Equivalence of Deterministic One-Counter Automata is NL-complete

Stanislav Böhm
Technical University of Ostrava

Stefan Göller
University of Bremen
CNRS/LIAFA

Petr Jančar
Technical University of Ostrava

ABSTRACT

We prove that language equivalence of deterministic one-counter automata is NL-complete. This improves the super-polynomial time complexity upper bound shown by Valiant and Paterson in 1975. Our main contribution is to prove that two deterministic one-counter automata are inequivalent if and only if they can be distinguished by a word of length polynomial in the size of the two input automata.

Categories and Subject Descriptors

F.1.1. [**Computation by Abstract Devices**]: Models of Computation; F.2.0 [**Analysis of Algorithms and Problem Complexity**]: General

Keywords

Language equivalence, Deterministic one-counter automata, Computational complexity

1. INTRODUCTION

In theoretical computer science, one of the most fundamental decision problems is the *equivalence problem* which asks whether two given machines behave equivalently. Among the various models of computation – such as Turing machines, random access machines and loop programs, just to mention a few of them – the equivalence problem already becomes undecidable when one imposes strong restrictions on their time and space consumption.

Emerging from formal language theory, a classical model of computation is that of pushdown automata. A folklore result is that already universality (and hence equivalence) of pushdown automata is undecidable. Concerning *deterministic pushdown automata (dpda)*, it is fair to say that the computer science community knows very little about the complexity of the equivalence problem.

Oyamaguchi proved that the equivalence problem for real-time dpda (dpda without ε-transitions) is decidable [12]. It took significant further innovation to show the decidability for general dpda, which is the celebrated result by Sénizergues [14], see also [15]. A couple of years later, Stirling showed that dpda equivalence is in fact primitive recursive [17], and his bound is still the best known upper bound for this problem. (A recent simplification of the proof [9] brings no improvement of the complexity bound.)

The upper bound by Stirling is far from the best known lower bound, i.e. from P-hardness (which straightforwardly follows from P-hardness of the emptiness problem). The same complexity gap persists even for real-time dpda. Thus, further subclasses of dpda have been studied. A coNP upper bound is known [16] for *finite-turn dpda* which are dpda where the number of switches between pushing and popping phases is bounded. For *simple dpda* (real-time single-state dpda), equivalence is even decidable in polynomial time [8] (see [4] for the currently best known upper bound).

Deterministic one-counter automata (doca) are one of the simplest infinite-state computational models, extending deterministic finite automata just with one nonnegative integer counter; doca are thus dpda over a singleton stack alphabet plus a bottom stack symbol. Doca were first studied by Valiant and Paterson in 1975 [18]; they showed that equivalence is decidable in time $2^{O(\sqrt{n \log n})}$, and a simple analysis of their proof reveals that the equivalence problem is in PSPACE. The problem is easily shown to be NL-hard, there is however an exponential gap between NL and PSPACE. There were attempts to settle the complexity of the doca equivalence problem (later we mention some) but the problem proved intricate. Though doca are perhaps not a notorious computational device, their close relation to finite automata and dpda has motivated us to tackle this research problem. Establishing NL-completeness for real-time doca [2] was a first step but it was far from clear if and how the proof can be extended to the general case.

One reason of the intricacy seems to be that a doca can exhibit a behaviour with exponential periodicity, demonstrated by the following example (which slightly adapts the version from [18]). We take a family $(\mathcal{A}_n)_{n\geq 1}$ where $\mathcal{A}_n$ is a doca accepting the regular language $L_n = \{a^m b_i \mid 1 \leq i \leq n, m \equiv 0 \pmod{p_i}\}$, where p_i denotes the i^{th} prime number. The index of the Myhill-Nerode congruence of L_n is obviously $2^{\Omega(n)}$ but we can easily construct $\mathcal{A}_n$ with $O(n^2 \log n)$ states. The example also demonstrates that doca are exponentially more succint than their real-time variant, since one can prove that real-time doca accepting L_n have $2^{\Omega(n)}$ states. Doca are also strictly more expressive than their real-time variant. Analogous expressiveness and succinctness results hold for dpda and real-time dpda, respectively.

STOC'13, June 1-4, 2013, Palo Alto, California, USA.

Our contribution. The main result here is that language equivalence of doca is NL-complete (while language inclusion is well-known to be undecidable); this closes the exponential complexity gap that has existed since 1970s when doca were introduced. Our approach helps to answer related questions as well; e.g., regularity of the language accepted by a given doca can be easily shown to be NL-complete.

Related work. Doca were introduced by Valiant and Paterson in [18], where the above-mentioned $2^{O(\sqrt{n \log n})}$ time upper bound for language equivalence was proven. Polynomial time algorithms for language equivalence and inclusion for strict subclasses of doca were provided in [6, 7]. In [1, 5] polynomial time learning algorithms were presented for doca. Simulation preorder and bisimulation equivalences on one-counter automata were studied in [3, 10, 11].
Remark: In [1, 13] it is stated that equivalence of doca can be decided in polynomial time. Unfortunately, the proofs provided in [1, 13] were not exact enough to be verified, and they raise several questions which are unanswered to date.

Overview of the proof. Instead of defining doca clasically as restricted dpda, we use a convenient equi-succinct way where we partition the control states (and thus the configurations) into *stable states*, in which the automaton waits for a letter to be read, and into *reset states*, in which the counter is reset to zero; in the latter case the residue class of the current counter value modulo the number, called a *period*, specified by the current reset state determines the successor (stable) state. (The periods correspond to the lengths of classical popping ε-cycles.) We explore *trace equivalence*, i.e. the classical language equivalence where all states are viewed as accepting. We use a natural notion of the *equivalence level*, the *eqlevel* for short, of two configurations, corresponding to the length of a shortest non-equivalence witness word, and stipulated to be ω when the configurations are equivalent. The formal definitions, and the ideas of a routine reduction from the classical setting to our setting, are given in Section 2. In Section 3 we prove the main theorem, saying that the eqlevels of two non-equivalent zero configurations are *small*, by which we mean that they are bounded by a polynomial (in the size of the given doca).

The only ingredient of our proof which we take directly from the previous works is a *cyclic form* of shortest positive paths in the transition system $\mathcal{T}(\mathcal{A})$ generated by a doca $\mathcal{A}$; this basic, but technical, fact was proven already in [18], and we recall it in Section 3.1.

Our central notion is the *extended deterministic transition system* $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ that is attached to a doca $\mathcal{A}$. Besides the standard transition system $\mathcal{T}(\mathcal{A})$, the extended system includes a special finite deterministic transition system that might be exponentially large in the size of $\mathcal{A}$ and that captures the *special mode* behaviour of $\mathcal{A}$. The special mode mimics the normal mode and is switched to the normal mode whenever a reset state is visited. The only difference is that when the zero counter value is reached (without a reset) then a multiple of all periods of the reset states is silently added to the counter; thus the counter never becomes zero in the special mode (until a reset state is visited and the normal mode applies). The above mentioned special finite system arises naturally once we note that the behaviour of a special mode configuration depends on the residue classes of the counter value modulo the periods of the reset states, and not on the concrete counter value itself.

Each normal configuration $p(m)$ (where p is the control state and m is the counter value) thus has the special mode counterpart $\bar{p}(m)$. A *crucial novelty* of our approach consists in an explicit definition of the above $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ and in a detailed analysis of the *quadruple* (b, ℓ, r, o) associated with a pair of configurations $(p(m), q(n))$ as follows (here EqL stands for *eqlevel*): $b = \mathsf{EqL}(p(m), q(n))$ (Basic), $\ell = \mathsf{EqL}(p(m), \bar{p}(m))$ (Left), $r = \mathsf{EqL}(q(n), \bar{q}(n))$ (Right), $o = \mathsf{EqL}(\bar{p}(m), \bar{q}(n))$ (mOd). A simple fact that $\min\{b, \ell, r, o\}$ must be equal to at least two components of (b, ℓ, r, o) turns out to be very useful.

For each non-equivalent pair $(p_0(m_0), q_0(n_0))$ with a shortest non-equivalence witness word w we define $(p_i(m_i), q_i(n_i))$ as the (stable) pair such that $p_0(m_0)$ is transformed to $p_i(m_i)$, and $q_0(n_0)$ is transformed to $q_i(n_i)$, by reading the prefix of w of length i. Each $(p_i(m_i), q_i(n_i))$ has the associated quadruple (b_i, ℓ_i, r_i, o_i), and we note that $b_i = b_0 - i$. Though we have in principle exponentially many pairs $(\bar{p}(m), \bar{q}(n))$, it is easy to show that the set of eqlevels $\{e \mid e = \mathsf{EqL}(\bar{p}(m), \bar{q}(n))\}$ is small (i.e., its cardinality is bounded by a polynomial); in other words, there are only few possible values o_i. A straightforward analysis also shows that for each natural number g there are only few $p(m)$ such that $\mathsf{EqL}(p(m), \bar{p}(m)) = g$. By using such observations we derive that if $m_0 = n_0 = 0$ then there are only few i such that $\ell_i \neq r_i$. Roughly speaking, $\ell_i = r_i < \omega$ implies that the counter values m_i and n_i are in one of only few linear relations. Hence if our sequence $(p_0(m_0), q_0(n_0))$, $(p_1(m_1), q_1(n_1))$, $(p_2(m_2), q_2(n_2))$, ... (with $m_0 = n_0 = 0$) was long then it would have a long segment where $\ell_i = r_i$ and the values m_i, n_i are increasing on the whole. We contradict the existence of such a long segment by another use of cyclicity and the properties of the quadruples (b, ℓ, r, o).

Sections 3.2–3.7 introduce $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ and the related useful notions; Sections 3.8 and 3.9 contain the main argument.

A complete version is at http://arxiv.org/abs/1301.2181.

2. DEFINITIONS AND RESULTS

By $\mathbb{N}$ we denote the set $\{0, 1, 2, \ldots\}$ of non-negative integers, and by $\mathbb{Z}$ the set of all integers. For a finite set X, by $|X|$ we denote its cardinality.

By Σ^* we denote the set of finite sequences of elements of Σ, i.e. of *words* over Σ. For $w \in \Sigma^*$, $|w|$ denotes the length of w. By ε we denote the empty word; hence $|\varepsilon| = 0$. If $w = uv$ then u is a *prefix* of w and v is a *suffix* of w.

By $\div$ we denote integer division; for $m, n \in \mathbb{N}$ where $n > 0$ we have $m = (m \div n) \cdot n + (m \bmod n)$. We use "mod" in two ways, clarified by the following example: $3 = 18 \bmod 5$, $8 \neq 18 \bmod 5$, $3 \equiv 18 \,(\mathrm{mod}\, 5)$, $8 \equiv 18 \,(\mathrm{mod}\, 5)$. For $m \in \mathbb{Z}$, $|m|$ denotes the absolute value of m.

We use ω to stand for infinity; we stipulate $z < \omega$ and $\omega + z = z + \omega = \omega$ for all $z \in \mathbb{Z}$.

A *deterministic labelled transition system*, a *det-LTS* for short, is a tuple

$$\mathcal{T} = (S_{\mathsf{St}}, S_\varepsilon, \Sigma, (\overset{a}{\mapsto})_{a \in \Sigma}, \overset{\varepsilon}{\mapsto})$$

where S_{St} and S_ε are disjoint sets of *stable states* and *unstable states*, respectively, Σ is a finite *alphabet*, $\overset{a}{\mapsto} \subseteq S_{\mathsf{St}} \times (S_{\mathsf{St}} \cup S_\varepsilon)$ for $a \in \Sigma$, and $\overset{\varepsilon}{\mapsto} \subseteq S_\varepsilon \times S_{\mathsf{St}}$ are sets of *labelled transitions*; for each $s \in S_\varepsilon$ there is precisely one $t \in S_{\mathsf{St}}$ such that $s \overset{\varepsilon}{\mapsto} t$, whereas for any $s \in S_{\mathsf{St}}$ and $a \in \Sigma$ there is at most one $t \in S_{\mathsf{St}} \cup S_\varepsilon$ such that $s \overset{a}{\mapsto} t$. For all $w \in \Sigma^*$, we define relations $\overset{w}{\longrightarrow} \subseteq S \times S$, where $S = S_{\mathsf{St}} \cup S_\varepsilon$, inductively: $s \overset{\varepsilon}{\longrightarrow} s$ for each $s \in S$; if $s \overset{\varepsilon}{\mapsto} t$ then $s \overset{\varepsilon}{\longrightarrow} t$; if $s \overset{a}{\mapsto} t$

$(a \in \Sigma)$ then $s \xrightarrow{a} t$; if $s \xrightarrow{u} s'$ and $s' \xrightarrow{v} t$ $(u, v \in \Sigma^*)$ then $s \xrightarrow{uv} t$. By $s \xrightarrow{w}$ we denote that w is *enabled in* s, i.e. $s \xrightarrow{w} t$ for some t.

Given $\mathcal{T} = (S_{\mathsf{St}}, S_\varepsilon, \Sigma, (\overset{a}{\mapsto})_{a\in\Sigma}, \overset{\varepsilon}{\mapsto})$, *trace equivalence* $\sim$ on $S = S_{\mathsf{St}} \cup S_\varepsilon$ is defined as follows:

$$s \sim t \quad \text{if} \quad \forall w \in \Sigma^* : s \xrightarrow{w} \Leftrightarrow t \xrightarrow{w}.$$

Hence two states are equivalent iff they enable the same set of words (also called traces). A word $w \in \Sigma^*$ is a *non-equivalence witness for* (s,t), a *witness for* (s,t) for short, if w is enabled in precisely one of s, t.

Remark. By the above definitions, $s \overset{\varepsilon}{\mapsto} t$ implies $s \sim t$. This suggests merging the states s and t but we keep them separate since this is convenient in the definitions of det-LTSs generated by deterministic one-counter automata.

We put $\Sigma^{\leq i} = \{w \in \Sigma^* : |w| \leq i\}$, and we note that $\sim = \bigcap\{\sim_i |\ i \in \mathbb{N}\}$ where the equivalences $\sim_0 \supseteq \sim_1 \supseteq \sim_2 \supseteq \ldots$ are defined as follows:

$$s \sim_i t \quad \text{if} \quad \forall w \in \Sigma^{\leq i} : s \xrightarrow{w} \Leftrightarrow t \xrightarrow{w}.$$

Each pair of states (s,t) has the *equivalence level*, the *eqlevel* for short, $\mathsf{EqL}(s,t) \in \mathbb{N} \cup \{\omega\}$:

$$\mathsf{EqL}(s,t) = \begin{cases} \omega & \text{if } s \sim t, \\ \max\{j \in \mathbb{N} \mid s \sim_j t\} & \text{otherwise.} \end{cases}$$

We also write $s \overset{e}{\longleftrightarrow} t$ instead of $\mathsf{EqL}(s,t) = e$ (where $e \in \mathbb{N} \cup \{\omega\}$). We note that the length of any *shortest* witness for (s,t), where $s \not\sim t$, is $\mathsf{EqL}(s,t)+1$. We also highlight the next simple fact (valid since our LTSs are *deterministic*).

Observation 1. *Suppose* $s \xrightarrow{w} s'$ *and* $t \xrightarrow{w} t'$ *in a given det-LTS. Then we have:*

1. $\mathsf{EqL}(s',t') \geq \mathsf{EqL}(s,t) - |w|$. *(Hence* $s' \sim t'$ *if* $s \sim t$.*)*
2. *If* w *is a prefix of a shortest witness for* (s,t) *then* $\mathsf{EqL}(s',t') = \mathsf{EqL}(s,t) - |w|$.

Deterministic one-counter automata, *doca* for short, are deterministic pushdown automata in which the stack alphabet is $\{0,1\}$ and the stack can only contain words of the form 1^n0, $n \geq 0$, where 0 is always at the bottom of the stack. For convenience we use the following definition of doca, adding a remark on its relation to the standard definition later.

A *doca* is a tuple

$$\mathcal{A} = (Q_{\mathsf{St}}, Q_{\mathsf{Res}}, \Sigma, \delta, (\mathsf{per}_s)_{s\in Q_{\mathsf{Res}}}, (\mathsf{goto}_s)_{s\in Q_{\mathsf{Res}}}) \qquad (1)$$

where Q_{St} and Q_{Res} are disjoint finite sets of *stable control states* and *reset control states*, respectively, Σ is a finite *alphabet*, $\delta \subseteq Q_{\mathsf{St}} \times \Sigma \times \{0,1\} \times (Q_{\mathsf{St}} \cup Q_{\mathsf{Res}}) \times \{-1,0,1\}$ is a set of *(transition) rules*, $\mathsf{per}_s \in \mathbb{N}$ are *periods* satisfying $1 \leq \mathsf{per}_s \leq |Q_{\mathsf{St}}|$, and $\mathsf{goto}_s : \{0,1,2,\ldots,\mathsf{per}_s-1\} \to Q_{\mathsf{St}}$ are *reset mappings*. For each $p \in Q_{\mathsf{St}}$, $a \in \Sigma$, $c \in \{0,1\}$ there is at most one pair (q,j) (where $q \in Q_{\mathsf{St}} \cup Q_{\mathsf{Res}}$, $j \in \{-1,0,1\}$) such that $(p,a,c,q,j) \in \delta$; moreover, if $c = 0$ then $j \neq -1$. The tuples $(p,a,0,q,j) \in \delta$ are called the *zero rules*, the tuples $(p,a,1,q,j) \in \delta$ are the *positive rules*.

A doca $\mathcal{A}$ as in (1) defines the det-LTS

$$\mathcal{T}(\mathcal{A}) = (Q_{\mathsf{St}} \times \mathbb{N}, Q_{\mathsf{Res}} \times \mathbb{N}, \Sigma, (\overset{a}{\mapsto})_{a\in\Sigma}, \overset{\varepsilon}{\mapsto}) \qquad (2)$$

where $\overset{a}{\mapsto}$ and $\overset{\varepsilon}{\mapsto}$ are defined by the following (deduction) rules.

1. If $(p,a,1,q,j) \in \delta$ and $n > 0$ then $(p,n) \overset{a}{\mapsto} (q, n+j)$.
2. If $(p,a,0,q,j) \in \delta$ then $(p,0) \overset{a}{\mapsto} (q,j)$. (Recall that $j \in \{0,1\}$ in this case.)
3. If $s \in Q_{\mathsf{Res}}$ and $n \geq 0$ then $(s,n) \overset{\varepsilon}{\mapsto} (q,0)$ where $q = \mathsf{goto}_s(n \bmod \mathsf{per}_s)$.

An example of a doca with the respective det-LTS is sketched in Fig. 1.

By a *configuration* C of the doca $\mathcal{A}$ we mean (p,m), usually written as $p(m)$, where p is its control state and $m \in \mathbb{N}$ is its *counter value*. If $C = p(0)$ then it is a *zero configuration*. If $p \in Q_{\mathsf{St}}$ then $C = p(m)$ is a *stable configuration*; if $p \in Q_{\mathsf{Res}}$ then $p(m)$ is a *reset configuration*.

The definition of (general) det-LTSs induces the relations $\xrightarrow{w}$ $(w \in \Sigma^*)$ on $Q \times \mathbb{N}$ where $Q = Q_{\mathsf{St}} \cup Q_{\mathsf{Res}}$. We are interested in the *doca equivalence problem*, denoted

Doca-Eq:

Instance: A doca $\mathcal{A}$ and two stable zero configurations $p(0), q(0)$.

Question: Is $p(0) \sim q(0)$ in $\mathcal{T}(\mathcal{A})$?

Our main aim is to show the following theorem.

Theorem 2. *There is a polynomial* poly $: \mathbb{N} \to \mathbb{N}$ *such that for any Doca-Eq instance* $\mathcal{A}, p(0), q(0)$ *where* $\mathcal{A}$ *has* k *control states we have that* $p(0) \not\sim q(0)$ *implies* $\mathsf{EqL}(p(0), q(0)) \leq \text{poly}(k)$.

By Theorem 2 we easily get the upper bound in the next theorem; the lower bound is implied by digraph reachability.

Theorem 3. *Doca-Eq is* NL*-complete.*

Remark. Classically a doca is a tuple $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ where q_0 is the *initial state* and $F \subseteq Q$ are the *accepting states*. Here δ can contain $(p, \varepsilon, c, q, j)$ $(c \in \{0,1\})$ if it does not contain (p,a,c,q',j') for any $a \in \Sigma$; moreover, for each $p \in Q$, $a \in \Sigma \cup \{\varepsilon\}$ and $c \in \{0,1\}$ there is at most one pair (q,j) such that $(p,a,c,q,j) \in \delta$. The *language accepted by* $\mathcal{A}$ is defined as $L(\mathcal{A}) = \{w \in \Sigma^* \mid q_0(0) \xrightarrow{w} q(n)$ for some $q \in F, n \in \mathbb{N}\}$. Such a doca $\mathcal{A}$, with k control states, can be routinely replaced by a language-equivalent doca $\mathcal{A}_{\mathsf{SC}}$ (with the "Shrinked Counter"), where a configuration $p(m)$ of $\mathcal{A}$ is represented by the configuration $p_i(j)$ of $\mathcal{A}_{\mathsf{SC}}$ where $i = (m \bmod k)$ and $j = (m \div k)$. A straightforward modification then restricts the ε-rules to the form $(p, \varepsilon, 1, q, -1)$, which then easily leads to our above form with stable and reset control states. A reduction from language equivalence to trace equivalence is also simple: if a stable configuration has no outgoing a-transition then we add it and lead to a special "sink loop state"; we then arrange that accepting control states are stable and add to them a loop-transition with a special fresh action.

3. PROOF OF THEOREM 2

Convention. When considering a doca $\mathcal{A}$, we will always tacitly assume the notation (1) if not said otherwise. We also reserve k for denoting the number of control states, i.e.

$$k = |Q_{\mathsf{St}}| + |Q_{\mathsf{Res}}|.$$

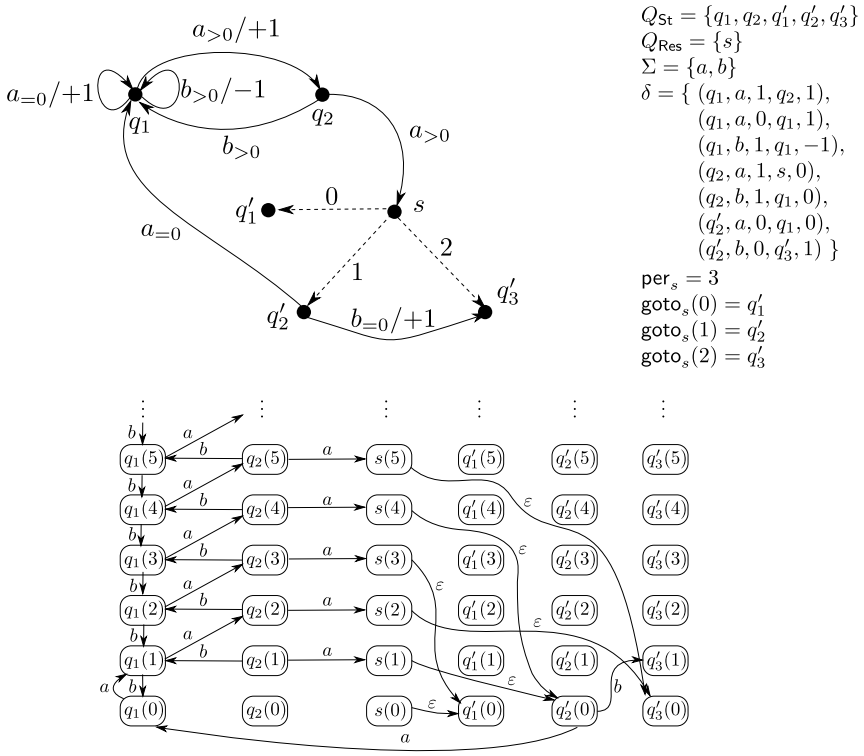

Figure 1: A doca $\mathcal{A}$, presented by a graph, and a fragment of $\mathcal{T}(\mathcal{A})$

To be more concise in the later reasoning concerning a given doca $\mathcal{A}$, we use the words "few", "small", or "short" when we mean that the relevant quantity is bounded by a polynomial in k; the polynomial is always independent of $\mathcal{A}$. By a small rational number we mean $\rho = \frac{a}{b}$ or $\rho = -\frac{a}{b}$ where $a, b \in \mathbb{N}$ are small. We also say that

a set is small if its cardinality is a small number.

We note that if all elements of a set X of (integer or rational) numbers are small then X is a small set; the opposite is not true in general. We often tacitly use the fact that

a quantity arising as the sum or the product of two small quantities is also small.

Though these expressions might look informal, they can be always easily replaced by the formal statements which they abridge. By this convention, Theorem 2 says that the eqlevel of any pair of zero configurations is small when finite.

Remark. It will be always obvious that we could calculate a concrete respective polynomial whenever we use "few", "small", "short" in our claims. But such calculations would add tedious technicalities, and they would be not particularly rewarding w.r.t. the degree of the polynomials. We thus prefer a transparent concise proof which avoids technicalities whenever possible.

3.1 Shortest positive paths in $\mathcal{T}(\mathcal{A})$

We first define the notion of paths in general det-LTSs, and then we look at special paths in $\mathcal{T}(\mathcal{A})$, for a doca $\mathcal{A}$.

Definition 4. *Let $\mathcal{T} = (S_{\mathsf{St}}, S_\varepsilon, \Sigma, (\overset{a}{\mapsto})_{a\in\Sigma}, \overset{\varepsilon}{\mapsto})$ be a det-LTS. A* path *in $\mathcal{T}$ is a sequence*

$$s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \dots \xrightarrow{a_z} s_z \ (z \in \mathbb{N})$$

where $s_i \in S_{\mathsf{St}}$ and $a_i \in \Sigma$ (for all $i, 0 \le i \le z$); it is a path from its start s_0 to its end s_z. *For any i_1, i_2, where $0 \le i_1 \le i_2 \le z$, the sequence $s_{i_1} \xrightarrow{a_{i_1+1}} s_{i_1+1} \xrightarrow{a_{i_1+2}} \cdots \xrightarrow{a_{i_2}} s_{i_2}$ is a* subpath *of the above path. Slightly abusing notation, we will also use $s \xrightarrow{w}$ and $s \xrightarrow{w} t$ ($s, t \in S_{\mathsf{St}}$) to denote paths.*

We also refer to $s \xrightarrow{a} t$ where $s, t \in S_{\mathsf{St}}$ and $a \in \Sigma$ as to a step. *If $s \overset{a}{\mapsto} t$ then it is a* simple step*; if $s \overset{a}{\mapsto} s' \overset{\varepsilon}{\mapsto} t$ then it is a* combined step. *The* length of a path $s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \dots \xrightarrow{a_z} s_z$ *is z, i.e. the number of its steps.*

When discussing the det-LTS $\mathcal{T}(\mathcal{A})$ for a doca $\mathcal{A}$, we use the term *reset steps* instead of combined steps. We now concentrate on positive paths in $\mathcal{T}(\mathcal{A})$, defined as follows.

Definition 5. *Given a doca $\mathcal{A}$ (in notation (1)), a* path

$$p_0(m_0) \xrightarrow{a_1} p_1(m_1) \xrightarrow{a_2} \cdots \xrightarrow{a_z} p_z(m_z) \qquad (3)$$

in $\mathcal{T}(\mathcal{A})$ is positive *if each step $p_i(m_i) \xrightarrow{a_{i+1}} p_{i+1}(m_{i+1})$ ($0 \le i < z$) is simple and is induced by a positive rule $(p_i, a_{i+1}, 1, p_{i+1}, j) \in \delta$ (where $j = m_{i+1} - m_i$).*

The effect *(or the* counter change*)* of the path *(3) is $m_z - m_0$; if the path is positive, its effect is an integer in the interval $[-z, z]$. The path (3) is a* control state cycle *if it is positive and we have $z > 0$ and $p_z = p_0$.*

We note that if (3) is positive then there is no reset step in the path and $m_i > 0$ for all $i, 0 \le i < z$; but we can have $m_z = 0$.

The next lemma can be easily derived from Lemma 2 in [18]. The claim is illustrated in Fig. 2: if there is a positive path from C to C' with a big difference of the counter

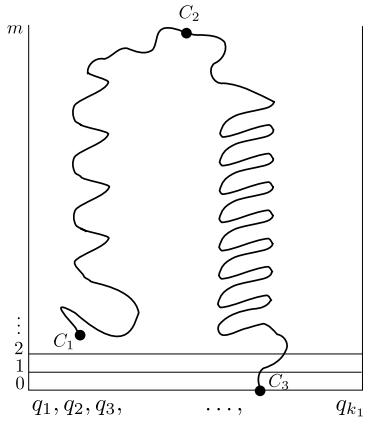

Figure 2: Shortest positive paths in $\mathcal{T}(\mathcal{A})$, one from a configuration C_1 to C_2 and one from C_2 to a zero configuration C_3. (Only the stable control states $q_1, q_2, \ldots, q_{k_1}$ are depicted.)

values then a shortest such path uses a short repeated cycle, besides a short prefix and a short suffix.

LEMMA 6. *If there is a positive path from $p(m)$ to $q(n)$ in $\mathcal{T}(\mathcal{A})$ then some of the shortest positive paths from $p(m)$ to $q(n)$ is of the form*

$$p(m) \xrightarrow{u_1} p'(m') \xrightarrow{v^i} p'(m'+id) \xrightarrow{u_2} q(n)$$

where u_1 is a short word, called the pre-phase, *$p'(m') \xrightarrow{v} p'(m'+d)$ is a short control state cycle with the effect $d \in \mathbb{Z}$, and u_2 is a short word, called the* post-phase. *(The cycle v is repeated i times, where $i \geq 0$.)*

We also note the following corollary:

COROLLARY 7. *If $|m-n|$ is small and there is a positive path from $p(m)$ to $q(n)$ then there is a short positive path from $p(m)$ to $q(n)$.*

3.2 The extended det-LTS $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$

We now introduce a central notion, the det-LTS $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$, which extends the det-LTS $\mathcal{T}(\mathcal{A})$ defined in (2), for a given doca $\mathcal{A} = (Q_{\mathsf{St}}, Q_{\mathsf{Res}}, \Sigma, \delta, (\mathsf{per}_s)_{s\in Q_{\mathsf{Res}}}, (\mathsf{goto}_s)_{s\in Q_{\mathsf{Res}}})$. We formalize the intuition described in the introduction. The det-LTS $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ arises from $\mathcal{T}(\mathcal{A})$ by adding the set Q_{Mod} of stable states, the set Q_{FixRes} of unstable states, and the transitions from Q_{Mod} and Q_{FixRes}, all defined below. The transitions from Q_{Mod} will only lead to $Q_{\mathsf{Mod}} \cup Q_{\mathsf{FixRes}}$, whereas the ε-transitions from Q_{FixRes} lead to zero configurations in $\mathcal{T}(\mathcal{A})$. There are no transitions leading from the configurations in $\mathcal{T}(\mathcal{A})$ to $Q_{\mathsf{Mod}} \cup Q_{\mathsf{FixRes}}$, and the subgraph of $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ arising by the restriction to the configurations of $\mathcal{T}(\mathcal{A})$ is $\mathcal{T}(\mathcal{A})$ itself. We thus also safely use the same symbols $\overset{a}{\mapsto}$, $\overset{\varepsilon}{\mapsto}$ in both $\mathcal{T}(\mathcal{A})$ and $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$. An example is sketched in Fig. 3.

DEFINITION 8. *Given a doca $\mathcal{A}$ as in (1), with the associated det-LTS $\mathcal{T}(\mathcal{A})$ (recall (2)), we define the det-LTS*

$$\mathcal{T}_{\mathsf{ext}}(\mathcal{A}) = \\ ((Q_{\mathsf{St}} \times \mathbb{N}) \cup Q_{\mathsf{Mod}}, (Q_{\mathsf{Res}} \times \mathbb{N}) \cup Q_{\mathsf{FixRes}}, \Sigma, (\overset{a}{\mapsto})_{a\in\Sigma}, \overset{\varepsilon}{\mapsto})$$

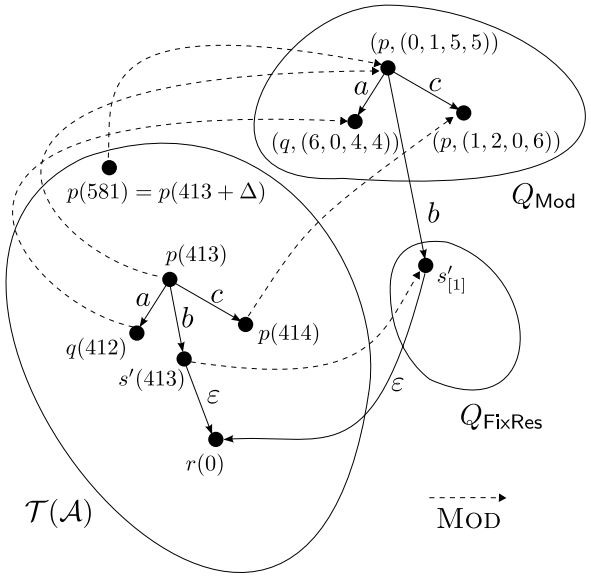

Figure 3: A fragment of $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ where: $\{p,q,r\} \subseteq Q_{\mathsf{St}}$, $Q_{\mathsf{Res}} = \{s,s',s'',s'''\}$, $\{a,b,c\} \subseteq \Sigma$, $\{(p,a,1,q,-1),(p,b,1,s',0),(p,c,1,p,1)\} \subseteq \delta$, $(\mathsf{per}_s, \mathsf{per}_{s'}, \mathsf{per}_{s''}, \mathsf{per}_{s'''}) = (7,4,6,8)$, $\mathsf{goto}_{s'}(1) = r$, $\Delta = lcm\{7,4,6,8\} = 168$.

as the extension of $\mathcal{T}(\mathcal{A})$ where

- $Q_{\mathsf{Mod}} = \{(p,(c_s)_{s\in Q_{\mathsf{Res}}}) \mid p \in Q_{\mathsf{St}}, 0 \leq c_s \leq \mathsf{per}_s - 1\}$,
- $Q_{\mathsf{FixRes}} = \{s_{[c]} \mid s \in Q_{\mathsf{Res}}, 0 \leq c \leq \mathsf{per}_s - 1\}$, *and*
- *the additional transitions are defined by the following (deduction) rules:*

  1. *If $(p,a,1,q,j) \in \delta$ and $q \in Q_{\mathsf{St}}$ then for each $(p,(c_s)_{s\in Q_{\mathsf{Res}}}) \in Q_{\mathsf{Mod}}$ we have*

     $$(p,(c_s)_{s\in Q_{\mathsf{Res}}}) \overset{a}{\mapsto} (q,(c'_s)_{s\in Q_{\mathsf{Res}}})$$

     where $c'_s = (c_s+j) \bmod \mathsf{per}_s$ for each $s \in Q_{\mathsf{Res}}$.
  2. *If $(p,a,1,s',j) \in \delta$ and $s' \in Q_{\mathsf{Res}}$ then for each $(p,(c_s)_{s\in Q_{\mathsf{Res}}}) \in Q_{\mathsf{Mod}}$ we have*

     $$(p,(c_s)_{s\in Q_{\mathsf{Res}}}) \overset{a}{\mapsto} s'_{[c]}$$

     where $c = (c_{s'}+j) \bmod \mathsf{per}_{s'}$.
  3. *For each $s_{[c]} \in Q_{\mathsf{FixRes}}$ we have $s_{[c]} \overset{\varepsilon}{\mapsto} q(0)$ where $q = \mathsf{goto}_s(c)$.*

A configuration *C is a state in $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$. If $C \in Q_{\mathsf{Mod}}$ or $C = p(m)$ where $p \in Q_{\mathsf{St}}$ then C is* stable, *otherwise C is* unstable.

Moreover, we define the mapping

$$\mathsf{Mod} : ((Q_{\mathsf{St}} \cup Q_{\mathsf{Res}}) \times \mathbb{N}) \to (Q_{\mathsf{Mod}} \cup Q_{\mathsf{FixRes}})\text{:}$$

- *if $p \in Q_{\mathsf{St}}$ then $\mathsf{Mod}(p(m)) = (p,(c_s)_{s\in Q_{\mathsf{Res}}}) \in Q_{\mathsf{Mod}}$ where $c_s = m \bmod \mathsf{per}_s$ for all $s \in Q_{\mathsf{Res}}$;*
- *if $s \in Q_{\mathsf{Res}}$ then $\mathsf{Mod}(s(m)) = s_{[c]} \in Q_{\mathsf{FixRes}}$ where $c = m \bmod \mathsf{per}_s$.*

We note that the cardinality of Q_{Mod} might be exponential in k (i.e. in the number of control states of $\mathcal{A}$); on the other hand, Q_{FixRes} is small. The next propositions can be easily derived from the definition of $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$. We stipulate $\min \emptyset = \omega$, and recall that $z + \omega = \omega$ for any $z \in \mathbb{N}$.

PROPOSITION 9.

1. *If* $(p,(c_s)_{s\in Q_{\mathsf{Res}}}) \xrightarrow{w} (q,(c'_s)_{s\in Q_{\mathsf{Res}}})$ *then for each* $(p,(d_s)_{s\in Q_{\mathsf{Res}}}) \in Q_{\mathsf{Mod}}$ *we have* $(p,(d_s)_{s\in Q_{\mathsf{Res}}}) \xrightarrow{w} (q,(d'_s)_{s\in Q_{\mathsf{Res}}})$ *where* $d'_s - c'_s \equiv d_s - c_s \pmod{\mathsf{per}_s}$ *for all* $s \in Q_{\mathsf{Res}}$.
2. *If* $(p,(c_s)_{s\in Q_{\mathsf{Res}}}) \xrightarrow{w} s'_{[c]}$ *then for each* $(p,(d_s)_{s\in Q_{\mathsf{Res}}}) \in Q_{\mathsf{Mod}}$ *we have* $(p,(d_s)_{s\in Q_{\mathsf{Res}}}) \xrightarrow{w} s'_{[d]}$ *where* $d - c \equiv d_{s'} - c_{s'} \pmod{\mathsf{per}_{s'}}$.
3. *For any* $s \in Q_{\mathsf{Res}}$ *we have* $s(m) \sim \mathsf{Mod}(s(m))$.
4. *If* $p \in Q_{\mathsf{St}}$ *then* $\mathsf{EqL}(p(m), \mathsf{Mod}(p(m))) = \min\{z + \mathsf{EqL}(q(0), \mathsf{Mod}(q(0))) \mid q \in Q_{\mathsf{St}}$ *and* z *is the length of a positive path from* $p(m)$ *to* $q(0)\}$.
5. *For any* $p \in Q_{\mathsf{St}}$, $m \in \mathbb{N}$, *and* $w \in \Sigma^*$ *there is some small positive* $d \in \mathbb{N}$ *such that*
   - *either for each* m' *such that* $m' \equiv m \pmod d$ *we have that* $\mathsf{Mod}(p(m'))$ *enables* w,
   - *or for each* m' *such that* $m' \equiv m \pmod d$ *we have that* $\mathsf{Mod}(p(m'))$ *does not enable* w.

We recall that $C \xleftrightarrow{e} C'$ denotes that $\mathsf{EqL}(C, C') = e$.

PROPOSITION 10.

1. *For any* $p, q \in Q_{\mathsf{St}}$ *and* $m, n \in \mathbb{N}$ *there are small positive* $d_1, d_2 \in \mathbb{N}$ *such that for any* $m', n' \in \mathbb{N}$ *we have: if* $m' \equiv m \pmod{d_1}$ *and* $n' \equiv n \pmod{d_2}$ *then*
$$\mathsf{EqL}(\mathsf{Mod}(p(m')), \mathsf{Mod}(q(n'))) \leq \mathsf{EqL}(\mathsf{Mod}(p(m)), \mathsf{Mod}(q(n))).$$
2. *The set* $\{e \mid$ *there are* $C, C' \in Q_{\mathsf{Mod}}$ *s.t.* $C \xleftrightarrow{e} C'\}$ *is small.*

PROPOSITION 11.

1. *For any* $p, q \in Q_{\mathsf{St}}$ *and* $m, n \in \mathbb{N}$ *there is some small positive* $d \in \mathbb{N}$ *such that for any* $m' \in \mathbb{N}$ *we have: if* $m' \equiv m \pmod d$ *then*
$$\mathsf{EqL}(\mathsf{Mod}(p(m')), q(n)) \leq \mathsf{EqL}(\mathsf{Mod}(p(m)), q(n)).$$
2. *For any (fixed)* $q(n)$, *the set* $\{e \mid$ *there is* $C \in Q_{\mathsf{Mod}}$ *s.t.* $C \xleftrightarrow{e} q(n)\}$ *is small.*

3.3 Eqlevels of pairs of zero configurations

Let us recall $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ defined in Def. 8. We could view the elements of $Q_{\mathsf{Mod}} \cup Q_{\mathsf{FixRes}}$ as additional control states of $\mathcal{A}$; in these states the counter value would play no role and could be formally viewed as zero. This observation justifies the name "zero configurations" in the following definition.

DEFINITION 12. *Given a doca* $\mathcal{A}$ *as in (1), with the associated* $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ *by Def. 8, a state* C *in* $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$ *is a* zero configuration *if either* $C \in Q_{\mathsf{Mod}} \cup Q_{\mathsf{FixRes}}$ *or* $C = p(0)$ *where* $p \in Q_{\mathsf{St}} \cup Q_{\mathsf{Res}}$. *We define the set* $\mathrm{ZE} \subseteq \mathbb{N}$ *(Zero configurations Eqlevels) as follows:*

$$\mathrm{ZE} = \{e \in \mathbb{N} \mid \textit{there are two stable zero configurations } C, C' \textit{ s.t. } C \xleftrightarrow{e} C'\}.$$

We thus have $\mathrm{ZE} = \mathrm{E}_1 \cup \mathrm{E}_2 \cup \mathrm{E}_3$ where

$\mathrm{E}_1 = \{e \in \mathbb{N} \mid p(0) \xleftrightarrow{e} q(0)$ for some $p, q \in Q_{\mathsf{St}}\}$,
$\mathrm{E}_2 = \{e \in \mathbb{N} \mid p(0) \xleftrightarrow{e} C$ for some $p \in Q_{\mathsf{St}}, C \in Q_{\mathsf{Mod}}\}$,
$\mathrm{E}_3 = \{e \in \mathbb{N} \mid C \xleftrightarrow{e} C'$ for some $C, C' \in Q_{\mathsf{Mod}}\}$.

Since the set $\{p(0) \mid p \in Q_{\mathsf{St}}\}$ is obviously small, by Prop. 10(2) and 11(2) we easily derive the following claim.

LEMMA 13. *The set* ZE *is small.*

The lemma does not claim that the elements of ZE are small numbers. This will be shown in the following subsections; we will thus prove the next strengthening of Theorem 2.

THEOREM 14. *There is a polynomial* $\mathrm{POLY} : \mathbb{N} \to \mathbb{N}$ *such that* $\max\{e \mid e \in \mathrm{ZE}\} \leq \mathrm{POLY}(k)$ *(for any doca* $\mathcal{A}$ *with* k *control states).*

Let $e_0 < e_1 < e_2 < \cdots < e_f$ be the ordered elements of ZE. We have shown that f is small but we have not yet shown that all e_i are small numbers. W.l.o.g. we can assume $e_0 = 0$ (by adding two special control states, say). For proving Theorem 14 it thus suffices to show that the "gaps" between e_i and e_{i+1}, i.e. the differences $e_{i+1} - e_i$, are small. We will later contradict the existence of a large gap between $e_i = e_D$ (Down) and $e_{i+1} = e_U$ (Up) depicted in Figure 4.

$e_0 - - e_1 - \cdots - e_D - e_U - \cdots - e_f$

Figure 4: Assumption of a large gap in ZE (to be contradicted later)

But we first explore some further notions related to a given doca $\mathcal{A}$ and the det-LTS $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$.

3.4 Independence level

We assume a doca $\mathcal{A}$ as in (1), and explore a notion which we have already touched on.

DEFINITION 15. *For* $p \in Q_{\mathsf{St}}$, $m \in \mathbb{N}$ *we put*
$$\mathsf{IL}(p(m)) = \mathsf{EqL}(p(m), \mathsf{Mod}(p(m))).$$

$\mathsf{IL}(p(m))$ can be understood as an "Independence Level" of $p(m)$ w.r.t. the concrete value m. The next proposition can be derived easily from Prop. 9(4) and Lemma 6 (and Fig. 2).

PROPOSITION 16. *For each* $p(m)$ *with* $\mathsf{IL}(p(m)) < \omega$ *there are small rational numbers* ρ, σ *(of the type* $\frac{a}{b}$, $-\frac{a}{b}$ *where* $a, b \in \mathbb{N}$ *are small) and some* $q \in Q_{\mathsf{St}}$ *such that*
$$\mathsf{IL}(p(m)) = \rho \cdot m + \sigma + \mathsf{IL}(q(0)).$$
Moreover, we can require $\rho \geq 0$, $\rho \cdot m + \sigma \geq 0$, *and if* m *is larger than a small bound then* $\rho > 0$.

Convention. We will further assume that each $p(m)$ with $\mathsf{IL}(p(m)) < \omega$ has a fixed associated equality $\mathsf{IL}(p(m)) = \rho \cdot m + \sigma + e$ where $e = \mathsf{IL}(q(0)) \in \mathrm{ZE}$ and ρ, σ, q have the claimed properties.

Figure 5 depicts $\mathsf{IL}(p(m))$ for a fixed $p \in Q_{\mathsf{St}}$ and for a few values m, by using black circles $\bullet$; e_1, e_2, e_3 are elements of ZE corresponding to $\mathsf{IL}(q(0))$ for several q. There

might be some "irregular" values $\mathsf{IL}(p(m)) = z + \mathsf{IL}(q(0))$ for small m and small z but for m larger than a small bound the values $\mathsf{IL}(p(m))$ lie on few lines, starting near some e_j and having small slopes. (In fact, we have $1 \leq \frac{|v|}{|\mathsf{effect}(v)|} \leq k$ for the respective cycles v in $w = u_1 v^i u_2$; the unit-length for the vertical axis is thus smaller than for the horizontal axis in Fig. 5.) The circles $\bullet$ and $\circ$ on one depicted line can correspond to the pairs $(m_0, z_0 + \mathsf{IL}(q(0)))$, $(m_0 + d, z_0 + d' + \mathsf{IL}(q(0)))$, $(m_0 + 2d, z_0 + 2d' + \mathsf{IL}(q(0)))$, ... where $d = |\mathsf{effect}(v)|$ and $d' = |v|$ (and $z_0 = |u_1 u_2|$, $z_0 + d' = |u_1 v u_2|$, $z_0 + 2d' = |u_1 v^2 u_2|$, ...). A white circle $\circ$ depicts that the respective value, corresponding to a positive path $p(m_0{+}id) \xrightarrow{u_1 v^i u_2} q(0)$, is not $\mathsf{IL}(p(m_0{+}id))$ since there is another, and shorter, witness in this case.

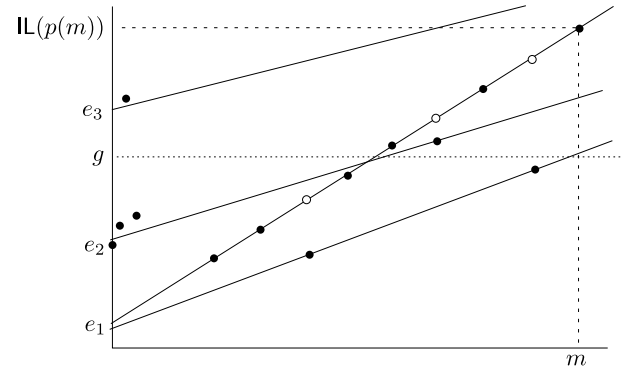

Figure 5: Illustrating $\mathsf{IL}(p(m))$ as a function of m

We now observe some further facts for later use.

PROPOSITION 17.

1. *For each $g \in \mathbb{N}$ there are only few $p(m)$ such that $\mathsf{IL}(p(m)) = g$.*
2. *For any $p(m)$ where $\mathsf{IL}(p(m)) < \omega$ there are some small numbers $\mathsf{base} \geq 0$ and $\mathsf{per} > 0$ such that the following condition holds:*
   for any m' such that $\mathsf{base} \leq m' < m$ and $m' \equiv m \pmod{\mathsf{per}}$ we have $\mathsf{IL}(p(m')) < \mathsf{IL}(p(m))$.

3.5 Eqlevel tuples

We introduce the eqlevel tuples illustrated in Fig. 6, assuming a given doca $\mathcal{A}$ as in (1), with the associated det-LTSs $\mathcal{T}(\mathcal{A})$ and $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$. A simple property of these tuples considerably simplifies the later analysis.

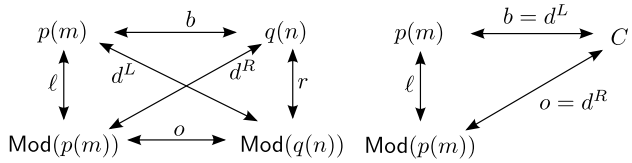

Figure 6: Eqlevel tuple $(b, \ell, r, o, d^L, d^R)$ associated to $(p(m), q(n))$, and to $(p(m), C)$ where $C \in Q_{\mathsf{Mod}}$.

DEFINITION 18. *(See Fig. 6.) Each pair $(p(m), q(n))$ of stable configurations in $\mathcal{T}(\mathcal{A})$ has the* associated eqlevel tuple *$(b, \ell, r, o, d^L, d^R)$ (of elements from $\mathbb{N} \cup \{\omega\}$) defined as follows: $b = \mathsf{EqL}(p(m), q(n))$ (Basic), $\ell = \mathsf{IL}(p(m))$ (Left), $r = \mathsf{IL}(q(n))$ (Right), $o = \mathsf{EqL}(\mathsf{Mod}(p(m)), \mathsf{Mod}(q(n)))$ (mOd), $d^L = \mathsf{EqL}(p(m), \mathsf{Mod}(q(n)))$ (Diagonal Left), $d^R = \mathsf{EqL}(q(n), \mathsf{Mod}(p(m)))$ (Diagonal Right).*

Each pair $(p(m), C)$ where $C \in Q_{\mathsf{Mod}}$ and $p(m)$ is a stable configuration in $\mathcal{T}(\mathcal{A})$ has the associated eqlevel tuple *$(b, \ell, r, o, d^L, d^R)$ defined as follows: $b = d^L = \mathsf{EqL}(p(m), C)$, $\ell = \mathsf{IL}(p(m))$, $r = \omega$, $o = d^R = \mathsf{EqL}(\mathsf{Mod}(p(m)), C)$.*

The analogous tuple associated to $(C, q(n))$ is not needed in later reasoning. The next proposition trivially follows from the fact that $\sim_i$ are equivalences; it holds for general LTSs but we confine ourselves to the introduced det-LTSs.

PROPOSITION 19. *Given states $s_1, s_2, \ldots, s_m$ in a det-LTS where $m \geq 2$ and $s_1 \xleftrightarrow{e_1} s_2$, $s_2 \xleftrightarrow{e_2} s_3$, ..., $s_{m-1} \xleftrightarrow{e_{m-1}} s_m$, $s_m \xleftrightarrow{e_m} s_1$, the minimum of $\{e_1, e_2, \ldots, e_m\}$ cannot be e_i for just one i.*

COROLLARY 20. *In the "triangle" (b, ℓ, d^R), we always have $b = \ell$ or $b = d^R$ or $\ell = d^R$ (or $b = \ell = d^R$) as the minimum. Similarly for the "triangles" (d^R, r, o), (b, d^L, r), and (ℓ, d^L, o). In the "rectangle" (b, ℓ, r, o), the minimum is also achieved by at least two elements (concretely by $b = \ell$, $b = r$, $b = o$, $\ell = r$, $\ell = o$, or $r = o$).*

3.6 Paths in $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$

Since we are interested in comparing two states in a det-LTS $\mathcal{T}$, it is useful to define the product $\mathcal{T} \times \mathcal{T}$; the transitions in $\mathcal{T} \times \mathcal{T}$ are just the letter-synchronized pairs of transitions in $\mathcal{T}$. Eqlevel-decreasing paths in $\mathcal{T} \times \mathcal{T}$ will be of particular interest. A formal definition follows.

DEFINITION 21. *Let $\mathcal{T} = (S_{\mathsf{St}}, S_\varepsilon, \Sigma, (\overset{a}{\mapsto})_{a \in \Sigma}, \overset{\varepsilon}{\mapsto})$ be a det-LTS. We define the det-LTS*

$$\mathcal{T} \times \mathcal{T} = (S_{\mathsf{St}} \times S_{\mathsf{St}}, S'_\varepsilon, \Sigma, (\overset{a}{\mapsto})_{a \in \Sigma}, \overset{\varepsilon}{\mapsto})$$

where $S'_\varepsilon = (S_{\mathsf{St}} \times S_\varepsilon) \cup (S_\varepsilon \times S_{\mathsf{St}}) \cup (S_\varepsilon \times S_\varepsilon)$ and the transitions are defined as follows:

1. *If $s, t \in S_{\mathsf{St}}$ and $s \overset{a}{\mapsto} s'$ and $t \overset{a}{\mapsto} t'$ (for $a \in \Sigma$) then $(s, t) \overset{a}{\mapsto} (s', t')$.*
2. *If $s \in S_{\mathsf{St}}$, $t \in S_\varepsilon$, and $t \overset{\varepsilon}{\mapsto} t'$ then $(s, t) \overset{\varepsilon}{\mapsto} (s, t')$.*
3. *If $s \in S_\varepsilon$, $t \in S_{\mathsf{St}}$, and $s \overset{\varepsilon}{\mapsto} s'$ then $(s, t) \overset{\varepsilon}{\mapsto} (s', t)$.*
4. *If $s \overset{\varepsilon}{\mapsto} s'$ and $t \overset{\varepsilon}{\mapsto} t'$ then $(s, t) \overset{\varepsilon}{\mapsto} (s', t')$.*

A path $(s_0, s'_0) \xrightarrow{a_1} (s_1, s'_1) \xrightarrow{a_2} (s_2, s'_2) \cdots \xrightarrow{a_z} (s_z, s'_z)$ *in $\mathcal{T} \times \mathcal{T}$ (where $(s_i, s'_i) \in S_{\mathsf{St}} \times S_{\mathsf{St}}$ by Def. 4) is* eqlevel-decreasing *if $\mathsf{EqL}(s_i, s'_i) > \mathsf{EqL}(s_{i+1}, s'_{i+1})$ for all $i \in \{0, 1, , \ldots, z{-}1\}$.*

We can easily verify that $\mathcal{T} \times \mathcal{T}$ is indeed a det-LTS. We also note that in eqlevel-decreasing paths we must have $\mathsf{EqL}(s_{i+1}, s'_{i+1}) = \mathsf{EqL}(s_i, s'_i) - 1$, by Observation 1.

OBSERVATION 22.

1. *Any subpath of an eqlevel-decreasing path in $\mathcal{T} \times \mathcal{T}$ is a shortest path from its start to its end.*

2. *Suppose the path* $(s,t) \xrightarrow{w} (s',t')$ *is eqlevel-decreasing. If* $(s,t) \xrightarrow{v} (s'',t'')$ *where* $|v| < |w|$ *then* $\mathsf{EqL}(s'',t'') > \mathsf{EqL}(s',t')$.

We now look at $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$ for a doca $\mathcal{A}$.

DEFINITION 23. *We call* $(p(m),q(n)) \xrightarrow{a} (p'(m'),q'(n'))$ *a* reset step *(in* $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$*) if at least one of component-steps* $p(m) \xrightarrow{a} p'(m')$, $q(n) \xrightarrow{a} q'(n')$ *is a reset step in* $\mathcal{T}(\mathcal{A})$. *If precisely one of component-steps is a reset step then* $(p(m),q(n)) \xrightarrow{a} (p'(m'),q'(n'))$ *is a* one-side reset step, *if both component-steps are reset steps then* $(p(m),q(n)) \xrightarrow{a} (p'(m'),q'(n'))$ *is a* both-side reset step.

We note that one of m', n' is 0 when $(p(m),q(n)) \xrightarrow{a} (p'(m'),q'(n'))$ is a one-side reset step, and $m' = n' = 0$ when it is a both-side reset step.

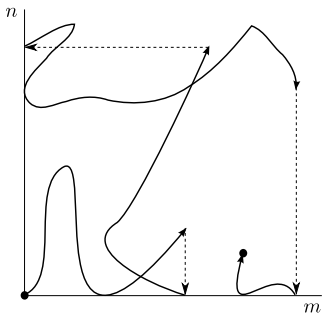

Figure 7: A path from $(p(0),q(0))$ **in** $\mathcal{T}(\mathcal{A})\times\mathcal{T}(\mathcal{A})$ **(with some one-side resets), projected to** $\mathbb{N}\times\mathbb{N}$.

Fig. 7 shows an example of a path $\mathcal{T}(\mathcal{A})\times\mathcal{T}(\mathcal{A})$, projected to $\mathbb{N}\times\mathbb{N}$ (a pair $(p(m),q(n))$ is projected to (m,n)); the dotted lines represent one-side reset steps. Theorem 2 claims, in fact, that the eqlevel-decreasing paths in $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$ whose start is projected to $(0,0)$ are short.

3.7 IL-equality lines

We assume a fixed doca $\mathcal{A}$, and consider the cases $\mathsf{IL}(p(m)) = \mathsf{IL}(q(n)) < \omega$ (i.e., $\ell = r < \omega$ in Fig. 6); we explore what we can say about the respective points $(m,n) \in \mathbb{N} \times \mathbb{N}$. By Convention after Prop. 16, each such case has the associated equalities $\mathsf{IL}(p(m)) = \rho \cdot m + \sigma + e$ and $\mathsf{IL}(q(n)) = \rho' \cdot n + \sigma' + e'$, and $\mathsf{IL}(p(m)) = \mathsf{IL}(q(n))$ thus implies $\rho \cdot m + \sigma + e = \rho' \cdot n + \sigma' + e'$.

Only in few cases we have $\rho = 0$ or $\rho' = 0$ (which is clear by Prop. 16 and Prop. 17(1)); in the other (many) cases we have $n = \frac{\rho}{\rho'}m + \frac{(\sigma-\sigma')+(e-e')}{\rho'}$ where $\frac{\rho}{\rho'} > 0$. This naturally leads to the following notions (illustrated in Fig. 8).

DEFINITION 24. *A pair* (μ,τ) *of rational numbers is a* valid slope-shift pair *if there are some* $p(m)$, $q(n)$ *with the associated equalities* $\mathsf{IL}(p(m)) = \rho \cdot m + \sigma + e$ *and* $\mathsf{IL}(q(n)) = \rho' \cdot n + \sigma' + e'$ *such that* $\rho \cdot m + \sigma + e = \rho' \cdot n + \sigma' + e'$, $\rho > 0$, $\rho' > 0$, $\mu = \frac{\rho}{\rho'}$, $\tau = \frac{(\sigma-\sigma')+(e-e')}{\rho'}$.

Each valid slope-shift pair (μ,τ) *defines an* IL-equality line*, or just a* line *for short, namely the set* $\{(x,y) \in \mathbb{N}\times\mathbb{N} \mid y = \mu \cdot x + \tau\}$.

Any maximal set of parallel lines (having the same slope but various shifts) is a line-bunch. *(Maximality is taken w.r.t. set inclusion.) We say that* $(x,y) \in \mathbb{N} \times \mathbb{N}$ *is in a line-bunch* H *if* (x,y) *is in a line in* H.

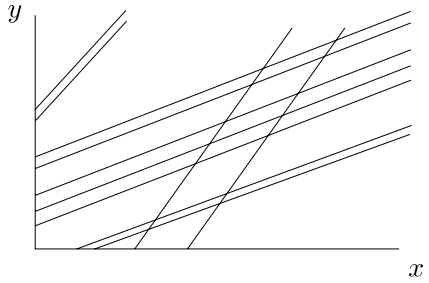

Figure 8: A sketch of IL-equality lines (in reality, the lines contain only points with integer coordinates)

Though each line contains at least one (m,n) such that $\mathsf{IL}(p(m)) = \mathsf{IL}(q(n)) < \omega$ for some p, q, the definition does not assume anything more specific about lines. The line-bunches can have various "gaps", and if a point (x,y) is not in a line-bunch H then it can still lie between two lines from H. The following proposition is easy to verify.

PROPOSITION 25.

1. *There are only few lines, and thus also few line-bunches.*
   The set $\{(x,y) \in \mathbb{N}\times\mathbb{N} \mid (x,y) \in L_1 \cap L_2$ *for two different lines* $L_1, L_2\}$ *is small.*
2. *There are only few pairs* $(p(m),q(n))$ *where* $\mathsf{IL}(p(m)) = \mathsf{IL}(q(n)) < \omega$ *and* (m,n) *is not in a line.*

3.8 Eqlevel-decreasing line-climbing paths are short

We recall Fig. 4 which assumes a large gap $e_U - e_D$; to finish a proof of Theorem 14, we aim to show that all gaps in ZE are, in fact, small. In the next subsection (3.9) we show that a large gap $e_U - e_D$ would entail a long eqlevel-decreasing line-climbing path in $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$ (depicted in Fig. 9). In this subsection we show that all such paths are, in fact, short. Fig. 9 illustrates a line-climbing path from a pair projected to P_1 to a larger pair projected to P_2. The cyclicity and further structures in the figure will be discussed later.

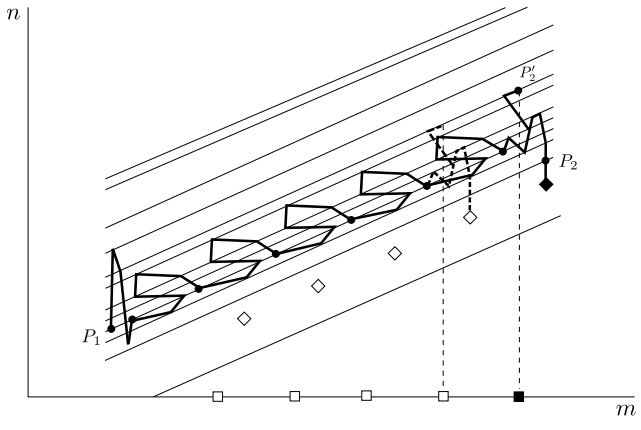

Figure 9: A line-climbing path (projections of all visited configuration-pairs are in IL-equality lines in one line-bunch)

DEFINITION 26. *A* path in $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$ *is* positive *if each pair* $(p(m), q(n))$ *in the path satisfies* $m > 0$, $n > 0$; *this entails that there are no reset steps in the path.*

A positive path $(p_0(m_0), q_0(n_0)) \xrightarrow{a_1} (p_1(m_1), q_1(n_1)) \xrightarrow{a_2} \cdots \xrightarrow{a_z} (p_z(m_z), q_z(n_z))$ *is* line-climbing *if* $m_0 < m_z$ *and all* (m_i, n_i), *for* $i = 0, 1, 2, \ldots, z$, *are in one line-bunch.*

We do not require that (m_0, n_0) and (m_z, n_z) are in the same line, and we might have $n_z \leq n_0$; hence "line-climbing" might be understood as a shorthand for "(left-to-right) line-bunch climbing".

We now sketch the ideas of a proof of Prop. 29; a crucial part of the proof is captured by Prop. 28. Let us consider a line-climbing eqlevel-decreasing (sub)path with the start projected to P_1 and the end projected to P_2, which is followed by a simple step leading out of the respective line-bunch, namely to the black-diamond point in Fig. 9. Our path in $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$ can be also naturally viewed as a path in $\mathcal{T}(\mathcal{B})$ for a doca $\mathcal{B}$ which is only polynomially bigger than $\mathcal{A}$: a pair $(p(m), q(n))$ in $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$ is viewed as the configuration $((p, q, L), m)$ in $\mathcal{T}(\mathcal{B})$ where L is the line containing (m, n) and the triple (p, q, L) is viewed as a control state of $\mathcal{B}$. By Observation 22(1), and Lemma 6 (with Fig. 2) applied to $\mathcal{B}$, our path from P_1 to P_2 is either short by Corollary 7, or can be assumed in a cyclic form, as depicted in Fig. 9.

Cutting off the copies of the cycle gives rise to the sequence of white-diamond points (i.e., to the respective paths in $\mathcal{T}(\mathcal{A}) \times \mathcal{T}(\mathcal{A})$ starting in P_1 and finishing in white-diamond points); if the pair projected to the black diamond is $(p'(m'), q'(n'))$ then the pairs projected to the white diamonds are of the form $(p'(m''), q'(n''))$ where $m'' < m'$ and $n'' < n'$. Each pair has its associated tuple $(b, \ell, r, o, d^L, d^R)$ (recall Fig. 6). By Observation 22(2), the values b for the pairs corresponding to white-diamond points are bigger than b for the pair corresponding to the black-diamond point. On the other hand, the white-diamond sequence has a periodic subsequence, with a short period, such that each pair in the subsequence has $\min\{b, \ell, r, o\}$ not bigger than $\min\{b, \ell, r, o\}$ of the black diamond. (This follows from Cor. 20 and Prop. 17(2), 10(1).) We note that we can have $\ell = r < \omega$ only few times (by Prop. 25(2) and the fact that the white diamonds are not in an IL-equality line). There are few possible values o (by Prop. 10(2)), and we can thus have $\ell = o < \omega$ only for few $p'(m'')$ (by Prop. 17(1)); similarly we can have $r = o < \omega$ only for few $q'(n'')$. Hence Corollary 20 implies that our subsequence is short, which in turn implies that the sequence of white diamonds is short, and thus our line-climbing eqlevel-decreasing path is short.

Fig. 9 also illustrates a similar path from P_1 to P_2' which is followed by another type of leaving the line-bunch, namely by a one-side reset step to the black-box point. Cutting off the copies of the cycle in the path would now give rise to the sequence of white-box points. In fact, we always cut off a small multiple of the cycle, to achieve that the white-box pairs are of the form $(p'(m''), q'(0))$ when the black-box pair is $(p'(m'), q'(0))$. We can show that the white-box sequence is short by a similar reasoning as above.

If the path reaches the zero eqlevel inside the line-bunch or is followed by a both-side reset step then it is short (again by using Observation 22 and cutting off the cycles).

The sequence of white-diamond (or white-box) points, finished by the black-diamond (or black-box) point, inspires the following definition.

DEFINITION 27. *For* $p, q \in Q_{\mathsf{St}}$, *a* sequence *of pairs*

$$(p(m_0), q(n_0)), (p(m_1), q(n_1)), \ldots, (p(m_z), q(n_z))$$

where $z \geq 1$ *is* strange periodic *if the following conditions hold:*

1. $(m_i, n_i) = (m_0 + i \cdot c_1, n_0 + i \cdot c_2)$ *for some* $c_1, c_2 \in \mathbb{N}$ *and* $i = 0, 1, \ldots, z$;
2. $\mathsf{EqL}(p(m_i), q(n_i)) > \mathsf{EqL}(p(m_z), q(n_z))$ *for all* $i \in \{0, 1, \ldots, z-1\}$ *(hence* $c_1 > 0$ *or* $c_2 > 0$*);*
3. *the pairs* $(m_0, n_0), (m_1, n_1), \ldots, (m_z, n_z)$ *are not all in one* IL*-equality line.*

Prop. 25 implies that in any strange periodic sequence there are only few pairs $(p(m_i), q(n_i))$ such that $\mathsf{IL}(p(m_i)) = \mathsf{IL}(q(n_i)) < \omega$. We have already sketched the proofs of the following propositions.

PROPOSITION 28. *Strange periodic sequences are short.*

PROPOSITION 29. *Eqlevel-decreasing line-climbing paths are short.*

3.9 Gaps in ZE are small

Assuming a doca $\mathcal{A}$, with the associated det-LTS $\mathcal{T}_{\mathsf{ext}}(\mathcal{A})$, by Def. 12 we have

$$\mathrm{ZE} = \{e \in \mathbb{N} \mid \text{there are two stable zero configurations } C, C' \text{ in } \mathcal{T}_{\mathsf{ext}}(\mathcal{A}) \text{ s.t. } C \overset{e}{\longleftrightarrow} C'\}.$$

We assumed $0 \in \mathrm{ZE}$ and we fixed an ordering $e_0 < e_1 < \cdots < e_f$ of ZE. We finally aim to contradict the existence of a large gap between $e_i = e_D$ and $e_{i+1} = e_U$ for some $i, 0 \leq i < f$ (recall Fig. 4); this will finish a proof of Theorem 14.

We sketch the ideas of a proof of Lemma 30, using Fig. 10.

Let us consider an eqlevel-decreasing path in $\mathcal{T}_{\mathsf{ext}}(\mathcal{A}) \times \mathcal{T}_{\mathsf{ext}}(\mathcal{A})$, which starts from a pair (C_0, C_0') of stable zero configurations satisfying $\mathsf{EqL}(C_0, C_0') = e_U$; let (C_j, C_j') be the pair visited by our path after j steps. If both C_0, C_0' are in Q_{Mod} (recall that $Q_{\mathsf{Mod}} = \{\mathsf{Mod}(p(m)) \mid p \in Q_{\mathsf{St}}, m \geq 0\}$) then also C_1, C_1' are stable zero configurations (maybe in $\mathcal{T}(\mathcal{A})$), and thus $e_D = e_U - 1$; the gap is really small in this case. We thus further assume $C_0 \notin Q_{\mathsf{Mod}}$ (hence $C_0 = p(0)$ is in $\mathcal{T}(\mathcal{A})$); this also handles the case $C_0' \notin Q_{\mathsf{Mod}}$ by symmetry.

We are now not primarily interested in studying how the concrete pairs (C_j, C_j') can look like; we are interested in the tuples $(b_j, \ell_j, r_j, o_j, d_j^L, d_j^R)$ associated with (C_j, C_j') by Def. 18 (recall Fig. 6). The dependence of this tuple on j is partly sketched in Fig. 10.

Since our path is eqlevel-decreasing (the eqlevel drops by 1 in each step), we know that $b_j = e_U - j$, which is depicted by a line (in the standard sense, having nothing to do with IL-equality lines) starting in point $(0, e_U)$ and having the slope -1. (For a better overall appearence, the vertical unit length in Fig. 10 is smaller than the horizontal one.)

Each o_j is either ω or an element of ZE (of E_3 after Def. 12); in particular, $o_j \geq e_U$ or $o_j \leq e_D$, which is depicted as a constraint in Fig. 10, using the horizontal lines at levels e_U and e_D.

We now recall Prop. 16 and the fact that each finite $\mathsf{IL}(q(0))$ is in ZE (in E_2 after Def. 12). Hence for each ℓ_j

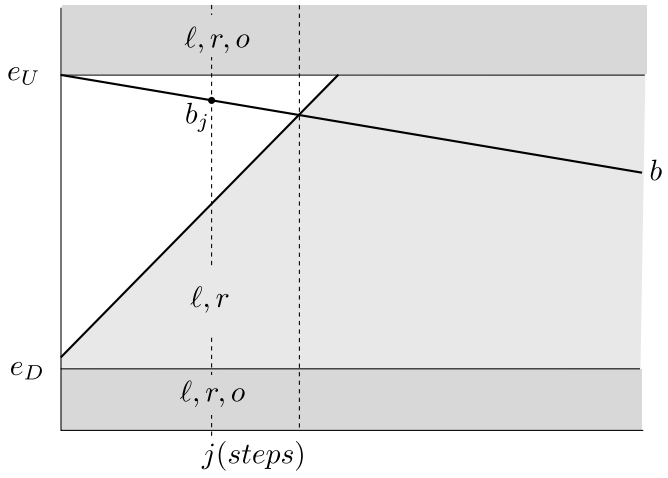

Figure 10: Constraints on b_j, ℓ_j, r_j, o_j after j steps of an eqlevel-decreasing path with $b_0 = e_U$

we have either $\ell_j \geq e_U$ or $\ell_j \leq e_D + \rho_{\text{M}} \cdot j + \sigma_{\text{M}}$ where ρ_{M} is the maximal number appearing as ρ in the fixed equalities $\mathsf{IL}(p(m)) = \rho \cdot m + \sigma + e$, and σ_{M} is the maximal number appearing there as σ. (We use the fact that the counter value is at most j in C_j, as well as in C'_j when C'_j is also in $\mathcal{T}(\mathcal{A})$, since we started from zero configurations.) We recall that both ρ_{M} and σ_{M} are small rational numbers. The above constraints on ℓ_j are also depicted in Fig. 10, using the horizontal line at level e_U and the line starting in $(0, e_D{+}\sigma_{\text{M}})$ and having the slope ρ_{M}. The same constraints hold for r_j.

We note that if the horizontal coordinate of the intersection of the "b-line" and the "ℓ, r-line" is small then $e_U - e_D$ is small. This is clear by noting that $b_j = e_U{-}j \leq e_D + \rho_{\text{M}} \cdot j + \sigma_{\text{M}}$ implies $e_U{-}e_D \leq (1{+}\rho_{\text{M}}) \cdot j + \sigma_{\text{M}}$.

Using Cor. 20 and a case analysis resembling the above analysis related to the white-diamond points in Fig. 9, we can show even something stronger: the maximal prefix of our path in which b_j (for $j > 0$) is "solitary", i.e. $b_j \notin \{\ell_j, r_j, o_j\}$, is short. The analysis shows that in a long b-solitary prefix we would "usually" have $\ell_j = r_j < \omega$, which would entail a long line-climbing segment; this would contradict Prop. 29.

LEMMA 30. *All gaps $e_U{-}e_D$ in* ZE *are small.*

Lemma 13 and 30 prove Theorem 14 and thus Theorem 2.

4. ACKNOWLEDGMENTS

S. Böhm and P. Jančar are supported by the Grant Agency of the Czech Rep. (project GAČR:P202/11/0340). S. Göller received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 259454.

5. REFERENCES

[1] P. Berman and R. Roos. Learning One-Counter Languages in Polynomial Time (Extended Abstract). In *Proc. of FOCS*, pages 61–67. IEEE, 1987.

[2] S. Böhm and S. Göller. Language Equivalence of Deterministic Real-Time One-Counter Automata Is NL-Complete. In *Proc. of MFCS*, volume 6907 of *Lecture Notes in Computer Science*, pages 194–205. Springer, 2011.

[3] S. Böhm, S. Göller, and P. Jančar. Bisimilarity of one-counter processes is PSPACE-complete. In *Proc. of CONCUR*, volume 6269 of *Lecture Notes in Computer Science*, pages 177–191. Springer, 2010.

[4] W. Czerwiński and S. Lasota. Fast equivalence-checking for normed context-free processes. In *Proc. FSTTCS'10*, volume 8 of *LIPIcs*. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2010.

[5] A. F. Fahmy and R. S. Roos. Efficient Learning of Real Time One-Counter Automata. In *Proc. of ALT*, volume 997 of *Lecture Notes in Computer Science*, pages 25–40. Springer, 1995.

[6] K. Higuchi, M. Wakatsuki, and E. Tomita. A polynomial-time algorithm for checking the inclusion for real-time deterministic restricted one-counter automata which accept by final state. *IEICE Trans. Information and Systems*, E78-D:939–950, 1995.

[7] K. Higuchi, M. Wakatsuki, and E. Tomita. A polynomial-time algorithm for checking the inclusion for real-time deterministic restricted one-counter automata which accept by accept mode. *IEICE Trans. Information and Systems*, E81-D:1–11, 1998.

[8] Y. Hirshfeld, M. Jerrum, and F. Moller. A Polynomial Algorithm for Deciding Bisimilarity of Normed Context-Free Processes. *Theor. Comput. Sci.*, 158(1&2):143–159, 1996.

[9] P. Jančar. Decidability of dpda language equivalence via first-order grammars. In *Proc. of LICS*, pages 415–424. IEEE, 2012.

[10] P. Jančar, A. Kučera, and F. Moller. Simulation and bisimulation over one-counter processes. In *Proc. of STACS*, volume 1770 of *Lecture Notes in Computer Science*, pages 334–345, 2000.

[11] R. Mayr. Undecidability of Weak Bisimulation Equivalence for 1-Counter Processes. In *Proc. of ICALP*, volume 2719 of *Lecture Notes in Computer Science*, pages 570–583, 2003.

[12] M. Oyamaguchi. The equivalence problem for real-time DPDAs. *J. ACM*, 34:731–760, 1987.

[13] R. Roos. *Deciding Equivalence of Deterministic One-Counter Automata in Polynomial Time with Applications to Learning*. PhD thesis, The Pennsylvania State University, 1988.

[14] G. Sénizergues. L(A)=L(B)? decidability results from complete formal systems. *Theor. Comput. Sci.*, 251(1-2):1–166, 2001.

[15] G. Sénizergues. L(A)=L(B)? A simplified decidability proof. *Theor. Comput. Sci.*, 281(1-2):555–608, 2002.

[16] G. Sénizergues. The Equivalence Problem for t-Turn DPDA Is Co-NP. In *Proc. of ICALP*, volume 2719 of *Lecture Notes in Computer Science*, pages 478–489. Springer, 2003.

[17] C. Stirling. Deciding DPDA Equivalence Is Primitive Recursive. In *Proc. of ICALP*, volume 2380 of *Lecture Notes in Computer Science*, pages 821–832. Springer, 2002.

[18] L. G. Valiant and M. Paterson. Deterministic one-counter automata. *J. Comput. Syst. Sci.*, 10(3):340–350, 1975.