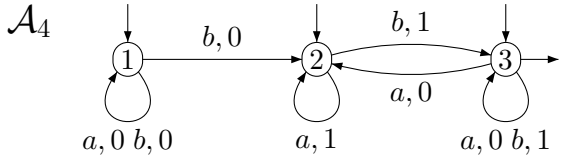
Example 3.2. Let $\Sigma = \{a, b\}$. We examine the WFA $\mathcal{A}_3$ shown below whereas $\lambda_3 = (0, 0, 0)$ and $\varrho_3 = (\infty, \infty, 0)$.



For every $w \in \Sigma^*$, we have $\lambda_3\theta_3(w)[1] = 0$. We can imagine $\mathcal{A}_3$ as a machine which reads words and manipulates two counters which correspond to the states 2 and 3. We do not imagine state 1 as a counter, since such a counter is just a constant zero.

The counter 3 counts the number of b's in the input word. When $\mathcal{A}_3$ reads the letter a, it increments the counter 2, but when it reads b, it sets counter 2 to zero. Thus, counter 2 counts the number of trailing a's in the input word. More precisely, we have for every $k \geq 0$, $w \in \Sigma^*$, $\lambda_3\theta_3(wba^k)[2] = k$.

We modify $\mathcal{A}_3$ by inserting two transitions between the states 2 and 3 and obtain an WFA $\mathcal{A}_4$ shown below whereas $\lambda_4 = \lambda_3$ and $\varrho_4 = \varrho_3$.



For every $w \in \Sigma^*$, we have $\lambda_4\theta_4(w)[1] = 0$, $\lambda_4\theta_4(w)[2] \geq 0$, and $\lambda_4\theta_4(w)[3] \geq 0$. Hence, we have $\min(\lambda_4\theta_4(w)) = 0$ and $\mathsf{nf}(\lambda_4\theta_4(w)) = \lambda_4\theta_4(w)$.

The WFA $\mathcal{A}_4$ is not polynomially ambiguous, because there are two different cycles at the state 3 which are labeled with ab.

When $\mathcal{A}_4$ reads the letter b, it increments the counter 3 and sets counter 2 to zero. However, when reading b, $\mathcal{A}_4$ increments counter 3 at most to the value of counter 2 plus 1.

When $\mathcal{A}_4$ reads the letter a, it does not change the counter 3. It increments the counter 2, if counter 2 is less than counter 3.

We verify condition (2) in Theorem 3.4 for $\mathcal{A}_4$. Let $v, w \in \Sigma^*$.

Assume $w \in a^*$. It is easy to see that for every $k \geq 1$, we have $\lambda_4\theta_4(v)[3] = \lambda_4\theta_4(vw^k)[3]$. Moreover, we have $0 \leq \lambda_4\theta_4(vw^k)[2] \leq \lambda_4\theta_4(vw^k)[3] = \lambda_4\theta_4(v)$. Consequently, the set $\{\lambda_4\theta_4(vw^k) \mid k \geq 1\}$ is finite, i.e., Mohri's algorithm terminates on the sequence $\lambda_4\theta_4(vw^k)$.

Now, assume $w \notin a^*$. Let $m \geq 0$ such that for every $k \geq 1$, the word a^{m+1} is not a factor of vw^k. Let $k \geq 1$ and u be a prefix of vw^k. If $u \in a^*$, then $u = a^\ell$ for some $\ell \leq m$, and hence, $\lambda_4\theta_4(u)[2] = \ell \leq m$. If $u \notin a^*$, then there are $u' \in \Sigma^*$, $\ell \leq m$ such that $u = u'ba^\ell$. We have $\lambda_4\theta_4(u'b)[2] = 0$ and $\theta_4(a^\ell) = \ell \leq m$, and hence, $\lambda_4\theta_4(u)[2] \leq m$.

There are some $u \in \Sigma^*$ and $\ell \leq m$ such that $vw^k = uba^\ell$. We have

$$\lambda_4\theta_4(uba^\ell)[3] \;\leq\; \lambda_4\theta_4(u)[2] + \theta_4(b)[2,3] + \theta_4(a^\ell)[3,3] \;\leq\; m + 1 + 0.$$

Thus, we have for every $k \geq 1$, $\lambda_4\theta_4(vw^k) \in \{0\} \times \{0, \ldots, m\} \times \{0, \ldots, m+1\}$. Consequently, Mohri's algorithm terminates on the sequence $(vw^k)_{k\geq 1}$, i.e., $\mathcal{A}_4$ satisfies (2) in Theorem 3.4.

Now, we consider the sequence defined by $w_1 := ba$ and $w_{k+1} := w_k ba^{k+1}$ for $k \geq 1$. We have $\lambda_4\theta_4(w_1) = (0, 1, 1)$. By an induction on k, one can easily show $\lambda_4\theta_4(w_k b) = (0, 0, k+1)$ and $\lambda_4\theta_4(w_{k+1}) = (0, k+1, k+1)$. Thus, we have $\lambda_4\theta_4(w_\ell) \neq \lambda_4\theta_4(w_k)$ for every $1 < \ell < k$. Consequently, Mohri's algorithm does not terminate on $\mathcal{A}_4$. □

By $\mathcal{A}_4$ in Example 3.2, (2) $\Rightarrow$ (1) in Theorem 3.4 is not true for arbitrary WFA over $\mathbb{Z}$.[2]

It is an interesting open question whether one can achieve a characterization similar to Theorem 3.4 for arbitrary WFA over $\mathbb{Z}$, maybe by utilizing HASHIGUCHI's k-expressions which provide a nested pumping technique and turned out to be very useful in the theory of WFA [10, 18, 26, 34].

Another open problem is to develop a practical algorithm to decide whether a given, polynomially ambiguous WFA satisfies the clones property.

4 The Main Proofs

4.1 On Boolean Matrices

Let $n \geq 1$ for this section. Let $e \in \mathsf{E}(\mathbb{B}_{n\times n})$. We associate a binary relation $\leq_e$ on $\{1,\ldots,n\}$ to e by setting $i \leq_e j$ iff $e[i,j] = 1$.

Lemma 4.1. *Let $e \in \mathsf{E}(\mathbb{B}_{n\times n})$.*

1. *The relation $\leq_e$ is transitive.*
2. *For every $1 \leq i,j \leq n$ satisfying $i \leq_e j$, there is some $1 \leq k \leq n$ such that $i \leq_e k$, $k \leq_e k$, and $k \leq_e j$.*

Proof. (1) Let $1 \leq i,j,k \leq n$ such that $i \leq_e j$ and $j \leq_e k$, i.e., $e[i,j] = 1 = e[j,k]$. Consequently, $1 = e^2[i,k] = e[i,k]$. Hence, $i \leq_e k$.

(2) Let $1 \leq i,j \leq n$ satisfying $i \leq_e j$, i.e., $e[i,j] = 1$. Since, $\mathbb{B}$ is an idempotent semiring and $e = e^{n+2}$, there are $i = i_0,\ldots,i_{n+1} = j$ such that $1 = e^{n+2}[i,j] = e[i_0,i_1] \wedge \cdots \wedge e[i_{n+1},i_{n+2}]$. By a counting argument, there are $1 \leq p < q \leq n$ such that $i_p = i_q$. We set $k = i_p$. Since, $1 = e[i_0,i_1] \wedge \cdots \wedge e[i_{p-1},i_p]$, we obtain $1 = e^p[i_0,i_p] = e[i,k]$, i.e., $i \leq_e k$, and similarly, $k \leq_e k$, and $k \leq_e j$. □

Let S be a subsemigroup of $\mathbb{B}^{n\times n}$ for the rest of this section. We call S *polynomially ambiguous* (resp. *finitely ambiguous*) if there is some polynomial $P : \mathbb{N} \to \mathbb{N}$ (resp. constant $P \in \mathbb{N}$) such that for every $k \geq 1$, $p_1,\ldots,p_k \in S$, and every $1 \leq i,j \leq n$, there are at most $P(k)$ (resp. P) tuples $(i_0,\ldots,i_k) \in \{1,\ldots,n\}^{k+1}$ which satisfy the conditions $i_0 = i$, $i_k = j$, and

$$p_1[i_0,i_1] \wedge \cdots \wedge p_k[i_{k-1},i_k] = 1.$$

Let $p \in S$ and $1 \leq i,j \leq n$ satisfying $p[i,j] = 1$. We call (i,j) *unambiguous in p* if for every $r,s \in S$ satisfying $p = rs$, there is exactly one $1 \leq k \leq n$ such that $r[i,k] \wedge s[k,j] = 1$.

Assume that (i,j) is unambiguous in p. Let $k \geq 1$, $p_1,\ldots,p_k \in S$ satisfying $p = p_1 \cdots p_k$. There are unique $i = i_0,\ldots,i_k = j$ such that $p_1[i_0,i_1] \wedge \cdots \wedge p_k[i_{k-1},i_k] = 1$ and for every $1 \leq \ell \leq k$, the pair $(i_{\ell-1},i_\ell)$ is unambiguous in p_ℓ.

Lemma 4.2. *Let $S \subseteq \mathbb{B}^{n\times n}$ be a subsemigroup. The following conditions are equivalent.*

1. *For every $p \in S$ and every i,j satisfying $p[i,i] = p[i,j] = p[j,i] = p[j,j] = 1$, we have $i = j$.*
2. *For every $p \in S$ and every i satisfying $p[i,i] = 1$, the pair (i,i) is unambiguous in p.*

[2] In the published version of the paper, it will be shown that $\mathcal{A}_4$ satisfies the clones property, and hence, (3) $\Rightarrow$ (1) in Theorem 3.4 is not true for arbitrary WFA over $\mathbb{Z}$.

Moreover, if S is polynomially ambiguous, then both conditions are satisfied.

Proof. (2)⇒(1) We have $p^2[i,i] = 1$. By (2) on p^2 and (i,i), there is a unique k such that $p[i,k] = p[k,i] = 1$. Thus, we have $i = k$ but also $j = k$.

(1)⇒(2) Let $p \in S$ and i satisfying $p[i,i] = 1$. Let $r, s \in S$ such that $p = rs$. Let k, ℓ such that $r[i,k] = s[k,i] = 1$ and $r[i,\ell] = s[\ell,i] = 1$. We have to show $k = \ell$. Since $s[\ell,i] = r[i,k] = 1$, we have $sr[\ell,k] = 1$, and similarly, $sr[k,k] = sr[k,\ell] = sr[\ell,\ell] = 1$. By applying (1) for sr and k, ℓ, we observe $k = \ell$.

Finally, assume that S is a polynomially ambiguous subsemigroup of $\mathbb{B}^{n\times n}$. We show (1). Let p and i, j as in (1). Let $k \geq 1$ and consider the product p^k. According to the definition of a polynomially ambiguous subsemigroup, the number of tuples in $\{i\} \times \{i,j\}^{k-1} \times \{j\}$ is bounded polynomially in k. Hence, $\{i,j\}$ is a singleton set, i.e., $i = j$. □

Let us mention that it was shown implicitly in [15, 13, 14] in an automata theoretic framework that every subsemigroup of $\mathbb{B}^{n\times n}$ which satisfies condition (2) in Lemma 4.2 is polynomially ambiguous (cf. Proof of Theorem 3.1 in [15] or Lemma 4.3 in [14]).

Assume that S is polynomially ambiguous and let $e \in \mathsf{E}(T)$. By Lemma 4.2(1), $\leq_e$ is antisymmetric. However, $\leq_e$ is not necessarily reflexive or irreflexive.

Lemma 4.3. *Let S be a polynomially ambiguous subsemigroup of $\mathbb{B}^{n\times n}$. Let $C \subseteq \{1,\ldots,n\}$ and let $e \in \mathsf{E}(S)$, and assume that e is stable on C. For every $i \in C$ which is minimal for $\leq_e$ in C, we have $e[i,i] = 1$.*

Proof. Let $i \in C$ be minimal. Since, e is stable on C, we have $(Ce)[i] = 1$, and hence, there is some $j \in C$ such that $e[j,i] = 1$. It follows $j \leq_e i$, and since i is minimal, we have $j = i$. Consequently, we have $e[i,i] = 1$. □

An important consequence from Lemma 4.3 is that for every $i \in C$, there exists some $j \in C$ such that $j \leq_e i$. Just assume that such a j does not exist. Then, i is minimal for $\leq_e$, and by Lemma 4.3, we have $j \leq_e i$ for $j := i$.

Lemma 4.4. *Let $S \subseteq \mathbb{B}^{n\times n}$ be a finitely ambiguous subsemigroup. For every $p \in S$ and every i, j satisfying $p[i,i] = p[i,j] = p[j,j] = 1$, we have $i = j$.*

Proof. By contradiction, let $p \in S$ and $i \neq j$ such that $p[i,i] = p[i,j] = p[j,j] = 1$. Let $k \geq 1$. We apply the definition of a finitely ambiguous semigroup to the entry (i,j) in the k-th power of p. For every $1 \leq \ell \leq k$, consider the tuple $\{i\}^\ell \times \{j\}^{k+1-\ell}$. Hence, there are at least k tuples, i.e., the number of tuples is not bounded by a constant. □

Lemma 4.5. *Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a trim WFA over $\mathbb{Z}$. The following assertions are equivalent.*

1. *The WFA $\mathcal{A}$ is polynomially (resp. finitely) ambiguous.*
2. *The subsemigroup $\alpha(\theta(\Sigma^*)) \subseteq \mathbb{B}^{Q\times Q}$ is polynomially (resp. finitely) ambiguous.*

Proof. Let $n := |Q|$ and assume $Q = \{1,\ldots,n\}$.

At first, we show the equivalence for the case of polynomial ambiguity.

(2) ⇒ (1) Let $P : \mathbb{N} \to \mathbb{N}$ be the polynomial from the definition of a polynomially ambiguous subsemigroup for $\alpha(\theta(\Sigma^*))$. Let I (resp. F) be the initial (resp. accepting) states of $\mathcal{A}$. Clearly, for every word $w \in \Sigma^*$ there are at most $|I| \cdot P(|w|) \cdot |F| \leq n^2 P(|w|)$ accepting paths for w.

(1) ⇒ (2) Let $P : \mathbb{N} \to \mathbb{N}$ be a polynomial such that every word $w \in \Sigma^*$ has at most $P(|w|)$ accepting paths in $\mathcal{A}$. We assume that P is monotonic, i.e., for every $k \leq k'$, we have $P(k) \leq P(k')$.

For every $k \in \mathbb{N}$, let $P'(k) := P\big(2^{n^2}k + 2n\big)$. Clearly, $P' : \mathbb{N} \to \mathbb{N}$ is a polynomial.

Let $S := \alpha(\theta(\Sigma^*))$. For every $p \in S$, there is some $w \in \Sigma^*$ such that $|w| \leq |S| \leq 2^{n^2}$ and $\alpha(\theta(w)) = p$.

Let $k \geq 1$, $p_1, \ldots, p_k \in S$, and $1 \leq i, j \leq n$ such that $(p_1 \ldots p_k)[i, j] = 1$.

Let $w_1, \ldots, w_k \in \Sigma^*$ such that for every $1 \leq \ell \leq k$, $|w|_\ell \leq 2^{n^2}$ and $\alpha(\theta(w_\ell)) = p_\ell$.

Since, $\mathcal{A}$ is trim, there are $w_0, w_{k+1} \in \Sigma^*$ such that $\alpha(\lambda\theta(w_0))[i] = 1$ and $\alpha(\theta(w_{k+1})\varrho)[j] = 1$. We can assume $|w_0| \leq n$ and $|w_{k+1}| \leq n$.

Let $i = i_0, \ldots, i_k = j$ such that $p_1[i_0, i_1] \wedge \cdots \wedge p_k[i_{k-1}, i_k] = 1$. For every $1 \leq \ell \leq k$, there is some path in $\mathcal{A}$ from $i_{\ell-1}$ to i_ℓ which is labeled with w_ℓ. Moreover, there is some path in $\mathcal{A}$ from an initial state to i which is labeled with w_0, and there is a path in $\mathcal{A}$ from j to some accepting state which is labeled with w_{k+1}. Consequently, we can associate to each tuple $i_0, \ldots, i_k$ an accepting path in $\mathcal{A}$ which is labeled with $w_0 \ldots w_{k+1}$. Clearly, this association is injective. Thus, the number of tuples is less than the number of accepting paths of $w_0 \ldots w_{k+1}$ in $\mathcal{A}$, i.e., the number of tuples is at most

$$P(|w_0 \ldots w_{k+1}|) \;\leq\; P\big(2^{n^2}k + 2n\big) \;=\; P'(k).$$

To show the equivalence for the case of finite ambiguity, we proceed in the same way by considering $P : \mathbb{N} \to \mathbb{N}$ as a constant. In particular, we can set $P' := P$ in (1) ⇒ (2). □

4.2 On the Span of Tuples

Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a polynomially ambiguous WFA over $\mathbb{Z}$ for this section. Let $n := |Q|$ and assume $Q = \{1, \ldots, n\}$.

Let $T := \theta(\Sigma^*) \subseteq \mathbb{Z}^{n \times n}$ and $S := \alpha(\theta(\Sigma^*)) = \alpha(T) \subseteq \mathbb{B}^{n \times n}$. By Lemma 4.5, S is polynomially ambiguous.

Let $C \subseteq Q$ and $A \in \mathbb{Z}^{n \times n}$. By an abuse of notation, we define a product $CA \in \mathbb{Z}^n$, by setting for every $1 \leq i \leq n$, $(CA)[i] = \min_{\ell \in C} A[\ell, i]$.

In Section 3.3, we already defined $\min(B) := \min_{1 \leq i \leq n} B[i]$ for $B \in \mathbb{Z}^n$. For every $B \in \mathbb{Z}^n \setminus \{(\infty, \ldots, \infty)\}$, let

1. $\max(B) := \max_{1 \leq i \leq n,\, B[i] \neq \infty} B[i]$,
2. $\mathsf{span}(B) := \max(B) - \min(B)$, and $\mathsf{span}\big((\infty, \ldots, \infty)\big) := 0$.

We show some connections between span, nf and the termination of Mohri's algorithm.

Remark 4.1. *Let $B \in \mathbb{Z}^n \setminus \{(\infty, \ldots, \infty)\}$ and $k \in \mathbb{Z} \setminus \{\infty\}$. We have:*

1. $\min(k \oplus B) = k + \min(B), \quad \max(k \oplus B) = k + \max(B)$
2. $\mathsf{span}(k \oplus B) = k + \max(B) - (k + \min(B)) = \mathsf{span}(B)$
3. $\min(\mathsf{nf}(B)) = \min\big((-\min(B)) \oplus B\big) = -\min(B) + \min(B) = 0$
4. $\mathsf{span}(\mathsf{nf}(B)) = \max(\mathsf{nf}(B)) - \min(\mathsf{nf}(B)) = \max(\mathsf{nf}(B))$
5. $\mathsf{span}(\mathsf{nf}(B)) = \mathsf{span}\big((-\min(B)) \oplus B\big) = \mathsf{span}(B)$

The equations (3) and (4) are not well-defined for $B = (\infty, \dots, \infty)$. However, the important claim (5) in Remark 4.1 is obviously true for $B = (\infty, \dots, \infty)$.

In Section 3.3, we explained that MOHRI's algorithm produces the set $Q' = \{\delta(q_0, w) \mid w \in \Sigma^*\}$.

For every $w \in \Sigma^+$, we have

$$\delta(q_0, w) \overset{(3.3)}{=} \mathsf{nf}\big(q_0\theta(w)\big) = \mathsf{nf}\big(\mathsf{nf}(\lambda)\theta(w)\big) \overset{(3.2)}{=} \mathsf{nf}\big(\lambda\theta(w)\big),$$

and $\delta(q_0, \varepsilon) = q_0 = \mathsf{nf}(\lambda) = \mathsf{nf}(\lambda\theta(\varepsilon))$. Consequently, we have

$$Q' = \{\mathsf{nf}(\lambda\theta(w)) \mid w \in \Sigma^*\}. \tag{4.1}$$

Lemma 4.6. *The following assertions are equivalent.*

1. MOHRI*'s algorithm terminates on* $\mathcal{A}$.
2. *There is some* $K \in \mathbb{N}$ *such that* $\mathsf{span}(\lambda\theta(w)) \leq K$ *for every* $w \in \Sigma^*$.

Proof. (1) ⇒ (2) Since, MOHRI's algorithm terminates, Q' is finite. Since, $Q' \neq \emptyset$, we can set $K := \max_{B \in Q'} \mathsf{span}(B)$. For every $w \in \Sigma^*$, have $\mathsf{nf}(\lambda\theta(w)) \in Q'$, and hence,

$$\mathsf{span}(\lambda\theta(w)) \overset{\text{Rem. 4.1(5)}}{=} \mathsf{span}(\mathsf{nf}(\lambda\theta(w))) \leq \max_{B \in Q'} \mathsf{span}(B) = K.$$

(2) ⇒ (1) We show that Q' is finite. Let $B \in Q' \setminus \{(\infty, \dots, \infty)\}$. There is some $w \in \Sigma^*$ such that $B = \mathsf{nf}(\lambda\theta(w))$. By Remark 4.1(4)(5), we have $\max\big(\mathsf{nf}(\lambda\theta(w))\big) = \mathsf{span}(\lambda\theta(w)) \leq K$. By Remark 4.1(3), we get $\min\big(\mathsf{nf}(\lambda\theta(w))\big) = 0$. Thus, $B = \mathsf{nf}(\lambda\theta(w)) \in \{0, \dots, K, \infty\}^n$, i.e., $Q' \subseteq \{0, \dots, K, \infty\}^n$. Hence, Q' is finite. □

4.3 The Proof of (2) ⇒ (3) in Theorem 3.4

Proof of (2) ⇒ (3) *in Theorem 3.4.* By contradiction, we assume that condition (3) is false, and we show words $u, v \in \Sigma^*$ which violate condition (2).

Since, $\mathcal{A}$ does not satisfy (3), there are some $C \in \mathsf{Clones}(\mathcal{A})$ and some word $w \in \Sigma^*$ such that

(a) $e := \alpha(\theta(w)) \in \mathsf{E}(\mathbb{B}^{n \times n})$,

(b) e is stable on C, and

(c) there is some $p \in C$ such that $\theta(w)[p, p] \neq \infty$, and every state $p' \in C$ satisfying $\theta(w)[p', p] \neq \infty$ does not have a minimal cycle in C and $\theta(w)$.

Let $p' \in C$ such that p' is minimal for $\leq_e$ and $p' \leq_e p$. Such a p' exists by Lemma 4.3. By Lemma 4.3, we have $e[p', p'] = 1$ and $\theta(w)[p', p'] \neq \infty$.

Let $q \in C$, such that q has a minimal cycle at C and $\theta(w)$. We have $\theta(w)[q, q] \neq \infty$.

By (c) above, we have $\theta(w)[p', p'] > \theta(w)[q, q]$.

Let $v \in \Sigma^*$ such that $C = \alpha(\lambda\theta(v))$. Let $k \geq 1$. We examine $\lambda\theta(vw^k) = \lambda\theta(v)\big(\theta(w)\big)^k$.

At first, we consider $\lambda\theta(vw^k)[p']$. We have

$$\lambda\theta(vw^k)[p'] = \Big(\big(\lambda\theta(v)\big)\big(\theta(w)\big)^k\Big)[p'] = \min_{r \in Q}\Big(\big(\lambda\theta(v)\big)[r] + \big(\theta(w)\big)^k[r, p']\Big) =$$

For every $i \in Q \setminus C$, we have $(\lambda\theta(v))[i] = \infty$. Since, p' is minimal in C for $\leq_e$, we have for every $i \in C \setminus \{p'\}$, $e[i,p'] = 0$, i.e., $\theta(w)[i,p'] = \infty$. Hence,

$$= \big(\lambda\theta(v)\big)[p'] + \big(\theta(w)\big)^k[p',p'].$$

Since, $\alpha(\theta(\Sigma^*))$ is polynomially ambiguous, the entry (p',p') is unambiguous in e by Lemma 4.2(2). Consequently, there are unique $p' = i_0, \ldots, i_k = p'$ such that $e[i_0,i_1] \wedge \cdots \wedge e[i_{k-1},i_k] = 1$. For every $0 < \ell < k$, we can have $p' \leq_e i_\ell$ and $i_\ell \leq_e p'$, and hence, $p' = i_\ell$. Thus, $(\theta(w))^k[p',p'] = k \cdot \big(\theta(w)[p',p']\big)$. To sum up,

$$\big(\lambda\theta(vw^k)\big)[p'] \;=\; \big(\lambda\theta(v)\big)[p'] + k \cdot \big(\theta(w)[p',p']\big).$$

On the other hand, we have

$$\big(\lambda\theta(vw^k)\big)[q] \;\leq\; \big(\lambda\theta(v)\big)[q] + k \cdot \big(\theta(w)[q,q]\big) \;\neq\; \infty.$$

From $\theta(w)[p',p'] > \theta(w)[q,q]$, it follows that for increasing integers k, the difference $\big(\lambda\theta(vw^k)\big)[p'] - \big(\lambda\theta(vw^k)\big)[q]$ tends to infinity. Consequently, MOHRI's algorithm does not terminate on the sequence $(vw^k)_{k\geq 1}$. □

4.4 The Side Entry Bound

Lemma 4.7. *Let $B \in \mathbb{Z}^n$ and $A \in \mathbb{Z}^{n\times n}$. We have* $\mathsf{span}(BA) \leq \mathsf{span}(B) + \mathsf{span}\big(\alpha(B)A\big)$.

Proof. If $BA = (\infty,\ldots,\infty)$, then the claim is obvious. We assume $BA \neq (\infty,\ldots,\infty)$ in the rest of the proof. There are $1 \leq i,j \leq n$ such that

$$\infty \;\geq\; \min(BA) \;=\; B[i] + A[i,j] \;\geq\; \min(B) + \min\big(\alpha(B)A\big). \tag{4.2}$$

Now, let $1 \leq j' \leq n$ such that $\max(BA) = BA[j']$. Let $i' \in \alpha(B)$ such that $A[i',j'] = \big(\alpha(B)A\big)[j'] \leq \max\big(\alpha(B)A\big)$. Hence,

$$\max(BA) \;=\; BA[j'] \;\leq\; B[i'] + A[i',j'] \;\leq\; \max(B) + \max\big(\alpha(B)A\big). \tag{4.3}$$

By combining (4.2) and (4.3), we obtain

$$\mathsf{span}(BA) \;=\; \max(BA) - \min(BA) \;\leq$$

$$\leq\; \max(B) + \max\big(\alpha(B)A\big) - \min(B) - \min\big(\alpha(B)A\big) \;=\; \mathsf{span}(B) + \mathsf{span}\big(\alpha(B)A\big).$$

□

Let $C \in \mathsf{Clones}(\mathcal{A})$ and $A \in T$. We denote the *side entry bound* of C and A by $\mathsf{seb}(C,A)$ and define it as the least integer which satisfies $\mathsf{seb}(C,A) \geq \mathsf{span}(CA)$ and the following condition:

> For every $i \in C$ and $1 \leq j \leq n$ such that (i,j) is unambiguous in $\alpha(A)$, we have
>
> if there is some $i' \in C \setminus \{i\}$ such that $A[i',j] \neq \infty$, then there is some $\hat{i} \in C \setminus \{i\}$ such that
>
> $$A[\hat{i},j] \;\leq\; \min(CA) \;+\; \mathsf{seb}(C,A).$$

Lemma 4.8. *Let $A_1, A_2 \in T$ and $C_1 \in \mathsf{Clones}(\mathcal{A})$ and set $C_2 := \alpha(C_1A_1) \in \mathsf{Clones}(\mathcal{A})$.*

1. *If* $C_1A_1A_2 \neq (\infty,\ldots,\infty)$, *then* $\min(C_1A_1A_2) \geq \min(C_1A_1) + \min(C_2A_2)$.
2. $\mathsf{span}(C_1A_1A_2) \leq \mathsf{span}(C_1A_1) + \mathsf{span}(C_2A_2)$
3. $\mathsf{seb}(C_1, A_1A_2) \leq \mathsf{seb}(C_1, A_1) + \mathsf{seb}(C_2, A_2)$

Proof. (1) If $C_1A_1A_2 \neq (\infty,\ldots,\infty)$, then there are $i \in C_1$, $j \in C_2$, and $1 \leq \ell \leq n$ such that

$$\infty \neq \min(C_1A_1A_2) = C_1A_1A_2[\ell] = A_1[i,j] + A_2[j,\ell].$$

Thus, $A_1[i,j] \neq \infty$ and $A_2[j,\ell] \neq \infty$, and hence, $C_1A_1 \neq (\infty,\ldots,\infty)$ and $C_2A_2 \neq (\infty,\ldots,\infty)$. We have $A_1[i,j] \geq C_1A_1[j] \geq \min(C_1A_1)$ and $A_2[j,\ell] \geq C_2A_2[\ell] \geq \min(C_2A_2)$, and (1) follows.

(2) Since, $C_2 = \alpha(C_1A_1)$ claim (2) follows from Lemma 4.7.

(3) To shorten our notation, we denote $b := \mathsf{seb}(C_1, A_1) + \mathsf{seb}(C_2, A_2)$, i.e., we have to show $\mathsf{seb}(C_1, A_1A_2) \leq b$. Above, $\mathsf{seb}(C_1, A_1A_2)$ was defined as the least number which satisfies two conditions. We show that b satisfies these two conditions, and henceforth, $\mathsf{seb}(C_1, A_1A_2) \leq b$. More precisely, we have to show the following two claims:

(3a) $b \geq \mathsf{span}(C_1A_1A_2)$

(3b) Let $i \in C_1$ and $1 \leq j \leq n$ such that (i,j) is unambiguous in $\alpha(A_1A_2)$. We have to show that if there is some $i' \in C_1 \setminus \{i\}$ such that $A_1A_2[i',j] \neq \infty$, then there is some $\hat{i} \in C_1 \setminus \{i\}$ such that $A_1A_2[\hat{i},j] \leq \min(C_1, A_1A_2) + b$.

By the definition of $\mathsf{seb}(C_1, A_1)$, $\mathsf{seb}(C_2, A_2)$, and (2), we have $b \geq \mathsf{span}(C_1A_1) + \mathsf{span}(C_2A_2) \geq \mathsf{span}(C_1A_1A_2)$ which proves (3a).

To show (3b), let $i \in C_1$ and $1 \leq j \leq n$ such that (i,j) is unambiguous in $\alpha(A_1A_2)$. Let $1 \leq \ell \leq n$ such that $A_1A_2[i,j] = A_1[i,\ell] + A_2[\ell,j]$. Since, (i,j) is unambiguous in $\alpha(A_1A_2)$, (i,ℓ) (resp. (ℓ,j)) is unambiguous in $\alpha(A_1)$ (resp. $\alpha(A_2)$). Let $i' \in C_1 \setminus \{i\}$ such that $A_1A_2[i',j] \neq \infty$. If such an i' does not exist, we are done.

Case 1: For every $\ell' \in C_2 \setminus \{\ell\}$, we have $A_2[\ell',j] = \infty$.

We have $C_2A_2[j] = A_2[\ell,j]$, and hence $A_2[\ell,j] \leq \min(C_2A_2) + \mathsf{span}(C_2A_2)$.

Moreover, we have $A_1[i',\ell] \neq \infty$. By the definition of $\mathsf{seb}(C_1, A_1)$, there is some $\hat{i} \in C_1 \setminus \{i\}$ such that $A_1[\hat{i},\ell] \leq \min(C_1A_1) + \mathsf{seb}(C_1, A_1)$. To sum up,

$$A_1A_2[\hat{i},j] \leq A_1[\hat{i},\ell] + A_2[\ell,j] \leq \min(C_1A_1) + \mathsf{seb}(C_1, A_1) + \min(C_2A_2) + \mathsf{span}(C_2A_2) \leq$$

$$\leq \min(C_1A_1A_2) + \mathsf{seb}(C_1A_1) + \mathsf{seb}(C_2, A_2).$$

Case 2: There is some $\ell' \in C_2 \setminus \{\ell\}$ such that $A_2[\ell',j] \neq \infty$.

By the definition of $\mathsf{seb}(C_2, A_2)$, there is some $\hat{\ell} \in C_2 \setminus \{\ell\}$ such that $A_2[\hat{\ell},j] \leq \min(C_2A_2) + \mathsf{seb}(C_2, A_2)$. By the definition of $\mathsf{span}(C_2A_2)$, there is some $\hat{i} \in C_1$ such that $A_1[\hat{i},\hat{\ell}] \leq \min(C_1A_1) + \mathsf{span}(C_1A_1)$. Hence,

$$A_1A_2[\hat{i},j] \leq A_1[\hat{i},\hat{\ell}] + A_2[\hat{\ell},j] \leq \min(C_1A_1) + \mathsf{span}(C_2A_2) + \min(C_2A_2) + \mathsf{seb}(C_2, A_2) \leq$$

$$\leq \min(C_1A_1A_2) + \mathsf{seb}(C_1, A_1) + \mathsf{seb}(C_2, A_2).$$

It remains to show $\hat{i} \neq i$. We have $\alpha(A_1)[\hat{i},\hat{\ell}] \wedge \alpha(A_2)[\hat{\ell},j] = 1$ and $\alpha(A_1)[i,\ell] \wedge \alpha(A_2)[\ell,j] = 1$. Since, $\hat{\ell} \neq \ell$ and (i,j) is unambiguous in $\alpha(A_1A_2)$, we have $\hat{i} \neq i$.

□

Lemma 4.9. *Assume that $\mathcal{A}$ satisfies the clones property. Let $k \geq 1$ and $A_1, \ldots, A_k \in T$ such that $\alpha(A_1) = \cdots = \alpha(A_k) \in \mathsf{E}(S)$. Let $C \in \mathsf{Clones}(\mathcal{A})$ such that $\alpha(A_1)$ is stable on C.*

1. $\mathsf{span}(CA_1 \cdots A_k) \leq 2(n-1) \max_{1 \leq \ell \leq k} \mathsf{seb}(C, A_\ell)$
2. $\mathsf{seb}(C, A_1 \cdots A_k) \leq 2n \max_{1 \leq \ell \leq k} \mathsf{seb}(C, A_\ell)$

Note that the bound on $\mathsf{span}(CA_1 \cdots A_k)$ in Lemma 4.9(1) depends on the side entry bound of C and A_ℓ for $1 \leq \ell \leq k$. As the following example shows, it is not possible to show an upper bound on $\mathsf{span}(CA_1 \cdots A_k)$ which is independent on the side entry bound of C and A_ℓ.

Example 4.1. Let $S := \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$. Let $C = \{1, 2\}$, $b \geq 1$, and $A_1 = \begin{pmatrix} 0 & b \\ \infty & 1 \end{pmatrix} \in T$.
Let $k \geq b$ and $A_\ell = A_1$ for $1 \leq \ell \leq k$.
For every $1 \leq \ell \leq k$, we have $\mathsf{span}(CA_\ell) = \mathsf{span}\big(\begin{pmatrix} 0 & 1 \end{pmatrix}\big) = 1$ and $\mathsf{seb}(C, A_\ell) = b$.
However, we have $A_1 \cdots A_k = \begin{pmatrix} 0 & b \\ \infty & k \end{pmatrix}$ and hence, $\mathsf{span}(CA_1 \cdots A_k) = \mathsf{span}\big(\begin{pmatrix} 0 & b \end{pmatrix}\big) = b$.

Consequently, we cannot derive an upper bound on $\mathsf{span}(CA_1 \cdots A_k)$ which is independent of $\mathsf{seb}(C, A_\ell)$ for $1 \leq \ell \leq k$. □

Proof of Lemma 4.9. Denote $e := \alpha(A_1)$ and $A := A_1 \ldots A_k$.

We assume $C \neq \emptyset$ since otherwise, the claim is obvious.

Assume $k = 1$. Claim (2) is obvious. If $n > 1$, then claim (1) is obvious. Moreover, we have claim (1) for $n = 1$ because $\mathsf{span}(CA_1) = 0$. We assume $k \geq 2$ in the rest of the proof.

Let $p \in C$ be minimal for $\leq_e$. By Lemma 4.3, we have $e[p, p] = 1$, and hence, $A_\ell[p, p] \neq \infty$ for every $1 \leq \ell \leq k$. Since, p is minimal, we have for every $1 \leq \ell \leq k$,

$$(CA_1 \cdots A_\ell)[p] \;=\; (A_1 \cdots A_\ell)[p, p] \;=\; \sum_{1 \leq \ell' \leq \ell} A_{\ell'}[p, p]. \tag{4.4}$$

Since, $\mathcal{A}$ satisfies the clones property, we have for every $1 \leq \ell \leq k$ and $q \in C$, $A_\ell[p, p] \leq A_\ell[q, q]$.

To shorten out notations, let $\mathsf{mx}_{\mathsf{span}} := \max_{1 \leq \ell \leq k} \mathsf{span}(CA_\ell)$ and $\mathsf{mx}_{\mathsf{seb}} := \max_{1 \leq \ell \leq k} \mathsf{seb}(C, A_\ell)$. By definition, $\mathsf{mx}_{\mathsf{span}} \leq \mathsf{mx}_{\mathsf{seb}}$.

In the first part of the proof, we show the following two claims (C1) and (C2). Finally, we derive claims (1) and (2) of the lemma from (C1) and (C2).

(C1) For every $j \in C$, we have $CA[j] \geq CA[p] - (n-1)\mathsf{mx}_{\mathsf{span}}$.

(C2) For every $1 \leq \ell \leq k$, $j \in C$, we have $(CA_1 \cdots A_\ell)[j] \leq (CA_1 \cdots A_\ell)[p] + (n-1)\mathsf{mx}_{\mathsf{seb}}$.

We show (C1). Let $j \in C$ be arbitrary. Let $1 \leq i_0, \ldots, i_k \leq n$, $i_k = j$ such that for every $1 \leq \ell \leq k$, we have $A_\ell[i_{\ell-1}, i_\ell] \neq \infty$. For every $1 \leq \ell \leq k$, we have $e[i_{\ell-1}, i_\ell] = 1$, i.e., $i_0 \leq_e i_1 \leq_e \ldots \leq_e i_k$. Since, e is stable on C, we have $i_0, \ldots, i_k \in C$.

For every $1 \leq \ell \leq k$, we have $e[i_{\ell-1}, i_\ell] = 1$, i.e., $i_0 \leq_e i_1 \leq_e \ldots \leq_e i_k$. Since, e is stable on C, we have $i_0, \ldots, i_k \in C$.

Let $1 \leq \ell \leq k$ such that $i_{\ell-1} \neq i_\ell$. Since p is minimal, we have $CA_\ell[p] = A_\ell[p, p]$. By the definition of $\mathsf{span}(CA_\ell)$, we have $A_\ell[i_{\ell-1}, i_\ell] \geq CA_\ell[p] - \mathsf{span}(CA_\ell) = A[p, p] - \mathsf{span}(CA_\ell)$.

Let $1 \leq \ell \leq k$ such that $i_{\ell-1} = i_\ell$. As seen above, we have $A_\ell[i_{\ell-1}, i_\ell] \geq A_\ell[p,p]$ for every $1 \leq \ell \leq k$.

From these bounds on $A_\ell[i_{\ell-1}, i_\ell]$, we obtain

$$\sum_{1\leq\ell\leq k} A_\ell[i_{\ell-1}, i_\ell] \;\geq\; \sum_{1\leq\ell\leq k} A_\ell[p,p] \;-\; \sum_{1\leq\ell\leq k,\, i_{\ell-1}\neq i_\ell} \mathsf{span}(CA_\ell)$$

Since, S is polynomially ambiguous, $\leq_e$ is antisymmetric and transitive, and hence, there are at most $n-1$ integers $1 \leq \ell \leq k$ such that $i_{\ell-1} \neq i_\ell$. Hence, we have

$$\sum_{1\leq\ell\leq k} A_\ell[i_{\ell-1}, i_\ell] \;\geq\; A[p,p] \;-\; (n-1)\mathsf{mx}_{\mathsf{span}},$$

and thus, $CA[j] \geq CA[p] - (n-1)\mathsf{mx}_{\mathsf{span}}$.

In the next part, we show (C2). Let $j \in C$. We define $\mathsf{ind}(j) := \big|\{i \in C \mid i \leq_e j,\, i \neq j\}\big|$. We have $0 \leq \mathsf{ind}(j) < n$. For every $i \leq_e j$ satisfying $i \neq j$, we have $\mathsf{ind}(i) < \mathsf{ind}(j)$.

To show (C2), we show that for every $j \in C$, $1 \leq \ell \leq k$, we have

$$(CA_1 \cdots A_\ell)[j] \;\leq\; (CA_1 \cdots A_\ell)[p] + \mathsf{ind}(j)\mathsf{mx}_{\mathsf{seb}}. \tag{4.5}$$

We show (4.5) by an induction on j via $\leq_e$.

Let $j \in C$ be minimal for $\leq_e$, i.e., $\mathsf{ind}(j) = 0$. Since, $\mathcal{A}$ satisfies the clones property, we have for every $1 \leq \ell' \leq k$, $A_{\ell'}[j,j] = A_{\ell'}[p,p]$. Moreover, we have for every $1 \leq \ell \leq k$

$$(CA_1 \cdots A_\ell)[j] \;=\; (A_1 \cdots A_\ell)[j,j] \;=\; \sum_{1\leq\ell'\leq\ell} A_{\ell'}[j,j].$$

In combination with (4.4), we obtain $(CA_1 \cdots A_\ell)[j] = (CA_1 \cdots A_\ell)[p]$ which proves (4.5) for j.

Now, let $j \in C$ and assume by induction, that (4.5) holds for every $1 \leq \ell \leq k$, $i \leq_e j$, $i \neq j$. Moreover, assume that j is not minimal for $\leq_e$ in C, i.e., $\mathsf{ind}(j) \geq 1$.

Next, we show that there exists some $i \in C$ such that $i \neq j$, $i \leq_e j$, and $A_\ell[i,j] \leq A_\ell[p,p] + \mathsf{seb}(C, A_\ell)$. For this, we distinguish two cases.

Case 1. $e[j,j] = 0$

We have $A_\ell[j,j] = \infty$. Let $i \in C$ such that $A_\ell[i,j] = CA_\ell[j]$. We have $CA_\ell[j] \leq CA_\ell[p] + \mathsf{span}(CA_\ell)$, i.e., $A_\ell[i,j] \leq A_\ell[p,p] + \mathsf{span}(CA_\ell) \leq A_\ell[p,p] + \mathsf{seb}(C, A_\ell)$. Since $A_\ell[i,j] \neq \infty$, we have $e[i,j] = 1$, and hence, $i \neq j$ and $i \leq_e j$.

Case 2. $e[j,j] = 1$

By Lemma 4.2, (j,j) is unambiguous in e. We utilize the notion of the side entry bound. Since, j is not minimal for $\leq_e$ in C, there is some i' such that $e[i',j] = 1$, i.e., $A_\ell[i',j] \neq \infty$. By the definition of $\mathsf{seb}(C, A_\ell)$, there is some $i \in C \setminus \{j\}$ such[3] that $A_\ell[i,j] \leq \min(CA_\ell) + \mathsf{seb}(C, A_\ell)$, i.e., $A_\ell[i,j] \leq A_\ell[p,p] + \mathsf{seb}(C, A_\ell)$. Obviously, $i \neq j$ and since, $A_\ell[i,j] \neq \infty$, we have $e[i,j] = 1$, i.e., $i \leq_e j$, which closes the case $e[j,j] = 1$.

We show (4.5) for $\ell = 1$. We have

$$(CA_1)[j] \;\leq\; A_1[i,j] \;\leq\; A_1[p,p] + \mathsf{seb}(C, A_1) \;\leq\; (CA_1)[p] + \mathsf{seb}(C, A_1) \;\leq$$

$$\leq\; (CA_1)[p] + \mathsf{ind}(j)\mathsf{mx}_{\mathsf{seb}}.$$

[3] The state i was called $\hat{i}$ in the definition of $\mathsf{seb}(C, A_\ell)$.

Now, we show (4.5) for $2 \leq \ell \leq k$. By induction, (4.5) holds for i, i.e.,

$$(CA_1 \cdots A_{\ell-1})[i] \;\leq\; (CA_1 \cdots A_{\ell-1})[p] + \mathsf{ind}(i)\mathsf{mx}_{\mathsf{seb}}. \tag{4.6}$$

We have

$$(CA_1 \cdots A_\ell)[j] \quad\leq\quad (CA_1 \cdots A_{\ell-1})[i] + A_\ell[i,j] \quad\leq$$

and by (4.6) and the bound on $A_\ell[i,j]$ shown above,

$$\leq \quad (CA_1 \cdots A_{\ell-1})[p] + \mathsf{ind}(i)\mathsf{mx}_{\mathsf{seb}} + A_\ell[p,p] + \mathsf{seb}(C, A_\ell) \quad\leq$$

and since, $\mathsf{ind}(i) < \mathsf{ind}(j)$

$$\leq \quad (CA_1 \cdots A_\ell)[p] + \mathsf{ind}(j)\mathsf{mx}_{\mathsf{seb}}$$

which proves (4.5) for j.

By combining (C1) and (C2) for $\ell = k$, we obtain for every $j \in C$,

$$CA[p] - (n-1)\mathsf{mx}_{\mathsf{seb}} \quad\leq\quad CA[j] \quad\leq\quad CA[p] + (n-1)\mathsf{mx}_{\mathsf{seb}}.$$

Consequently, we have $\mathsf{span}(CA) \leq (n-1)(\mathsf{mx}_{\mathsf{span}} + \mathsf{mx}_{\mathsf{seb}})$ which proves claim (1) of the lemma.

We show claim (2) of the lemma. Let $i \in C$ and $1 \leq j \leq n$ such that (i,j) is unambiguous in e. Let $i' \in C \setminus \{i\}$ such that $A[i',j] \neq \infty$. If such an i' does not exist, then we are done.

Let $1 \leq \ell \leq n$ such that $(A_1 \cdots A_{k-1})[i,\ell] + A_k[\ell,j] \neq \infty$. Since (i,j) is unambiguous, ℓ is unique and $A[i,j] = (A_1 \cdots A_{k-1})[i,\ell] + A_k[\ell,j]$.

By contradiction, assume that there is exactly one $\ell' \in C$ such that $e[\ell',j] = 1$. Hence, there is exactly one $\ell' \in C$ such that $A[\ell',j] = 1$. Consequently, $i = i'$ which is a contradiction.

Thus, there is some $\ell' \in C \setminus \{\ell\}$ such that $e[\ell',j] = 1$.

By the definition of $\mathsf{seb}(C, A_k)$, there is some $\hat{\ell} \in C \setminus \{\ell\}$ such that $A_k[\hat{\ell},j] \;\leq\; \min(CA_k) + \mathsf{seb}(C, A_k) \;\leq\; A_k[p,p] + \mathsf{seb}(C, A_k)$.

By applying (C2) on $CA_1 \cdots A_{k-1}$, we obtain some $\hat{i} \in C$ such that

$$(A_1 \cdots A_{k-1})[\hat{i},\hat{\ell}] \;\leq\; (CA_1 \cdots A_{k-1})[p] + (n-1)\mathsf{mx}_{\mathsf{seb}}.$$

To sum up,

$$A[\hat{i},j] \;\leq\; (A_1 \cdots A_{k-1})[\hat{i},\hat{\ell}] + A_k[\hat{\ell},j] \;\leq$$

$$\leq\; (CA_1 \cdots A_{k-1})[p] + (n-1)\mathsf{mx}_{\mathsf{seb}} + A_k[p,p] + \mathsf{seb}(C, A_k) \;\leq$$

$$\leq\; (CA)[p] + n\mathsf{mx}_{\mathsf{seb}} \overset{\text{(C1)}}{\leq} \min(CA) + (n-1)\mathsf{mx}_{\mathsf{span}} + n\mathsf{mx}_{\mathsf{seb}} \;\leq\; \min(CA) + 2n\mathsf{mx}_{\mathsf{seb}}.$$

It remains to show $i \neq \hat{i}$. We have $e[i,\ell] \wedge e[\ell,j] = 1$ and $e[\hat{i},\hat{\ell}] \wedge e[\hat{\ell},j] = 1$. Since, $\ell \neq \hat{\ell}$ and (i,j) is unambiguous in e, we have $i \neq \hat{i}$. □

4.5 The Proof of (3) ⇒ (1) in Theorem 3.4

To derive the proof of (3) ⇒ (1) in Theorem 3.4 from Lemmas 4.8 and 4.9, we need the following important theorem due to Simon.

Theorem 4.10 (factorization forest theorem [32, 33, 4])**.** *Let S be a finite semigroup and $h : \Sigma^* \to S$ be a homomorphism. There is a mapping $d : \Sigma^* \to \{1, \ldots, 7|S|\}$ such that every $w \in \Sigma^*$ satisfies the following two conditions:*

1. *if* $d(w) = 1$, *then* $|w| \leq 1$, *and*
2. *if* $d(w) \geq 2$, *then there are some* $k \geq 2$, $w_1, \ldots, w_k \in \Sigma^+$ *such that*
   (a) $w_1 \ldots w_k = w$,
   (b) *for every* $1 \leq \ell \leq k$, $d(w_\ell) < d(w)$, *and*
   (c) *if* $k \geq 3$, *then* $h(w_1) = \cdots = h(w_k) = h(w) \in \mathsf{E}(S)$.

Simon's original version of the factorization forest theorem from 1990 [32] utilized a mapping $d : \Sigma^* \to \{1, \ldots, 9|S|\}$. The improvement on the range of d to $\{1, \ldots, 7|S|\}$ and a simplified proof are due to Chalopin and Leung [4].

Proof of (3) ⇒ (1) *in Theorem 3.4.* We utilize the factorization forest theorem on the homomorphism $\alpha \circ \theta : \Sigma^* \to S$. Let $d : \Sigma^* \to \{1, \ldots, 7|S|\}$ be a mapping from Theorem 4.10.

We denote $\mathsf{mx}_{\mathsf{seb}} := \max_{C \in \mathsf{Clones}(\mathcal{A}),\, a \in \Sigma} \mathsf{seb}(C, \theta(a))$.

We show the following claim by an induction on $d(w)$:

(C1) For every $C \in \mathsf{Clones}(\mathcal{A})$ and every $w \in \Sigma^*$, we have $\mathsf{seb}(C, \theta(w)) \leq (2n+1)^{d(w)-1} \cdot \mathsf{mx}_{\mathsf{seb}}$.

By Lemma 4.6, (C1) is sufficient for the termination of Mohri's algorithm on $\mathcal{A}$.

Let $w \in \Sigma^*$ such that $d(w) = 1$, i.e., w is a letter. (C1) follows from the definition of $\mathsf{mx}_{\mathsf{seb}}$.

Now, let $w \in \Sigma^*$ such that $d(w) > 1$ and assume by induction, that claim (C1) is true for every $w' \in \Sigma^*$ satisfying $d(w') < d(w)$.

We distinguish two cases according to Theorem 4.10(2).

Case 1. There are $w_1, w_2 \in \Sigma^+$ such that $w = w_1 w_2$, $d(w_1) < d(w)$, and $d(w_2) < d(w)$.

Let $C \in \mathsf{Clones}(\mathcal{A})$ be arbitrary and let $C' := C\alpha(\theta(w_1))$. By Lemma 4.8(3) and the inductive hypothesis, we have

$$\mathsf{seb}(C, \theta(w_1 w_2)) \leq \mathsf{seb}(C, \theta(w_1)) + \mathsf{seb}(C', \theta(w_2)) \leq 2 \cdot (2n+1)^{d(w)-2} \mathsf{mx}_{\mathsf{seb}}.$$

Case 2. There are $k \geq 2$ and $w_0, \ldots, w_k \in \Sigma^+$ such that $w = w_0 \ldots w_k$, and for every $0 \leq \ell \leq k$, we have $d(w_\ell) < d(w)$ and $\alpha(\theta(w_0)) = \alpha(\theta(w_\ell)) \in \mathsf{E}(S)$.

Let $C \in \mathsf{Clones}(\mathcal{A})$ and $C' := C\alpha(\theta(w_0))$.

We have $C'\alpha(\theta(w_1)) = C\alpha(\theta(w_0))\alpha(\theta(w_1)) = C\alpha(\theta(w_0)) = C'$, i.e., C' is stable $\alpha(\theta(w_0))$. From Lemma 4.9(2) on C' and $\theta(w_1), \ldots, \theta(w_k)$, we obtain

$$\mathsf{seb}(C', \theta(w_1 \ldots w_k)) \leq 2n \max_{1 \leq \ell \leq k} \mathsf{seb}(C', \theta(w_\ell)). \tag{4.7}$$

By applying Lemma 4.8(3) on C, $\theta(w_0)$ and C', $\theta(w_1 \ldots w_k)$, and using (4.7), we obtain

$$\mathsf{seb}(C, \theta(w)) \leq \mathsf{seb}(C, \theta(w_0)) + 2n \max_{1 \leq \ell \leq k} \mathsf{seb}(C', \theta(w_\ell)) \leq$$

and by the inductive hypothesis,

$$\leq (2n+1)^{d(w)-2} \mathsf{mx}_{\mathsf{seb}} + 2n(2n+1)^{d(w)-2} \mathsf{mx}_{\mathsf{seb}}$$

and (C1) follows.

□

4.6 The Proof of Theorem 3.6

Proof of Theorem 3.6. It remains to show (1) ⇒ (2). Let $q, q' \in Q$ be siblings. Let $C \in \mathsf{Clones}(\mathcal{A})$ such that $q, q' \in C$. Let $w \in \Sigma^*$ such that $\theta(w)[q,q] \neq \infty$ and $\theta(w)[q',q'] \neq \infty$.

There is some $k \geq 1$ such that $(\theta(w))^k = \theta(w^k) \in \mathsf{E}(\mathbb{B}^{n\times n})$.

By Lemma 4.5, $\alpha(\theta(\Sigma^*))$ is finitely ambiguous. Since, finitely ambiguous semigroups are polynomially ambiguous, we can apply Lemma 4.2 on $\alpha(\theta(\Sigma^*))$. From (2) in Lemma 4.2, we can derive $\theta(w^k)[q,q] = k \cdot \theta(w)[q,q]$ and $\theta(w^k)[q',q'] = k \cdot \theta(w)[q',q']$.

Let $C' := C\alpha(\theta(w^k))$. We have $C' \in \mathsf{Clones}(\mathcal{A})$. Since, $\alpha(\theta(w^k))$ is idempotent, C' is stable on $\alpha(\theta(w^k))$. By (1), C' and $\theta(w^k)$ have the clones property. Consequently, there is some $p \in C'$ such that p has a minimal cycle in C' and $\theta(w^k)$ and $\theta(w^k)[p,q] \neq \infty$. By Lemma 4.4, we have $p = q$. Thus, q has a minimal cycle in C' and $\theta(w^k)$. In the same way, q' has a minimal cycle in C' and $\theta(w^k)$. Hence, $\theta(w^k)[q,q] = \theta(w^k)[q',q']$, i.e., $\theta(w)[q,q] = \theta(w)[q',q']$. □

4.7 Trimming and Mohri's Algorithm

Let $\mathcal{A} = [Q, \theta, \lambda, \varrho]$ be a WFA over the tropical semiring. Let $R \subseteq Q$ be the accessible states of $\mathcal{A}$.

Let $\theta_R : \Sigma^* \to \mathbb{Z}^{R\times R}$ be defined by $\theta_R(w)[i,j] := \theta(w)[i,j]$ for every $w \in \Sigma^*$, $i, j \in R$. Let $\lambda_R, \varrho_R \in \mathbb{Z}^R$ be the restriction of λ (resp. ϱ) to R.

Clearly, $\theta_R(\varepsilon)$ is the identity matrix in $\mathbb{Z}^{R\times R}$. Let $u, v \in \Sigma^*$, $i, j \in R$ be arbitrary. We have

$$\big(\theta_R(u)\theta_R(v)\big)[i,j] \;=\; \min_{\ell\in R}\big(\theta_R(u)[i,\ell] + \theta_R(v)[\ell,j]\big) \;=\; \min_{\ell\in R}\big(\theta(u)[i,\ell] + \theta(v)[\ell,j]\big) \;=$$

Let $\ell \in Q$ and assume $\theta(v)[i,\ell] \neq \infty$ and $\theta(v)[\ell,j] \neq \infty$. Since, $i \in R$, there is some $u' \in \Sigma^*$ such that $\lambda\theta(u')[i] \neq \infty$, and hence, $\lambda\theta(u'u)[\ell] \neq \infty$. Similarly, there is some $v' \in \Sigma^*$ such that $\theta(vv')\varrho[\ell] \neq \infty$. Thus, $\ell \in R$. Consequently, we have for every $\ell \in Q \setminus R$, $\theta(v)[i,\ell] = \infty$ and $\theta(v)[\ell,j] = \infty$. Hence, we can then extend the range of ℓ from R to Q and obtain

$$= \min_{\ell\in Q}\big(\theta(v)[i,\ell] + \theta(v)[\ell,j]\big) \;=\; \big(\theta(u)\theta(v)\big)[i,j] \;=\; \big(\theta(uv)\big)[i,j] \;=\; \big(\theta_R(uv)\big)[i,j].$$

Consequently, θ_R is a homomorphism and $\mathcal{A}_R := [R, \theta_R, \lambda_R, \varrho_R]$ is a WFA.

Let $w \in \Sigma^*$. Let $i, j \in Q$ such that $\lambda[i] + \theta(w)[i,j] + \varrho[j] \neq \infty$. We can easily conclude that $\lambda\theta(w)[j]$, $\theta(\varepsilon)\varrho[j]$, $\lambda\theta(\varepsilon)[i]$, and $\theta(w)\varrho[i]$ are different from ∞. Hence, $i, j \in R$. Consequently, we obtain for every $w \in \Sigma^*$

$$|\mathcal{A}|(w) \;=\; \min_{i,j\in Q}\big(\lambda[i] + \theta(w)[i,j] + \varrho[j]\big) \;=\; \min_{i,j\in R}\big(\lambda[i] + \theta(w)[i,j] + \varrho[j]\big) \;=$$

$$= \min_{i,j\in R}\big(\lambda_R[i] + \theta_R(w)[i,j] + \varrho_R[j]\big) \;=\; |\mathcal{A}_R|(w).$$

Thus, $\mathcal{A}$ and $\mathcal{A}_R$ are equivalent.

Let $w \in \Sigma^*$ and $i \in R$. We have

$$\lambda\theta(w)[i] \;=\; \min_{\ell\in Q}\big(\lambda[\ell] + \theta(w)[\ell,i]\big) \;=\; \min_{\ell\in R}\big(\lambda[\ell] + \theta(w)[\ell,i]\big) \;=\; \lambda_R\theta_R(w)[i]. \tag{4.8}$$

Proof of Theorem 3.8. Assume that Mohri's algorithm terminates on $\mathcal{A}$. Hence, the set $Q' = \{\mathsf{nf}(\lambda\theta(w)) \mid w \in \Sigma^*\}$ is finite. We have to show that the set $R' = \{\mathsf{nf}(\lambda_R\theta_R(w)) \mid w \in \Sigma^*\}$ is finite.

For this, we show that for every words $u, v \in \Sigma^*$ satisfying $\mathsf{nf}(\lambda\theta(u)) = \mathsf{nf}(\lambda\theta(v))$, we have $\mathsf{nf}(\lambda_R\theta_R(u)) = \mathsf{nf}(\lambda_R\theta_R(v))$. Let $u, v \in \Sigma^*$ satisfying $\mathsf{nf}(\lambda\theta(u)) = \mathsf{nf}(\lambda\theta(v))$.

If $\lambda\theta(u) = (\infty, \ldots, \infty)$, then $\lambda\theta(v) = (\infty, \ldots, \infty)$, and hence, $\mathsf{nf}(\lambda_R\theta_R(u)) = (\infty, \ldots, \infty) = \mathsf{nf}(\lambda_R\theta_R(v))$. We assume $\lambda\theta(u) \neq (\infty, \ldots, \infty)$ in the rest of the proof.

Clearly, $\mathsf{nf}(\lambda\theta(u))$, $\mathsf{nf}(\lambda\theta(v))$, and $\lambda\theta(v)$ are different from $(\infty, \ldots, \infty)$.

Let $k_u := \min(\lambda\theta(u))$ and $k_v := \min(\lambda\theta(v))$. By the definition of nf, we have $\mathsf{nf}(\lambda\theta(u)) = (-k_u) \oplus (\lambda\theta(u))$ and $\mathsf{nf}(\lambda\theta(v)) = (-k_v) \oplus (\lambda\theta(v))$. Consequently, $(-k_u) \oplus (\lambda\theta(u)) = (-k_v) \oplus (\lambda\theta(v))$, and hence, $(\lambda\theta(u)) = (k_u - k_v) \oplus (\lambda\theta(v))$. By (4.8), we have $\lambda_R\theta_R(u) = (k_u - k_v) \oplus (\lambda_R\theta_R(v))$. As seen in (3.1) in Section 3.3, we have $\mathsf{nf}(\lambda_R\theta_R(u)) = \mathsf{nf}(\lambda_R\theta_R(v))$. □

References

[1] C. Allauzen and M. Mohri. Efficient algorithms for testing the twins property. *Journal of Automata, Languages and Combinatorics*, 8(2):117–144, 2003.

[2] J. Berstel and C. Reutenauer. *Rational Series and Their Languages*, volume 12 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Berlin Heidelberg New York, 1984.

[3] A.L. Buchsbaum, R. Giancarlo, and J.R. Westbrook. On the determinization of weighted finite automata. *SIAM Journal of Computing*, pages 1502–1531, 2000.

[4] J. Chalopin and H. Leung. A note on factorization forests of finite height. *Theoretical Computer Science*, 310(1-3):489–499, 2004.

[5] C. Choffrut. Une caracterisation des fonctions sequentielles et des fonctions sous-sequentielles en tant que relations rationnelles. *Theoretical Computer Science*, 5(3):325–337, 1977.

[6] K. Culik II and J. Kari. Image compression using weighted finite automata. *Computer & Graphics*, 17:305–313, 1993.

[7] G. Grahne and A. Thomo. Approximate reasoning in semi-structured databases. In M. Lenzerini et al., editors, *8th International Workshop on Knowledge Representation meets Databases (KRDB2001)*, volume 45 of *CEUR Workshop Proceedings*, 2001.

[8] U. Hafner. *Low Bit-Rate Image and Video Coding with Weighted Finite Automata*. PhD thesis, Universität Würzburg, 1999.

[9] K. Hashiguchi. Algorithms for determining relative star height and star height. *Information and Computation*, 78:124–169, 1988.

[10] K. Hashiguchi. Improved limitedness theorems on finite automata with distance functions. *Theoretical Computer Science*, 72(1):27–38, 1990.

[11] K. Hashiguchi. New upper bounds to the limitedness of distance automata. *Theoretical Computer Science*, 233:19–32, 2000.

[12] K. Hashiguchi, K. Ishiguro, and S. Jimbo. Decidability of the equivalence problem for finitely ambiguous finance automata. *International Journal of Algebra and Computation*, 12(3):445–461, 2002.

[13] J. Hromkovič, J. Karhumäki, H. Klauck, G. Schnitger, and S. Seibert. Measures of nondeterminism in finite automata. In U. Montanari et al., editors, *ICALP'00 Proceedings*, volume 1853 of *Lecture Notes in Computer Science*, pages 199–210. Springer-Verlag, Berlin, 2000.

[14] J. Hromkovič, J. Karhumäki, H. Klauck, G. Schnitger, and S. Seibert. Communication complexity method for measuring nondeterminism in finite automata. *Information and Computation*, 172(2):202–217, 2002.

[15] O. Ibarra and B. Ravikumar. On sparseness, ambiguity and other decision problems for acceptors and transducers. In B. Monien and G. Vidal-Naquet, editors, *STACS'86 Proceedings*, volume 210 of *Lecture Notes in Computer Science*, pages 171 – 179. Springer-Verlag, Berlin, 1986.

[16] Z. Jiang, B. Litov, and O. de Vel. Similarity enrichments in image compression through weighted finite automata. In *COCOON'00 Proceedings*, volume 1858 of *Lecture Notes in Computer Science*, pages 447–456. Springer-Verlag, Berlin, 2000.

[17] F. Katritzke. *Refinements of Data Compression using Weighted Finite Automata*. PhD thesis, Universität Siegen, 2001.

[18] D. Kirsten. Distance desert automata and the star height problem. *R.A.I.R.O. - Informatique Théorique et Applications, special issue of selected best papers from FoSSaCS 2004*, 39(3):455–509, 2005.

[19] D. Kirsten and I. Mäurer. On the determinization of weighted automata. *Journal of Automata, Languages and Combinatorics*, 10(2/3):287–312, 2005.

[20] I. Klimann, S. Lombardy, J. Mairesse, and C. Prieur. Deciding unambiguity and sequentiality from a finitely ambiguous max-plus automaton. *Theoretical Computer Science*, 327(3):349–373, 2004.

[21] D. Krob. The equality problem for rational series with multiplicities in the tropical semiring is undecidable. *International Journal of Algebra and Computation*, 4(3):405–425, 1994.

[22] W. Kuich. Semirings and formal power series. In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Languages, Vol. 1, Word, Language, Grammar*, pages 609–677. Springer-Verlag, Berlin, 1997.

[23] W. Kuich and A. Salomaa, editors. *Semirings, Automata, Languages*, volume 5 of *Monographs in Theoretical Computer Science. An EATCS Series*. Springer-Verlag, Berlin, 1986.

[24] H. Leung. Limitedness theorem on finite automata with distance functions: An algebraic proof. *Theoretical Computer Science*, 81(1):137–145, 1991.

[25] H. Leung. Separating exponentially ambiguous finite automata from polynomially ambiguous finite automata. *SIAM Journal of Computing*, 27(4):1073–1082, 1998.

[26] H. Leung. The topological approach to the limitedness problem on distance automata. In J. Gunawardena, editor, *Idempotency*, pages 88–111. Cambridge University Press, 1998.

[27] H. Leung and V. Podolskiy. The limitedness problem on distance automata: Hashiguchi's method revisited. *Theoretical Computer Science*, 310(1-3):147–158, 2004.

[28] Y. Métivier and G. Richomme. New results on the star problem in trace monoids. *Information and Computation*, 119(2):240–251, 1995.

[29] M. Mohri. Finite-state transducers in language and speech processing. *Computational Linguistics*, 23:269–311, 1997.

[30] A. Salomaa and M. Soittola. *Automata-Theoretic Aspects of Formal Power Series*. Texts and Monographs on Computer Science. Springer-Verlag, Berlin Heidelberg New York, 1978.

[31] I. Simon. Recognizable sets with multiplicities in the tropical semiring. In M. P. Chytil et al., editors, *MFCS'88 Proceedings*, volume 324 of *Lecture Notes in Computer Science*, pages 107–120. Springer-Verlag, Berlin, 1988.

[32] I. Simon. Factorization forests of finite height. *Theoretical Computer Science*, 72:65–94, 1990.

[33] I. Simon. A short proof of the factorization forest theorem. In M. Nivat and A. Podelski, editors, *Tree Automata and Languages*, pages 433–438. Elsevier Science Publishers B.V., 1992.

[34] I. Simon. On semigroups of matrices over the tropical semiring. *R.A.I.R.O. - Informatique Théorique et Applications*, 28:277–294, 1994.

[35] A. Weber. Distance automata having large finite distance or finite ambiguity. *Mathematical Systems Theory*, 26:169–185, 1993.

[36] A. Weber. Finite valued distance automata. *Theoretical Computer Science*, 134:225–251, 1994.