Bidimensional linear recursive sequences and universality of unambiguous register automata

Corentin Barloy
École Normale Supérieure de Paris, PSL, France

Lorenzo Clemente
University of Warsaw, Poland

Abstract

We study the universality and inclusion problems for register automata over equality data $(\mathbb{A}, =)$. We show that the universality $L(B) = (\Sigma \times \mathbb{A})^*$ and inclusion problems $L(A) \subseteq L(B)$ can be solved with 2-EXPTIME complexity when both automata are without guessing and B is unambiguous, improving on the currently best-known 2-EXPSPACE upper bound by Mottet and Quaas. When the number of registers of both automata is fixed, we obtain a lower EXPTIME complexity, also improving the EXPSPACE upper bound from Mottet and Quaas for fixed number of registers. We reduce inclusion to universality, and then we reduce universality to the problem of counting the number of orbits of runs of the automaton. We show that the orbit-counting function satisfies a system of bidimensional linear recursive equations with polynomial coefficients (linrec), which generalises analogous recurrences for the Stirling numbers of the second kind, and then we show that universality reduces to the zeroness problem for linrec sequences. While such a counting approach is classical and has successfully been applied to unambiguous finite automata and grammars over finite alphabets, its application to register automata over infinite alphabets is novel.

We provide two algorithms to decide the zeroness problem for bidimensional linear recursive sequences arising from orbit-counting functions. Both algorithms rely on techniques from linear non-commutative algebra. The first algorithm performs variable elimination and has elementary complexity. The second algorithm is a refined version of the first one and it relies on the computation of the Hermite normal form of matrices over a skew polynomial field. The second algorithm yields an EXPTIME decision procedure for the zeroness problem of linrec sequences, which in turn yields the claimed bounds for the universality and inclusion problems of register automata.

2012 ACM Subject Classification Theory of computation - Automata over infinite objects.

Keywords and phrases unambiguous register automata, universality and inclusion problems, multi-dimensional linear recurrence sequences.

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

Funding *Corentin Barloy*: Partially supported by the Polish NCN grant 2017/26/D/ST6/00201.
Lorenzo Clemente: Partially supported by the Polish NCN grant 2017/26/D/ST6/00201.

Acknowledgements We would like to thank Daniel Robertz for kindly providing us with the `LDA` package for Maple 16.

42nd Conference on Very Important Topics (CVIT 2016).
Editors: John Q. Open and Joan R. Access; Article No. 23; pp. 23:1–23:38
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Register automata. *Register automata* extend finite automata with finitely many registers holding values from an infinite *data domain* $\mathbb{A}$ which can be compared against the data appearing in the input. The study of register automata arises naturally in automata theory as a conservative generalisation of finite automata over finite alphabets Σ to richer but well-behaved classes of infinite alphabets. The seminal work of Kaminski and Francez introduced *finite-memory automata* as the study of register automata over the data domain $(\mathbb{A}, =)$ consisting of an infinite set $\mathbb{A}$ and the equality relation [29]. The recent book [4] studies automata theory over other data domains such as $(\mathbb{Q}, \leq)$, and more generally homogeneous [36] or even ω-categorical relational structures. Another motivation for the study of register automata comes from the area of database theory: XML documents can naturally be modelled as finite unranked trees where data values from an infinite alphabet are necessary to model the *attribute values* of the document (c.f. [41] and the survey [47]).

The central verification question for register automata is the *inclusion problem*, which, for two given automata A, B, asks whether $L(A) \subseteq L(B)$. In full generality the problem is undecidable and this holds already in the special case of the *universality problem* $L(B) = (\Sigma \times \mathbb{A})^*$ [41, Theorem 5.1], when B has only two registers [4, Theorem 1.8] (or even just one register in the more powerful model *with guessing* [4, Exercise 9], i.e., non-deterministic reassignment in the terminology of [30]). One way to obtain decidability is to restrict the automaton B. One such restriction requires that B is *deterministic*: Since deterministic register automata are effectively closed under complementation, the inclusion problem reduces to non-emptiness of $L(A) \cap (\Sigma \times \mathbb{A})^* \setminus L(B)$, which can be checked in PSPACE. Another, incomparable, restriction demands that B has only one register: In this case the problem becomes decidable [29, Appendix A][1] and non-primitive recursive [22, Theorem 5.2].

Unambiguity. *Unambiguous automata* are a natural class of automata intermediate between deterministic and nondeterministic automata. An automaton is unambiguous if there is at most one accepting run on every input word. Unambiguity has often been used to generalise decidability results for deterministic automata at the price of a usually modest additional complexity. For instance, the universality problem for deterministic finite automata (which is PSPACE-complete in general [52]) is NL-complete, while for the unambiguous variant it is in PTIME [51, Corollary 4.7], and even in NC^2 [55]. An even more dramatic example is provided by universality of context-free grammars, which is undecidable in general [28, Theorem 9.22], PTIME-complete for deterministic context-free grammars, and decidable for unambiguous context-free grammars [45, Theorem 5.5] (even in PSPACE [15, Theorem 10]). (The more general equivalence problem is decidable for deterministic context-free grammars [48], but it is currently an open problem whether equivalence is decidable for unambiguous context-free grammars, as well as for the more general *multiplicity equivalence* of context-free grammars [33].) Other applications of unambiguity for universality and inclusion problems in automata theory include Büchi automata [7, 2], probabilistic automata [21], Parikh automata [9, 5], vector addition systems [20], and several others (c.f. also [18, 19]).

[1] Decidability even holds for the so-called “two-window register automata”, which combined with the restriction in [29] demanding that the last data value read must always be stored in some register boils down to a slightly more general class of “$1\frac{1}{2}$-register automata”.

Number sequences and the counting approach. The universality problem for a language over finite words $L \subseteq \Sigma^*$ is equivalent to whether its associated *word counting function* $f_L(n) := |L \cap \Sigma^n|$ equals $|\Sigma|^n$ for every n. The most classical way of exploiting unambiguity of a computation model A (finite automaton, context-free grammar, ...) is to use the fact that it yields a bijection between the recognised language $L(A)$ and the set of accepting runs. In this way, $f_L(n)$ is also the number of accepting runs of length n, and for the latter recursive descriptions usually exist. When the class of number sequences to which f_L belongs contains $|\Sigma|^n$ and is closed under difference, this is equivalent to the *zeroness* problem for $g(n) := |\Sigma|^n - f_L(n)$, which amounts to decide whether $g = 0$. This approach has been pioneered by Chomsky and Schützenberger [14] who have shown that the generating function $g_L(x) = \sum_{n=0}^{\infty} f_L(n) \cdot x^n$ associated to an unambiguous context-free language L is algebraic (c.f. [8]). A similar observation by Stearns and Hunt [51] shows that $g_L(x)$ is rational [50, Chapter 4], when L is regular, and more recently by Bostan et al. [5] who have shown that $g_L(x)$ is holonomic [49] when L is recognised by an unambiguous Parikh automaton. Since the zeroness problem for rational, algebraic, and holonomic generating functions is decidable, one obtains decidability of the corresponding universality problems.

Unambiguous register automata. Returning to register automata, Mottet and Quaas have recently shown that the inclusion problem in the case where B is an unambiguous register automaton over equality data (without guessing) can be decided in 2-EXPSPACE, and in EXPSPACE when the numbers of registers of B is fixed [37, Theorem 1]. Note that already decidability is interesting, since unambiguous register automata without guessing are not closed under complement in the class of nondeterministic register automata without guessing [30, Example 4], and thus the classical approach via complementing B fails for register automata[2]. (In fact, even for finite automata complementation of unambiguous finite automata cannot lead to a PTIME universality algorithm, thanks to Raskin's recent super-polynomial lower-bound for the complementation problem for unambiguous finite automata in the class of non-deterministic finite automata [44]). Mottet and Quaas obtain their result by showing that inclusion can be decided by checking a reachability property of a suitable graph of triply-exponential size obtained by taking the product of A and B, and then applying the standard NL algorithm for reachability in directed graphs.

Our contributions. In view of the widespread success of the counting approach to unambiguous models of computation, one may wonder whether it can be applied to register automata as well. This is the topic of our paper. A naïve counting approach for register automata immediately runs into trouble since there are infinitely many data words of length n. The natural remedy is to use the fact that $\mathbb{A}^n$, albeit infinite, is *orbit-finite* [4, Sec. 3.2], which is a crucial notion generalising finiteness to the realm of relational structures used to model data. In this way, we naturally count the number of *orbits* of words/runs of a given length, which in the context of model theory is sometimes known as the *Ryll-Nardzewski function* [46]. For example, in the case of equality data $(\mathbb{A}, =)$, the number of orbits of words of length n is the well-known *Bell number* $B(n)$, and for $(\mathbb{Q}, \leq)$ one obtains the *ordered Bell numbers* (a.k.a. *Fubini numbers*); c.f. Cameron's book for more examples [11, Ch. 7].

[2] In the more general class of register automata with guessing, an unproved conjecture proposed by Colcombet states that unambiguous register automata with guessing are effectively closed under complement [19, Theorem 12], implying decidability of the universality and containment problems for unambiguous register automata with guessing and, a posteriori, unambiguous register automata without guessing as considered in this paper. No published proof of this conjecture has appeared as of yet.

When considering orbits of runs, the run length n seems insufficient to obtain recurrence equations. To this end, we also consider the number of distinct data values k that appear on the word labelling the run. For instance, in the case of equality data, the corresponding orbit-counting function is the well-known sequence of *Stirling numbers of the second kind* $S(n, k) : \mathbb{Q}^{\mathbb{N}^2}$, which satisfies $S(0, 0) = 1$, $S(m, 0) = S(0, m) = 0$ for $m \geq 1$, and

$$S(n, k) = S(n - 1, k - 1) + k \cdot S(n - 1, k), \qquad \text{for } n, k \geq 1. \tag{1}$$

These intuitions lead us to define the class of *bidimensional linear recursive sequences with polynomial coefficients* (linrec; c.f. (2)) which are a class of number sequences in $\mathbb{Q}^{\mathbb{N}^2}$ satisfying a system of shift equations with polynomial coefficients generalising (1). Linrec are sufficiently general to model the orbit-counting functions of register automata and yet amenable to algorithmic analysis. Our first result is a complexity upper bound for the zeroness problem for a class of linrec sequences which suffices to model register automata.

▶ **Theorem 1.** *The zeroness problem for linrec sequences with univariate polynomial coefficients from $\mathbb{Q}[k]$ is in* EXPTIME*.*

This is obtained by modelling linrec equations as systems of linear equations with *skew polynomial coefficients* (introduced by Ore [43]) and then using complexity bounds on the computation of the Hermite normal form of skew polynomial matrices by Giesbrecht and Kim [26]. Our second result is a reduction of the universality and inclusion problems to the zeroness problem of a system of linrec equations of exponential size. Together with Theorem 1, this yields improved upper bounds on the former problems.

▶ **Theorem 2.** *The universality $L(B) = (\Sigma \times \mathbb{A})^*$ and the inclusion problem $L(A) \subseteq L(B)$ for register automata A, B without guessing with B unambiguous are in* 2-EXPTIME*, and in* EXPTIME *for a fixed number of registers of A, B. The same holds for the equivalence problem $L(A) = L(B)$ when both automata are unambiguous.*

The rest of the paper is organised as follows. In Sec. 2, we introduce linrec sequences (c.f. Appendix A.3 for a comparison with well known sequence families from the literature such as the C-recursive, P-recursive, and the more recent polyrec sequences [10]). In Sec. 3, we introduce unambiguous register automata and we present an efficient reduction of the inclusion (and thus equivalence) problem to the universality problem, which allows us to concentrate on the latter in the rest of the paper. In Sec. 4, we present a reduction of the universality problem to the zeroness problem for linrec. In Sec. 5, we show with a simple argument based on elimination that the zeroness problem for linrec is decidable, and in Sec. 6 we derive a complexity upper bound using non-commutative linear algebra. Finally, in Sec. 7 we conclude with further work and an intriguing conjecture. Full proofs, additional definitions, and examples are provided in Appendices A–E.

Notation. Let $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ be the set of non-negative integers, resp., rationals. The *height* of an integer $k \in \mathbb{Z}$ is $|k|_\infty = |k|$, and for a rational number $a \in \mathbb{Q}$ uniquely written as $a = \frac{p}{q}$ with $p \in \mathbb{Z}, q \in \mathbb{N}$ co-prime we define $|a|_\infty = \max\{|p|_\infty, |q|_\infty\}$. Let $\mathbb{Q}[n, k]$ denote the ring of bivariate polynomials. The *(combined) degree* $\deg P$ of $P = \sum_{i,j} a_{ij} n^i k^j \in \mathbb{Q}[n, k]$ is the maximum $i + j$ s.t. $a_{ij} \neq 0$ and the *height* $|P|_\infty$ is $\max_{i,j} |a_{ij}|_\infty$. For a nonempty set A and $n \in \mathbb{N}$, let A^n be the set of sequences of elements from A of length n, In particular, $A^0 = \{\varepsilon\}$ contains only the empty sequence ε. Let $A^* = \bigcup_{n \in \mathbb{N}} A^n$ be the set of all finite sequences over A. We use the *soft-Oh* notation $\tilde{O}(f(n))$ to denote $\bigcup_{c \geq 0} O(f(n) \cdot \log^c f(n))$.

2 Bidimensional linear recursive sequences with polynomial coefficients

Let $f(n,k) : \mathbb{Q}^{\mathbb{N}^2}$ be a bidimensional sequence. For $L \in \mathbb{N}$, the *first L-section* of f is the one-dimensional sequence $f(L,k) : \mathbb{Q}^{\mathbb{N}}$ obtained by fixing its first component to L; the *second L-section* $f(n,L)$ is defined similarly. The two *shift operators* $\partial_1, \partial_2 : \mathbb{Q}^{\mathbb{N}^2} \to \mathbb{Q}^{\mathbb{N}^2}$ are

$$(\partial_1 f)(n,k) = f(n+1,k) \quad \text{and} \quad (\partial_2 f)(n,k) = f(n,k+1), \quad \text{for all } n,k \geq 0.$$

An *affine operator* is a formal expression of the form $A = p_{00} + p_{01} \cdot \partial_1 + p_{10} \cdot \partial_2$ where $p_{00}, p_{01}, p_{10} \in \mathbb{Q}[n,k]$ are bivariate polynomials over n,k with rational coefficients. Let $\{f_1, \ldots, f_m\}$ be a set of variables denoting bidimensional sequences[3]. A *system of linear shift equations* over $f_1, \ldots, f_m$ consists of m equations of the form

$$\begin{cases} \partial_1\partial_2 f_1 & = & A_{1,1} \cdot f_1 + \cdots + A_{1,m} \cdot f_m, \\ & \vdots & \\ \partial_1\partial_2 f_m & = & A_{m,1} \cdot f_1 + \cdots + A_{m,m} \cdot f_m, \end{cases} \tag{2}$$

where the $A_{i,j}$'s are affine operators. A bidimensional sequence $f : \mathbb{Q}^{\mathbb{N}^2}$ is *linear recursive of order m, degree d, and height h* (abbreviated, linrec) if the following two conditions hold:

1) there are auxiliary bidimensional sequences $f_2, \ldots, f_m : \mathbb{Q}^{\mathbb{N}^2}$ which together with $f = f_1$ satisfy a system of linear shift equations as in (2) where the polynomial coefficients have (combined) degree $\leq d$ and height $\leq h$.
2) for every $1 \leq i \leq m$ there are constants denoted $f_i(0, \geq 1), f_i(\geq 1, 0) \in \mathbb{Q}$ s.t. $f_i(0,k) = f_i(0, \geq 1)$ and $f_i(n,0) = f_i(\geq 1, 0)$ for every $n,k \geq 1$.

If we additionally fix the initial values $f_1(0,0), \ldots, f_m(0,0)$, then the system (2) has a unique solution, which is computable in PTIME.

▶ **Lemma 3.** *The values $f_i(n,k)$'s are computable in deterministic time $\tilde{O}(m \cdot n \cdot k)$.*

In the following we will use the following effective closure under section.

▶ **Lemma 4.** *If $f : \mathbb{Q}^{\mathbb{N}^2}$ is linrec of order $\leq m$, degree $\leq d$, and height $\leq h$, then its L-sections $f(L,k), f(n,L) : \mathbb{Q}^{\mathbb{N}}$ are linrec of order $\leq m \cdot (L+3)$, degree $\leq d$, and height $\leq h \cdot L^d$.*

We are interested in the following central algorithmic problem for linrec.

Zeroness problem.
Input: A system of linrec equations (2) together with all initial conditions.
Output: Is it the case that $f_1 = 0$?

In Sec. 4 we use linrec sequences to model the orbit-counting functions of register automata, which we introduce next.

3 Unambiguous register automata

We consider register automata over the relational structure $(\mathbb{A}, =)$ consisting of a countable set $\mathbb{A}$ equipped with equality as the only relational symbol. Let $\bar{a} = a_1 \cdots a_n \in \mathbb{A}^n$ be a finite sequence of n data values. An *$\bar{a}$-automorphism* of $\mathbb{A}$ is a bijection $\alpha : \mathbb{A} \to \mathbb{A}$

[3] We abuse notation and silently identify variables denoting sequences with the sequences they denote.

s.t. $\alpha(a_i) = a_i$ for every $1 \leq i \leq n$, which is extended pointwise to $\bar{a} \in \mathbb{A}^n$ and to $L \subseteq \mathbb{A}^*$. For $\bar{b}, \bar{c} \in \mathbb{A}^n$, we write $\bar{b} \sim_{\bar{a}} \bar{c}$ whenever there is an $\bar{a}$-automorphism α s.t. $\alpha(\bar{b}) = \bar{c}$. The *$\bar{a}$-orbit* of $\bar{b}$ is the equivalence class $[\bar{b}]_{\bar{a}} = \{\bar{c} \in \mathbb{A}^n \mid \bar{b} \sim_{\bar{a}} \bar{c}\}$, and the set of $\bar{a}$-orbits of sequences in $L \subseteq \mathbb{A}^*$ is $\mathsf{orbits}_{\bar{a}}(L) = \{[\bar{b}]_{\bar{a}} \mid \bar{b} \in L\}$. In the special case when $\bar{a} = \varepsilon$ is the empty tuple, we just speak about *automorphism* α and *orbit* $[\bar{b}]$. A set X is *orbit-finite* if $\mathsf{orbits}(X)$ is a finite set [4, Sec. 3.2]. All definitions above extend to $\mathbb{A}_\perp := \mathbb{A} \cup \{\perp\}$ with $\perp \notin \mathbb{A}$ in the expected way. A *constraint* φ is a quantifier-free[4] formula generated by $\varphi, \psi ::\equiv x = \perp \mid x = y \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \neg\varphi$, where x, y are variables and $\perp$ is a special constant denoting an undefined value. The semantics of a constraint $\varphi(x_1, \ldots, x_n)$ with n free variables $x_1, \ldots, x_n$ is the set of tuples of n elements which satisfies: $[\![\varphi]\!] = \{a_1, \ldots, a_n \in \mathbb{A}_\perp^n \mid \mathbb{A}_\perp, x_1 : a_1, \ldots, x_n : a_n \models \varphi\}$. A *register automaton* of *dimension* $d \in \mathbb{N}$ is a tuple $A = (d, \Sigma, \mathsf{L}, \mathsf{L}_I, \mathsf{L}_F, \to)$ where d is the number of registers, Σ is a finite alphabet, L is a finite set of *control locations*, of which we distinguish those which are *initial* $\mathsf{L}_I \subseteq \mathsf{L}$, resp., *final* $\mathsf{L}_F \subseteq \mathsf{L}$, and "$\to$" is a set of rules of the form $p \xrightarrow{\sigma, \varphi} q$, where $p, q \in \mathsf{L}$ are control locations, $\sigma \in \Sigma$ is an input symbol from the finite alphabet, and $\varphi(x_1, \ldots, x_d, y, x'_1, \ldots, x'_d)$ is a constraint relating the current register values x_i's, the current input symbol (represented by the variable y), and the next register values of x'_i's.

▶ **Example 5.** Let A over $|\Sigma| = 1$ have one register x, and four control locations p, q, r, s, of which p is initial and s is final. The transitions are $p \xrightarrow{x=\perp \wedge x'=y} q$, $p \xrightarrow{x=\perp \wedge x'=y} r$, $q \xrightarrow{x \neq y \wedge x'=x} q$, $q \xrightarrow{x=y \wedge x'=x} s$, $r \xrightarrow{x=y \wedge x'=x} r$, and $r \xrightarrow{x \neq y \wedge x'=x} s$. The automaton accepts all words of the form $a(\mathbb{A} \setminus \{a\})^* a$ or $aa^*(\mathbb{A} \setminus \{a\})$ with $a \in \mathbb{A}$.

A register automaton is *orbitised* if every constraint φ appearing in some transition thereof denotes an orbit $[\![\varphi]\!] \in \mathsf{orbits}(\mathbb{A}_\perp^{2 \cdot d+1})$. For example, when $d = 1$ the constraint $\varphi \equiv x = x'$ is not orbitised, however $[\![\varphi]\!] = [\![\varphi_0]\!] \cup [\![\varphi_1]\!]$ splits into two disjoint orbits for the orbitised constraints $\varphi_0 \equiv x = x' \wedge x = y$ and $\varphi_1 \equiv x = x' \wedge x \neq y$. The automaton from Example 5 is orbitised. Every register automaton can be transformed in orbitised form by replacing every transition $p \xrightarrow{\sigma, \varphi} q$ with exponentially many transitions $p \xrightarrow{\sigma, \varphi_1} q, \ldots, p \xrightarrow{\sigma, \varphi_n} q$, for each orbit $[\![\varphi_i]\!]$ of $[\![\varphi]\!] \subseteq \mathbb{A}_\perp^{2 \cdot d+1}$.

A *register valuation* is a tuple of (possibly undefined) values $\bar{a} = (a_1, \ldots, a_d) \in \mathbb{A}_\perp^d$. A *configuration* is a pair $(p, \bar{a})$, where $p \in \mathsf{L}$ is a control location and $\bar{a} \in \mathbb{A}_\perp^d$ is a register valuation; it is *initial* if $p \in \mathsf{L}_I$ is initial and all registers are initially undefined $\bar{a} = (\perp, \ldots, \perp)$, and it is *final* whenever $p \in \mathsf{L}_F$ is so. The *semantics* of a register automaton A is the infinite transition system $[\![A]\!] = (C, C_I, C_F, \to)$ where C is the set of configurations, of which $C_I, C_F \subseteq C$ are the initial, resp., final ones, and $\to \subseteq C \times (\Sigma \times \mathbb{A}) \times C$ is the set of all transitions of the form

$$(p, \bar{a}) \xrightarrow{\sigma, a} (q, \bar{a}'), \qquad \text{with } \sigma \in \Sigma, a \in \mathbb{A}, \text{ and } \bar{a}, \bar{a}' \in \mathbb{A}_\perp^d,$$

s.t. there exists a rule $p \xrightarrow{\sigma, \varphi} q$ where satisfying the constraint $\mathbb{A}_\perp, \bar{x} : \bar{a}, y : a, \bar{x}' : \bar{a}' \models \varphi$. A *data word* is a sequence $w = (\sigma_1, a_1) \cdots (\sigma_n, a_n) \in (\Sigma \times \mathbb{A})^*$. A *run over* a data word w *starting at* $c_0 \in C$ and *ending at* $c_n \in C$ is a sequence π of transitions of $[\![A]\!]$ of the form $\pi = c_0 \xrightarrow{\sigma_1, a_1} c_1 \xrightarrow{\sigma_2, a_2} \cdots \xrightarrow{\sigma_n, a_n} c_n$. We denote with $\mathsf{Runs}(c_0; w; c_n)$ the set of runs over w starting at c_0 and ending in c_n, and with $\mathsf{Runs}(C_I; w; c_n)$ the set of *initial runs*, i.e., those runs over w starting at some initial configuration $c_0 \in C_I$ and ending in c_n. The run π is

[4] Since $(\mathbb{A}, =)$ is a homogeneous relational structure, and thus it admits quantifier elimination, we would obtain the same expressive power if we would consider more general first-order formulas instead.

accepting if $c_n \in C_F$. The language $L(A, c)$ recognised from configuration $c \in C$ is the set of data words labelling some accepting run starting at c; the language recognised from a set of configurations $D \subseteq C$ is $L(A, D) = \bigcup_{c \in D} L(A, c)$, and the language recognised by the register automaton A is $L(A) = L(A, C_I)$. Similarly, the *backward language* $L^{\mathsf{R}}(A, c)$ is the set of words labelling some run starting at an initial configuration and ending at c. Thus, we also have $L(A) = L^{\mathsf{R}}(A, C_F)$. A register automaton is *deterministic* if for every input word there exists at most one initial run, and *unambiguous* if for every input word there is at most one initial and accepting run. A register automaton is *without guessing* if, for every initial run $(p, \bot^d) \xrightarrow{w} (q, \bar{a})$ every non-$\bot$ data value in $\bar{a}$ occurs in the input w, written $\bar{a} \subseteq w$. In the rest of the paper we will study exclusively automata without guessing. A deterministic automaton is unambiguous and without guessing. These semantic properties can be decided in PSPACE with simple reachability analyses (c.f. [19]).

▶ **Example 6.** The automaton from Example 5 is unambiguous and without guessing. An example of language which can only be recognised by ambiguous register automata is the set of words where the same data value appears two times $L = \{u \cdot a \cdot v \cdot a \cdot w \mid a \in \mathbb{A}; u, v, w \in \mathbb{A}^*\}$.

▶ **Lemma 7.** *If A is an unambiguous register automaton, then there is a bijection between the language it recognises $L(A) = L(A, C_I) = L^{\mathsf{R}}(A, C_F)$ and the set of runs starting at some initial configuration in C_I and ending at some final configuration in C_F.*

We are interested in the following decision problem.

Inclusion problem.
Input: Two register automata A, B over the same input alphabet Σ.
Output: Is it the case that $L(A) \subseteq L(B)$?

The *universality problem* asks $L(A) = (\Sigma \times \mathbb{A})^*$, and the *equivalence problem* $L(A) = L(B)$. In general, universality reduces to equivalence, which in turn reduces to inclusion. In our context, inclusion reduces to universality and thus all three problems are equivalent.

▶ **Lemma 8.** *Let A and B be two register automata.*

1. *The inclusion problem $L(A) \subseteq L(B)$ with A orbitised and without guessing reduces in* PTIME *to the case where A is deterministic. The reduction preserves whether B is 1) unambiguous, 2) without guessing, and 3) orbitised.*
2. *The inclusion problem $L(A) \subseteq L(B)$ with A deterministic reduces in* PTIME *to the universality problem for some register automaton C. If B is unambiguous, then so is C. If B is without guessing, then so is C. If A and B are orbitised, then so is C.*

4 Universality of unambiguous register automata without guessing

We reduce universality of unambiguous register automata without guessing to zeroness of bidimensional linrec sequences with univariate polynomial coefficients. The *width* of a sequence of data values $\bar{a} = a_1 \cdots a_n \in \mathbb{A}^n$ is $\#\bar{a} = |\{a_1, \dots, a_n\}|$, for a word $w = (\sigma_1, a_1) \cdots (\sigma_n, a_n) \in (\Sigma \times \mathbb{A})^*$ we set $\#w = \#(a_1 \cdots a_n)$, and for a run π over w we set $\#\pi = \#w$. Let the *Ryll-Nardzewski function* $G_{p,\bar{a}}(n, k)$ of a configuration $(p, \bar{a}) \in C = \mathsf{L} \times \mathbb{A}_\bot^d$ count the number of $\bar{a}$-orbits of initial runs of length n and width k ending in $(p, \bar{a})$:

$$G_{p,\bar{a}}(n, k) = |\{[\pi]_{\bar{a}} \mid w \in (\Sigma \times \mathbb{A})^n, \pi \in \mathsf{Runs}(C_I; w; p, \bar{a}), \#w = k\}| \,. \tag{3}$$

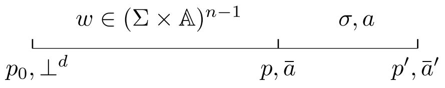

Figure 1 Last-step decomposition.

▶ **Lemma 9.** *Let $\bar{a}, \bar{b} \in \mathbb{A}_\bot^d$. If $[\bar{a}] = [\bar{b}]$, then $G_{p,\bar{a}}(n,k) = G_{p,\bar{b}}(n,k)$ for every $n, k \geq 0$.*
We thus overload the notation and write $G_{p,[\bar{a}]}$ instead of $G_{p,\bar{a}}$. Since $\mathbb{A}_\bot^d$ is orbit-finite, this yields finitely many variables $G_{p,[\bar{a}]}$'s. By slightly abusing notation, let $G_{C_F}(n,k) = \sum_{[(p,\bar{a})] \in \mathsf{orbits}(C_F)} G_{p,[\bar{a}]}(n,k)$ be the sum of the Ryll-Nardzewski function over all orbits of accepting configurations. When the automaton is unambiguous, thanks to Lemma 7, $G_{C_F}(n,k)$ is also the number of orbits of accepted words of length n and width k.

▶ **Lemma 10.** *Let A be an unambiguous register automaton w/o guessing over Σ and let $S_\Sigma(n,k)$ be the number of orbits of all words of length n and width k. We have $L(A) = (\mathbb{A} \times A)^*$ if, and only if, $\forall n, k \in \mathbb{N} \cdot G_{C_F}(n,k) = S_\Sigma(n,k)$.*
In other words, universality of A reduces to zeroness of $G := S_\Sigma - G_{C_F}$. The sequence S_Σ is linrec since it satisfies the recurrence in Figure 2 with initial conditions $S_\Sigma(0,0) = 1$ and $S_\Sigma(n+1,0) = S_\Sigma(0,k+1) = 0$ for $n, k \geq 0$. We show that all the sequences of the form $G_{p,[\bar{a}]}$ are also linrec and thus also G will be linrec. We perform a last-step decomposition of an initial run; c.f. Figure 1. Starting from some initial configuration $(p_0, \bot^d)$, the automaton has read a word w of length $n-1$ leading to $(p, \bar{a})$. Then, the automaton reads the last letter (σ, a) and goes to $(p', \bar{a}')$ via the transition $t = (p, \bar{a} \xrightarrow{\sigma,a} p', \bar{a}')$. The question is in how many distinct ways can an orbit of the run over w be extended into an orbit of the run over $w \cdot (\sigma, a)$. We distinguish three cases.

I: Assume that a appears in register $\bar{a}_i = a$. Since the automaton is without guessing, $a \in w$ has appeared earlier in the input word and $\bar{a}' \subseteq \bar{a}$ (ignoring $\bot$'s). Thus, each $\bar{a}$-orbit of runs $[p_0, \bot^d \xrightarrow{w} p, \bar{a}]_{\bar{a}}$ yields, via the fixed t, an $\bar{a}'$-orbit of runs $[p_0, \bot^d \xrightarrow{w} p, \bar{a} \xrightarrow{\sigma,a} p', \bar{a}']_{\bar{a}'}$ of the same width in just one way.

II: Assume that a is globally fresh $a \notin w$, and thus in particular $a \notin \bar{a}$ since the automaton is without guessing. Each $\bar{a}$-orbit of runs $[p_0, \bot^d \xrightarrow{w} p, \bar{a}]_{\bar{a}}$ of width $\#w$ yields, via the fixed t, a single $\bar{a}'$-orbit of runs $[p_0, \bot^d \xrightarrow{w} p, \bar{a} \xrightarrow{\sigma,a} p', \bar{a}']_{\bar{a}'}$ of width $\#(w \cdot a) = \#w + 1$.

III: Assume that $a \in w$ is not globally fresh, but it does not appear in any register $a \notin \bar{a}$. Since the automaton is without guessing, every value in $\bar{a}$ appears in w. Consequently, a can be any of the $\#w$ distinct values in w, with the exception of $\#\bar{a}$ values. Each $\bar{a}$-orbit of runs $[p_0, \bot \xrightarrow{w} p, \bar{a}]_{\bar{a}}$ of width $\#w$ yields $\#w - \#\bar{a} \geq 0$ $\bar{a}'$-orbits of runs $[p_0, \bot^d \xrightarrow{w} p, \bar{a} \xrightarrow{\sigma,a} p', \bar{a}']_{\bar{a}'}$ of the same width.

(As expected, we do not need unambiguity at this point, since we are counting orbits of runs.) We obtain the equations in Figure 2, where the sums range over orbits of transitions. This set of equations is finite since there are finitely many orbits $[\bar{a}] \in \mathsf{orbits}(\mathbb{A}_\bot^d)$ of register valuations, and moreover we can effectively represent each orbit by a constraint [4, Ch. 4]. Strictly speaking, the equations are not linrec due to the "max" operator, however they can easily be transformed to linrec by considering $G_{p,[\bar{a}]}(n,K)$ separately for $1 \leq K < d$; in the interest of clarity, we omit the full linrec expansion. The initial condition is $G_{p,[\bar{a}]}(0,0) = 1$ if $p \in I$ initial, and $G_{p,[\bar{a}]}(0,0) = 0$ otherwise. The two 0-sections satisfy $G_{p,[\bar{a}]}(n+1,0) = 0$ for $n \geq 0$ (if the word is nonempty, then there is at least one data value) and $G_{p,[\bar{a}]}(0,k+1) = 0$ for $k \geq 0$ (an empty word does not have any data value).

▶ **Lemma 11.** *The sequences $G_{p,[\bar{a}]}$'s satisfy the system of equations in Figure 2.*

$$\begin{aligned}
G_{p',[\bar a']}(n+1,k+1) = {} & \sum_{[p,\bar a \xrightarrow{\sigma,a} p',\bar a']\colon\, a\in\bar a} \underbrace{G_{p,[\bar a]}(n,k+1)}_{\mathbf{I}} + {} \\
& \sum_{[p,\bar a \xrightarrow{\sigma,a} p',\bar a']\colon\, a\notin\bar a} \left(\underbrace{G_{p,[\bar a]}(n,k)}_{\mathbf{II}} + \underbrace{\max(k+1-\#[\bar a],0)\cdot G_{p,[\bar a]}(n,k+1)}_{\mathbf{III}} \right), \\
S_\Sigma(n+1,k+1) = {} & |\Sigma|\cdot S_\Sigma(n,k) + |\Sigma|\cdot(k+1)\cdot S_\Sigma(n,k+1), \\
G(n,k) = {} & S_\Sigma(n,k) - \sum_{[p,\bar a]\in \mathsf{orbits}(C_F)} G_{p,[\bar a]}(n,k).
\end{aligned}$$

Figure 2 Linrec automata equations.

▶ **Example 12.** The equations corresponding to the automaton in Example 5 are as follows. (Since the automaton is orbitised, we can omit the orbit.) We have $G_p(0,0) = 1$, $G_q(0,0) = G_r(0,0) = G_s(0,0) = 0$ and for $n,k \geq 0$:

$$\begin{aligned}
&G_p(n+1,k+1) = 0, \\
&G_q(n+1,k+1) = \underbrace{G_p(n,k)}_{\mathbf{II}} + \underbrace{(k+1)\cdot G_p(n,k+1)}_{\mathbf{III}} + \underbrace{G_q(n,k)}_{\mathbf{II}} + \underbrace{k\cdot G_q(n,k+1)}_{\mathbf{III}}, \\
&G_r(n+1,k+1) = \underbrace{G_p(n,k)}_{\mathbf{II}} + \underbrace{(k+1)\cdot G_p(n,k+1)}_{\mathbf{III}} + \underbrace{G_r(n,k+1)}_{\mathbf{I}}, \\
&G_s(n+1,k+1) = \underbrace{G_q(n,k+1)}_{\mathbf{I}} + \underbrace{G_r(n,k)}_{\mathbf{II}} + \underbrace{k\cdot G_r(n,k+1)}_{\mathbf{III}}.
\end{aligned}$$

▶ **Lemma 13.** *Let A be an unambiguous register automaton over equality atoms without guessing with d registers and ℓ control locations. The universality problem for A reduces to the zeroness problem of the linrec sequence G defined by the system of equations in Figure 2 containing $O(\ell\cdot 2^{d\cdot\log d})$ variables and equations and constructible in* PSPACE*. If A is already orbitised, then the system of equations has size $O(\ell)$.*

5 Decidability of the zeroness problem

In this section, we present an algorithm to solve the zeroness problem of bidimensional linrec sequences with univariate polynomial coefficients, which is sufficient for linrec sequences from Figure 2. We first give a general presentation on elimination for bivariate polynomial coefficients, and then we use the univariate assumption to obtain a decision procedure. We model the non-commutative operators appearing in the definition of linrec sequences (2) with Ore polynomials (a.k.a. skew polynomials) [43][5]. Let R be a (not necessarily commutative) ring and σ an automorphism of R. The ring of *(shift) skew polynomials* $R[\partial;\sigma]$ is defined as the ring of polynomials but where the multiplication operation satisfies the following commutation rule: For a coefficient $a \in R$ and the unknown ∂, we have

$$\partial\cdot a = \sigma(a)\cdot\partial.$$

[5] The general definition of the Ore polynomial ring $R[\partial;\sigma,\delta]$ uses an additional component $\delta : R \to R$ in order to model differential operators. We present a simplified version which is enough for our purposes.

(The usual ring of polynomials is recovered when σ is the identity.) The multiplication extends to monomials as $a\partial^k \cdot b\partial^l = a\sigma^k(b) \cdot \partial^{k+l}$ and to the whole ring by distributivity. The *degree* of a skew monomial $a \cdot \partial^k$ is k, and the degree $\deg P$ of a skew polynomial P is the maximum of the degrees of its monomials. The degree function satisfies the expected identities $\deg(P \cdot Q) = \deg P + \deg Q$ and $\deg(P + Q) \leq \max(\deg P, \deg Q)$. A skew polynomial is *monic* if the coefficient of its monomial of highest degree is 1. The crucial and only property that we need in this section is that skew polynomial rings admit a Euclidean pseudo-division algorithm, which in turns allows one to find common left multiples. A skew polynomial ring $R[\partial; \sigma]$ has *pseudo-division* if for any two skew polynomials $A, B \in R[\partial; \sigma]$ with $\deg A \geq \deg B$ there is a coefficient $a \in R$ and skew polynomials $Q, R \in R[\partial; \sigma]$ s.t. $a \cdot A = P \cdot B + Q$ and $\deg Q < \deg B$. We say that a ring R has the *common left multiple* (CLM) property if for every $a, b \neq 0$, there exists $c, d \neq 0$ such that $c \cdot a = d \cdot b$.

▶ **Theorem 14** (c.f. [42, Sec. 1]). *If R has the CLM property, then 1) $R[\partial; \sigma]$ has a pseudo-division, and 2) $R[\partial; \sigma]$ also has the CLM property.*

The most important instances of skew polynomials are the *first* and *second Weyl algebras*:

$$W_1 = \mathbb{Q}[n, k][\partial_1; \sigma_1] \quad \text{and} \quad W_2 = W_1[\partial_2; \sigma_2] = \mathbb{Q}[n, k][\partial_1; \sigma_1][\partial_2; \sigma_2], \tag{4}$$

where $\mathbb{Q}[n, k]$ is the ring of bivariate polynomials, and the shifts satisfy $\sigma_1(p(n, k)) := p(n + 1, k)$ and $\sigma_2\left(\sum_i p_i(n, k)\partial_1^i\right) := \sum_i p_i(n, k + 1)\partial_1^i$. Skew polynomials in W_2 act on bidimensional sequences $f : \mathbb{Q}^{\mathbb{N}^2}$ by interpreting ∂_1 and ∂_2 as the two shifts. A linrec system of equations (2) can thus be interpreted as a system of linear equations with variables $f_1, \ldots, f_m$ and coefficients in W_2.

▶ **Example 15.** Continuing our running Example 12, we obtain the following linear system of equations with W_2 coefficients:

$$\begin{array}{rrrrl}
\partial_1\partial_2 \cdot G_p & & & & = 0, \\
-(1 + (k + 1)\partial_2) \cdot G_p & +(\partial_1\partial_2 - k\partial_2 - 1) \cdot G_q & & & = 0, \\
-(1 + (k + 1)\partial_2) \cdot G_p & & +(\partial_1\partial_2 - \partial_2) \cdot G_r & & = 0, \\
& -\partial_2 \cdot G_q & -(1 + k\partial_2) \cdot G_r & +\partial_1\partial_2 \cdot G_s & = 0,
\end{array}$$

$$\begin{aligned}
&(\partial_1\partial_2 - (k + 1)\partial_2 - 1) \cdot S_1 = 0, \\
&G_s - S_1 + G = 0.
\end{aligned}$$

Since $W_0 = \mathbb{N}[n, k]$ is commutative, it obviously has the CLM property. By two applications of Theorem 14, we have (see Appendix D.1 for CLM examples):

▶ **Corollary 16.** *The two Weyl algebras W_1 and W_2 have the CLM property.*

A (linear) *cancelling relation* (CR) for a bidimensional sequence $f : \mathbb{Q}^{\mathbb{N}^2}$ is a linear equation of the form

$$p_{i^*,j^*}(n, k) \cdot \partial_1^{i^*}\partial_2^{j^*} f = \sum_{(i,j) <_{\text{lex}} (i^*,j^*)} p_{i,j}(n, k) \cdot \partial_1^i \partial_2^j f, \tag{CR-2}$$

where $p_{i^*,j^*}(n, k), p_{i,j}(n, k) \in \mathbb{Q}[n, k]$ are bivariate polynomial coefficients and $<_{\text{lex}}$ is the lexicographic ordering. Cancelling relations for a one-dimensional sequence $g : \mathbb{Q}^{\mathbb{N}}$ are defined analogously (we use the second variable k as the index for convenience):

$$q_{j^*}(k) \cdot \partial_2^{j^*} g = \sum_{0 \leq j < j^*} q_j(k) \cdot \partial_2^j g. \tag{CR-1}$$

We use cancelling relations as certificates of zeroness for f when the $p_{i,j}$'s are univariate. We do not need to construct any cancelling relation, just knowing that some exists with the required bounds suffices.

▶ **Lemma 17.** *The zeroness problem for a bidimensional linrec sequence $f : \mathbb{Q}^{\mathbb{N}^2}$ of order $\leq m$ and univariate polynomial coefficients in $\mathbb{Q}[k]$ admitting some cancelling relation* (CR-2) *with leading coefficient $p_{i^*,j^*}(k) \in \mathbb{Q}[k]$ of degree $\leq e$ and height $\leq h$ s.t. each of the one-dimensional sections $f(M, k) \in \mathbb{Q}^{\mathbb{N}}$ for $1 \leq M \leq i^*$ also admits some cancelling relation* (CR-1) *of ∂_2-degree $\leq d$ with leading polynomial coefficients of degrees $\leq e$ and height $\leq h$ is decidable in deterministic time $\tilde{O}(p(m, i^*, j^*, d, e, h))$ for some polynomial p.*

Elimination already yields decidability with elementary complexity for the zeroness problem and thus for the universality/equivalence/inclusion problems of unambiguous register automata without guessing.

▶ **Theorem 18.** *The zeroness problem for linrec sequences with univariate polynomial coefficients from $\mathbb{Q}[k]$ (or from $\mathbb{Q}[n]$) is decidable.*

▶ **Example 19.** Continuing our running Example 15, we subsequently eliminate G_p, G_s, G_r, G_q, S finally obtaining (c.f. Example 34 in Appendix D.2 for details)

$$\begin{aligned} G(n+4, k+4) = \quad & (k+3) \cdot G(n+3, k+4) + G(n+3, k+3) + \\ & -(k+2) \cdot G(n+2, k+4) - G(n+2, k+3). \end{aligned} \tag{5}$$

As expected, all coefficients are polynomials in $\mathbb{Q}[k]$ and in particular they do not involve the variable n. Moreover, we note that the relation above is *monic*, in the sense that the lexicographically leading term $G(n+4, k+4)$ has coefficient 1 (c.f. Sec. 7). (C.f. Example 35 for elimination in a two-register automaton and Example 36 for a one-register automaton accepting all words of length ≥ 2.)

We omit a precise complexity analysis of elimination because better bounds can be obtained by resorting to linear non-commutative algebra, which is the topic of the next section.

6 Complexity of the zeroness problem

In this section we present an EXPTIME algorithm to solve the zeroness problem and we apply this result to register automata. We compute the *Hermite normal form* (HNF) of the matrix with skew polynomial coefficients associated to (2) in order to do elimination in a more efficient way. The complexity bounds provided by Giesbrecht and Kim [26] on the computation of the HNF lead to the following bounds for cancelling relations; c.f. Appendix E for further details and full proofs.

▶ **Lemma 20.** *A linrec sequence $f \in \mathbb{Q}^{\mathbb{N}^2}$ of order $\leq m$, degree $\leq d$, and height $\leq h$ admits a cancelling relation* (CR-2) *with the orders i^*, j^* and the degree of p_{i^*,j^*} polynomially bounded, and with height $|p_{i^*,j^*}|_\infty$ exponentially bounded. Similarly, its one-dimensional sections $f(0, k), \ldots, f(i^*, k) \in \mathbb{Q}^{\mathbb{N}}$ also admit cancelling relations* (CR-1) *of polynomially bounded orders and degree, and exponentially bounded height.*

This allows us to prove below the EXPTIME upper-bound for zeroness of Theorem 1, and the 2-EXPTIME algorithm for inclusion of Theorem 2.

Proof of Theorem 1. Thanks to the bounds from Lemma 20, i^*, j^* are polynomially bounded; we can find a polynomial bound d on the ∂_2-degrees of the cancelling relations $R_0, \ldots, R_{i^*}$

for the sections $f(0,k),\ldots,f(i^*,k)$, respectively; we can find a polynomial bound e on the degrees of $p_{i^*,j^*}(k)$ and the leading polynomial coefficients of the R_i's; and an exponential bound h on $|p_{i^*,j^*}|_\infty$ and the heights of the leading polynomial coefficients of the R_i's. We thus obtain an EXPTIME algorithm by Lemma 17. ◀

This yields the announced upper-bounds for the inclusion problem for register automata.

Proof of Theorem 2. For the universality problem $L(B)=(\Sigma\times\mathbb{A})^*$, let d be the number of registers and ℓ the number of control locations of B. By Lemma 13, the universality problem reduces in PSPACE to zeroness of a linrec system with polynomial coefficients in $\mathbb{Q}[k]$ containing $O(\ell\cdot 2^{d\cdot\log d})$ variables $G_{p,[\bar{a}]}$ and the same number of equations. By Theorem 1, we get a 2-EXPTIME algorithm. When the numbers of registers d is fixed, we get an EXPTIME algorithm. For the inclusion problem $L(A)\subseteq L(B)$, we first orbitise A into an equivalent orbitised register automaton without guessing A'. A close inspection of the two constructions leading to C in the proof of Lemma 8 reveal that transitions in C are either transitions from A' (and thus already orbitised), or pairs of a transition in B together with a transition in A', the second of which is already orbitised. It follows that orbitising C incurs in an exponential blow-up w.r.t. the number of registers of B, but only polynomial w.r.t. the number of registers of A' (and thus of A), since the A'-part in C is already orbitised. Consequently, we can write (in PSPACE) a system of linrec equations for the universality problem of C of size exponential in the number of registers of A and of B. By reasoning as in the first part of the proof, we obtain a EXPTIME algorithm for the universality problem of C, and thus a 2-EXPTIME algorithm for the original inclusion problem $L(A)\subseteq L(B)$. If both the number of registers of A and of B is fixed, we get an EXPTIME algorithm. The equivalence problem $L(A)=L(B)$ with both automata A,B unambiguous reduces to two inclusion problems. ◀

7 Further remarks and conclusions

We say that $P=\sum_{i,j}p_{i,j}(n,k)\cdot\partial_1^i\partial_2^j$ is *monic* if $p_{i^*,j^*}=1$ where (i^*,j^*) is the lexicographically largest pair (i,j) s.t. $p_{i,j}\neq 0$. The cancelling relation (CR-2) in our examples (5), (10), (11), (15) happens to be monic in this sense.

▶ **Conjecture 21** (Monicity conjecture). *There always exists a* monic *cancelling relation* (CR-2) *for linrec systems obtained from automata equations in Figure 2, and similarly for their sections* (CR-1).

Conjecture 21 has important algorithmic consequences. The exponential complexity in Theorem 1 comes from the exponential growth of the rational number coefficients (heights) in the HNF. This is due to the use of Lemma 17, whose complexity depends on the maximal root of the leading polynomial $p_{i^*,j^*}(n,k)$ from (CR-2). If Conjecture 21 holds, then $p_{i^*,j^*}(n,k)=1$, Lemma 17 would yield a PTIME algorithm for zeroness, and consequently all complexities in Theorem 2, would drop by one exponential. This provides ample motivation to investigate the monicity conjecture.

In order to obtain the lower EXPTIME complexity for $L(A)\subseteq L(B)$ in Theorem 2 we have to fix the number of registers in *both* automata A and B. The EXPSPACE upper bound of Mottet and Quaas [37] holds already when only the number of registers of B is fixed, while we only obtain a 2-EXPTIME upper bound in this case. It is left for future work whether the counting approach can yield better bounds without fixing the number of registers of A.

The fact that the automata are non-guessing is crucial in each of the cases **I**, **II**, and **III** of the equations in Figure 2 in order to correctly count the number of orbits of runs.

For automata with guessing from the fact that the current input a is stored in a register we cannot deduce that a actually appeared previously in the input word w, and thus our current parametrisation in terms of length and width does not lead to a recursive characterisation.

in the last-step decomposition since we need to know that all values in $\bar{a}$

Finally, it is also left for further work to extend the counting approach to other data domains such as total order atoms, random graph atoms, etc. . . , and, more generally, to arbitrary homogeneous and ω-categorical atoms under suitable computability assumptions (c.f. [16]), and to other models of computation such as register pushdown automata [13, 39].

References

1 Ronald Alter and K.K Kubota. Prime and prime power divisibility of Catalan numbers. *Journal of Combinatorial Theory, Series A*, 15(3):243 – 256, 1973.

2 Christel Baier, Stefan Kiefer, Joachim Klein, Sascha Klüppelholz, David Müller, and James Worrell. Markov Chains and Unambiguous Büchi Automata. In Swarat Chaudhuri and Azadeh Farzan, editors, *Proc. of CAV'16*, pages 23–42, Cham, 2016. Springer International Publishing.

3 M. Benedikt, T. Duff, A. Sharad, and J. Worrell. Polynomial automata: Zeroness and applications. In *Proc. of LICS'17*, pages 1–12, June 2017. doi:10.1109/LICS.2017.8005101.

4 Mikołaj Bojańczyk. *Slightly Infinite Sets.* 2019. URL: https://www.mimuw.edu.pl/~bojan/paper/atom-book.

5 Alin Bostan, Arnaud Carayol, Florent Koechlin, and Cyril Nicaud. Weakly-Unambiguous Parikh Automata and Their Link to Holonomic Series. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *Proc. of ICALP'20*, volume 168 of *LIPIcs*, pages 114:1–114:16, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

6 Alin Bostan, Frédéric Chyzak, Bruno Salvy, and Ziming Li. Fast computation of common left multiples of linear ordinary differential operators. In *Proc. of ISAAC'12*, pages 99–106, New York, NY, USA, 2012. ACM.

7 Nicolas Bousquet and Christof Löding. Equivalence and inclusion problem for strongly unambiguous büchi automata. In Adrian-Horia Dediu, Henning Fernau, and Carlos Martín-Vide, editors, *Proc. of LATA'10*, pages 118–129, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

8 Mireille Bousquet-Mélou. Algebraic generating functions in enumerative combinatorics and context-free languages. In Volker Diekert and Bruno Durand, editors, *Proc. of STACS'05*, pages 18–35, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

9 Michaël Cadilhac, Alain Finkel, and Pierre McKenzie. Unambiguous constrained automata. In Hsu-Chun Yen and Oscar H. Ibarra, editors, *Proc. of DLT'12*, volume 7410 of *LNCS*, pages 239–250. Springer Berlin Heidelberg, 2012.

10 Michaël Cadilhac, Filip Mazowiecki, Charles Paperman, Michał Pilipczuk, and Géraud Sénizergues. On Polynomial Recursive Sequences. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *Proc. of ICALP'20*, volume 168 of *LIPIcs*, pages 117:1–117:17, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

11 Peter J. Cameron. *Notes on Counting: An Introduction to Enumerative Combinatorics.* Australian Mathematical Society Lecture Series. Cambridge University Press, 1 edition, 2017.

12 Giusi Castiglione and Paolo Massazza. On a class of languages with holonomic generating functions. *Theoretical Computer Science*, 658:74–84, 2017.

13 Edward Y. C. Cheng and Michael Kaminski. Context-free languages over infinite alphabets. *Acta Inf.*, 35(3):245–267, 1998.

14 N. Chomsky and M. P. Schützenberger. The algebraic theory of context-free languages. In P. Braffort and D. Hirschberg, editors, *Computer Programming and Formal Systems*, volume 35 of *Studies in Logic and the Foundations of Mathematics*, pages 118–161. Elsevier, 1963.

15 Lorenzo Clemente. On the complexity of the universality and inclusion problems for unambiguous context-free grammars. In Laurent Fribourg and Matthias Heizmann, editors, Proceedings 8th International Workshop on *Verification and Program Transformation* and 7th Workshop on *Horn Clauses for Verification and Synthesis,* Dublin, Ireland, 25-26th April 2020, volume 320 of *EPTCS*, pages 29–43. Open Publishing Association, 2020. doi:10.4204/EPTCS.320.2.

16 Lorenzo Clemente and Slawomir Lasota. Reachability analysis of first-order definable pushdown systems. In Stephan Kreutzer, editor, *Proc. of CSL'15*, volume 41 of *LIPIcs*, pages 244–259, Dagstuhl, 2015.

17 P. M. Cohn. *Skew Fields: Theory of General Division Rings*, volume 57 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, 1995.

18 Thomas Colcombet. Forms of Determinism for Automata (Invited Talk). In Christoph Dürr and Thomas Wilke, editors, *Proc. of STACS'12*, volume 14 of *LIPIcs*, pages 1–23, Dagstuhl, Germany, 2012. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

19 Thomas Colcombet. Unambiguity in automata theory. In Jeffrey Shallit and Alexander Okhotin, editors, *Descriptional Complexity of Formal Systems*, pages 3–18, Cham, 2015. Springer International Publishing.

20 Wojciech Czerwiński, Diego Figueira, and Piotr Hofman. Universality Problem for Unambiguous VASS. In Igor Konnov and Laura Kovács, editors, *Proc. of CONCUR'20*, volume 171 of *LIPIcs*, pages 36:1–36:15, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

21 Laure Daviaud, Marcin Jurdzinski, Ranko Lazic, Filip Mazowiecki, Guillermo A. Pérez, and James Worrell. When is Containment Decidable for Probabilistic Automatal. In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *Proc. of ICALP'18*, volume 107 of *LIPIcs*, pages 121:1–121:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

22 Stéphane Demri and Ranko Lazić. LTL with the freeze quantifier and register automata. *ACM Trans. Comput. Logic*, 10(3):16:1–16:30, April 2009.

23 Philippe Flajolet, Stefan Gerhold, and Bruno Salvy. On the non-holonomic character of logarithms, powers, and the nth prime function. *Electr. J. Comb.*, 11(2), 2005.

24 Stefan Gerhold. On some non-holonomic sequences. *Electr. J. Comb.*, 11(1), 2004.

25 M. Giesbrecht. Factoring in skew-polynomial rings over finite fields. *Journal of Symbolic Computation*, 26(4):463–486, 1998. URL: `http://www.sciencedirect.com/science/article/pii/S0747717198902243`, `doi:https://doi.org/10.1006/jsco.1998.0224`.

26 Mark Giesbrecht and Myung Sub Kim. Computing the Hermite form of a matrix of Ore polynomials. *Journal of Algebra*, 376:341–362, 2013.

27 Vesa Halava, Tero Harju, Mika Hirvensalo, and Juhani Karhumäki. Skolem's problem - on the border between decidability and undecidability, 2005.

28 John Hopcroft, Rajeev Motwani, and Jeffrey Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, 2000.

29 Michael Kaminski and Nissim Francez. Finite-memory automata. *Theoretical Computer Science*, 134(2):329–363, 1994.

30 Michael Kaminski and Daniel Zeitlin. Finite-memory automata with non-deterministic reassignment. *International Journal of Foundations of Computer Science*, 21(05):741–760, 2010.

31 Ravindran Kannan and Achim Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM Journal on Computing*, 8(4):499–507, 1979.

32 Martin Klazar. Bell numbers, their relatives, and algebraic differential equations. *Journal of Combinatorial Theory, Series A*, 102(1):63–87, 2003. URL: `http://www.sciencedirect.com/science/article/pii/S0097316503000141`, `doi:https://doi.org/10.1016/S0097-3165(03)00014-1`.

33 Werner Kuich. On the multiplicity equivalence problem for context-free grammars. In *Proceedings of the Colloquium in Honor of Arto Salomaa on Results and Trends in Theoretical Computer Science*, pages 232—250, Berlin, Heidelberg, 1994. Springer-Verlag.

34 George Labahn, Vincent Neiger, and Wei Zhou. Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix. *Journal of Complexity*, 42:44–71, 2017.

35 Leonard Lipshitz. D-finite power series. *Journal of Algebra*, 122(2):353–373, 1989.

36 Dugald Macpherson. A survey of homogeneous structures. *Discrete Math.*, 311(15):1599–1634, August 2011.

37 Antoine Mottet and Karin Quaas. The containment problem for unambiguous register automata and unambiguous timed automata. *Theory of Computing Systems*, 2020. `doi:10.1007/s00224-020-09997-2`.

38 T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *Journal of Symbolic Computation*, 35(4):377–401, 2003.

39 A.S. Murawski, S.J. Ramsay, and N. Tzevelekos. Reachability in pushdown register automata. *Journal of Computer and System Sciences*, 87:58–83, 2017.

40 Vincent Neiger, Johan Rosenkilde, and Grigory Solomatov. Computing Popov and Hermite forms of rectangular polynomial matrices. In *Proc. of ISAAC'18*, pages 295—302, New York, NY, USA, 2018. ACM.

41 Frank Neven, Thomas Schwentick, and Victor Vianu. Finite state machines for strings over infinite alphabets. *ACM Trans. Comput. Logic*, 5(3):403—435, July 2004.

42 Oystein Ore. Linear equations in non-commutative fields. *Annals of Mathematics*, 32(3):463–477, 1931. URL: http://www.jstor.org/stable/1968245.

43 Oystein Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480–508, 1933. URL: http://www.jstor.org/stable/1968173.

44 Mikhail Raskin. A Superpolynomial Lower Bound for the Size of Non-Deterministic Complement of an Unambiguous Automaton. In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *Proc. of ICALP'18*, volume 107 of *LIPIcs*, pages 138:1–138:11, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

45 Arto Salomaa and Marti Soittola. *Automata-theoretic aspects of formal power series.* Texts and Monographs in Computer Science. Springer, 1978.

46 James Schmerl. A decidable $\aleph_0$-categorical theory with a non-recursive Ryll-Nardzewski function. *Fundamenta Mathematicae*, 98(2):121–125, 1978.

47 Luc Segoufin. Automata and logics for words and trees over an infinite alphabet. In Zoltán Ésik, editor, *Computer Science Logic*, volume 4207 of *LNCS*, pages 41–57. Springer Berlin Heidelberg, 2006.

48 Géraud Sénizergues. The equivalence problem for deterministic pushdown automata is decidable. In Pierpaolo Degano, Roberto Gorrieri, and Alberto Marchetti-Spaccamela, editors, *Proc. of ICALP'97*, pages 671–681, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

49 Richard P. Stanley. Differentiably finite power series. *European Journal of Combinatorics*, 1(2):175–188, 1980.

50 Richard P. Stanley. *Enumerative Combinatorics.* The Wadsworth & Brooks/Cole Mathematics Series 1. Springer, 1 edition, 1986.

51 R. Stearns and H. Hunt. On the equivalence and containment problems for unambiguous regular expressions, grammars, and automata. In *Proc. of SFCS'81*, pages 74–81, Washington, DC, USA, 1981. IEEE Computer Society. URL: http://dx.doi.org/10.1109/SFCS.1981.29, doi:10.1109/SFCS.1981.29.

52 L. J. Stockmeyer and A. R. Meyer. Word problems requiring exponential time (preliminary report). In *Proc. of STOC'73*, pages 1–9, New York, NY, USA, 1973. ACM.

53 Wen-Guey Tzeng. A polynomial-time algorithm for the equivalence of probabilistic automata. *SIAM J. Comput.*, 21(2):216–227, April 1992.

54 G. Villard. Computing Popov and Hermite forms of polynomial matrices. In *Proc. of ISAAC'96*, pages 250—258, New York, NY, USA, 1996. Association for Computing Machinery.

55 Tzeng Wen-Guey. On path equivalence of nondeterministic finite automata. *Information Processing Letters*, 58(1):43–46, 1996.

A Additional material for Sec. 2

A.1 One-dimensional linear recursive sequences

Let $f(n) : \mathbb{Q}^{\mathbb{N}}$ be a one-dimensional sequence. The shift operator $\partial : \mathbb{Q}^{\mathbb{N}} \to \mathbb{Q}^{\mathbb{N}}$ is defined as $(\partial f)(n) = f(n+1)$ for every $n \in \mathbb{N}$. A one-dimensional sequence f is *linear recursive* (linrec) if there are auxiliary sequences $f = f_1, f_2, \dots, f_m : \mathbb{Q}^{\mathbb{N}}$ satisfying a system of equations of the form

$$\begin{cases} \partial f_1 &= p_{1,1} \cdot f_1 + \cdots + p_{1,m} \cdot f_m, \\ &\vdots \\ \partial f_m &= p_{m,1} \cdot f_1 + \cdots + p_{m,m} \cdot f_m, \end{cases} \tag{6}$$

where the $p_{i,j} \in \mathbb{Q}[n]$ are univariate polynomials. The *order* of a linrec sequence is the smallest m s.t. it admits a description as above. Allowing terms on the r.h.s. of the form $p \in \mathbb{Q}[n]$ does not increase the expressiveness power since univariate polynomials are already linrec and thus p could be replaced by introducing an auxiliary variable for it. If we fix the initial conditions $f_1(0), \dots, f_m(0)$, then the system above has unique solution, and we can moreover compute all the values $f_i(n)$'s by unfolding the definition. Amongst innumerable others, the *Fibonacci sequence* $\partial^2 f = \partial f + f$ is linrec (even constant recursive) since we can introduce an auxiliary sequence g and write $\partial f = f + g$ and $\partial g = f$. An example using non-constant polynomial coefficients is provided by the number $t(n)$ of *involutions* of $\{1, \dots, n\}$ (a.k.a. *telephone numbers*) since $\partial^2 t = \partial t + (n+1) \cdot t$; by introducing an auxiliary sequence $s(n)$, we have a linrec system $\partial t = t + n \cdot s$ and $\partial s = t$.

A.2 Examples of bidimensional linrec sequences

There is a wealth of examples of linrec sequences. The power sequence n^k is bidimensional linrec since for $n, k \geq 1$, $n^k = n \cdot n^{k-1}$ and the two sections 0^k and n^0 are certainly constant after the first element. The sequence of *binomial coefficients* $\binom{n}{k}$ is linrec since $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ for $n, k \geq 1$ and the two sections satisfy $\binom{n}{0} = 1$ for $n \geq 0$ and $\binom{0}{k} = 0$ for $k \geq 1$. The *Stirling numbers of the first kind* $s(n,k)$ are linrec since $s(n,k) = s(n-1,k-1) - (n-1) \cdot s(n-1,k)$ for $n, k \geq 1$ and the two sections $s(n,0) = s(0,k) = 0$ are constant for $n, k \geq 1$. Similar recurrences appear for the Stirling numbers of the second kind $S(n,k)$ (as remarked in the introduction), the *Eulerian numbers* $A(n,k) = (n-k) \cdot A(n-1, m-1) + (k+1) \cdot A(n-1,m)$ the *triangle numbers* $T(n,k) = k \cdot T(n-1,k-1) + k \cdot T(n-1,k)$, and many more.

As an additional example, consider the *Bell numbers* $B(n)$, which count the number of non-empty partitions of a set of n elements. Notice that $B(n)$ is not linrec, in fact not even P-recursive [32, 24]. The well-known relationship $B(n) = \sum_{k=0}^{n} S(n,k)$ suggests to consider the partial sums $C(n,k) = \sum_{i=0}^{k-1} S(n,k)$. We have $C(n,0) = 0$ and $C(n+1,k+1) = S(n,k) + C(n+1,k)$, thus C is linrec and $B(n) = C(n+1,n+1)$ is its diagonal (shifted by one).

A.3 Comparison with other classes of sequences

Linrec vs. C-recursive. A sequence $f : \mathbb{Q}^{\mathbb{N}^d}$ is *C-recursive* if it satisfies a recursion as in (2) where the affine operators $A_{i,j}$ are restricted to be of the form $c_{i,j,0} + c_{i,j,1}\partial_1 + c_{i,j,2}\partial_2$ for some constants $c_{i,j,0}, c_{i,j,1}, c_{i,j,2} \in \mathbb{Q}$. Thus bidimensional C-recursive sequences are linrec by definition. Since the asymptotic growth of a 1-dimensional C-recursive sequence $f(n)$ is $O(r^n)$ for some constant $r \in \mathbb{Q}$, the sequence $n! = n \cdot (n-1)!$ is linrec but not C-recursive, and thus the inclusion is strict. An useful fact is that zeroness of C-recursive sequences can be solved in PTIME [51, 53].

▶ **Lemma 22.** *The zeroness problem for a one-dimensional C-recursive sequence can be solved in* PTIME.

Proof. It is well-known that a one-dimensional C-recursive sequence f of order m represented as in (6) where the $p_{i,j}$'s are rational numbers in $\mathbb{Q}$, can be transformed into a single recurrence

$$\partial_m f = c_0 \cdot \partial_0 f + \cdots + c_{m-1} \cdot \partial_{m-1} f,$$

where $c_0, \cdots, c_{m-1} \in \mathbb{Q}$. C.f. the proof of [27, Lemma 1] relying on the Cayley-Hamilton theorem, or the more recent proof of [10, Proposition 1] relying on a linear independence argument. It follows that $f = 0$ if, and only if, $f(n) = 0$ for $0 \leq n \leq m-1$. The latter condition can be checked in PTIME by Lemma 3. ◀

Linrec vs. P-recursive. In dimension one, linrec sequences are a special case of *P-recursive sequences* [49]. The latter class can be defined as those sequences $f : \mathbb{Q}^\mathbb{N}$ satisfying a linear equation of the form $p_k(n)f(n) + p_{k-1}(n)f(n-1) + \cdots + p_0(n)f(n-k) = 0$ for every $n \geq k$, where $p_k(n), \ldots, p_0(n) \in \mathbb{Q}[n]$. Thus linrec corresponds to P-recursive with leading polynomial coefficient $p_k(i) = 1$. The inclusion is strict. The Catalan numbers $C(n)$ are P-recursive since they satisfy $(n+2) \cdot C(n+1) = (4n+2) \cdot C(n)$ for every $n \geq 0$. However, they are not linrec, and in fact not even polyrec (a more general class, c.f. below), since 1) by [10, Theorem 6] polyrec (and thus linrec) sequences are ultimately periodic modulo every sufficiently large prime, and 2) $C(n)$ is not ultimately periodic modulo any prime p [1].

In dimension two, linrec and P-recursive sequences [35] are incomparable. The sequence $f(m,n) = m^n$ is linrec since $f(m+1,n+1) = (m+1) \cdot f(m+1,n)$, $f(m,0) = 1$, and $f(0,n+1) = 0$. The diagonal of f is thus $f(n,n) = n^n$. Since P-recursive sequences are closed under taking diagonals [35, Theorem 3.8] and n^n is not P-recursive [23, Section 1, page 5], it follows that m^n is not P-recursive either (as a two-dimensional sequence).

Linrec vs. polyrec A one-dimensional sequence $f : \mathbb{Q}^\mathbb{N}$ is *polynomial recursive* (polyrec) if it satisfies a system of equations as in (6) where the rhs' are polynomial expressions in $\mathbb{Q}[f_1(n), \ldots, f_m(n)]$ [10, Definition 3][6]. In dimension one, the class of linrec sequences is strictly included in the class of polyrec sequences. Consider the sequence $f(n) = 2^{2^n}$. On the one hand, it is polyrec since $f(n+1) = f(n)^2$. On the other hand, it is not linrec, and in fact not even P-recursive, since a P-recursive sequence $g(n)$ has growth rate $O((n!)^c)$ for some constant $c \in \mathbb{N}$ [35, Proposition 3.11]. To the best of our knowledge, polyrec sequences in higher dimension have not been studied yet.

A.4 Zeroness problem

Zeroness of one-dimensional C-recursive sequences is decidable in NC^2 [53] (and thus in polylogarithmic space); we recalled a simple argument leading to a PTIME algorithm in Lemma 22. Zeroness of one-dimensional P-recursive sequences is decidable (c.f. [12] and the corrections in [5, Section 5]). Zeroness of one-dimensional polyrec sequences is decidable, and in fact the more general zeroness problem for polynomial automata is decidable with non-primitive recursive complexity [3] (polyrec sequences correspond to polynomial automata over a unary alphabet $\Sigma = \{a\}$).

[6] Since polynomial coefficients can already be defined in this formalism, we would obtain the same class by allowing more general expressions in $\mathbb{Q}[n][f_1(n), \ldots, f_m(n)]$.

A.5 Proofs for Sec. 2

▶ **Lemma 4.** *If $f : \mathbb{Q}^{\mathbb{N}^2}$ is linrec of order $\leq m$, degree $\leq d$, and height $\leq h$, then its L-sections $f(L, k), f(n, L) : \mathbb{Q}^{\mathbb{N}}$ are linrec of order $\leq m \cdot (L + 3)$, degree $\leq d$, and height $\leq h \cdot L^d$.*

Proof. We prove the lemma for the L-section $f^L(n)$ defined as $f(n, L)$. Let the auxiliary sequences be $f = f_1, \ldots, f_m$ as in (2), and fix the initial conditions $f_j(0, \geq 1), f_j(\geq 1, 0), f_j(0, 0) \in \mathbb{Q}$ for every $1 \leq j \leq m$. Let $f_j^K(n)$ be a new variable denoting the K-section $f_j(n, K)$, for every $1 \leq j \leq m$ and $0 \leq K \leq L$. We show by induction on K that all the f_j^K's are linrec. In the base case $K = 0$, $f_j^0(n)$ is linrec by setting $f_j^0(0) = f_j(0, 0) \in \mathbb{Q}$ and $\partial_1 f_j^0(n) = f_j(n + 1, 0) = f_j(\geq 1, 0) \in \mathbb{Q}$. Notice that, strictly speaking, the latter is not a legal linrec equation since constants are allowed only in the base case and not in (6) (which are linear systems and not affine ones). To this end, we introduce an extra variable $g_j(n)$ and we define $g_j(0) = f_j(\geq 1, 0) \in \mathbb{Q}$, and we have the linrec equations

$$\partial_1 f_j^0(n) = g_j(n),$$
$$\partial_1 g_j(n) = g_j(n).$$

For the inductive step, we write

$$\begin{aligned}\partial_1 f_j^{M+1}(n) &= \partial_1 \partial_2 f_j(n, M)\\ &= \sum_i (p_{i00}(n, M) + p_{i01}(n, M) \cdot \partial_1 + p_{i11}(n, M) \cdot \partial_2) f_i(n, M)\\ &= \sum_i \left((p_{i00}(n, M) + p_{i01}(n, M) \cdot \partial_1) f_i^M(n) + p_{i11}(n, M) \cdot f_i^{M+1}(n)\right).\end{aligned}$$

By induction, each f_i^M is one-dimensional linrec, and we can thus adjoin their corresponding systems of equations. We have introduced $m \cdot (L + 1)$ new variables f_j^L's and m variables g_j's (thus $m + m \cdot (L + 1) + m = m \cdot (L + 3)$ in total), and the same number of additional equations. The initial condition for the new variables f_j^M is $f_j^M(0) = f_j(0, M)$, which can be computed in PTIME by Lemma 3. Moreover every polynomial coefficient appears already in the original system, but with the second parameter fixed to some $0 \leq M \leq L$. Therefore the degree does not increase and the height is bounded by $h \cdot L^d$. ◀

B Proofs for Sec. 3

▶ **Lemma 8.** *Let A and B be two register automata.*

1. *The inclusion problem $L(A) \subseteq L(B)$ with A orbitised and without guessing reduces in* PTIME *to the case where A is deterministic. The reduction preserves whether B is 1) unambiguous, 2) without guessing, and 3) orbitised.*
2. *The inclusion problem $L(A) \subseteq L(B)$ with A deterministic reduces in* PTIME *to the universality problem for some register automaton C. If B is unambiguous, then so is C. If B is without guessing, then so is C. If A and B are orbitised, then so is C.*

The two reductions in Lemma 8 are sufficiently generic to be useful also in other contexts. For instance, in the context of nondeterministic finite automata they imply that the inclusion problem $L(A) \subseteq L(B)$ with A nondeterministic and B unambiguous reduces in PTIME to the universality problem of an unambiguous finite automaton. Since the latter problem is in PTIME [51, Corollary 4.7], the inclusion problem is in PTIME as well. Notice that we didn't assume that A is unambiguous, as it is often done in analogous circumstances [51], [5, Section 5]. A similar reduction has recently been used in the context of inclusion problems between context-free grammars and finite automata [15, Sec. 3.1] In the context of register automata, the results of [37] do not make any unambiguity assumption on A.

Proof. Consider two register automata A and B over finite alphabet Σ with transition relations $\rightarrow_A$, resp., $\rightarrow_B$. We assume w.l.o.g. that they have the same number of registers. Regarding the first point, consider the new finite alphabet $\Sigma' = \rightarrow_A$ which equals exactly the set of transition rules of A. Let $h : \Sigma' \to \Sigma$ be the surjective homomorphism allowing us to recover the original letter and defined as $h(p \xrightarrow{\sigma,\varphi} q) = \sigma$; We extend h to a function $\hat{h} : (\Sigma' \times \mathbb{A}) \to (\Sigma \times \mathbb{A})$ by preserving the data value $\hat{h}(t, a) = (h(t), a)$. Consider the automaton A' obtained from A by replacing every transition rule $t = (p \xrightarrow{\sigma,\varphi}_A q)$ of A with $p \xrightarrow{t,\varphi}_{A'} q$. Since A' has the same set of control locations and number of transitions as A, it is clearly of polynomial size. Since A is without guessing and orbitised, φ uniquely determines the next register contents given the current configuration and input (σ, a). Thus the only source of nondeterminism in A resides in the fact that there may be several transitions over the same σ. This nondeterminism is removed in A', since σ is replaced by the transition t itself. Consequently, A' is deterministic.

Consider the automaton B' obtained from B by replacing every transition rule $p \xrightarrow{\sigma,\varphi}_B q$ with *all* transitions of the form $p \xrightarrow{t,\varphi}_{B'} q$ s.t. $h(t) = \sigma$. Clearly, B' has the same control locations as B and number of transitions $O(|\rightarrow_A| \cdot |\rightarrow_B|)$. Moreover, if B is orbitised, then so it is B' Thus B' is of polynomial size and by definition $L(B') = \hat{h}^{-1}(L(B))$ and $L(B) = \hat{h}(L(B'))$. The correctness of the reduction follows from the following claims.

▷ Claim. $L(A) \subseteq L(B)$ if, and only if, $L(A') \subseteq L(B')$.

Proof of the claim. For the "only if" direction, assume $L(A) \subseteq L(B)$ and let $w \in L(A')$. By the definition of A', $\hat{h}(w) \in L(A)$, and thus $\hat{h}(w) \in L(B)$ by assumption. It follows that $w \in \hat{h}^{-1}(L(B)) = L(B')$, as required.

For the "if" direction, assume $L(A') \subseteq L(B')$ and let $w = (\sigma_1, a_1) \cdots (\sigma_n, a_n) \in L(A)$. Let the corresponding accepting run in A be

$$\pi = (p_0, \bar{a}_0) \xrightarrow{\sigma_1,a_1} \cdots \xrightarrow{\sigma_n,a_n} (p_n, \bar{a}_n).$$

induced by the sequence of transitions $t_1 = (p_0 \xrightarrow{\sigma_1,\varphi_1} p_1), \ldots, t_n = (p_{n-1} \xrightarrow{\sigma_n,\varphi_n} p_n)$. By the definition of A', $\rho := (t_1, a_1) \cdots (t_n, a_n) \in L(A')$, and thus $\rho \in L(B')$ by assumption. By definition of B', $w = \hat{h}(\rho) \in \hat{h}(L(B')) = L(B)$, as required. ◀

▷ Claim. If B is unambiguous, then so it is B'.

Proof of the claim. If there are two distinct accepting runs in B' over the same input word $w \in (\Sigma' \times \mathbb{A})*$, then applying $\hat{h}$ yields two distinct accepting runs in B over $\hat{h}(w) \in (\Sigma \times \mathbb{A})^*$. ◀

▷ Claim. If B is without guessing, then so it is B'.

Proof of the claim. If there is a reachable transition in $[\![B']\!]$ of the form $(p, \bar{a}) \xrightarrow{t,a} (q, \bar{a}')$ s.t. some fresh a'_i occurs in $\bar{a}'$, then the same holds for $(p, \bar{a}) \xrightarrow{h(t),a} (q, \bar{a}')$ in $[\![B]\!]$. ◀

We now show the second point, and we thus assume that A is deterministic. By pure set-theoretic manipulations, we have

$$L(A) \subseteq L(B) \text{ iff } L(B) \cup L(A)^c = (\mathbb{A} \times A)^* \text{ iff } (L(B) \cap L(A)) \cup L(A)^c = (\mathbb{A} \times A)^*,$$

where $L(A)^c$ denotes $(\mathbb{A} \times A)^* \setminus L(A)$. It suffices to observe that 1) $L(A)^c$ is recognisable by a deterministic (and thus unambiguous and without guessing) register automaton constructible in PTIME, 2) $L(B) \cap L(A)$ is recognisable by an unambiguous and without guessing automaton of polynomial size (since A is deterministic and B unambiguous and without guessing), and 3) the disjoint union of two unambiguous and without guessing languages is unambiguous and without guessing, and the complexity is again polynomial. We thus take as C any unambiguous and without guessing automaton of polynomial size s.t. $L(C) = (L(B) \cap L(A)) \cup L(A)^c$. Finally, if A and B are orbitised, then C is also orbitised. ◀

C Proofs for Sec. 4

▶ **Lemma 9.** *Let $\bar{a}, \bar{b} \in \mathbb{A}^d_\perp$. If $[\bar{a}] = [\bar{b}]$, then $G_{p,\bar{a}}(n,k) = G_{p,\bar{b}}(n,k)$ for every $n, k \geq 0$.*

Proof. Let $R_{p,\bar{a}}(n,k)$ be the set whose cardinality is counted by $G_{p,\bar{a}}(n,k)$:

$$R_{p,\bar{a}}(n,k) = \{[\pi]_{\bar{a}} \mid w \in (\Sigma \times \mathbb{A})^n, \pi \in \mathsf{Runs}(C_I; w; p, \bar{a}), \#w = k\}. \tag{7}$$

Let $\alpha : \mathbb{A} \to \mathbb{A}$ be an automorphism s.t. $\alpha(\bar{a}) = \bar{b}$. We claim that there exists a bijective function from $R_{p,\bar{a}}(n,k)$ to $R_{p,\bar{b}}(n,k)$. Consider the function f that maps $\bar{a}$-orbits of runs to $\bar{b}$-orbits of runs defined as

$$f([\pi]_{\bar{a}}) = [\alpha(\pi)]_{\alpha(\bar{a})} = [\alpha(\pi)]_{\bar{b}}.$$

Since runs $\pi \in R_{p,\bar{a}}(n,k)$ are $\bar{a}$-supported and f preserves the length of the run and the width of the data word labelling it, f has the right type $f : R_{p,\bar{a}}(n,k) \to R_{p,\bar{b}}(n,k)$. We claim that f is injective on $R_{p,\bar{a}}(n,k)$. Towards a contradiction, assume $[\pi]_{\bar{a}} \neq [\rho]_{\bar{a}}$ but $[\alpha(\pi)]_{\bar{b}} = [\alpha(\rho)]_{\bar{b}}$. There exists a $\bar{b}$-automorphism $\beta : \mathbb{A} \to \mathbb{A}$ s.t. $\beta(\alpha(\pi)) = \alpha(\rho)$. Consequently, $\alpha^{-1}(\beta(\alpha(\pi))) = \rho$ maps π to ρ. Moreover, $\alpha^{-1}\beta\alpha$ is an $\bar{a}$-automorphism since

$$\begin{aligned}
\alpha^{-1}(\beta(\alpha(\bar{a}))) &= \alpha^{-1}(\beta(\bar{b})) && \text{(def. of } \alpha\text{)} \\
&= \alpha^{-1}(\bar{b}) && (\beta \text{ is a } \bar{b}\text{-automorphism}) \\
&= \bar{a} && \text{(def. of } \alpha\text{).}
\end{aligned}$$

It follows that $[\pi]_{\bar{a}} = [\rho]_{\bar{a}}$, which is a contradiction. Thus, f is injective. By a symmetric argument, there exists also an injective function $g : R_{p,\bar{b}}(n,k) \to R_{p,\bar{a}}(n,k)$. ◀

▶ **Lemma 11.** *The sequences $G_{p,[\bar{a}]}$'s satisfy the system of equations in Figure 2.*

Proof. We show that $G_{p,[\bar{a}]}(n,k)$ counts the number of orbits of initial runs over words of length n and width k ending in a configuration in the orbit $(p, [\bar{a}])$. Let $S_{p,\bar{a}}(n,k)$ be the set of initial runs ending in $(p, \bar{a})$ over words w of length n and width k:

$$S_{p,\bar{a}}(n,k) = \{\pi \mid w \in (\Sigma \times \mathbb{A})^n, \pi \in \mathsf{Runs}(C_I; w; p, \bar{a}), \#w = k\}. \tag{8}$$

We have $R_{p,\bar{a}}(n,k) = \mathsf{orbits}_{\bar{a}}(S_{p,\bar{a}}(n,k)) = \{[\pi]_{\bar{a}} \mid \pi \in S_{p,\bar{a}}(n,k)\}$. We observe the following decomposition for $n, k \geq 0$:

$$\begin{aligned} S_{p',\bar{a}'}(n+1,k+1) = & \underbrace{\bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\in\bar{a}} \{\pi \cdot t \mid \pi \in S_{p,\bar{a}}(n,k+1)\}}_{\mathbf{I}} \cup \\ & \underbrace{\bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\notin\bar{a}} \{\pi \cdot t \mid \pi \in S_{p,\bar{a}}(n,k), a \notin \pi\}}_{\mathbf{II}} \cup \\ & \underbrace{\bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\notin\bar{a}} \{\pi \cdot t \mid \pi \in S_{p,\bar{a}}(n,k+1), a \in \pi\},}_{\mathbf{III}} \end{aligned}$$

where the three unions marked by $\mathbf{I}, \mathbf{II}, \mathbf{III}$ are mutually disjoint. When we pass to their $\bar{a}'$-orbits, we also get a disjoint union of orbits:

$$\begin{aligned} R_{p',\bar{a}'}(n+1,k+1) = & \bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\in\bar{a}} \{[\pi \cdot t]_{\bar{a}'} \mid \pi \in S_{p,\bar{a}}(n,k+1)\} \cup \\ & \bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\notin\bar{a}} \{[\pi \cdot t]_{\bar{a}'} \mid \pi \in S_{p,\bar{a}}(n,k), a \notin \pi\} \cup \\ & \bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\notin\bar{a}} \{[\pi \cdot t]_{\bar{a}'} \mid \pi \in S_{p,\bar{a}}(n,k+1), a \in \pi\}. \end{aligned}$$

By taking cardinalities on both sides, we get

$$\begin{aligned} |R_{p',\bar{a}'}(n+1,k+1)| = & \left| \bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\in\bar{a}} \underbrace{\{[\pi \cdot t]_{\bar{a}'} \mid \pi \in S_{p,\bar{a}}(n,k+1)\}}_{R_t^{\mathbf{I}}} \right| + \\ & \left| \bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\notin\bar{a}} \underbrace{\{[\pi \cdot t]_{\bar{a}'} \mid \pi \in S_{p,\bar{a}}(n,k), a \notin \pi\}}_{R_t^{\mathbf{II}}} \right| + \\ & \left| \bigcup_{t=(p,\bar{a}\xrightarrow{\sigma,a}p',\bar{a}'),a\notin\bar{a}} \underbrace{\{[\pi \cdot t]_{\bar{a}'} \mid \pi \in S_{p,\bar{a}}(n,k+1), a \in \pi\}}_{R_t^{\mathbf{III}}} \right|. \end{aligned}$$

▷ Claim 23. Fix two transitions $t_1 = (p_1, \bar{a}_1 \xrightarrow{\sigma_1,a_1} p', \bar{a}')$ and $t_2 = (p_2, \bar{a}_2 \xrightarrow{\sigma_2,a_2} p', \bar{a}')$. If $R^{\mathbf{I}}_{t_1} \cap R^{\mathbf{I}}_{t_2} \neq \emptyset$ then $[t_1] = [t_2]$.

Proof of the claim. Let $[\pi_1 \cdot t_1]_{\bar{a}'} = [\pi_2 \cdot t_2]_{\bar{a}'}$ for two runs $\pi_1 \in S_{p_1,\bar{a}_1}(n-1,k)$ and $\pi_2 \in S_{p_2,\bar{a}_2}(n-1,k)$. There exists an ($\bar{a}'$-)automorphism α s.t. $\alpha(\pi_1 \cdot t_1) = \pi_2 \cdot t_2$. In particular, $\alpha(t_1) = t_2$, i.e., $[t_1] = [t_2]$ as required. ◀

The claim above implies that the $R^{\mathbf{I}}_t$'s are disjoint for distinct orbits $[t]$'s, and similarly for

$R_t^{\mathbf{II}}$ and $R_t^{\mathbf{III}}$. We thus obtain the equations

$$\begin{aligned}|R_{p',\bar a'}(n+1,k+1)| = &\sum_{[t=(p,\bar a\xrightarrow{\sigma,a}p',\bar a')]:\ a\in\bar a} |\underbrace{\{[\pi\cdot t]_{\bar a'} \mid \pi\in S_{p,\bar a}(n,k+1)\}}_{R_t^{\mathbf{I}}}| + \\ &\sum_{[t=(p,\bar a\xrightarrow{\sigma,a}p',\bar a')]:\ a\not\in\bar a} |\underbrace{\{[\pi\cdot t]_{\bar a'} \mid \pi\in S_{p,\bar a}(n,k), a\not\in\pi\}}_{R_t^{\mathbf{II}}}| + \\ &\sum_{[t=(p,\bar a\xrightarrow{\sigma,a}p',\bar a')]:\ a\not\in\bar a} |\underbrace{\{[\pi\cdot t]_{\bar a'} \mid \pi\in S_{p,\bar a}(n,k+1), a\in\pi\}}_{R_t^{\mathbf{III}}}|.\end{aligned}$$

▷ Claim 24. The set of orbits $R_t^{\mathbf{I}}$ is in bijection with the set of orbits

$$R_{p,\bar a}(n,k+1) = \{[\pi]_{\bar a} \mid \pi\in S_{p,\bar a}(n,k+1)\}.$$

Proof of the claim. Indeed, consider the mapping $f : R_t^{\mathbf{I}} \to R_{p,\bar a}(n,k+1)$ defined as

$$f([\pi\cdot t]_{\bar a'}) = [\pi]_{\bar a} \quad \text{with } t=(p,\bar a\xrightarrow{\sigma,a}p',\bar a').$$

First of all f is well-defined as a function: Assume $[\pi_1\cdot t]_{\bar a'} = [\pi_2\cdot t]_{\bar a'}$ for two paths π_1,π_2 both ending in configuration $(p,\bar a)$. There exists an $\bar a'$-automorphism α s.t. $\alpha(\pi_1\cdot t)=\pi_2\cdot t$. In particular, $\alpha(\pi_1)=\pi_2$ and since π_1,π_2 end up in the same configuration $(p,\bar a)$, $\alpha(\bar a)=\bar a$. Thus α is in fact a $\bar a$-automorphism and $[\pi_1]_{\bar a}=[\pi_1]_{\bar a}$ as required. Secondly, f is of the right type since $[\pi]_{\bar a}\in R_{p,\bar a}(n,k+1)$: $\pi\cdot t$ is a run over a word $w\cdot a$ of width $k+1$ and thus π is a run over a word w also of width $k+1$ because $a\in\bar a$, implying $a\in w$ since the automaton is non-guessing. We argue that f is a bijection. First of all, f is injective: If $f([\pi_1\cdot t]_{\bar a'}) = f([\pi_2\cdot t]_{\bar a'})$, then by definition of f we have $[\pi_1]_{\bar a}=[\pi_2]_{\bar a}$. There exists an $\bar a$-automorphism α s.t. $\alpha(\pi_1)=\pi_2$. Since the automaton is without guessing, $\bar a'\subseteq\bar a$, and thus α is also an $\bar a'$-automorphism. Since $\alpha(t)=t$ (due to the fact that $a\in\bar a$ and thus $\alpha(a)=a$), $\alpha(\pi_1\cdot t)=\pi_2\cdot t$ and thus $[\pi_1\cdot t]_{\bar a'}=[\pi_2\cdot t]_{\bar a'}$ as required.

The mapping f is also surjective. Indeed, let $[\pi]_{\bar a}\in R_{p,\bar a}(n,k+1)$. Thus π ends in configuration $(p,\bar a)$ and therefore $\pi\cdot t$ is a run. Consequently, $[\pi\cdot t]_{\bar a'}\in R_t^{\mathbf{I}}$. This is enough since, by the definition of f, $[\pi]_{\bar a}=f([\pi\cdot t]_{\bar a'})$. ◀

▷ Claim 25. The set of orbits $R_t^{\mathbf{II}}$ is in bijection with the set of orbits

$$R_{p,\bar a}(n,k) = \{[\pi]_{\bar a} \mid \pi\in S_{p,\bar a}(n,k)\}.$$

Proof of the claim. Consider the mapping

$$f([\pi\cdot t]_{\bar a'}) = [\pi]_{\bar a}, \quad \text{with } t=(p,\bar a\xrightarrow{\sigma,a}p',\bar a').$$

First of all, f is well-defined as a function, and the argument is as in the previous point. Secondly, f has the right type. If $\pi\cdot t$ is a run over a word $w\cdot a$ of width $k+1$, then π is a run over w of width k since $a\not\in w$. Thus f is indeed a mapping from $R_{\mathbf{II}}$ to $R_{p,\bar a}(n,k)$. We argue that f is bijective. First of all, f is injective. Consider $\bar a'$-orbit of runs $[\pi_1\cdot t]_{\bar a'},[\pi_2\cdot t]_{\bar a'}\in R_{\mathbf{II}}$ with $a\not\in\pi_1\cup\pi_2$. If $f([\pi_1\cdot t]_{\bar a'})=f([\pi_2\cdot t]_{\bar a'})$, then by definition of f we have $[\pi_1]_{\bar a}=[\pi_2]_{\bar a}$. There exists an $\bar a$-automorphism α s.t. $\alpha(\pi_1)=\pi_2$. Since $a\not\in\pi_1\cup\pi_2$, there is an automorphism β s.t. β agrees with α on every data value in π_1 (in particular, $\beta(\pi_1)=\pi_2$ and $\beta(\bar a)=\bar a$), and $\beta(a)=a$. Since the automaton is without guessing, $\bar a'\subseteq\bar a\cup\{a\}$. Thus, β is a $\bar a'$-automorphism and $\beta(\pi_1\cdot t)=\beta(\pi_1)\cdot\beta(t)=\pi_2\cdot t$, i.e., $[\pi_1\cdot t]_{\bar a'}=[\pi_2\cdot t]_{\bar a'}$ as required. The mapping f is surjective by an argument as in the proof of Claim 24. ◀

▷ Claim 26. The set of orbits $R_t^{\mathbf{III}}$ with $k+1 \geq \#\bar{a}$ is in bijection with $k+1-\#\bar{a}$ disjoint copies of the set of orbits

$$R_{p,\bar{a}}(n, k+1) = \{[\pi]_{\bar{a}} \mid \pi \in S_{p,\bar{a}}(n, k+1)\},$$

and it is empty if otherwise $k+1 < \#\bar{a}$.

Proof of the claim. If $k+1 < \#\bar{a}$, then clearly since the automaton is non-guessing it could not have stored more distinct data values $\#\bar{a}$ in the register than the number of distinct data values $k+1$ in the input, and thus $R_t^{\mathbf{III}} = \emptyset$ in this case. In the following, thus assume $k+1 \geq \#\bar{a}$. Let $w = a_1 \cdots a_n \in \mathbb{A}^n$ be the sequence of data values labelling the run π, and consider the non-contiguous subsequence $D_\pi = a_{i_1} \cdots a_{i_{k+1-\#\bar{a}}}$ of w consisting of the $k+1-\#\bar{a}$ distinct elements in $w \setminus \bar{a}$ in their order of appearance in w (and thus in π). Consider the function f defined as

$$f([\pi \cdot t]_{\bar{a}'}) = (j, [\pi]_{\bar{a}}) \quad \text{ with } t = (p, \bar{a} \xrightarrow{\sigma, a} p', \bar{a}'),$$

where $a \notin \bar{a}$ equals the unique $a_{i_j} \in D_\pi$. First of all, f is well-defined as a function: Assume $([\pi_1 \cdot t]_{\bar{a}'}, (j_1, [\pi_1]_{\bar{a}})), ([\pi_2 \cdot t]_{\bar{a}'}, (j_2, [\pi_2]_{\bar{a}})) \in f$ with $[\pi_1 \cdot t]_{\bar{a}'} = [\pi_2 \cdot t]_{\bar{a}'}$. There is an $\bar{a}'$-automorphism α s.t. $\alpha(\pi_1 \cdot t) = \pi_2 \cdot t$. In particular, $\alpha(\pi_1) = \pi_2$ and $\alpha(t) = t$, which also implies $\alpha(a_1) = a_2$. From $\alpha(\pi_1) = \pi_2$, we even have that α is a $\bar{a}$-automorphism, and thus $[\pi_1]_{\bar{a}} = [\pi_2]_{\bar{a}}$. We now argue that $j_1 = j_2$. Assume a appears in position j_1 in D_{π_1} and in position j_2 in D_{π_2}. Assume by way of contradiction that $j_1 \neq j_2$. We have that $\alpha(a) = a$ appears in position j_1 in $\alpha(D_{\pi_1}) = D_{\alpha(\pi_1)} = D_{\pi_2}$, i.e., a also appears in position j_1 in D_{π_2}. This is a contradiction, since all elements in D_{π_2} are distinct. Thus f is indeed a mapping from $R_{\mathbf{III}}$ to $\{1, \ldots, k+1-\#\bar{a}\} \times R_{p,\bar{a}}(n, k+1)$.

We argue that f is bijective. First of all, f is injective. Consider $\bar{a}'$-orbit of runs $[\pi_1 \cdot t]_{\bar{a}'}, [\pi_2 \cdot t]_{\bar{a}'} \in R_t^{\mathbf{III}}$ with $a \notin \bar{a}, a \in \pi_1, a \in \pi_2$. Assume $f([\pi_1 \cdot t]_{\bar{a}'}) = f([\pi_2 \cdot t]_{\bar{a}'})$. By the definition of f, we have $[\pi_1]_{\bar{a}} = [\pi_2]_{\bar{a}}$, and a occurs in the same position j in D_{π_1}, resp., D_{π_2}. Consequently $\alpha(a)$ occurs at position j in $\alpha(D_{\pi_1}) = D_{\alpha(\pi_1)} = D_{\pi_2}$, and thus $\alpha(a) = a$. There exists an $\bar{a}$-automorphism α s.t. $\alpha(\pi_1) = \pi_2$. Since the automaton is without guessing, $\bar{a}' \subseteq \bar{a} \cup \{a\}$, and thus α is even an $\bar{a}'$-automorphism. This means $[\pi_1]_{\bar{a}'} = [\pi_2]_{\bar{a}'}$ and $\alpha(t) = t$, and thus $[\pi_1 \cdot t]_{\bar{a}'} = [\pi_2 \cdot t]_{\bar{a}'}$ as required. The mapping f is surjective by an argument analogous as in the proof of Claim 24. ◀

Thanks to Claims 24–26, we obtain the equations

$$\begin{aligned} |R_{p',\bar{a}'}(n+1, k+1)| = & \sum_{[p,\bar{a} \xrightarrow{\sigma,a} p', \bar{a}']:\ a \in \bar{a}} |R_{p,\bar{a}}(n, k+1)| \ + \\ & \sum_{[p,\bar{a} \xrightarrow{\sigma,a} p', \bar{a}']:\ a \notin \bar{a}} |R_{p,\bar{a}}(n, k)| \ + \\ & \sum_{[p,\bar{a} \xrightarrow{\sigma,a} p', \bar{a}']:\ a \notin \bar{a}} |\{1, \ldots, k+1-\#\bar{a}\} \times R_{p,\bar{a}}(n, k+1)| \,. \end{aligned}$$

By recalling the definition $G_{p,\bar{a}}(n+1, k+1) = |R_{p,\bar{a}}(n+1, k+1)|$, we obtain, as required,

$$\begin{aligned} G_{p',\bar{a}'}(n+1, k+1) = & \sum_{[p,\bar{a} \xrightarrow{\sigma,a} p', \bar{a}']:\ a \in \bar{a}} G_{p,\bar{a}}(n, k+1) \ + \\ & \sum_{[p,\bar{a} \xrightarrow{\sigma,a} p', \bar{a}']:\ a \notin \bar{a}} (G_{p,\bar{a}}(n, k) + \max\{k+1-\#\bar{a}, 0\} \cdot G_{p,\bar{a}}(n, k+1)). \end{aligned}$$ ◀

▶ **Lemma 13.** *Let A be an unambiguous register automaton over equality atoms without guessing with d registers and ℓ control locations. The universality problem for A reduces to the zeroness problem of the linrec sequence G defined by the system of equations in Figure 2 containing $O(\ell \cdot 2^{d \cdot \log d})$ variables and equations and constructible in* PSPACE*. If A is already orbitised, then the system of equations has size $O(\ell)$.*

Proof. We can effectively enumerate all orbits of transitions $[p, \bar{a} \xrightarrow{\sigma, a} p', \bar{a}']$ by enumerating all the exponentially many constraints up to logical equivalence [4, Ch. 4], which can be done in PSPACE since this is the complexity of first-order logic over the equality relation. Recall that the Bell number $B(n)$ counts the number of non-empty partitions of a set of n elements. The system in Figure 2 contains $\ell \cdot B(d) + 2 = O(\ell \cdot 2^{d \cdot \log d})$ equations and variables. ◀

D Proofs and additional material for Sec. 5

▶ **Theorem 14** (c.f. [42, Sec. 1]). *If R has the* CLM *property, then 1) $R[\partial; \sigma]$ has a pseudo-division, and 2) $R[\partial; \sigma]$ also has the* CLM *property.*

Proof. We adapt a proof by Giesbrecht given in the case when R is a field, for which there even is a *least* common left multiple [25, Sec. 2] (c.f. also [43, Sec. 2]). We consider the more general case where R is a ring, in which case we will not have any minimality guarantee for the common left multiple.

We first prove that $R[\partial; \sigma]$ has pseudo-division. Let consider the nonzero skew polynomials

$$A = a_m \cdot \partial^m + \cdots + a_0 \quad \text{and} \quad B = b_n \cdot \partial^n + \cdots + b_0$$

where $m \geq n$. Let $R_0 = A$. The leading term of B is $b_n \cdot \partial^n$ and thus the leading term of $\partial^{m-n} \cdot B$ is $\partial^{m-n} \cdot b_n \cdot \partial^n = \sigma^{m-n}(b_n) \cdot \partial^m$. Since R is CLM, there are a'_0 and b'_0 s.t. $a'_0 \cdot a_m = b'_0 \cdot \sigma^{m-n}(b_n)$. Therefore, $R_1 := a'_0 \cdot R_0 - b'_0 \cdot \partial^{m-n} \cdot B$ has degree strictly less than $m_0 := m = \deg R_0$. We repeat this operation obtaining a sequence of remainders:

$$\begin{aligned}
a'_0 \cdot R_0 &= b'_0 \cdot \partial^{m_0 - n} \cdot B + R_1, \\
a'_1 \cdot R_1 &= b'_1 \cdot \partial^{m_1 - n} \cdot B + R_2, \\
&\vdots \\
a'_{k-1} \cdot R_{k-1} &= b'_{k-1} \cdot \partial^{m_{k-1} - n} \cdot B + R_k, \\
a'_k \cdot R_k &= b'_k \cdot \partial^{m_k - n} \cdot B + R_{k+1},
\end{aligned}$$

where $m_i := \deg R_i$, $R_{i+1} := a'_i \cdot R_i - b'_i \cdot \partial^{m_i - n}$, and the degrees satisfy $m_0 > m_1 > \cdots > m_k > n > m_{k+1}$. By defining $a = a'_k a'_{k-1} \cdots a'_0 \in R$, taking as quotient the skew polynomial

$$P = b'_k \cdot \partial^{m_k - n} + a'_k b'_{k-1} \cdot \partial^{m_{k-1} - n} + \cdots + a'_k a'_{k-1} \cdots a'_1 b'_0 \cdot \partial^{m_0 - n} \in R[\partial; \sigma]$$

and as a remainder $Q = R_{k+1}$ we have, as required, $\deg Q < m$ and

$$a \cdot A = P \cdot B + Q.$$

We now show that $R[\partial; \sigma]$ has the CLM property. To this end, let $A_1, A_2 \in R[\partial; \sigma]$ with $\deg A_1 \geq \deg A_2$ be given. We apply the pseudo-division algorithm above to obtain the sequence

$$\begin{aligned}
a_1 \cdot A_1 &= Q_1 \cdot A_2 + A_3,\\
a_2 \cdot A_2 &= Q_2 \cdot A_3 + A_4,\\
&\vdots\\
a_{k-2} \cdot A_{k-2} &= Q_{k-2} \cdot A_{k-1} + A_k,\\
a_{k-1} \cdot A_{k-1} &= Q_{k-1} \cdot A_k + A_{k+1},
\end{aligned}$$

with $a_1, \ldots, a_{k-1} \in R$, $A_{k+1} = 0$, and the degrees of the A_i's are strictly decreasing: $\deg A_2 > \deg A_3 > \cdots > \deg A_k$. Consider the following two sequences of skew polynomials

$$\begin{aligned}
&S_1 = 1, \quad S_2 = 0, \quad S_i = a_{i-2} \cdot S_{i-2} - Q_{i-2} \cdot S_{i-1}, \text{ and}\\
&T_1 = 0, \quad T_2 = 1, \quad T_i = a_{i-2} \cdot T_{i-2} - Q_{i-2} \cdot T_{i-1}.
\end{aligned}$$

It can easily be verified that $S_i \cdot A_1 + T_i \cdot A_2 = A_i$ for every $0 \leq i \leq k+1$: The base cases $i = 0$ and $i = 1$ are clear; inductively, we have

$$\begin{aligned}
S_i A_1 + T_i A_2 &= (a_{i-2} \cdot S_{i-2} - Q_{i-2} \cdot S_{i-1}) A_1 + (a_{i-2} \cdot T_{i-2} - Q_{i-2} \cdot T_{i-1}) A_2 =\\
&= a_{i-2}(S_{i-2} A_1 + T_{i-2} A_2) - Q_{i-2}(S_{i-1} A_1 + T_{i-1} A_2) =\\
&= a_{i-2} A_{i-2} - Q_{i-2} A_{i-1} = A_i.
\end{aligned}$$

In particular, at the end $S_{k+1} \cdot A_1 + T_{k+1} \cdot A_2 = 0$, as required.

It remains to check that S_{k+1} is nonzero. We show the stronger property that $\deg S_i = \deg A_2 - \deg A_{i-1}$ for every $3 \leq i \leq k+1$. The base case $i = 3$ is clear. For the inductive step, notice that $\deg Q_{i-2} = \deg A_{i-2} - \deg A_{i-1} > 0$. Thus $\deg(Q_{i-2} \cdot S_{i-1}) = \deg A_{i-2} - \deg A_{i-1} + \deg A_2 - \deg A_{i-2} = \deg A_2 - \deg A_{i-1}$. Moreover, $\deg(a_{i-2} \cdot S_{i-2}) = \deg S_{i-2} = \deg A_2 - \deg A_{i-3} < \deg A_2 - \deg A_{i-2}$. Thus, $\deg S_i = \deg(Q_{i-2} \cdot S_{i-1}) = \deg A_2 - \deg A_{i-1}$, as required. ◀

▶ **Lemma 17.** *The zeroness problem for a bidimensional linrec sequence $f : \mathbb{Q}^{\mathbb{N}^2}$ of order $\leq m$ and univariate polynomial coefficients in $\mathbb{Q}[k]$ admitting some cancelling relation* (CR-2) *with leading coefficient $p_{i^*,j^*}(k) \in \mathbb{Q}[k]$ of degree $\leq e$ and height $\leq h$ s.t. each of the one-dimensional sections $f(M, k) \in \mathbb{Q}^{\mathbb{N}}$ for $1 \leq M \leq i^*$ also admits some cancelling relation* (CR-1) *of ∂_2-degree $\leq d$ with leading polynomial coefficients of degrees $\leq e$ and height $\leq h$ is decidable in deterministic time $\tilde{O}(p(m, i^*, j^*, d, e, h))$ for some polynomial p.*

Proof. We recall Lagrange's classical bound on the roots of univariate polynomials.

▶ **Theorem 27** (Lagrange, 1769). *The roots of a complex polynomial $p(z) = \sum_{i=0}^{d} a_i \cdot z^i$ of degree d are bounded by $1 + \sum_{0 \leq i \leq d-1} \frac{|a_i|}{|a_n|}$. In particular, the maximal root of a polynomial $p(k) \in \mathbb{Q}[k]$ with integral coefficients is at most $1 + d \cdot \max_i |a_i|$.*

By Theorem 27, the largest root of the leading polynomial coefficient $p_{i^*,j^*}(k)$ is $\leq 1 + \deg_k p_{i^*,j^*} \cdot |p_{i^*,j^*}|_\infty < 2 + e \cdot h$ and similarly the roots of all the leading polynomial coefficients of the cancelling relations for the sections $f(0, n), \ldots, f(i^*, n)$ are $< 2 + e \cdot h$. In the following, let

$$K = 2 + j^* + e \cdot h.$$

▷ Claim 28. The one-dimensional section $f(n, L) \in \mathbb{Q}^{\mathbb{N}}$ for a fixed $L \geq 0$ is identically zero if, and only if, $f(0, L) = f(1, L) = \cdots = f(m \cdot (L + 3), L) = 0$.

Proof of the claim. The "only if" direction is obvious. By Lemma 4, for any fixed $L \in \mathbb{N}$ the 1-dimensional L-section $f(n, L)$ is linrec of order $\leq m \cdot (L + 3)$. In fact, it is C-recursive of the same order since the coefficients do not depend on n and are thus constants. It follows that if $f(0, L) = f(1, L) = \cdots = f(m \cdot (L + 3), L) = 0$, then in fact $f(n, L) = 0$ for every $n \in \mathbb{N}$ (c.f. the proof of Lemma 22). ◀

▷ Claim 29. The one-dimensional section $f(M, k) \in \mathbb{Q}^{\mathbb{N}}$ for a fixed $0 \leq M \leq i^*$ is identically zero if, and only if, $f(M, 0) = f(M, 1) = \cdots = f(M, d + e \cdot h) = 0$.

Proof of the claim. The "only if" direction is obvious. By assumption, $f(M, k)$ admits a cancelling relation (CR-1) of ∂_2-degree $\ell^* \leq d$ and leading polynomial coefficient $q_{\ell^*}(k)$ of degree $\leq e$ and height $\leq h$. By Theorem 27, the roots of $q_{\ell^*}(k)$ are bounded by $O(e \cdot h)$. It follows that if $f(M, 0) = f(M, 1) = \cdots = f(M, d + e \cdot h) = 0$ then $f(M, n)$ is identically zero. ◀

▷ Claim 30. $f = 0$ if, and only if, all the one-dimensional sections

$$f(n, 0), \ldots, f(n, K), f(0, k), \ldots, f(i^*, k) \in \mathbb{Q}^{\mathbb{N}}$$

are identically zero.

Proof of the claim. The "only if" direction is obvious. For the "if" direction, assume all the sections above are identically zero as one-dimensional sequences. By way of contradiction, let (n, k) be the pair of indices which is minimal for the lexicographic order s.t. $f(n, k) \neq 0$. By assumption, we necessarily have $n > i^*$ and $k > K$. By (CR-2) we have

$$p_{i^*,j^*}(k - j^*) \cdot f(n, k) = \sum_{(i,j) <_{\text{lex}} (i^*,j^*)} p_{i,j}(n - i^*, k - j^*) \cdot f(n - (i^* - i), k - (j^* - k)).$$

Since $k > K$, $k - j^* > K - j^* \geq 2 + e \cdot h$, we have $p_{i^*,j^*}(k - j^*) \neq 0$ since the largest root of p_{i^*,j^*} is $\leq 1 + e \cdot h$. Consequently, there exists $(i, j) <_{\text{lex}} (i^*, j^*)$ s.t. $f(n - (i^* - i), k - (j^* - k)) \neq 0$, which contradicts the minimality of (n, k). ◀

By putting together the three claims above it follows that f is identically zero if, and only if, f is zero on the set of inputs

$$\{0, \ldots, m \cdot (K + 3)\} \times \{0, \ldots, K\} \cup \{0, \ldots, i^*\} \times \{0, \ldots, d + e \cdot h\}.$$

Let $N = 1 + \max\{m \cdot (K + 3), i^*\}$ and $K' = 1 + \max\{K, d + e \cdot h\}$. The condition above can be verified by computing $O(N \cdot K')$ values for $f(n, k)$, each of which can be done in deterministic time $\tilde{O}(m \cdot N \cdot K')$ thanks to Lemma 3, together yielding $\tilde{O}(m \cdot N^2 \cdot (K')^2)$ which is $\tilde{O}(p(m, i^*, j^*, d, e, h))$ for a suitable polynomial p. ◀

▶ **Theorem 18.** *The zeroness problem for linrec sequences with univariate polynomial coefficients from $\mathbb{Q}[k]$ (or from $\mathbb{Q}[n]$) is decidable.*

Proof. We interpret the system of equations (2) as the following linear system of equations with coefficients $P_{i,j} \in W_2$.

$$\left\{ \begin{array}{rcl} P_{1,1} \cdot f_1 + \cdots + P_{1,m} \cdot f_m &=& 0, \\ &\vdots& \\ P_{m,1} \cdot f_1 + \cdots + P_{m,m} \cdot f_m &=& 0. \end{array} \right. \tag{9}$$

The idea is to eliminate all variables $f_m, \ldots, f_2$ from (9) until a CR for f_1 remains. W.l.o.g. We show how to remove the last variable f_m. The skew polynomial coefficients of f_m in equations $1, \ldots, m$ are $P_{1,m}, \ldots, P_{m,m} \in W_2$. By m applications of Corollary 16, we can find left multipliers $Q_1, \ldots, Q_m \in W_2$ s.t. $Q_1 \cdot P_{1,m} = Q_2 \cdot P_{2,m} = \cdots = Q_m \cdot P_{m,m}$. We obtain the new system not containing f_m

$$\begin{cases} (Q_1 P_{1,1} - Q_m P_{m,1}) \cdot f_1 + \cdots & +(Q_1 P_{1,m-1} - Q_m P_{m,m-1}) \cdot f_{m-1} &= & 0, \\ & & & \vdots \\ (Q_{m-1} P_{m-1,1} - Q_m P_{m,1}) \cdot f_1 + \cdots & +(Q_{m-1} P_{m-1,m-1} - Q_m P_{m,m-1}) \cdot f_{m-1} &= & 0. \end{cases}$$

After eliminating all the other variables $f_{m-1}, \ldots, f_2$ in the same way, we are finally left with an equation $R \cdot f_1 = 0$ with $R \in W_2$. Thanks to a linear independence-argument that will be presented in Lemma 37, the operator R is not zero. (Notice that the univariate assumption is not necessary to carry over the elimination procedure and obtain a cancelling relation.) Notice that the polynomial coefficients in R are univariate polynomials in $\mathbb{Q}[k]$. Let $p_{i^*,j^*}(k)$ be leading polynomial coefficient of R when put in the form (CR-2). By an analogous elimination argument we can find cancelling relations $R_1, \ldots, R_{i^*}$ for each of the one-dimensional sections $f^*(0,k), \ldots, f(i^*,k) \in \mathbb{Q}^{\mathbb{N}}$ (which are effectively one-dimensional linrec sequences by Lemma 4) respectively. We then conclude by Lemma 17. ◀

The elimination algorithm presented so far suffices to decide the universality, inclusion, and equivalence problems for unambiguous register automata without guessing.

▶ **Corollary 31.** *The universality and equivalence problems for unambiguous register automata without guessing are decidable. The inclusion problem $L(A) \subseteq L(B)$ for register automata without guessing is decidable when B is unambiguous.*

Notice that in the inclusion problem $L(A) \subseteq L(B)$ we do not assume that A is unambiguous.

Proof. By Lemma 8, inclusion and equivalence reduce to universality. By Lemma 10, the universality problem reduces to the zeroness problem of the sequence G from Figure 2, which is linrec by its definition and Lemma 11. Since the polynomial coefficients in Figure 2 are univariate, we can decide zeroness of G by Theorem 18. ◀

D.1 CLM examples

In this section we illustrate the CLM property with two examples, the first for W_1 and the second for W_2.

▶ **Example 32.** We give an example of application of the CLM property in W_1. Consider the two polynomials $F_1 = \partial_1^2 - (k+1)\partial_1$ and $F_2 = -\partial_1^2 + \partial_1$. Since k and ∂_1 commute, $F_2 \cdot F_1 = F_1 \cdot F_2$ and the multipliers have degree 2. The CLM algorithm finds multipliers of degree 1:

$$\begin{aligned} 1 \cdot F_1 &= (-1) \cdot F_2 + F_3 && \text{with } F_3 = -k\partial_1, \\ k \cdot F_2 &= \partial_1 \cdot F_3 + F_4 && \text{with } F_4 = k\partial_1, \\ 1 \cdot F_3 &= (-1) \cdot F_4. \end{aligned}$$

We have $s_1 = 1, s_2 = 0, s_3 = 1, s_4 = -\partial_1, s_5 = -\partial_1 + 1$ and $t_1 = 0, t_2 = 1, t_3 = 1, t_4 = -k + \partial_1, t_5 = -k + \partial_1 + 1$. We can thus verify that $s_5 \cdot F_1 = -t_5 \cdot F_2$.

▶ **Example 33.** We give an example of CLM property in W_2. Consider the skew polynomials $G_1 = (-\partial_1^2 + \partial_1)\partial_2^2$ and $G_2 = (\partial_1^2 - k\partial_1)\partial_2 - \partial_1$. Since $\partial_2 G_2 = (\partial_1^2 - (k+1)\partial_1)\partial_2^2 - \partial_1\partial_2$, thanks to Example 32 we have

$$(\partial_1 - k - 1) \cdot G_1 = (-\partial_1 + 1)\partial_2 \cdot G_2 + G_3, \qquad \text{with } G_3 = (-\partial_1^2 + \partial_1)\partial_2,$$

which gives the first pseudo-division. Analogously, since $(-\partial_1 + 1) \cdot (\partial_1^2 - k\partial_1) = (\partial_1 - k) \cdot (-\partial_1^2 + \partial_1)$, we have the second and third pseudo-divisions

$$\begin{aligned} (-\partial_1 + 1) \cdot G_2 &= (\partial_1 - k) \cdot G_3 + G_4, \qquad && \text{with } G_4 = \partial_1^2 - \partial_1, \\ 1 \cdot G_3 &= -\partial_2 \cdot G_4. \end{aligned}$$

We thus have $s_1 = 1, s_2 = 0, s_3 = \partial_1 - k - 1, s_4 = -(\partial_1 - k) \cdot (\partial_1 - k - 1), s_5 = (\partial_1 - k - 1) - \partial_2 \cdot (\partial_1 - k) \cdot (\partial_1 - k - 1) = (\partial_1 - k - 1) - (\partial_1 - k - 1) \cdot (\partial_1 - k - 2)\partial_2$ and $t_1 = 0, t_2 = 1, t_3 = -(-\partial_1 + 1)\partial_2, t_4 = (-\partial_1 + 1) + (\partial_1 - k) \cdot (-\partial_1 + 1)\partial_2, t_5 = -(-\partial_1 + 1)\partial_2 + \partial_2 \cdot ((-\partial_1 + 1) + (\partial_1 - k) \cdot (-\partial_1 + 1)\partial_2) = (\partial_1 - k - 1) \cdot (-\partial_1 + 1)\partial_2^2$. One can check that $s_5 \cdot G_1 = -t_5 \cdot G_2$.

D.2 CR examples

In this section we present detailed examples of CR.

▶ **Example 34.** We continue our running Example 15. Recall the starting equations:

$$\begin{array}{rrrrl} \partial_1\partial_2 \cdot G_p & & & & = 0, \\ -(1 + (k+1)\partial_2) \cdot G_p & +(\partial_1\partial_2 - k\partial_2 - 1) \cdot G_q & & & = 0, \\ -(1 + (k+1)\partial_2) \cdot G_p & & +(\partial_1\partial_2 - \partial_2) \cdot G_r & & = 0, \\ & -\partial_2 \cdot G_q & -(1 + k\partial_2) \cdot G_r & +\partial_1\partial_2 \cdot G_s & = 0, \end{array}$$

$$\begin{aligned} &(\partial_1\partial_2 - (k+1)\partial_2 - 1) \cdot S_1 = 0, \\ &G_s - S_1 + G = 0. \end{aligned}$$

In order to eliminate G_p, we need to find a common left multiple of $a_0 = \partial_1\partial_2$ and $b_0 = 1 + (k+1)\partial_2$, i.e., we need to find skew polynomials c, d s.t. $c \cdot a_0 = d \cdot b_0$. It can be verified that taking $c = 1 + (k+2)\partial_2$ and $d = \partial_1\partial_2$ fits the bill. We thus remove the first equation and left-multiply by d the second and third equations (with $S_1 = S$ for simplicity from now on):

$$\begin{array}{rrrl} \underbrace{(\partial_1^2\partial_2^2 - (k+1)\partial_1\partial_2^2 - \partial_1\partial_2)}_{a_1} \cdot G_q & & & = 0, \\ & +(\partial_1^2\partial_2^2 - \partial_1\partial_2^2) \cdot G_r & & = 0, \\ -\underbrace{\partial_2}_{b_1} \cdot G_q & -(1 + k\partial_2) \cdot G_r & +\partial_1\partial_2 \cdot G_s & = 0, \end{array}$$

$$\begin{aligned} &(\partial_1\partial_2 - (k+1)\partial_2 - 1) \cdot S = 0, \\ &G_s - S + G = 0. \end{aligned}$$

We now remove G_q. Since its coefficient $b_1 = \partial_2$ in the third equation is already a multiple of its coefficient $a_1 = \partial_1^2\partial_2^2 - (k+1)\partial_1\partial_2^2 - \partial_1\partial_2$ in the first equation, it suffices to remove the first equation and left-multiply the third equation by "$\partial_1^2\partial_2 - (k+1)\partial_1\partial_2 - \partial_1$":

$$\begin{aligned}
&\underbrace{(\partial_1^2\partial_2^2 - \partial_1\partial_2^2)}_{a_2}\cdot G_r && &&= 0,\\
-&\underbrace{(\partial_1^2\partial_2 - (k+1)\partial_1\partial_2 - \partial_1)(1+k\partial_2)}_{b_2}\cdot G_r && +(\partial_1^2\partial_2 - (k+1)\partial_1\partial_2 - \partial_1)\partial_1\partial_2\cdot G_s &&= 0,
\end{aligned}$$

$$\begin{aligned}
&(\partial_1\partial_2 - (k+1)\partial_2 - 1)\cdot S = 0,\\
&G_s - S + G = 0.
\end{aligned}$$

We now remove G_r, and thus we need to find a CLM of $a_2 = \partial_1^2\partial_2^2 - \partial_1\partial_2^2 = (\partial_1 - 1)\partial_1\partial_2^2$ and $b_2 = (\partial_1^2\partial_2 - (k+1)\partial_1\partial_2 - \partial_1)(1+k\partial_2) = (\partial_1\partial_2 - (k+1)\partial_2 - 1)(1+k\partial_2)\partial_1$. It can be checked that for $d = (\partial_1 - 1)\partial_2^2$ there exists some c (whose exact value is not relevant here) s.t. $c\cdot a_2 = d\cdot b_2$. We can thus remove the first equation and left-multiply the second one by d:

$$\begin{aligned}
\underbrace{(\partial_1 - 1)\partial_2^2(\partial_1^2\partial_2 - (k+1)\partial_1\partial_2 - \partial_1)\partial_1\partial_2}_{a_3}\cdot G_s &= 0,\\
(\partial_1\partial_2 - (k+1)\partial_2 - 1)\cdot S &= 0,\\
G_s - S + G &= 0.
\end{aligned}$$

We can now immediately remove G_s by left-multiplying the last equation by its coefficient a_3 in the first equation:

$$\begin{aligned}
\underbrace{(\partial_1\partial_2 - (k+1)\partial_2 - 1)}_{b_3}\cdot S &= 0,\\
\underbrace{(\partial_1 - 1)\partial_2^2(\partial_1^2\partial_2 - (k+1)\partial_1\partial_2 - \partial_1)\partial_1\partial_2}_{a_3}\cdot(-S + G) &= 0.
\end{aligned}$$

In order to finish it remains to remove S. The general approach is to find a CLM of a_3 and b_3, but we would like to avoid performing too many calculations here. Since $b_3\cdot S = 0$, we also have $b_3\partial_1^2\partial_2\cdot S = 0$ (since $\partial_1^2\partial_2\cdot S$ is just a shifted version of S, and since a_3 can be written as $a_3 = (\partial_1 - 1)\partial_2^2(\partial_1\partial_2 - (k+1)\partial_2 - 1)\partial_1^2\partial_2 = (\partial_1 - 1)\partial_2^2\cdot b_3\cdot\partial_1^2\partial_2$, it follows that $a_3\cdot S = 0$ and we immediately have

$$\underbrace{(\partial_1 - 1)\partial_2^2(\partial_1\partial_2 - (k+1)\partial_2 - 1)\partial_1^2\partial_2}_{a_4}\cdot G = 0.$$

Since a_4 can be expanded to (as a sum of products).

$$\begin{aligned}
a_4 &= (\partial_1 - 1)\partial_2^2(\partial_1\partial_2 - (k+1)\partial_2 - 1)\partial_1^2\partial_2 =\\
&= (\partial_1\partial_2 - (k+3)\partial_2 - 1)\partial_1^2(\partial_1 - 1)\partial_2^3 =\\
&= \partial_1^4\partial_2^4 - (k+3)\partial_1^3\partial_2^4 - \partial_1^3\partial_2^3 - \partial_1^3\partial_2^4 + (k+3)\partial_1^2\partial_2^4 + \partial_1^2\partial_2^3 =\\
&= \partial_1^4\partial_2^4 - (k+4)\partial_1^3\partial_2^4 - \partial_1^3\partial_2^3 + (k+3)\partial_1^2\partial_2^4 + \partial_1^2\partial_2^3,
\end{aligned}$$

the sought cancelling relation for G, obtained by expanding the equation above, is

$$\begin{aligned}
G(n+4, k+4) = {}&(k+4)\cdot G(n+3, k+4) + G(n+3, k+3) +\\
&- (k+3)\cdot G(n+2, k+4) - G(n+2, k+3).
\end{aligned}$$

▶ **Example 35.** We show a CR example coming from a two-register deterministic automaton. There are three control locations p, q, r, which are all accepting and p is initial. When going from p to q the automaton stores the input in its first register x_1. When going from q to r, the automaton checks that the input is different from what is stored in x_1 and stores it in x_2. Then the automaton goes from r to r itself by reading an input y different from both registers, $x_1' = x_2$ and $x_2' = y$. In this way the automaton accepts all words s.t. any three consecutive data values are pairwise distinct. We have the counting equations:

$$\begin{aligned}
G_p(n+1,k+1) &= 0,\\
G_q(n+1,k+1) &= G_p(n,k) + (k+1)\cdot G_q(n,k+1),\\
G_r(n+1,k+1) &= G_q(n,k) + k\cdot G_q(n,k+1) + G_r(n,k) + (k-1)\cdot G_r(n,k+1),\\
G(n,k) &= S(n,k) - G_p(n,k) - G_q(n,k) - G_r(n,k).
\end{aligned}$$

We find the following CR:

$$\begin{aligned}
G(n+4,k+3) \;\; = \;\; & (2k+4)\cdot G(n+3,k+3) + 2\cdot G(n+3,k+2) + \\
& -(k^2+4k+3)\cdot G(n+2,k+3) + \\
& -(2k+3)\cdot G(n+2,k+2) - G(n+2,k+1).
\end{aligned} \tag{10}$$

In the last example we consider an automaton which is almost universal.

▶ **Example 36.** Consider the following register automaton A with one register x with unary finite alphabet $|\Sigma| = 1$. There are four control locations p, q, r, s of which p is initial and s is final. The automaton accepts all words of length ≥ 2 by unambiguously guessing whether or not the last two letters are equal. The transitions are $p \xrightarrow{x=\bot\wedge x'=\bot} p$, $p \xrightarrow{x=\bot\wedge x'=y} q$, $p \xrightarrow{x=\bot\wedge x'=y} r$, $q \xrightarrow{x=y\wedge x'=x} s$, $r \xrightarrow{x\neq y\wedge x'=x} s$. Equations:

$$\begin{aligned}
G_p(n+1,k+1) &= G_p(n,k) + (k+1)\cdot G_p(n,k+1),\\
G_q(n+1,k+1) &= G_p(n,k) + (k+1)\cdot G_p(n,k+1) = G_p(n+1,k+1),\\
G_r(n+1,k+1) &= G_p(n,k) + (k+1)\cdot G_p(n,k+1) = G_p(n+1,k+1),\\
G_s(n+1,k+1) &= G_q(n,k+1) + G_r(n,k) + k\cdot G_r(n,k+1) =\\
&= (k+2)G_p(n,k+1) + G_p(n,k),\\
G(n,k) &= S(n,k) - G_s(n,k).
\end{aligned}$$

We find the following CR:

$$G(n+3,k+3) = G(n+2,k+2) + (k+3)\cdot G(n+2,k+3). \tag{11}$$

Thanks to the relationship above, we manually check that $G(2,0) = G(2,1) = G(2,2) = 0$, we can conclude that $G(n,k) = 0$ for every $n, k \geq 2$. Indeed, the automaton accepts all words of length ≥ 2.

E Hermite forms

In this section we present an elimination algorithm based on the computation of the Hermite normal form for matrices of skew polynomials. An easy but important observation in order to get good bounds is that the first Weyl algebra $W_1 = \mathbb{Q}[k][\partial_1; \sigma_1]$ from Sec. 5 is in fact isomorphic to the (commutative) ring of bivariate polynomials $\mathbb{Q}[k, \partial_1]$. In places where we need to obtain good complexity bounds, we will use W_1' instead of W_1 and W_2' instead of W_2, where

$$W_1' = \mathbb{Q}[k, \partial_1] \quad \text{and} \quad W_2' = W_1'[\partial_2; \sigma_2] = \mathbb{Q}[k, \partial_1][\partial_2; \sigma_2]. \tag{12}$$

A skew polynomial $P \in W_2$ (or W_2') can be written in a unique way as a finite sum $\sum_{i,j,k} a_{i,j,k} z^i \partial_1^j \partial_2^k$ with $a_{i,j,k} \in \mathbb{Q}$. We define $\deg_z P$ as the largest i s.t. $a_{i,j,k} \neq 0$ for some j, k; $\deg_{\partial_1}$ and $\deg_{\partial_2}$ are defined similarly. The *combined degree* $\deg_{\partial_1 + \partial_2} P$ is the largest $j + k$ s.t. $a_{i,j,k} \neq 0$ for some i, and similarly for $\deg_{z+\partial_1}$. The *height* of P is $|P|_\infty = \max_{i,j,k} |a_{i,j,k}|_\infty$.

Rational skew fields. The improved elimination algorithm does not work in the skew polynomial ring, but in its rational field extension. To this end we need to introduce skew fields. A *skew field* $\mathbb{F}$ is a field where multiplication is not necessarily commutative [17]. (Skew fields are sometimes called *division rings* since they are noncommutative rings where multiplicative inverses exist.) In the same way as the ring of polynomials $\mathbb{F}[x]$ over a field $\mathbb{F}$ can be extended to a rational polynomial field $\mathbb{F}(x)$, a skew polynomial ring $\mathbb{F}[\partial; \sigma]$ over a skew field $\mathbb{F}$ can be extended to a *rational skew field* $\mathbb{F}(\partial; \sigma)$. Its elements are formal fractions $\frac{P}{Q} = Q^{-1}P$ quotiented by $Q^{-1}P \sim S^{-1}R$ if there exist $A, B \in \mathbb{F}[\partial; \sigma]$ s.t. $A \cdot P = B \cdot R$ and $A \cdot Q = B \cdot S$. Given $P, Q, R, S \in \mathbb{F}[\partial; \sigma]$ s.t. $S_1 \cdot Q = Q_1 \cdot S$ and $S_1 \cdot P = P_1 \cdot S$ for some $P_1, S_1, Q_1 \in \mathbb{F}[\partial; \sigma]$, we can define the operations:

$$\frac{P}{Q} + \frac{R}{S} = \frac{S_1 \cdot P + Q_1 \cdot R}{S_1 \cdot Q}, \qquad \frac{P}{Q} \cdot \frac{R}{S} = \frac{P_1 R}{S_1 Q}, \qquad \left(\frac{P}{Q}\right)^{-1} = \frac{Q}{P}.$$

It was shown by O. Ore that this yields a well-defined skew field structure to $\mathbb{F}(\partial; \sigma)$ and that unique reduced representations $\frac{P}{Q}$ exist [42][7]. In our context, we define the skew fields

$$\mathbb{F}(W_1') = \mathbb{Q}(k, \partial_1) \quad \text{and} \quad \mathbb{F}(W_2') = \mathbb{F}(W_1')(\partial_2; \sigma_2) = \mathbb{Q}(k, \partial_1)(\partial_2; \sigma_2) \tag{13}$$

associated to the corresponding iterated Weyl algebras W_1' and W_2'. Note that $\mathbb{F}(W_1')$ is in fact just a rational (commutative) field of bivariate polynomials. For $R = \frac{P}{Q} \in \mathbb{F}(W_1')$ or $\mathbb{F}(W_2')$ written in reduced form, we define $|R|_\infty = \max\{|P|_\infty, |Q|_\infty\}$.

Non-commutative linear algebra. Let $\mathbb{F}$ be a skew field. We denote by $\mathbb{F}^{n \times m}$ the ring of matrices A with n rows and m columns with entries in $\mathbb{F}$, equipped with the usual matrix operations "+" and "·". The *height* of $A \in \mathbb{F}^{n \times m}$ is $|A|_\infty = \max_{i,j} |A_{i,j}|_\infty$. The *left* $\mathbb{F}$-*module* spanned by the rows of $A = (u_1, \ldots, u_n)$ is the set of vectors in $\mathbb{F}^n$ of the form $a_1 \cdot u_1 + \cdots + a_n \cdot v_n$ for some $a_1, \ldots, a_n \in \mathbb{F}$. The *rank* of A is the dimension of the left $\mathbb{F}$-module spanned by its rows. In other words, the rank of A is the largest integer r s.t. we can extract r rows $u_{i_1}, \ldots, u_{i_r}$ that are free: for every $a_1, \ldots, a_r \in \mathbb{F}$, $a_1 \cdot u_{i_1} + \cdots + a_k \cdot u_{i_k} = 0$ implies $a_1 = \cdots = a_k = 0$. A square matrix $A \in \mathbb{F}^{n \times n}$ is *non-singular* if there exists a matrix B such that $A \cdot B = I$, where $I \in \mathbb{F}^{n \times n}$ is the identity matrix.

The following lemma implies that matrices arising from linrec systems have full rank. We used this lemma to justify why the elimination algorithm in the proof of Theorem 18 successfully produces a non-zero CR.

[7] Actually, Ore considered formal quotients of the form PQ^{-1}, but we found it more convenient to work in the symmetric definition.

▶ **Lemma 37.** *Let $A \in W_2 = \mathbb{Q}[n,k][\partial_1;\sigma_1][\partial_2;\sigma_2]^{n\times n}$ be a matrix of skew polynomials s.t. the combined degree $\deg_{\partial_1+\partial_2} A_{i,i}$ of the diagonal entries is strictly larger than the combined degree $\deg_{\partial_1+\partial_2} A_{j,i}$ of every other entry $j \neq i$ in the same column i. Then A has rank n.*

Indeed, the combined degree of diagonal entries $\partial_1\partial_2$ in a system of linrec equations (2) is 2, while every other entry has the form $p(n,k)$, $p(n,k)\cdot\partial_1$, or $p(n,k)\cdot\partial_2$ with $p(n,k) \in Q[n,k]$ and thus has combined degree 1.

Proof. We denote by A_i the i^{th} row of A. By contradiction, assume A does not have full rank. There exist rows $A_{i_1},\ldots,A_{i_k}$ and nonzero coefficients $P_1,\cdots,P_k \in W_2$ such that:

$$P_{i_1}\cdot A_{i_1} + \cdots + P_{i_k}\cdot A_{i_k} = 0.$$

Let $j_1 = i_1$. Since $\deg_{\partial_1+\partial_2} A_{i_1,i_1} > \deg_{\partial_1+\partial_2} A_{i_r,i_1}$ for $r \geq 2$, there is an index j_2 such that $\deg_{\partial_1+\partial_2} P_{j_2} > \deg_{\partial_1+\partial_2} P_{j_1}$. By repeating this process, we have a sequence of indices $j_1,\ldots,j_{k+1}$ such that

$$\deg_{\partial_1+\partial_2} P_{j_{k+1}} > \deg_{\partial_1+\partial_2} P_{j_k} > \cdots > \deg_{\partial_1+\partial_2} P_{j_1}.$$

This is a contradiction because there are only k different P_i's. ◀

Hermite normal forms. Let $A \in \mathbb{F}[\partial;\sigma]^{n\times n}$ be a skew polynomial square matrix. Let $\deg_\partial A = \max_{i,j}\deg_\partial A_{i,j}$. We say that A is *unimodular* if it is invertible in $\mathbb{F}(\partial;\sigma)^{n\times n}$ and moreover the inverse matrix A^{-1} has coefficients already in the skew polynomial ring $\mathbb{F}[\partial;\sigma]$. We say that A of rank r is in *Hermite form* if a) exactly its first r rows are non-zero, and the first (leading) non-zero entry in each row satisfies the following conditions: b.1) it is a monic skew polynomial (its leading coefficient is $1 \in \mathbb{F}$), b.2) all entries below it are zero, and b.3) all entries above it have strictly lower degree. (In particular, a matrix in Hermite form is upper triangular.) The *Hermite normal form* (HNF) of a skew polynomial matrix A of full rank n is the (unique) matrix $H \in \mathbb{F}[\partial;\sigma]^{n\times n}$ in Hermite form which can be obtained by applying a (also unique) unimodular transformation $U \in \mathbb{F}[\partial;\sigma]^{n\times n}$ as $H = U\cdot A$. Existence of U (and thus of H) has been shown in [26, Theorem 2.4], and uniqueness in [26, Theorem 2.5]. The Hermite form H yields directly a cancelling relationship (CR-2) for the n-th linrec variable f_n, as we show in the following example. (By reordering the equations, we can get an analogous relationship for f_1.)

▶ **Example 38.** Consider the following system of linrec equations:

$$\begin{cases} (\partial_1-1)\partial_2\cdot G_r & -\partial_2\cdot G_s & = 0,\\ -(k\partial_2+1)\cdot G_r & +\partial_1\partial_2\cdot G_s & = 0. \end{cases}$$

In matrix form we have

$$\underbrace{\begin{pmatrix} (\partial_1-1)\partial_2 & -\partial_2\\ -k\partial_2-1 & \partial_1\partial_2 \end{pmatrix}}_{A\in W_2^{2\times 2}}\cdot\underbrace{\begin{pmatrix} G_r\\ G_s\end{pmatrix}}_{x} = 0. \tag{14}$$

The matrix A above is not in Hermite form; one reason is that $(\partial_1-1)\partial_2$ is not monic as a polynomial in W_2 (because its leading coefficient is $\partial_1 - 1 \neq 1$); another reason is that the entry $-k\partial_2 - 1$ below it is nonzero. We show in Example 47 that the Hermite form $H = U \cdot A$ of A is

$$H = \begin{pmatrix} 1 & (\frac{k}{\partial_1 - 1} - \partial_1)\partial_2 \\ 0 & \partial_2^2 - \frac{1}{\partial_1^2 - \partial_1 - (k+1)}\partial_2 \end{pmatrix}.$$

This allows us to immediately obtain a cancelling relation for the variable G_s corresponding to the last row. Going back to our initial matrix equation $A \cdot x = 0$, we have $UAx = Hx = 0$ where $x = (G_r\ G_s)^T$, yielding

$$\left(\partial_2^2 - \frac{1}{\partial_1^2 - \partial_1 - (k+1)}\partial_2\right) \cdot G_s = 0.$$

By clearing out the denominator (an ordinary bivariate polynomial from $\mathbb{Q}[k, \partial_1]$), we obtain

$$((\partial_1^2 - \partial_1 - (k+1)) \cdot \partial_2^2 - \partial_2) \cdot G_s = (\partial_1^2\partial_2^2 - \partial_1\partial_2^2 - (k+1)\partial_2^2 - \partial_2) \cdot G_s = 0 \qquad (15)$$

yielding the sought cancelling relation for G_s not mentioning any other sequence:

$$G_s(k+2, n+2) = G_s(n+1, k+2) + (k+1) \cdot G_s(n, k+2) + G_s(n, k+1).$$

In order to bound the complexity of the Hermite form H in our case of interest, we will use results from [26], instantiated in the special case of Ore shift polynomials. These results generalise to skew polynomials analogous complexity bounds for the HNF over integer matrices $\mathbb{Z}^{n\times n}$ [31] and integer univariate polynomial matrices $\mathbb{Z}[z]^{n\times n}$ [54, 38, 34, 40].

▶ **Theorem 39.** *Let $A \in \mathbb{F}[\partial; \sigma]^{n\times n}$ of full rank n with HNF $H = U \cdot A \in \mathbb{F}[\partial; \sigma]^{n\times n}$.*

1. $\sum_i \deg_\partial H_{i,i} \le n \cdot \deg_\partial A$ *[26, Theorem 4.7, point (a)]. In particular,*

$$\deg_\partial H \le n \cdot \deg_\partial A. \qquad (16)$$

2. *For $A \in \mathbb{F}[z][\partial; \sigma]^{n\times n}$ and $H \in \mathbb{F}(z)[\partial; \sigma]^{n\times n}$ [26, Theorem 5.6, point (a)],*

$$\deg_z H = O(n^2 \cdot \deg_z A \cdot \deg_\partial A) \qquad (17)$$

3. *For $A \in \mathbb{Z}[z][\partial; \sigma]^{n\times n}$ and $H \in \mathbb{Q}(z)[\partial; \sigma]^{n\times n}$ we have [26, Corollary 5.9],*

$$\log |H|_\infty = \tilde{O}(n^2 \cdot \deg_z A \cdot (\deg_\partial A + \log |A|_\infty)). \qquad (18)$$

We lift the results of Theorem 39 from univariate polynomial rings $\mathbb{F}[z], \mathbb{Z}[z]$ to the bivariate polynomial rings $\mathbb{F}[k, \partial_1], \mathbb{Z}[k, \partial_1]$ that we need in our complexity analysis by noticing that the latter behave like the former if we replace $\deg_z$ with $\deg_{k+\partial_1}$. The formal result that we need is the following.

▶ **Lemma 40.** *Let A be an invertible matrix in $\mathbb{Z}[k, \partial_1]^{n\times n}$. Then $\deg_{k+\partial_1} A^{-1} \le n{\cdot}\deg_{k+\partial_1} A$ and $\log |A^{-1}|_\infty \le n^2(1 + \log |A|_\infty + \log \deg_{k+\partial_1} A)$.*

Proof. By Cramer's formula, every coefficient of A^{-1} is the quotient of the determinant of a submatrix of A and the determinant of A. By Lipschitz' formula we have $\det(A) = \sum_\sigma \mathrm{sign}(\sigma) A_{1,\sigma_1} \cdots A_{n,\sigma_2}$, where $\mathrm{sign}(\sigma) \in \{-1, 1\}$ and σ ranges over all permutations of $\{1, \ldots, n\}$. Then we can bound the size of the determinant ◀

The two bounds in Lemma 41 below are obtained from the last two bounds in Theorem 39 by inspecting the proofs in [26] and using the the bounds on inversion of matrices of bivariate polynomials from Lemma 40.

▶ **Lemma 41.** **1.** *For $A \in \mathbb{F}[k, \partial_1][\partial; \sigma]^{n\times n}$ and $H \in \mathbb{F}(k, \partial_1)[\partial; \sigma]^{n\times n}$,*

$$\deg_{k+\partial_1} H = O(n^2 \cdot \deg_{k+\partial_1} A \cdot \deg_\partial A) \tag{19}$$

2. *For $A \in \mathbb{Z}[k, \partial_1][\partial; \sigma]^{n\times n}$ and $H \in \mathbb{Q}(k, \partial_1)[\partial; \sigma]^{n\times n}$ we have*

$$\log |H|_\infty = \tilde{O}(n^2 \cdot \deg_{k+\partial_1} A \cdot (\deg_\partial A + \log |A|_\infty)). \tag{20}$$

Putting everything together, the bounds from point 1. of Theorem 39 and the two bounds from Lemma 41 yield the following corollary.

▶ **Corollary 42.** *Let $A \in (W_2')^{m\times m} = \mathbb{Q}[k, \partial_1][\partial_2; \sigma_2]^{m\times m}$ of full rank m with HNF $H = U \cdot A \in \mathbb{Q}(k, \partial_1)[\partial_2; \sigma_2]^{m\times m}$. We have:*

$$\begin{aligned}\deg_{\partial_2} H &\leq n \cdot \deg_{\partial_2} A,\\ \deg_{k+\partial_1} H &= O(n^2 \cdot \deg_{k+\partial_1} A \cdot \deg_{\partial_2} A),\\ \log |H|_\infty &= \tilde{O}(m^2 \cdot \deg_{\partial_2} A \cdot (\deg_{k+\partial_1} A + \log |A|_\infty)).\end{aligned}$$

Thus, the degrees of the HNF are polynomially bounded, and the heights are exponentially bounded. The bounds from Corollary 42 yield the complexity upper-bound on the zeroness problem that we are after.

▶ **Lemma 20.** *A linrec sequence $f \in \mathbb{Q}^{\mathbb{N}^2}$ of order $\leq m$, degree $\leq d$, and height $\leq h$ admits a cancelling relation* (CR-2) *with the orders i^*, j^* and the degree of p_{i^*,j^*} polynomially bounded, and with height $|p_{i^*,j^*}|_\infty$ exponentially bounded. Similarly, its one-dimensional sections $f(0, k), \ldots, f(i^*, k) \in \mathbb{Q}^\mathbb{N}$ also admit cancelling relations* (CR-1) *of polynomially bounded orders and degree, and exponentially bounded height.*

Proof. Let f be a linrec sequence of order $\leq m$, degree $\leq d$, and height $\leq h$. Since $\deg_{\partial_2} = \deg_{\partial_1} = 1$ in A from linrec, thanks to Corollary 42 the Hermite form H has $\deg_{\partial_2} H \leq m$, $\deg_{k+\partial_1} H$ is polynomially bounded (and thus $\deg_k H$ and $\deg_{\partial_1} H$ as well), and $|H|_\infty$ is exponentially bounded. Thanks to the fact that the Hermite form is triangular, we can immediately extract from $H \cdot x = 0$ the existence of a cancelling relation (CR-2) for f_1 where i^*, j^* are polynomially bounded, the degree of p_{i^*,j^*} is polynomially bounded, and the height of $|p_{i^*,j^*}|_\infty$ is exponentially bounded.

Moreover, consider the one-dimensional sections $f(0, k), \ldots, f(i^*, k) \in \mathbb{Q}^\mathbb{N}$. By Lemma 4, they are linrec of order $\leq m \cdot (i^* + 3)$, degree $\leq d$, and height $\leq h \cdot (i^*)^d$, and thus there are associated matrices $A_0, \ldots, A_{i^*}$ of the appropriate dimensions $\leq (m \cdot (i^* + 3)) \times (m \cdot (i^* + 3))$ with coefficients in $\mathbb{Q}[k][\partial_2; \sigma_2]$. The bounds from Corollary 42 can be applied to this case as well and we obtain for each $0 \leq i \leq i^*$ a cancelling relation (CR-1) R_i with leading polynomial coefficient $q_{i,\ell_i^*}(k)$ where ℓ_i^* is polynomially bounded, its degree in k is polynomially bounded, and the height $\left|q_{i,\ell_i^*}\right|_\infty$ is exponentially bounded. ◀

E.1 Extended example

We conclude this section with an extended example showing how to compute the Hermite form of a skew polynomial matrix, thus illustrating the techniques of Giesbrecht and Kim [26] leading to Theorem 39. We apply the algorithm on our running example. For $n \in \mathbb{N}$, denote with $\mathbb{F}[\partial; \sigma]_n$ the semiring of skew polynomials of degree at most n with coefficients in the field $\mathbb{F}$. Let $\phi_n : \mathbb{F}[\partial; \sigma]_n \to \mathbb{F}^{n+1}$ be the bijection that associates to a skew polynomial of degree $\leq n$ the vector of its coefficients, starting from the one of highest degree. For instance,

$$\phi_5(5 \cdot \partial^3 + 4 \cdot \partial^2 + 7) = (0, 0, 5, 4, 0, 7).$$

The *m-Sylvester matrix* of a skew polynomial $P \in \mathbb{F}[\partial;\sigma]_{n-m}$ of degree $\leq n-m$ is the matrix $S_n^m(P) \in \mathbb{F}^{(m+1)\times(n+1)}$ defined by

$$S_n^m(P) = \begin{pmatrix} \phi_n(\partial^m P) \\ \phi_n(\partial^{m-1} P) \\ \vdots \\ \phi_n(\partial^0 P) \end{pmatrix}. \tag{21}$$

For example, for $P = 5\cdot\partial^3 + 4\cdot\partial^2 + 7$ we have

$$S_5^2(P) = \begin{pmatrix} \phi_5(\partial^2 P) \\ \phi_5(\partial^1 P) \\ \phi_5(\partial^0 P) \end{pmatrix} = \begin{pmatrix} 5 & 4 & 0 & 7 & 0 & 0 \\ 0 & 5 & 4 & 0 & 7 & 0 \\ 0 & 0 & 5 & 4 & 0 & 7 \end{pmatrix}.$$

The next lemma shows that sufficiently large Sylvester matrices can be used to express product of polynomials in terms of products of matrices. This crucial idea allows one to transform problems on skew polynomials in $\mathbb{F}[\partial,\sigma]$ to linear algebra problems in the underlying field (or just semiring) $\mathbb{F}$.

▶ **Lemma 43** (c.f. [6, Sec. 1, eq. (1)]). *Let $P, Q \in \mathbb{F}[\partial;\sigma]$ and $n, m \in \mathbb{N}$ s.t. $\deg P \leq m$ and $\deg Q \leq n - \deg P$. Then,*

$$\phi_n(Q\cdot P) = \phi_m(Q)\cdot S_n^m(P).$$

We extend both ϕ_n and S_n^m to skew polynomial matrices in $\mathbb{F}[\partial;\sigma]_n^{k\times k}$ by point-wise application and then merging all the obtained matrices into a single one.

▶ **Example 44.** For instance, $\phi_2(A)$ with $A \in \mathbb{Q}[k][\partial_1;\sigma_1][\partial_2;\sigma_2]^{2\times 2}$ from (14) equals

$$\begin{aligned} \phi_2(A) &= \phi_2\begin{pmatrix} (\partial_1 - 1)\partial_2 & -\partial_2 \\ -k\partial_2 - 1 & \partial_1\partial_2 \end{pmatrix} = \begin{pmatrix} \phi_2((\partial_1 - 1)\partial_2) & \phi_2(-\partial_2) \\ \phi_2(-k\partial_2 - 1) & \phi_2(\partial_1\partial_2) \end{pmatrix} \\ &= \begin{pmatrix} 0 & \partial_1 - 1 & 0 & 0 & -1 & 0 \\ 0 & -k & -1 & 0 & \partial_1 & 0 \end{pmatrix} \in \mathbb{Q}[k][\partial_1;\sigma_1]^{2\times 6} \end{aligned}$$

and thus $S_2^1(A) \in \mathbb{Q}[k][\partial_1;\sigma_1]^{4\times 6}$ is

$$\begin{aligned} S_2^1(A) &= S_2^1\begin{pmatrix} (\partial_1 - 1)\partial_2 & -\partial_2 \\ -k\partial_2 - 1 & \partial_1\partial_2 \end{pmatrix} = \\ &= \begin{pmatrix} S_2^1((\partial_1 - 1)\partial_2) & S_2^1(-\partial_2) \\ S_2^1(-k\partial_2 - 1) & S_2^1(\partial_1\partial_2) \end{pmatrix} = \\ &= \begin{pmatrix} \begin{pmatrix} \phi_2(\partial_2(\partial_1 - 1)\partial_2) \\ \phi_2((\partial_1 - 1)\partial_2) \end{pmatrix} & \begin{pmatrix} \phi_2(\partial_2(-\partial_2)) \\ \phi_2(-\partial_2) \end{pmatrix} \\ \begin{pmatrix} \phi_2(\partial_2(-k\partial_2 - 1)) \\ \phi_2(-k\partial_2 - 1) \end{pmatrix} & \begin{pmatrix} \phi_2(\partial_2\partial_1\partial_2) \\ \phi_2(\partial_1\partial_2) \end{pmatrix} \end{pmatrix} = \\ &= \begin{pmatrix} \begin{pmatrix} (\partial_1 - 1\ 0\ 0) \\ (0\ \partial_1 - 1\ 0) \end{pmatrix} & \begin{pmatrix} (-1\ 0\ 0) \\ (0\ -1\ 0) \end{pmatrix} \\ \begin{pmatrix} (-(k+1)\ -1\ 0) \\ (0\ -k\ -1) \end{pmatrix} & \begin{pmatrix} (\partial_1\ 0\ 0) \\ (0\ \partial_1\ 0) \end{pmatrix} \end{pmatrix} = \\ &= \begin{pmatrix} \partial_1 - 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & \partial_1 - 1 & 0 & 0 & -1 & 0 \\ -(k+1) & -1 & 0 & \partial_1 & 0 & 0 \\ 0 & -k & -1 & 0 & \partial_1 & 0 \end{pmatrix}. \end{aligned}$$

By definition of the Hermite form, we have that $H = U \cdot A$. By (16) every degree of skew polynomials appearing therein is bounded by $n \cdot \deg A$. Hence setting $\rho = n \cdot \deg A$, we have the following matrix equation with coefficients in $\mathbb{F}$:

$$\phi_{\rho+d}(H) = \phi_\rho(U) \cdot S^\rho_{\rho+d}(A).$$

The *diagonal degree vector* of the Hermite form for A is the unique vector d s.t. $d_i = \deg H_{i,i}$. The algorithm will guess such a vector, and it can detect whether the guess was correct or not. If it is the right one, then H and U can be computed.

▶ **Example 45.** The correct diagonal degree vector for our running example is $(0, 2)$. The Hermite normal form $H = U \cdot A$ of the 2×2 matrix A from our running example has the form

$$H = \begin{pmatrix} H_{11} & H_{12} \\ 0 & H_{22} \end{pmatrix}, \quad U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \in \mathbb{Q}[k][\partial_1; \sigma_1][\partial_2; \sigma_2]^{2\times 2}$$

where $H_{11}, H_{22} \in \mathbb{Q}[k][\partial_1; \sigma_1][\partial_2; \sigma_2]$ are *monic* skew polynomials of degree respectively 0 and 2 and $H_{12}, U_{11}, U_{12}, U_{21}, U_{22} \in \mathbb{Q}[k][\partial_1; \sigma_1][\partial_2; \sigma_2]$ are skew polynomials of degree 1. It follows that

$$\begin{aligned}
\phi_2(H) = {} & \begin{pmatrix} \phi_2(H_{11}) & \phi_2(H_{12}) \\ 0 & \phi_2(H_{22}) \end{pmatrix} = \\
= {} & \begin{pmatrix} \phi_2(1) & \phi_2(a_{121}\partial_2 + a_{120}) \\ 0 & \phi_2(\partial_2^2 + a_{221}\partial_2 + a_{220}) \end{pmatrix} = \\
= {} & \begin{pmatrix} 0 & 0 & 1 & 0 & a_{121} & a_{120} \\ 0 & 0 & 0 & 1 & a_{221} & a_{220} \end{pmatrix} \in \mathbb{Q}[k][\partial_1; \sigma_1]^{2\times 6}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\phi_1(U) = {} & \begin{pmatrix} \phi_1(U_{11}) & \phi_1(U_{12}) \\ \phi_1(U_{21}) & \phi_1(U_{22}) \end{pmatrix} = \begin{pmatrix} \phi_1(u_{111}\partial_2 + u_{110}) & \phi_1(u_{121}\partial_2 + u_{120}) \\ \phi_1(u_{211}\partial_2 + u_{210}) & \phi_1(u_{221}\partial_2 + u_{220}) \end{pmatrix} = \\
= {} & \begin{pmatrix} u_{111} & u_{110} & u_{121} & u_{120} \\ u_{211} & u_{210} & u_{221} & u_{220} \end{pmatrix} \in \mathbb{Q}[k][\partial_1; \sigma_1]^{2\times 4}.
\end{aligned}$$

By putting the pieces together, we obtain the following matrix equation with entries in $\mathbb{Q}[k][\partial_1; \sigma_1]$

$$\begin{aligned}
& \underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 & a_{121} & a_{120} \\ 0 & 0 & 0 & 1 & a_{221} & a_{220} \end{pmatrix}}_{\phi_2(H)} = \\
& \qquad \underbrace{\begin{pmatrix} u_{111} & u_{110} & u_{121} & u_{120} \\ u_{211} & u_{210} & u_{221} & u_{220} \end{pmatrix}}_{\phi_1(U)} \cdot \underbrace{\begin{pmatrix} \partial_1 - 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & \partial_1 - 1 & 0 & 0 & -1 & 0 \\ -(k+1) & -1 & 0 & \partial_1 & 0 & 0 \\ 0 & -k & -1 & 0 & \partial_1 & 0 \end{pmatrix}}_{S_2^1(A)}.
\end{aligned}$$

It is shown in [26, Theorem 5.2] that if we guessed the diagonal degree vector right, then we can remove columns from $\phi_{\rho+d}(H)$ corresponding to under-determined entries, and corresponding columns in $S^\rho_{\rho+d}(A)$, in order to obtain two matrices $\tilde{A}$ and $\tilde{H}$ such that:

- $\tilde{H}$ is only made of 0's and 1's.
- $\tilde{A}$ is a square matrix.
- The matrix equation $T\tilde{A} = \tilde{H}$ of unknown T (of the same dimensions as $\phi_\rho(U)$) has a unique solution. In particular, $\tilde{A}$ has full rank and hence is invertible.

▶ **Example 46.** The reduced system $\tilde{H} = \phi_1(U) \cdot \tilde{A}$ in our running example is obtained by removing columns $5, 6$ from $\phi_2(H)$ and correspondingly from $S_2^1(A)$:

$$\underbrace{\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{\tilde{H}} = \underbrace{\begin{pmatrix} u_{111} & u_{110} & u_{121} & u_{120} \\ u_{211} & u_{210} & u_{221} & u_{220} \end{pmatrix}}_{\phi_1(U)} \cdot \underbrace{\begin{pmatrix} \partial_1 - 1 & 0 & 0 & -1 \\ 0 & \partial_1 - 1 & 0 & 0 \\ -(k+1) & -1 & 0 & \partial_1 \\ 0 & -k & -1 & 0 \end{pmatrix}}_{\tilde{A}} .$$

Now the obtained $\tilde{A}$ is invertible. Hence we can determine U thanks to the equation $\phi_1(U) = \tilde{H}\tilde{A}^{-1}$.

▶ **Example 47.** In the example, we obtain

$$T = \begin{pmatrix} -\frac{k}{\partial_1 - 1} & -1 \\ \frac{k+1}{\partial_1^2 - \partial_1 - (k+1)}\partial_2 + \frac{1}{\partial_1^2 - \partial_1 - (k+1)} & \frac{1}{\partial_1^2 - \partial_1 - (k+1)}\partial_2 \end{pmatrix},$$

yielding the Hermite form:

$$\begin{aligned} H = T \cdot A &= \begin{pmatrix} -\frac{k}{\partial_1 - 1} & -1 \\ \frac{k+1}{\partial_1^2 - \partial_1 - (k+1)}\partial_2 + \frac{1}{\partial_1^2 - \partial_1 - (k+1)} & \frac{1}{\partial_1^2 - \partial_1 - (k+1)}\partial_2 \end{pmatrix} \cdot \begin{pmatrix} (\partial_1 - 1)\partial_2 & -\partial_2 \\ -k\partial_2 - 1 & \partial_1\partial_2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (\frac{k}{\partial_1 - 1} - \partial_1)\partial_2 \\ 0 & \partial_2^2 - \frac{1}{\partial_1^2 - \partial_1 - (k+1)}\partial_2 \end{pmatrix} . \end{aligned} \tag{22}$$