# Degree and dimension estimates for invariant ideals of *P*-solvable recurrences

Marc Moreno Maza[1] and Rong Xiao[2]

[1] University of Western Ontario, Canada moreno@csd.uwo.ca
[2] University of Western Ontario, Canada rong@csd.uwo.ca

**Abstract.** Motivated by the generation of polynomial loop invariants of computer programs, we study $P$-solvable recurrences. While these recurrences may contain non-linear terms, we show that the solutions of any such relation can be obtained by solving a system of linear recurrences. We also study invariant ideals of $P$-solvable recurrences (or equivalently of while loops with no branches). We establish sharp degree and dimension estimates of those invariant ideals.

## 1 Introduction

In many applications, such as program verification, non-linear recurrence relations, like the following one, may arise:

$$\begin{cases} x(n+1) = x(n) + 1 \\ y(n+1) = y(n) + x(n)^2 + 1 \end{cases}, \text{ with } \begin{array}{l} x(0) = 1 \\ y(0) = 1. \end{array}$$

In these recurrences, some variables may appear non-linearly, but not in a completely arbitrary way. A fundamental case is that of the so-called $P$-solvable recurrences. This paper focuses on $P$-solvable recurrences with rational coefficients, that we define formally below.

**Definition 1 ($P$-solvable recurrence)** *Let $n_1, \ldots, n_k$ be positive integers and define $s := n_1 + \cdots + n_k$. Let $M$ be a square matrix over $\mathbb{Q}$ and with order $s$. We assume that $M$ is block-diagonal with the following shape:*

$$M := \begin{pmatrix} \mathbf{M}_{n_1 \times n_1} & & & \\ & \mathbf{M}_{n_2 \times n_2} & & \\ & & \ddots & \\ & & & \mathbf{M}_{n_k \times n_k} \end{pmatrix}.$$

*Consider an $s$-variable recurrence relation $R$ in the variables $x_1, x_2, \ldots, x_s$ and with the following form:*

$$\begin{pmatrix} x_1(n+1) \\ x_2(n+1) \\ \vdots \\ x_s(n+1) \end{pmatrix} = M \times \begin{pmatrix} x_1(n) \\ x_2(n) \\ \vdots \\ x_s(n) \end{pmatrix} + \begin{pmatrix} \mathbf{f}_1 \\ \mathbf{f}_2 \\ \vdots \\ \mathbf{f}_k \end{pmatrix},$$

*where* $\mathbf{f}_1$ *is a vector of length* $n_1$ *with coordinates in* $\mathbb{Q}$ *and where* $\mathbf{f}_i$ *is a tuple of length* $n_i$ *with coordinates in the polynomial ring* $\mathbb{Q}[x_1, \ldots, x_{n_1+\cdots+n_{i-1}}]$*, for* $i = 2, \ldots, k$*. Then, the recurrence relation* $R$ *is called* $P$-solvable *over* $\mathbb{Q}$ *and the matrix* $M$ *is called the* coefficient matrix *of* $R$*.*

Example 6 in Section 4 illustrates the above definition with a 2-block matrix and non-linear terms, while Example 1 below is a simpler case with a 1-block matrix. Our study of $P$-solvable recurrences originates in a previous work [8] dedicated to the computation of loop invariants of while-loops of the following shape:

```
while cond do
      X := A(X);
end do
```

where the recurrence $X(n+1) = A(X(n))$ induced by the assignments in the loop body is a $P$-solvable recurrence. We call *$P$-solvable* such while-loops.

**Example 1** *Consider the following code segment:*

```
a, b := 0, 1 ;
while true do
      a, b := b, a + b;
end do
```

*At each iteration, the variables* $a, b$ *hold two consecutive elements in the Fibonacci sequence. To be more precise, let us associate a counter variable* $n$ *to the variables* $a, b$*. Let us initialize* $n$ *to* 0 *before entering the loop and let us increase* $n$ *by* 1 *after each loop iteration. Then we have*

$$\begin{cases} a(n+1) := b(n) \\ b(n+1) := a(n) + b(n) \end{cases}, \text{ with } \begin{array}{l} a(0) := 0 \\ b(0) := 1 \end{array}.$$

*which is clearly a* $P$*-solvable recurrence.*

There are several variants of the notion of a $P$-solvable recurrence, see the concept of *solvable mapping* in [13] or that of *solvable loop* in [7].

For a recurrence $X(n+1) = A(X(n))$, or equivalently for a $P$-solvable while loop, an *invariant* is a condition on the recurrence variables which holds for all values of $n$. In this paper, we are mainly interested by invariants which are polynomial equations, as defined formally below.

**Definition 2** *Given an* $s$*-variable* $P$*-solvable recurrence* $R$ *with recurrence variables* $x_1, x_2, \ldots, x_s$*, a polynomial* $p$ *in* $\mathbb{Q}[x_1, x_2, \ldots, x_s]$ *is called a* polynomial invariant *of* $R$ *if for all* $n$*, we have* $p(x_1(n), x_2(n), \ldots, x_s(n)) = 0$*. All polynomial invariants of* $R$ *form an ideal of the polynomial ring* $\mathbb{Q}[x_1, x_2, \ldots, x_s]$*; this ideal is called the (polynomial)* invariant ideal *of* $R$*.*

It is known that, for instance in [13], that $P$-solvable recurrences have poly-geometrical expressions (which are defined formally in Definition 3) as closed form solutions. However, solving $P$-solvable recurrences, even linear ones, is a computationally hard problem, since many algebraic numbers could be involved.

Returning to the question of computing polynomial invariants of $P$-solvable recurrences, there are approaches based on solving those recurrences explicitly. See the work of Kauers and Zimmermann in [6] and that of Kovács in [7]. In contrast, our goal in [8] as that of Kapur and Rodriguez-Carbonell in [2], is to compute polynomial invariants of $P$-solvable recurrences without explicitly solving those recurrences. In [8], we proposed a method, based on interpolating polynomials at finitely many points on the trajectory (i.e. point sequence) of the recurrence under study. This interpolation process yields "candidate invariants" which are then checked by a criterion performing a polynomial ideal membership test.

The objective of the present paper is to provide degree and dimension estimates for invariant ideals. These results are clearly needed by the interpolation method of [8] and can benefit any methods for computing polynomial invariants that require a degree bound as input, such as the method by Kapur and Rodriguez-Carbonell [12].

Our paper proposes the following original results. We show that $P$-solvable recurrences and linear recurrences are equivalent in the sense that every $P$-solvable recurrence can be obtained by solving a system of linear recurrences (Theorem 1). We also supply a sharp degree bound (Theorems 2 and 3) for *invariant ideals* as well as a dimension analysis (Theorem 4) of those ideals. In addition, Corollary 2 states a sufficient condition for a given invariant ideal to be trivial.

The paper is organized as follows. In Section 2, we review some results on symbolic summation; those results are related to the properties of closed form solutions of $P$-solvable recurrences. We also include a brief review on the notion of a degree of a polynomial ideal. In Section 3, we show how solving $P$-solvable recurrence reduces to solving linear recurrences; thus we refer to that process as "linearizing" a $P$-solvable recurrence. Finally, in Section 4, we exhibit degree and dimension estimates for invariant ideals of $P$-solvable recurrences. We conclude this introduction with an example illustrating the notion of an invariant ideal together with our results on dimension and degree of invariant ideals.

**Example 2** *Consider the following $P$-solvable recurrence relation with $x, y$ as recurrence variables:*

$$x(n+1) = y(n), y(n+1) = x(n) + y(n), \text{ with } x(0) = 0, y(0) = 1.$$

*Closed form formulas for $x(n)$ and $y(n)$ are easily obtained:*

$$x(n) = \frac{(\frac{\sqrt{5}+1}{2})^n}{\sqrt{5}} - \frac{(\frac{-\sqrt{5}+1}{2})^n}{\sqrt{5}},$$
$$y(n) = \frac{\sqrt{5}+1}{2}\frac{(\frac{\sqrt{5}+1}{2})^n}{\sqrt{5}} - \frac{-\sqrt{5}+1}{2}\frac{(\frac{-\sqrt{5}+1}{2})^n}{\sqrt{5}}.$$

*Let $a, u, v$ be 3 variables. Replace $(\frac{\sqrt{5}+1}{2})^n$ (resp. $(\frac{-\sqrt{5}+1}{2})^n$) by $u$ (resp. by $v$) and replace $\sqrt{5}$ by $a$. Taking into account the dependencies $u^2\,v^2 = 1, a^2 = 5$, one can check that the invariant ideal is given by:*

$$\langle x - \frac{au}{5} + \frac{av}{5}, y - a\frac{a+1}{2}\frac{u}{5} + a\frac{-a+1}{2}\frac{v}{5}, a^2 - 5, u^2v^2 - 1\rangle \cap \mathbb{Q}[x, y],$$

*which turns out to be $\langle 1 - y^4 + 2xy^3 + x^2y^2 - 2x^3y - x^4\rangle$. Observe that this ideal has dimension 1 and degree 4.*

*Now, we use Theorem 3 to estimate the degree of this invariant ideal. Denote by $A := \frac{-\sqrt{5}+1}{2}, \frac{\sqrt{5}+1}{2}$, the eigenvalues of the coefficient matrix of the input $P$-solvable recurrence. One can easily check that the set $A$ is weakly multiplicatively independent, see Definition 6 for this notion. Note that the multiplicative relation ideal, See Definition 5, of $A$ associated with the variables $u, v$ is generated by $u^2v^2 - 1$ and thus has degree 4 and dimension 1 in $\mathbb{Q}[u, v]$. Therefore, by Theorem 3, the degree of the invariant ideal is bounded by 4. This implies that the degree bound given by Theorem 3 is sharp. Meanwhile, Theorem 4 estimates the dimension as 1, which is also sharp.*

## 2 Preliminaries

Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Let $\mathbb{Q}^*$ (resp. $\overline{\mathbb{Q}}^*$) denote the non zero elements in $\mathbb{Q}$ (resp. $\overline{\mathbb{Q}}$) .

### 2.1 Poly-geometric summation

In this subsection, we recall several well-known notions together with related results around the topic of $P$-solvable recurrences. Those notions and results are adapted to our needs and could be stated in a more general context. For instance, the notion of multiplicative relation can be defined among elements of an arbitrary Abelian group, whereas we define it for a multiplicative group of algebraic numbers.

**Definition 3** *Let $\alpha_1, \ldots, \alpha_k$ be $k$ pairwise distinct elements of $\overline{\mathbb{Q}}^* \setminus \{1\}$. Let $n$ be a variable taking non-negative integer values. We regard $n, \alpha_1^n, \ldots, \alpha_k^n$ as independent variables and we call $\alpha_1^n, \ldots, \alpha_k^n$ $n$-exponential variables. Any polynomial of $\overline{\mathbb{Q}}[n, \alpha_1^n, \ldots, \alpha_k^n]$ is called a* poly-geometrical expression in $n$ over $\overline{\mathbb{Q}}$ *w.r.t. $\alpha_1, \ldots, \alpha_k$.*

*Let $f, g$ be two poly-geometrical expressions $n$ over $\overline{\mathbb{Q}}$ w.r.t. $\alpha_1, \ldots, \alpha_k$. Given a non-negative integer number $i$, we denote by $f|_{n=i}$ the* evaluation *of $f$ at $i$, which is obtained by substituting all occurrences of $n$ by $i$ in $f$. We say that $f$ and $g$ are* equal *whenever $f|_{n=i} = g|_{n=i}$ holds for all non-negative integer $i$.*

*We say that $f(n)$ is in* canonical form *if there exist*

(*i*) *finitely many numbers $c_1, \ldots, c_m \in \overline{\mathbb{Q}}^*$, and*

(*ii*) *finitely many pairwise different couples* $(\beta_1, e_1), \ldots, (\beta_m, e_m)$ *all in* $(\overline{\mathbb{Q}}^* \setminus \{1\}) \times \mathbb{Z}_{\geq 0}$, *and*
(*iii*) *a polynomial* $c_0(n) \in \mathbb{Q}[n]$,

*such that each* $\beta_1, \ldots, \beta_m$ *is a product of some of the* $\alpha_1, \ldots, \alpha_k$ *and such that the poly-geometrical expressions* $f(n)$ *and* $\sum_{i=1}^{m} c_i \, \beta_i^n \, n^{e_i} + c_0(n)$ *are equal. When this holds, the polynomial* $c_0(n)$ *is called the* exponential-free part *of* $f(n)$.

**Remark 1** *Note that sometime when referring to poly-geometrical expressions, for simplicity, we allow* $n$*-exponential terms with base* $0$ *or* $1$, *that is, terms with* $0^n$ *or* $1^n$ *as factors. Such terms will always be evaluated to* $0$ *or* $1$ *respectively.*

Proving the following result is routine.

**Lemma 1** *With the notations of Definition 3, let* $f$ *a poly-geometrical expression in* $n$ *over* $\overline{\mathbb{Q}}$ *w.r.t.* $\alpha_1, \ldots, \alpha_k$. *There exists a unique poly-geometrical expression* $c$ *in* $n$ *over* $\overline{\mathbb{Q}}$ *w.r.t.* $\alpha_1, \ldots, \alpha_k$ *such that* $c$ *is in canonical form and such that* $f$ *and* $c$ *are equal. We call* $c$ *the* canonical form *of* $f$.

**Example 3** *The closed form* $f := \frac{(n+1)^2 \, n^2}{4}$ *of* $\sum_{i=0}^{n} i^3$ *is a poly-geometrical expression in* $n$ *over* $\overline{\mathbb{Q}}$ *without* $n$*-exponential variables. The expression* $g := n^2 \, 2^{(n+1)} - n \, 2^n \, 3^{\frac{n}{2}}$ *is a poly-geometrical in* $n$ *over* $\overline{\mathbb{Q}}$ *w.r.t.* $2, 3$. *Some evaluations are:* $f|_{(n=0)} = 0, f|_{n=1} = 1, g|_{n=0} = 0, g|_{n=2} = 8$.

**Notation 1** *Let* $x$ *be an arithmetic expression and let* $k \in \mathbb{N}$. *Following [3], we call* $k$-th falling factorial of $x$ *and denote by* $x^{\underline{k}}$ *the product*

$$x \, (x-1) \cdots (x-k+1).$$

*For* $i = 1, \ldots, k$, *we denote by* $\left\{ {k \atop i} \right\}$ *the number of ways to partition* $k$ *into* $i$ *non-zero summands, that is, the* Stirling number of the second kind *also denoted by* $S(n, k)$. *We define* $\left\{ {k \atop 0} \right\} := 0$.

**Example 4** *Consider a fixed non-negative integer* $k$. *The sum* $\sum_{i=1}^{n-1} i^k$ *has* $n-1$ *terms while its closed form [3] below*

$$\sum_{i=1}^{k} \left\{ {k \atop i} \right\} \frac{n^{\underline{i+1}}}{i+1}$$

*has a fixed number of terms and thus is poly-geometrical in* $n$ *over* $\overline{\mathbb{Q}}$.

The following result is well-known and one can find a proof in [3].

**Lemma 2** *Let* $x$ *be an arithmetic expression and let* $k \in \mathbb{N}$. *Then we have*

$$x^k \; = \; \sum_{i=1}^{k} \left\{ {k \atop i} \right\} x^{\underline{i}}.$$

**Notation 2** *Let $r \in \overline{\mathbb{Q}}$ and let $k \in \mathbb{N}$. We denote by $H(r,k,n)$ the following symbolic summation*

$$H(r,k,n) := \sum_{i=0}^{n-1} r^i \; i^{\underline{k}}.$$

Let's denote by $H(r,0,n)$ the symbolic summation $\sum_{i=0}^{n-1} r^i$. One can easily check that $H(r,0,n) = \frac{r^n-1}{r-1}$ holds for $r \neq 1$. Moreover, we have the following result.

**Lemma 3** *Assume $r \neq 0$. Then, we have*

$$(r-1)\,H(r,k,n) \;=\; (n-1)^{\underline{k}}\, r^n - r\,k\; H(r,k-1,n-1). \tag{1}$$

*In addition, we have*

(*i*) *if $r = 1$, then $H(r,k,n)$ equals to $\frac{n^{\underline{k+1}}}{k+1}$, which is a polynomial in $n$ over $\overline{\mathbb{Q}}$ of degree $k+1$.*

(*ii*) *if $r \neq 1$, then $H(r,k,n)$ has a closed form like $r^n\, f(n) + c$, where $f(n)$ is a polynomial in $n$ over $\overline{\mathbb{Q}}$ of degree $k$ and $c$ is a constant in $\overline{\mathbb{Q}}$.*

Proof**:** We can verify Relation (1) by expanding $H(r,k,n)$ and $H(r,k-1,n-1)$. Now let us show the rest of the conclusion. First, assume $r = 1$. With Relation (1), we have

$$k\,H(r,k-1,n-1) = (n-1)^{\underline{k}}.$$

Therefore, we deduce

$$H(r,k,n) = \frac{n^{\underline{k+1}}}{k+1}.$$

One can easily check that $\frac{n^{\underline{k+1}}}{k+1}$ is a polynomial in $n$ over $\overline{\mathbb{Q}}$ and the degree of $n$ is $k+1$.

From now on assume $r \neq 1$. We proceed by induction on $k$. When $k = 0$, we have $H(r,0,n) = \frac{r^n-1}{r-1}$. We rewrite $\frac{r^n-1}{r-1}$ as

$$r^n\,\frac{1}{r-1} - \frac{1}{r-1},$$

which is such a closed form. Assume there exists a closed form $r^{n-1}\, f_{k-1}(n-1) + c_{k-1}$ for $H(r,k-1,n-1)$, where $f_{k-1}(n-1)$ is a polynomial in $n-1$ over $\overline{\mathbb{Q}}$ of degree $k-1$. Substitute $H(r,k-1,n-1)$ by $r^{n-1}\, f_{k-1}(n-1) + c_{k-1}$ in Relation (1) and solve $H(r,k,n)$, we have

$$H(r,k,n) = \frac{(n-1)^{\underline{k}}\, r^n - r\,k\,(r^{n-1}\, f_{k-1}(n-1) + c_{k-1})}{r-1}.$$

We rewrite the right hand side of the above equation as

$$r^n\,\frac{(n-1)^{\underline{k}} - k\, f_{k-1}(n-1)}{r-1} - \frac{r\,k\,c_{k-1}}{r-1},$$

from which one can easily check it satisfies the requirements of $(ii)$ in the conclusion. This completes the proof. □

**Lemma 4** *Let $k \in \mathbb{N}$ and let $\lambda$ be a non zero algebraic number over $\mathbb{Q}$. Consider the symbolic summation*

$$S := \sum_{i=1}^{n} i^k \lambda^i.$$

1. *if $\lambda = 1$, then there exists a closed form $s(n)$ for $S$, where $s$ is a polynomial in $n$ over $\overline{\mathbb{Q}}$ of degree $k+1$.*
2. *if $\lambda \neq 1$, then there exists a closed form $\lambda^n s(n) + c$ for $S$, where $s$ is a polynomial in $n$ over $\overline{\mathbb{Q}}$ of degree $k$ and $c \in \overline{\mathbb{Q}}$ is a constant.*

PROOF**:** By Lemma 2, we deduce

$$\begin{aligned} \textstyle\sum_{i=1}^{n} i^k \lambda^i &= \textstyle\sum_{i=1}^{n} \left( \sum_{j=1}^{k} \left\{ {k \atop j} \right\} i^{\underline{j}} \right) \lambda^i \\ &= \textstyle\sum_{j=1}^{k} \left( \left\{ {k \atop j} \right\} \sum_{i=1}^{n} i^{\underline{j}} \lambda^i \right) \\ &= \textstyle\sum_{j=1}^{k} \left( \left\{ {k \atop j} \right\} H(\lambda, j, n) \right) \end{aligned}$$

Then, the conclusions on each case follow from the corresponding results in Lemma 3. □

The following definition is a specialization of the general definition of multiplicative relation to the case of non-zero algebraic numbers.

**Definition 4 (Multiplicative relation)** *Let $k$ be a positive integer. Let $A := (\alpha_1, \ldots, \alpha_k)$ be a sequence of $k$ non-zero algebraic numbers over $\mathbb{Q}$ and $\mathbf{e} := (e_1, \ldots, e_k)$ be a sequence of $k$ integers. We say that $\mathbf{e}$ is a* multiplicative relation *on $A$ if $\prod_{i=1}^{k} \alpha_i^{e_i} = 1$ holds. Such a multiplicative relation is said* non-trivial *if there exists $i \in \{1, \ldots, n\}$ such that $e_i \neq 0$ holds. If there exists a non-trivial multiplicative relation on $A$, then we say that $A$ is* multiplicatively dependent*; otherwise, we say that $A$ is* multiplicatively independent*.*

All multiplicative relations of $A$ form a lattice, called the *multiplicative relation lattice* on $A$, which can effectively be computed, for instance with the algorithm proposed by G. Ge in his PhD thesis [4].

For simplicity, we need the following generalized notion of multiplicative relation ideal, which is defined for a sequence of algebraic numbers that may contain 0 and repeated elements.

**Definition 5** *Let $A := (\alpha_1, \ldots, \alpha_k)$ be a sequence of $k$ algebraic numbers over $\mathbb{Q}$. Assume w.l.o.g. that there exists an index $\ell$, with $1 \leq \ell \leq k$, such that $\alpha_1, \ldots, \alpha_\ell$ are non-zero and $\alpha_{\ell+1}, \ldots, \alpha_k$ are all zero. We associate each $\alpha_i$ with a variable $y_i$, where $y_1, \ldots, y_k$ are pairwise distinct. We call the* multiplicative

relation ideal of $A$ associated with variables $y_1, \ldots, y_k$, *the binomial ideal of* $\mathbb{Q}[y_1, y_2, \ldots, y_k]$ *generated by*

$$\{ \prod_{j \in \{1,\ldots,\ell\},\, v_j > 0} y_j^{v_j} - \prod_{i \in \{1,\ldots,\ell\},\, v_i < 0} y_i^{-v_i} \mid (v_1, \ldots, v_\ell) \in Z \}$$

*and* $\{y_{\ell+1}, \ldots, y_k\}$, *denoted by* $\mathrm{MRI}(A; y_1, \ldots, y_k)$, *where* $Z$ *is the multiplicative relation lattice on* $(\alpha_1, \ldots, \alpha_\ell)$. *When no confusion is possible, we shall not specify the associated variables* $y_1, \ldots, y_k$.

**Lemma 5** *Let* $\alpha_1, \ldots, \alpha_k$ *be* $k$ *multiplicatively independent elements of* $\overline{\mathbb{Q}}$ *and let* $n$ *be a non-negative integer variable. Let* $f(n)$ *be a poly-geometrical expression in* $n$ *w.r.t.* $\alpha_1, \ldots, \alpha_k$. *Assume that* $f|_{(n=i)} = 0$ *holds for all* $i \in \mathbb{N}$. *Then,* $f$ *is the zero polynomial of* $\overline{\mathbb{Q}}[n, \alpha_1^n, \ldots, \alpha_k^n]$.

The following definition will be convenient in later statements.

**Definition 6 (Weak multiplicative independence)** *Let* $A := (\alpha_1, \ldots, \alpha_k)$ *be a sequence of* $k$ *non-zero algebraic numbers over* $\mathbb{Q}$ *and let* $\beta \in \overline{\mathbb{Q}}$. *We say that* $\beta$ *is* weakly multiplicatively independent *w.r.t.* $A$, *if there exist no non-negative integers* $e_1, e_2, \ldots, e_k$ *such that* $\beta = \prod_{i=1}^{k} \alpha_1^{e_i}$ *holds. Furthermore, we say that* $A$ *is* weakly multiplicatively independent *if*

(*i*) $\alpha_1 \neq 1$ *holds, and*
(*ii*) $\alpha_i$ *is weakly multiplicatively independent w.r.t.* $\{\alpha_1, \ldots, \alpha_{i-1}, 1\}$, *for all* $i = 2, \ldots, s$.

Lemma 7 is a structural result for the closed form solutions of single-variable linear recurrences involving poly-geometrical expressions. For the proof, we need Lemma 6, which is easy to check, see for instance [11].

**Lemma 6** *Let* $n$ *a variable holding non-negative integer values. Let* $a$ *and* $b$ *be two sequences in* $\mathbb{Q}$ *indexed by* $n$. *Consider the following recurrence equation of variable* $x$:

$$x(n) = a(n-1)\, x(n-1) + b(n-1).$$

*Then we have*

$$x(n) = \prod_{i=0}^{n-1} a(i) \left( x(0) + \sum_{j=0}^{n-1} \frac{b(j)}{\prod_{s=0}^{j} a(s)} \right).$$

**Lemma 7** *Let* $\alpha_1, \ldots, \alpha_k$ *be* $k$ *elements in* $\overline{\mathbb{Q}}^* \setminus \{1\}$. *Let* $\lambda \in \overline{\mathbb{Q}}^*$ . *Let* $h(n)$ *be a poly-geometrical expression in* $n$ *over* $\overline{\mathbb{Q}}$ *w.r.t.* $\alpha_1, \ldots, \alpha_k$. *Consider the following single-variable recurrence relation* $R$:

$$x(n+1) = \lambda x(n) + h(n).$$

*Then, there exists a poly-geometrical expression $s(n)$ in $n$ over $\overline{\mathbb{Q}}$ w.r.t. $\alpha_1, \ldots, \alpha_k$ such that we have*

$$\deg(s(n), \alpha_i^n) \leq \deg(h(n), \alpha_i^n) \quad \text{and} \quad \deg(s(n), n) \leq \deg(h(n), n) + 1,$$

*and such that*

- *if $\lambda = 1$ holds, then $s(n)$ solves $R$,*
- *if $\lambda \neq 1$ holds, then there exists a constant $c$ depending on $x(0)$ (that is, the initial value of $x$) such that $c\,\lambda^n + s(n)$ solves $R$.*

*Moreover, in both cases, if the exponential-free part of the canonical form of $(\frac{1}{\lambda})^n\, h(n)$ is 0, then we can further require that $\deg(s(n), n) \leq \deg(h(n), n)$ holds.*

Proof: By Lemma 6, we have

$$x(n) = \lambda^n \left( x(0) + \sum_{j=0}^{n-1} \frac{h(j)}{\lambda^{j+1}} \right). \tag{2}$$

Denote by $\texttt{terms}(h)$ all the terms of the canonical form of $h(n)$. Assume each $t \in \texttt{terms}(h)$ is of form

$$c_t\, n^{q_t}\, \beta_t^n,$$

where $c_t$ is a constant in $\overline{\mathbb{Q}}$, $q_t$ is a non-negative integer and $\beta_t$ is a product of finitely many elements (with possible repetitions) from $\{\alpha_1, \ldots, \alpha_k\}$. Define $g(n) := \frac{h(n)}{\lambda^{n+1}}$. Then $g(n)$ is a poly-geometrical expression in $n$ w.r.t. $\{\beta_t\}_{t \in \texttt{terms}(h)}, \frac{1}{\lambda}$. Clearly we have

$$g(n) = \sum_{t \in \texttt{terms}(h(n))} \frac{c_t}{\lambda}\, n^{q_t}\, (\frac{\beta_t}{\lambda})^n.$$

Therefore, we have

$$\sum_{j=0}^{n-1} \frac{h(j)}{\lambda^{j+1}} = \sum_{t \in \texttt{terms}(h)} \sum_{j=0}^{n-1} \frac{c_t}{\lambda}\, j^{q_t}\, (\frac{\beta_t}{\lambda})^j. \tag{3}$$

According to Lemma 4, for each $t \in \texttt{terms}(h)$, we can find a poly-geometrical expression

$$s_t := (\frac{\beta_t}{\lambda})^n\, f_t(n) + a_t$$

in $n$ over $\overline{\mathbb{Q}}$ w.r.t. $\frac{\beta_t}{\lambda}$ satisfying

1. $s_t = \sum_{j=0}^{n-1} \frac{c_t}{\lambda}\, j^{q_t}\, (\frac{\beta_t}{\lambda})^j$;
2. $f_t$ is a polynomial in $n$ over $\overline{\mathbb{Q}}$ of degree $q_t$ ( if $\beta_t \neq \lambda$) or $q_t + 1$ (if $\beta_t = \lambda$), and $a_t$ is a constant in $\overline{\mathbb{Q}}$; note in the later case, $c_t\, n^{q_t}\, (\frac{\beta_t}{\lambda})^n$ is a summand of the constant term of the canonical form of $(\frac{1}{\lambda})^n\, h(n)$ is 0 when viewed as a polynomial of the $n$-exponential variables.

Therefore, using $s_t$, for $t \in \mathtt{terms}(h)$, we can simplify the right hand side of Equation (2) to

$$\left( x(0) + \sum_{t \in \mathtt{terms}(h)} a_t \right) \lambda^n + \sum_{t \in \mathtt{terms}(h)} f_t(n)\, \beta_t^n. \tag{4}$$

Assume that, for each $t \in \mathtt{terms}(h)$, we have $\beta_t = \alpha_1^{e_{t,1}}\, \alpha_1^{e_{t,2}} \cdots \alpha_1^{e_{t,k}}$. Define

$$\beta_t(n) := (\alpha_1^n)^{e_{t,1}}\, (\alpha_1^n)^{e_{t,2}} \cdots (\alpha_1^n)^{e_{t,k}},$$

$$c := x(0) + \sum_{t \in \mathtt{terms}(h)} a_t \quad \text{and} \quad s(n) := \sum_{t \in \mathtt{terms}(h)} f_t(n)\, \beta_t(n).$$

We easily deduce $\deg(s(n), \alpha_i^n) = \max_{t \in \mathtt{terms}(h)}(\deg(\beta_t(n), \alpha_i^n) \leq \deg(h(n), \alpha_i^n)$. Finally, one can easily verify that $c$ and $s(n)$ satisfy the requirements of the conclusion. □

**Remark 2** *In Lemma 7, if $\lambda$ is weakly multiplicatively independent w.r.t. $\alpha_1, \ldots, \alpha_k$, then we know that the exponential-free part of the canonical form of $(\frac{1}{\lambda})^n\, h(n)$ is 0, without computing the canonical form explicitly.*

### 2.2 Degree of a polynomial ideal

In this subsection, we review some notions and results on the degree of a polynomial ideal. Up to our knowledge, Proposition 1 is a new result which provides a degree estimate for an ideal of a special shape and which can be applied to estimate the degree of invariant ideals of $P$-solvable recurrences. Throughout this section, $\mathbb{K}$ is an algebraically closed field. Let $F$ be a set of polynomials of $\mathbb{K}[x_1, x_2, \ldots, x_s]$. We denote by $V_{\mathbb{K}^s}(F)$ (or simply by $V(F)$ when no confusion is possible) the zero set of the ideal generated by $F \subset \mathbb{K}[x_1, x_2, \ldots, x_s]$ in $\mathbb{K}^s$.

**Definition 7** *Let $V \subset \mathbb{K}^s$ be an $r$-dimensional equidimensional algebraic variety. The number of points of intersection of $V$ with an $(s-r)$-dimensional generic linear subspace $L \subset \mathbb{K}^s$ is called the* degree *of $V$ [1], denoted by* $\deg(V)$. *The degree of a non-equidimensional variety is defined to be the sum of the degrees of its equidimensional components. The degree of an ideal $I \subseteq \mathbb{K}[x_1, x_2, \ldots, x_s]$ is defined to be the degree of the variety of $I$ in $\mathbb{K}^s$.*

We first recall a few well-known results. Note that, for a zero-dimensional algebraic variety, the degree is just the number of points in that variety.

**Lemma 8** *Let $V \subset \mathbb{K}^s$ be an $r$-dimensional equidimensional algebraic variety of degree $\delta$. Let $L$ be an $(s-r)$-dimensional linear subspace. Then, the intersection of $L$ and $V$ is either of positive dimension or consists of no more than $\delta$ points.*

**Lemma 9** *Let $V \subset \mathbb{K}^s$ be an algebraic variety. Let $L$ be a linear map from $\mathbb{K}^s$ to $\mathbb{K}^k$, for some integer $k > 0$. Then, we have* $\deg(L(V)) \leq \deg(V)$.

**Lemma 10 ([5])** *Let $I \subset \mathbb{Q}[x_1, x_2, \ldots, x_s]$ be a radical ideal of degree $\delta$. Then there exist finitely many polynomials in $\mathbb{Q}[x_1, x_2, \ldots, x_s]$ generating $I$ and such that each of these polynomials has total degree less than or equal to $\delta$.*

The following Lemma is a generalized form of Bézout's Theorem.

**Lemma 11** *Let $V, W, V_1, V_2, \ldots V_e$ be algebraic varieties in $\mathbb{K}^s$ such that we have $V = W \cap \cap_{i=1}^{e} V_i$ Define $r := \dim(W)$. Then, we have*

$$\deg(V) \leq \deg(W) \max(\{\deg(V_i) \mid i = 1 \cdots e\})^r.$$

**Proposition 1** *Let $X = x_1, x_2, \ldots, x_s$ and $Y = y_1, y_2, \ldots, y_t$ be pairwise different $s + t$ variables. Let $M$ be an ideal in $\mathbb{Q}[Y]$ of degree $d_M$ and dimension $r$. Let $f_1, f_2, \ldots, f_s$ be $s$ polynomials in $\mathbb{Q}[Y]$, each with maximum total degree $d_f$. Denote by $I$ the ideal $\langle x_1 - f_1, x_2 - f_2, \ldots, x_s - f_s \rangle$. Then the ideal $J := I + M$ has degree upper bounded by $d_M \, {d_f}^r$.*

PROOF**:** We assume first that $M$ is equidimensional. Let $L := l_1, l_2, \ldots, l_r$ be $r$ linear forms in $X, Y$ such that the intersection of the corresponding $r$ hyperplanes and $V(J)$ consists of finitely many points, i.e. $H_L := J + \langle L \rangle$ is zero-dimensional. By virtue of Lemma 8, the degree of $J$ equals the maximum degree of $H_L$ among all possible choices of linear forms $l_1, l_2, \ldots, l_r$ satisfying the above conditions.

Let $L^* := l_1^*, l_2^*, \ldots, l_r^*$, where each $l_j^*$ $(j = 1 \cdots r)$ is the polynomial obtained by substituting $x_i$ with $f_i$, for $i = 1 \cdots s$, in the polynomial $l_j$. Consider the ideal $L^* + M$ in $\mathbb{Q}[Y]$. It is easy to show that the canonical projection map $\Pi_Y$ onto the space of $Y$ coordinates is a one-one-map between $V_{\mathbb{C}^t}(M + L^*)$ and $\Pi_Y(V_{\mathbb{C}^{t+s}}(H_L))$. Therefore, $V_{\mathbb{C}^t}(M + L^*)$ is zero-dimensional and $\deg(M + L^*) = \deg(H_L)$. Hence, viewing $V_{\mathbb{C}^t}(M + L^*)$ as

$$V_{\mathbb{C}^t}(M) \bigcap_{j=1}^{r} V_{\mathbb{C}^t}(l_j^*)$$

and thanks to Lemma 11, we have $\deg(V_{\mathbb{C}^t}(M + L^*)) \leq d_M \, d_f^r$. Therefore, we deduce that $\deg(J) = \max_L \deg(M + L^*) \leq d_M \, d_f^r$ holds, by Lemma 8.

Assume now that $V_{\mathbb{C}^t}(M)$ is not necessarily equidimensional. Let $V_1, V_2, \ldots, V_k$ be an irredundant equidimensional decomposition of $V_{\mathbb{C}^t}(M)$, with corresponding radical ideals $P_1, P_2, \ldots, P_k$. Then, applying the result proved in the first part of the proof to each $I + P_i$ $(i = 1 \cdots k)$, we deduce

$$\begin{aligned} \deg(J) &= \textstyle\sum_{i=1}^{k} \deg(I + P_i) \\ &\leq \textstyle\sum_{i=1}^{k} \deg(P_i) \, d_f^{r_i} \\ &\leq \textstyle\sum_{i=1}^{k} \deg(P_i) \, d_f^{r} \\ &= d_M \, d_f^r, \end{aligned}$$

where $r_i$ is the dimension of $P_i$ in $\mathbb{Q}[Y]$. This completes the proof. □

**Remark 3** *For $J$ in Proposition 1, a less tight degree bound, namely*

$$d_M\, d_f^{r+s},$$

*can easily be deduced from a generalized form of Bezout's bound, since $V_{\mathbb{C}^{t+s}}(M)$ has degree $d_M$ and is of dimension $r+s$ in $\mathbb{C}^{t+s}$.*

**Example 5** *Consider $M := \langle n^2 - m^3 \rangle$, $g_1 := x - n^2 - n - m$, $g_2 := y - n^3 - 3n + 1$, and the ideal $J := M + \langle g_1, g_2 \rangle$. The ideal $M$ has degree 3, and is of dimension 1 in $\mathbb{Q}[n, m]$. The degree of $J$ is 9, which can be obtained by computing the dimension of*

$$\mathbb{Q}(a, b, c, d, e)[x, y, m, n]/(J + \langle a\, x + b\, y + c\, n + d\, m + e \rangle),$$

*where $a, b, c, d, e$ are indeterminates. The degree bound estimated by Proposition 1 is $3 \times 3$, which agrees with the actual degree.*

## 3 Linearization of *P*-solvable recurrences

In this section, we show that every $P$-solvable recurrence can be "linearized", that is, given an $s$-variable $P$-solvable recurrence $R$, there exists an affine recurrence $L$, such that the first $s$ components of the solution to $L$ solves $R$. In other words, although non-linear terms are allowed in $P$-solvable recurrences, these recurrences are essentially linear ones.

We will first show that, every poly-geometrical expression is a component of the solution of some affine recurrence.

**Lemma 12** *Given a positive integer $k$, there exists a $k$-variable affine recurrence $A$ with rational coefficients such that $(n, n^2, \ldots, n^{k-1}, n^k)$ is the solution to $A$.*

Proof**:** We proceed by induction on $k$. The case $k = 1$ is easy: $n$ solves the recurrence $x(n) = x(n-1) + 1$. Now assume that there exists a $(k-1)$-variable affine recurrence $B$ of variables $x_1, x_2, \ldots, x_{k-1}$ with rational coefficients, whose solution is $(n, n^2, \ldots, n^{k-1})$. Let $x_k(n) = n^k$ and consider $x_k(n) - x_k(n-1)$, which is a polynomial in $n$ of degree $k-1$. Therefore, $x_k(n) - x_k(n-1)$ can be written as a linear form with basis $1, n-1, (n-1)^2, \ldots, (n-1)^{k-1}$ (say by Taylor expansion) with coefficients $c_0, c_1, \ldots, c_{k-1}$. We deduce that:

$$x_k(n) = c_0 + x_k(n-1) + \sum_{i=1}^{k-1} c_i\, x_i(n-1) \tag{5}$$

Let $A$ be the affine recurrence of recurrence variables $x_1, x_2, \ldots, x_k$ defined by the recurrence equations from $B$ and Equation (5). Clearly $(n, n^2, \ldots, n^k)$ is the solution to the $k$-variable affine recurrence $A$, which coefficients are all rational. □

Similarly, for hyper-geometrical terms in $n$, we have the following result.

**Lemma 13** *Given a non-negative integer $k$ and an algebraic number $\lambda$ ($\lambda \neq 1$), there exists an $(k+1)$-variable affine recurrence $A$ such that $(\lambda^n, n\,\lambda^n, \ldots, n^k\,\lambda^n)$ is the solution of $A$.*

PROOF**:** We proceed by induction on $k$ as well. The case of $k = 0$ is trivial: the recurrence $x(n) = \lambda\, x(n-1)$ has the properties specified in the conclusion. Now assume there exists a $k$-variable affine recurrence $B$ with recurrence variables $x_0, x_1, \ldots, x_{k-1}$, whose solution is $(\lambda^n, n\,\lambda^n, n^2, \ldots, n^{k-1}\,\lambda^n)$. Consider $x_k(n) = n^k\lambda^n$, which can be rewritten as $(n^k\lambda)\,\lambda^{n-1}$. Now consider $n^k\,\lambda$, which can be rewritten as a linear combination $c_0 + c_1\,(n-1) + \cdots + c_k(n-1)^k$ where $c_0, c_1, \ldots, c_k$ are constants. Therefore, we have:

$$x_k(n) = \sum_{i=0}^{k} c_i\, x_i(n-1) \tag{6}$$

Let $A$ be the affine recurrence with recurrence variables $x_0, x_1, \ldots, x_k$ defined by the recurrence equations from $B$ and Equation (6). Clearly $(\lambda^n, n\,\lambda^n, \ldots, n^k\,\lambda^n)$ is the solution to the $(k+1)$-variable affine recurrence $A$. □

Next, as a consequence, we shall show that every poly-geometrical expression is a component of the solution of some affine recurrence.

**Proposition 2** *Given a poly-geometrical expression $h$ in $n$, there exists an affine recurrence $A$ such that $h$ equals the first component of the solution to $A$.*

PROOF**:** Assume w.l.o.g. that $h$ is in canonical form and has $m$ terms, say $h = \sum_{i=1}^{m} c_i\, t_i(n)$. We know that each term $t_i(n)$ of $h$ is either of the form $n^k$ or the form $n^k\,\lambda^n$. According to Lemma 12 and Lemma 13, we can substitute each term $t_i(n)$ by a recurrence variable $x_i$ from some affine recurrence, say $A_i$. We can assume w.l.o.g the variables in those recurrences are all pairwise different.

Then, we can form a new affine recurrence $A$ by putting together $x_0(n) = \sum_{t=0}^{m} c_i\, x_i(n)$ and the equations in $A_j$, for $j = 1 \cdots m$, yielding a system where $h$ will be the first component of the solution to $A$. □

Since the solutions to $P$-solvable recurrences consist of poly-geometrical expressions, Proposition 2 implies that there exists a 'linearization" procedure for $P$-solvable recurrences. Next, we show that we can "linearize" $P$-solvable recurrences without knowing their solutions. More precisely, Theorem 1 states that if one has a $P$-solvable recurrence $R$ with rational coefficients, we can always find an affine recurrence $A$ with rational coefficients such that each component of a solution of $R$ is a component of a solution of $A$. One of the key point is the construction made in Lemma 14.

**Lemma 14** *Given any two recurrence variables $x_1$ and $x_2$ from an affine recurrence $A$ with rational coefficients, there exists an affine recurrence $A^*$ with rational coefficients such that $x_1(n)\,x_2(n)$ is a component of the solution to $A^*$.*

PROOF: Let $x_1, x_2, \ldots, x_s$ be all the recurrence variables in $A$. For each pair $(i, j)$, with $1 \leq i \leq j \leq s$, we define a new recurrence variable $y_{i,j} = x_i x_j$. It is easy to check that $y_{i,j}(n)$ can be represented as a linear combination of $y_{k,\ell}(n-1)$ with rational coefficients, for $1 \leq k, \ell \leq s$. Indeed, each $x_i(n)$, $i = 1 \cdots s$, is a linear combination of $x_j(n-1)$, for $j = 1 \cdots s$. □

**Theorem 1** *Given a P-solvable recurrence $R$ with rational coefficients, we can find an affine recurrence $A^*$ with rational coefficients, without solving the recurrence $R$, such that each component of the solution of $R$ is a component of the solution of $A^*$.*

PROOF: Assume $R$ has $k$ blocks. If $k = 1$, then $R$ is an affine recurrence and nothing needs to be done for this case.

From now on, we assume $k > 1$. As we shall see, however, treating the case of two blocks is sufficient to raise the key argument in the construction. Thus, for clarity, we assume that the coefficient matrix $M$ of $R$ is 2-block diagonal.

Let $x_{i_1}(n-1)x_{i_2}(n-1)\cdots x_{i_j}(n-1)$ be a non-linear term occuring in the second block. Note that $x_{i_1}, x_{i_2}, \ldots, x_{i_j}$ are actually variables of the affine recurrence induced by the first block. According in Lemma 14, there exists an affine recurrence $A$ with rational coefficients, such that $x_{i_1}\, x_{i_2}$ is solution to some variable $y$ of $A$. Substitute in $R$ each occurrence of $x_{i_1}(n-1)x_{i_2}(n-1)$ by $y(n-1)$ we obtain recurrence equations $A_y$. Let $A^1$ be the recurrence defined by the equations in $A_y$ and $R$. Note that

(1) $A^1$ is a $P$-solvable recurrence with rational coefficients and allows a 2 block coefficient matrix;
(2) each component of the solution of $R$ is a component of the solution of $A^1$.

If $A^1$ still has non-linear terms, we apply again the above trick to $A^1$, yielding a recurrence $A^2$. It is easy to check, that this "linearization" process will be completed in a finite number of steps. Finally, we obtain an affine recurrence $A^*$ with rational coefficients, such that each component of the solution of $R$ is a component of the solution of $A^*$. □

Actually, the proof of Theorem 1 implies an algorithm for "linearizing" any $P$-solvable recurrence. However, the resulting affine recurrence by this an algorithm will have exponentially many (roughly $\binom{n+d+1}{d}$ variables, which is hardly of practical use. An interesting problem would be to find an "optimal linearization", with a minimum number of recurrence variables.

## 4 Invariant ideal of *P*-solvable recurrences

We will first formalize the notion of a $P$-solvable recurrence. Then in the rest of this section, we will investigate the shape of the closed form solutions of a $P$-solvable recurrence equation, for studying the degree and the dimension of

invariant ideal. We will provide degree estimates for the invariant ideal, which is useful for all invariant generation methods which need a degree bound, like the proposed polynomial interpolation based method and those in [9, 10, 2]. Last but not least, we will investigate the dimension of the invariant ideal. So that we can get a sufficient for non-trivial polynomial invariants of a given $P$-solvable recurrence to exist. Note that in our invariant generation method, we do not need (thus never compute) the closed form solutions explicitly.

It is known that the solutions to $P$-solvable recurrences are poly-geometrical expressions in $n$ w.r.t. the eigenvalues of the matrix $M$, see for example [13]. However, we need to estimate the "shape", e.g. the degree of those poly-geometrical expression solutions, with the final goal of estimating the "shape" (e.g. degree, height, dimension) of the invariant ideal. In this paper, we focus on degree and dimension estimates.

We first generalize the result of Lemma 7 to the multi-variable case.

**Proposition 3** *Let $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}}^* \setminus \{1\}$. Let $\lambda \in \overline{\mathbb{Q}}$ and $M \in \overline{\mathbb{Q}}^{s\times s}$ be a matrix in the following Jordan form*

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & 0 & 0 & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}.$$

*Consider an $s$-variable recurrence $R$ defined as follows:*

$$X(n+1)_{s\times 1} = M_{s\times s}\, X(n)_{s\times 1} + F(n)_{s\times 1}, \text{ where}$$

(a) *$X := x_1, x_2, \ldots, x_s$ are the recurrence variables;*
(b) *$F := (f_1, f_2, \ldots, f_s)$ is a list of poly-geometrical expression in $n$ w.r.t. $\alpha_1, \ldots, \alpha_m$, with maximal total degree $d$.*

*Then we have:*

1. *if $\lambda = 0$, then $(f_1, f_1 + f_2, \ldots, f_1 + f_2 + \cdots + f_s)$ solves $R$.*
2. *if $\lambda = 1$, then there exist $s$ poly-geometric expressions $(g_1, g_2, \ldots, g_s)$ in $\alpha_1, \ldots, \alpha_m$ such that for each $i \in 1 \cdots s$, $g_i$ is a poly-geometrical expression in $n$ w.r.t. $\alpha_1, \ldots, \alpha_m$ with total degree less or equal than $d + i$.*
3. *if $\lambda \notin \{0, 1\}$, then there exists a solution of $R$, say $(y_1, y_2, \ldots, y_s)$, such that for each $i = 1, \ldots, s$ we have*

$$y_i := c_i \lambda_i^n + g_i, \text{ where} \tag{7}$$

*for each $i \in 1 \cdots s$: (a) $c_i$ is a constant depending only on the initial value of the recurrence; and (b) $g_i$ is like in the case of $\lambda = 1$. Moreover, assume furthermore that the following conditions hold:*

(*i*) $\lambda$ *is weakly multiplicatively independent w.r.t.* $\alpha_1, \ldots, \alpha_m$*;*
(*ii*) $\deg(f_j, n) = 0$ *holds for all* $j \in \{1, 2, \ldots, s\}$.
*Then, for all* $i = 1, \ldots, s$*, we can further choose* $g_i$ *such that* $\deg(g_i, n) = 0$ *holds and the total degree of* $g_i$ *is less or equal than* $\max(d, 1)$.

PROOF**:** We observe that the recurrence variables of $R$ can be solved one after the other, from $x_1$ to $x_s$. When $\lambda = 0$, the conclusion is easy to verify. The case $\lambda \neq 0$ is easy to prove by induction on $s$ with Lemma 7. □

**Proposition 4** *Let* $\lambda_1, \ldots, \lambda_s, \alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}}^* \setminus \{1\}$*. Let* $M \in \overline{\mathbb{Q}}^{s \times s}$ *be a matrix in the following Jordan form*

$$\begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 \\ \epsilon_{2,1} & \lambda_2 & 0 & \cdots & 0 & 0 \\ 0 & \epsilon_{3,2} & \lambda_3 & 0 & 0 & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & \lambda_{s-1} & 0 \\ 0 & 0 & 0 & \cdots & \epsilon_{s,s-1} & \lambda_s \end{pmatrix},$$

*where for* $i = 2, \ldots, s$*,* $\epsilon_{i,i-1}$ *is either* 0 *or* 1*. Consider an* $s$*-variable recurrence* $R$ *defined as follows:*

$$X(n+1)_{s\times 1} = M_{s\times s}\, X(n)_{s\times 1} + F(n)_{s\times 1},$$

*where*

1. $X := x_1, x_2, \ldots, x_s$ *are the recurrence variables;*
2. $F := (f_1, f_2, \ldots, f_s)$ *is a list of poly-geometrical expression in* $n$ *w.r.t.* $\alpha_1, \ldots, \alpha_m$*, with maximal total degree* $d$*.*

*Then there exists a solution of* $R$*, say* $(y_1, y_2, \ldots, y_s)$*, such that for each* $i = 1, \ldots, s$ *we have*

$$y_i := c_i \lambda_i^n + g_i, \tag{8}$$

*where*

(*a*) $c_i$ *is a constant depending only on the initial value of the recurrence and*
(*b*) $g_i$ *is a poly-geometrical expression in* $n$ *w.r.t.* $\lambda_1, \ldots, \lambda_{i-1}$, $\alpha_1, \ldots, \alpha_m$*, with total degree less or equal than* $d + i$*.*

*Assume furthermore that the following conditions hold:*

(*i*) *the sequence consisting of* $\lambda_1, \lambda_2, \ldots, \lambda_s$ *is weakly multiplicatively independent;*
(*ii*) $\deg(f_j, n) = 0$ *holds for all* $j \in \{1, 2, \ldots, s\}$.

*Then, for all* $i = 1, \ldots, s$*, we can further choose* $y_i$ *such that* $\deg(g_i, n) = 0$ *holds and the total degree of* $g_i$ *is less or equal than* $\max(d, 1)$.

PROOF: We observe that the recurrence variables of $R$ can be solved one after the other, from $x_1$ to $x_s$. We proceed by induction on $s$. The case $s = 1$ follows directly from Lemma 7. Assume from now on that $s > 1$ holds and that we have found solutions $(y_1, y_2, \ldots, y_{s-1})$ for the first $s-1$ variables satisfying the requirements, that is, Relation (8) with $(a)$ and $(b)$. We define

$$\tilde{f}(n) = f_s(n) - \epsilon_{s,s-1}\, y_{s-1}(n+1). \tag{9}$$

Note that $\tilde{f}(n)$ is a poly-geometrical expression in $n$ w.r.t. $\lambda_1, \ldots, \lambda_{s-1}, \alpha_1, \ldots, \alpha_m$ with total degree less than or equal to $d+s-1$. Moreover, for $v \in \{n, \lambda_1^n, \ldots, \lambda_{s-1}^n, \alpha_1^n, \ldots, \alpha_m^n\}$ we have

$$\deg(\tilde{f}(n), v) \leq \max\left(\deg(f_s(n), v), \deg(y_{s-1}(n), v)\right). \tag{10}$$

It remains to solve $x_s$ from

$$x_s(n+1) = \lambda_s\, x_s(n) + \tilde{f}(n) \tag{11}$$

in order to solve all the variables $x_1, \ldots, x_s$. Again, by Lemma 7, there exists a poly-geometrical expression

$$y_s := c_s\, \lambda_s^n + g_s(n),$$

where $g_s(n)$ is poly-geometrical expression in $n$ w.r.t. $\lambda_1, \ldots, \lambda_{s-1}, \alpha_1, \ldots, \alpha_m$, of total degree upper bounded by $d+s$. This completes the proof of the properties $(a)$ and $(b)$ for $y_s$.

Now we assume that $(i)$, $(ii)$ hold and we prove the second half of the conclusion. Observe that we have $\deg(g_s(n), n) = \deg(\tilde{f}(n), n)$, which is 0, according to Relation (10) and the fact that we can choose $y_{s-1}$ such that $\deg(y_{s-1}(n), n) = 0$ holds. Next, we observe that for each

$$v \in \{n, \lambda_1^n, \ldots, \lambda_{s-1}^n, \alpha_1^n, \ldots, \alpha_m^n\},$$

we have $\deg(g_s(n), v) = \deg(\tilde{f}(n), v)$, which is less or equal to $\deg(y_{s-1}(n), v)$ by Relation (10). Therefore, the total degree of $g_s$ is less or equal than the total degree of $y_{s-1}$, which is less or equal than $\max(d, 1)$ by our induction hypothesis. This completes the proof. □

**Theorem 2** *Let $R$ be a P-solvable recurrence relation. Using the same notations $M, k, s, F, n_1, n_2, \ldots, n_k$ as in Definition 1. Assume $M$ is in a Jordan form. Assume the eigenvalues $\lambda_1, \ldots, \lambda_s$ of $M$ (counted with multiplicities) are different from $0, 1$, with $\lambda_i$ being the $i$-th diagonal element of $M$. Assume for each block $j$ the total degree of any polynomial in $\mathbf{f}_j$ (for $i = 2 \cdots k$) is upper bounded by $d_j$. For each $i$, we denote by $b(i)$ the block number of the index $i$, that is,*

$$\sum_{j=1}^{b(i)-1} n_j < i \leq \sum_{j=1}^{b(i)} n_j. \tag{12}$$

*Let $D_1 := n_1$ and for all $j \in \{2, \ldots, k\}$ let $D_j := d_j\, D_{j-1} + n_j$. Then, there exists a solution $(y_1, y_2, \ldots, y_s)$ for $R$ of the following form:*

$$y_i := c_i \lambda_i^n + g_i, \tag{13}$$

*for all $i \in 1 \cdots s$, where*

(a) *$c_i$ is a constant depending only on the initial value of the recurrence;*
(b) *$g_i$ is a poly-geometrical expression in $n$ w.r.t. $\lambda_1, \ldots, \lambda_{i-1}$, and with total degree less or equal than $D_{b(i)}$.*

*Moreover, if the sequence consisting $\{\lambda_1, \ldots, \lambda_s\}$ is weakly multiplicatively independent, then, for all $i = 1, \ldots, k$, we can further choose $y_i$ such that $\deg(g_i, n) = 0$ holds and the total degree of $g_i$ is less or equal than $\prod_{2 \le t \le b(i)} \max(d_t, 1)$.*

PROOF**:** We proceed by induction on the number of blocks, that is, $k$. The case $k = 1$ follows immediately from Proposition 4. Assume from now on that the conclusion holds for a value $k = \ell$, with $\ell \ge 1$ and let us prove that it also holds for $k = \ell + 1$. We apply the induction hypothesis to solve the first $\ell$ blocks of variables, and suppose that $\mathbf{y}_\ell$ is a solution satisfying the properties in the conclusion. For solving the variables in the $(\ell+1)$-th block, we substitute $\mathbf{y}_\ell$ to $f_{\ell+1}$ and obtain a tuple of poly-geometrical expressions in $n$ w.r.t the eigenvalues of the first $\ell$ blocks and with total degree bounded by $d_\ell\, D_\ell$. Therefore, applying again Proposition 4, we can find solutions for the variables in the $(\ell+1)$-th block satisfying the properties required in the conclusion. This completes the proof. □

Note that the degree estimate in Theorem 2 depends on how the block structure of the recurrence is exploited, for example, a $2 \times 2$ diagonal matrix can be viewed as a matrix with a single block or a matrix with two $1 \times 1$ diagonal blocks.

In practice, one might want to decouple the recurrence first, and then study the recurrence variable one by one (after a linear coordinate change) to get better degree estimates for the poly-geometrical expression solutions, regarded as polynomials of $n$-exponential terms as the eigenvalues of the coefficient matrix. We will just use a simple example to illustrate this idea.

**Example 6** *Consider the recurrence:*

$$\begin{pmatrix} x(n+1) \\ y(n+1) \\ z(n+1) \end{pmatrix} := \begin{pmatrix} 2\,0\,0 \\ 0\,3\,0 \\ 0\,0\,3 \end{pmatrix} \times \begin{pmatrix} x(n) \\ y(n) \\ z(n) \end{pmatrix} + \begin{pmatrix} 0 \\ x(n)^2 \\ x(n)^3 \end{pmatrix}$$

*Viewing the recurrence as two blocks corresponding to variables $(x)$ and $(y, z)$ respectively, the degree estimate according to Theorem 2 would be bounded by $5 = 3 \times 1 + 2$.*

*If we decouple the $(y, z)$ block to the following two recurrences*

$$y(n+1) = 3\, y(n) + x(n)^2 \text{ and } z(n+1) = 3\, z(n) + x(n)^3,$$

*then we can easily deduce that the degree of the poly-geometrical expression for $y$ and $z$ are upper bounded by 2 and 3 respectively, again according to Theorem 2.*

It is easy to generalize the previous results to the case of a matrix $M$ which is not in Jordan form. Let $Q$ be a non-singular matrix such that $J := Q\,M\,Q^{-1}$ is a Jordan form of $M$. Let the original recurrence $R$ be

$$X(n+1) = M\,X(n) + F.$$

Consider the following recurrence $R_Q$

$$Y(n+1) = J\,Y(n) + QF.$$

It is easy to check that if

$$(y_1(n), y_2(n), \ldots, y_s(n))$$

solves $R_Q$, then

$$Q^{-1}\ (y_1(n), y_2(n), \ldots, y_s(n))$$

solves $R$. Note that an invertible matrix over $\overline{\mathbb{Q}}$ maps a tuple of poly-geometrical expressions to another tuple of poly-geometrical expressions; moreover it preserves the highest degree among the expressions in the tuple.

We turn now our attention to the question of estimating the degree of the invariant ideal of a $P$-solvable recurrence relation.

**Proposition 5** *Let $R$ be an $s$-variable $P$-solvable recurrence relation, with recurrence variables $(x_1, x_2, \ldots, x_s)$. Let $\mathcal{I} \subset \mathbb{Q}[x_1, x_2, \ldots, x_s]$ be the invariant ideal of $R$. Denote by $\mathcal{I}^e$ the extension of $\mathcal{I}$ in $\overline{\mathbb{Q}}[x_1, x_2, \ldots, x_s]$. Let $A = \alpha_1, \alpha_2, \ldots, \alpha_s$ be the eigenvalues (counted with multiplicities) of the coefficient matrix of $R$. Let $\mathcal{M}$ be the multiplicative relation ideal of $A$ associated with variables $y_1, \ldots, y_s$. Then, there exists a sequence of $s$ poly-geometrical expressions in $n$ w.r.t. $\alpha_1, \alpha_2, \ldots, \alpha_s$, say*

$$f_1(n, \alpha_1^n, \ldots, \alpha_k^n), \ldots, f_s(n, \alpha_1^n, \ldots, \alpha_k^n),$$

*which solves $R$. Moreover, we have*

$$\mathcal{I}^e \;=\; (\mathcal{S} + \mathcal{M}) \;\cap\; \overline{\mathbb{Q}}[x_1, x_2, \ldots, x_s],$$

*where $\mathcal{S}$ is the ideal generated by $\langle x_1 - f_1(n, y_1, \ldots, y_s), \ldots, x_s - f_s(n, y_1, \ldots, y_s)$ in $\overline{\mathbb{Q}}[x_1, x_2, \ldots, x_s, n, y_1, \ldots, y_s]$.*

PROOF: The existence of $f_1, f_2, \ldots, f_s$ follows by Theorem 2 and the fact that linear combination of poly-geometrical expressions w.r.t. $n$ are still poly-geometrical expressions. The conclusion follows from Lemma 5. □

The following lemma is not hard to prove and one can find a proof in [6].

**Lemma 15** *Let $R$ be a $P$-solvable recurrence relation defining $s$ sequences in $\mathbb{Q}^s$, with recurrence variables $(x_1, x_2, \ldots, x_s)$. Let $\mathcal{I}$ be the invariant ideal of $R$ in $\mathbb{Q}[x_1, x_2, \ldots, x_s]$; let $\overline{\mathcal{I}}$ be the invariant ideal of $R$ in $\overline{\mathbb{Q}}[x_1, x_2, \ldots, x_s]$. Then $\overline{\mathcal{I}}$ equals to $\mathcal{I}^e$, the extension of $\mathcal{I}$ in $\overline{\mathbb{Q}}[x_1, x_2, \ldots, x_s]$.*

With Proposition 5 and Proposition 1, we are able to estimate the degree of polynomials in a generating system of the invariant ideals. Now we are able to estimate the total degree of closed form solutions of a $P$-solvable recurrence without solving the recurrence explicitly.

**Theorem 3** *Let $R$ be a $P$-solvable recurrence relation defining $s$ sequences in $\mathbb{Q}^s$, with recurrence variables $(x_1, x_2, \ldots, x_s)$. Let $\mathcal{I} \subset \mathbb{Q}[x_1, x_2, \ldots, x_s]$ be the invariant ideal of $R$. Let $A = \alpha_1, \alpha_2, \ldots, \alpha_s$ be the eigenvalues (counted with multiplicities) of the coefficient matrix of $R$. Let $\mathcal{M}$ be the multiplicative relation ideal of $A$ associated with variables $y_1, \ldots, y_k$. Let $r$ be the dimension of $\mathcal{M}$. Let $f_1(n, \alpha_1^n, \ldots, \alpha_k^n), \ldots, f_s(n, \alpha_1^n, \ldots, \alpha_k^n)$ be a sequence of $s$ poly-geometrical expressions in $n$ w.r.t. $\alpha_1, \alpha_2, \ldots, \alpha_s$ that solves $R$. Suppose $R$ has a $k$ block configuration as $(n_1, 1), (n_2, d_2), \ldots, (n_k, d_k)$. Let $D_1 := n_1$; and for all $j \in \{2, \ldots, k\}$, let $D_j := d_j\, D_{j-1} + n_j$. Then we have*

$$\deg(\mathcal{I}) \leq \deg(\mathcal{M})\, D_k^{r+1}.$$

*Moreover, if the degrees of $n$ in $f_i$ $(i = 1 \cdots s)$ are $0$, then we have*

$$\deg(\mathcal{I}) \leq \deg(\mathcal{M})\, D_k^{r}.$$

PROOF**:** Denoting by $\Pi$ the standard projection from $\overline{\mathbb{Q}}^{s+1+s}$ to $\overline{\mathbb{Q}}^s$:

$$(x_1, x_2, \ldots, x_s, n, y_1, \ldots, y_s) \mapsto (x_1, x_2, \ldots, x_s),$$

we deduce by Proposition 5 that

$$V(\mathcal{I}) = \overline{\Pi(V(\mathcal{S} + \mathcal{M}))}, \tag{14}$$

where $\mathcal{S}$ is the ideal generated by $\langle x_1 - f_1(n, y_1, \ldots, y_s), \ldots, x_s - f_s(n, y_1, \ldots, y_s)$ in $\overline{\mathbb{Q}}[x_1, x_2, \ldots, x_s, n, y_1, \ldots, y_s]$. Thus, by Lemma 9, we have

$$\deg(\mathcal{I}) \leq \deg(\mathcal{S} + \mathcal{M}).$$

It follows from Proposition 1 that

$$\deg(\mathcal{S} + \mathcal{M}) \leq \deg(\mathcal{M})\, D_k^{r+1},$$

since the total degree of $f_i$ of $R$ is bounded by $D_k$ according to Theorem 2 and the dimension of $\mathcal{M}$ is $r + 1$ is in $\mathbb{Q}[n, y_1, \ldots, y_s]$.

With similar arguments, the second part of the conclusion follows from the fact that $S + M$ can be viewed as an ideal in in $\overline{\mathbb{Q}}[x_1, x_2, \ldots, x_s, n, y_1, \ldots, y_s]$, where $M$ has dimension $r$. □

Indeed, the degree bound in Theorem 3 is "sharp" in the sense that it is reached by many of the examples (Example 2) we have considered.

In the rest of this section, we are going to investigate the dimension of the invariant ideal of a $P$-solvable recurrence. This can help checking whether or not the invariant ideal of a $P$-solvable recurrence over $\mathbb{Q}$ is the trivial ideal of $\mathbb{Q}[x_1, \ldots, x_s]$. Note that it is obvious that the invariant ideal is not the whole polynomial ring.

**Theorem 4** *Using the same notations as in Definition 1. Let $\lambda_1, \lambda_2, \ldots, \lambda_s$ be the eigenvalues of $M$ counted with multiplicities. Let $\mathcal{M}$ be the multiplicative relation ideal of $\lambda_1, \lambda_2, \ldots, \lambda_s$. Let $r$ be the dimension of $\mathcal{M}$. Let $\mathcal{I}$ be the invariant ideal of $R$. Then $\mathcal{I}$ is of dimension at most $r+1$. Moreover, for generic initial values,*

1. *the dimension of $\mathcal{I}$ is at least $r$;*
2. *if $0$ is not an eigenvalue of $M$ and the sequence consisting of $\lambda_1, \lambda_2, \ldots, \lambda_s$ is weakly multiplicatively independent, then $\mathcal{I}$ has dimension $r$.*

PROOF**:** Assume without loss of genericity that $M$ is in Jordan form. By Theorem 2, we deduce that $R$ has a solution $(f_1, f_2, \ldots, f_s)$ as follows

$$(c_1\,\lambda_1^n + h_1(n), c_2\,\lambda_2^n + h_2(n), \ldots, c_s\,\lambda_s^n + h_s(n))\,,$$

where for each $i \in 1 \cdots s$, $c_i$ is a constant in $\overline{\mathbb{Q}}$ depending only on the initial value of $R$, and $h_i$ is a poly-geometrical expression in $n$ w.r.t. $\lambda_1, \ldots, \lambda_{i-1}$. Moreover, we have

1. for generic initial values, none of $c_1, c_2, \ldots, c_s$ is 0;
2. if the eigenvalues of $M$ can be ordered in $\lambda_1, \lambda_2, \ldots, \lambda_s$ s.t. $\lambda_1 \neq 1$ and for each $i \in 2 \cdots s$, $\lambda_i$ is weakly multiplicatively independent w.r.t. $\lambda_1, \lambda_2, \ldots, \lambda_{i-1}$, then we can require that, for all $i \in 1 \cdots s$, we have $\deg(f_i, n) = 0$.

Viewing $n$, $\lambda_i^n$ (for $i = 1, \ldots, s$) as indeterminates, let us associate coordinate variable $u_0$ to $n$, $u_i$ to $\lambda_i^n$ (for $i = 1, \ldots, s$). Denote by $V$ the variety of $\mathcal{I}$ in $\overline{\mathbb{Q}}^s$ (with coordinates $x_1, x_2, \ldots, x_s$). Note that we have

$$\dim(V) = \dim(\mathcal{I}).$$

Denote by $W_1, W_2$ respectively the variety of $\mathcal{M}$ in $\overline{\mathbb{Q}}^s$ (with coordinates $u_1, u_2, \ldots, u_s$) and in $\overline{\mathbb{Q}}^{s+1}$ (with coordinates $u_0, u_1, u_2, \ldots, u_s$). Note that we have

$$\dim(W_1) = r \text{ and } \dim(W_2) = r+1.$$

Consider first the map $F_0$ defined below:

$$\begin{gathered} F_0 : \overline{\mathbb{Q}}^{s+1} \mapsto \overline{\mathbb{Q}}^{s+1} \\ (u_0, u_1, \ldots, u_s) \to (c_1\,u_1 + f_1, \ldots, c_s\,u_s + f_s). \end{gathered}$$

By Theorem 3, we have $V = \overline{F_0(W_2)}$. Therefore, we have we have $\dim(\mathcal{I}) = \dim(V) \leq \dim(W_2) = r+1$.

Now assume the initial value of $R$ is generic, thus we have $c_i \neq 0$, for all $i \in 1 \cdots s$. Let us consider the map $F_1$ defined below:

$$\begin{gathered} F_1 : \overline{\mathbb{Q}}^{s+1} \mapsto \overline{\mathbb{Q}}^{s+1} \\ (u_0, u_1, \ldots, u_s) \to (u_0, c_1\,u_1 + f_1, \ldots, c_s\,u_s + f_s). \end{gathered}$$

Let us denote by $V_2$ the variety $\overline{F_1(W_2)}$. By virtue of Theorem 3, we have $\dim(V_2) = \dim(W_2) = r + 1$. Denote by $\Pi$ the standard projection map that forgets the first coordinate, that is, $u_0$. We observe that $V = \overline{\Pi(V_2)}$. Therefore, we have $\dim(V) \geq \dim(\overline{\Pi(V_2)}) - 1 = r$.

Now we further assume $\lambda_1 \neq 1$ and for each $i \in 2 \cdots s$, $\lambda_i$ is weakly multiplicatively independent w.r.t. $\lambda_1, \lambda_2, \ldots, \lambda_{i-1}$ the invariant ideal of $R$. In this case, we have that for all $i \in 1 \cdots s$, $\deg(f_i, n) = 0$. Let us consider the map $F_2$ defined below:

$$F_2 : \overline{\mathbb{Q}}^s \mapsto \overline{\mathbb{Q}}^s$$
$$(u_1, \ldots, u_s) \to (c_1\, u_1 + f_1, c_2\, u_2 + f_2, \ldots, c_s\, u_s + f_s).$$

By Theorem 3, we have $V = \overline{F_2(W_1)}$. Therefore, we have $\dim(\mathcal{I}) = \dim(V) = \dim(W_1) = r$. This completes the proof. □

The following result, which is a direct consequence of Theorem 4, can serve as a sufficient condition for the invariant ideal to be non-trivial. This condition is often satisfied when there are eigenvalues with multiplicities or when 0 and 1 are among the eigenvalues.

**Corollary 1** *Using the same notations as in Theorem 4. If $r + 1 < s$ holds, then $\mathcal{I}$ is not the zero ideal in $\mathbb{Q}[x_1, x_2, \ldots, x_s]$.*

The following corollary indicates that, the fact that the invariant ideal of a given $P$-solvable recurrence is trivial could be determined by just investigating the multiplicative relation among the eigenvalues of the underlying recurrence.

**Corollary 2** *Using the same notations as in Theorem 4, consider an $s$ variable $P$-solvable recurrence $R$ with initial value $x_1(0) := a_1, \ldots, x_s(0) := a_s$, where $a_1, \ldots, a_s$ are indeterminates. If the eigenvalues of $R$ are multiplicatively independent, then the invariant ideal of $R$ is $\langle 0 \rangle$ in $\mathbb{Q}(a_1, \ldots, a_s)[x_1, x_2, \ldots, x_s]$.*

PROOF**:** The assumption implies that the multiplicative relation ideal of the eigenvalues is of dimension $s$. By Theorem 4, the dimension of the invariant ideal of $R$ must be at least $s$, thus the invariant ideal of $R$ must be zero ideal in $\mathbb{Q}(a_1, \ldots, a_s)[x_1, \ldots, x_s]$. □

**Example 7** *Consider the recurrence:*

$$(x(n+1), y(n+1)) := (3\, x(n) + y(n), 2\, y(n)) \text{ with } x(0) = a, y(0) = b.$$

*The two eigenvalues f the coefficient matrix are* 2 *and* 3 *which are multiplicatively independent. Therefore, by Corollary 2, the invariant ideal of the recurrence is trivial.*

Note in Theorem 4, if we drop the "generic" assumption on the initial values, then the conclusion might not hold. The following example illustrate this for the case when all the eigenvalues are different and multiplicatively independent, but the invariant ideal is not trivial.

**Example 8** *Consider the linear recurrence* $x(n+1) = 3\,x(n) - y(n), y(n+1) = 2\,y(n)$ *with* $(x(0), y(0)) = (a, b)$*. The eigenvalues of the coefficient matrix are* $2, 3$*, which are multiplicatively independent. One can check that, when* $a = b$*, the invariant ideal is generated by* $x - y$*. However, generically, that is when* $a \neq b$ *holds, the invariant ideal is the zero ideal.*

## 5 Concluding remarks

In this article, we study the equivalence between $P$-solvable recurrences and linear recurrences, and supply sharp estimate on the degree and dimension of invariant ideals of $P$-solvable recurrences. As future work, we would be interested on finding simple linearizations of $P$-solvable recurrences, which could help obtaining more precise estimates on the degree of the invariant ideal.

## References


1. D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Graduate Text in Mathematics, 185. Springer-Verlag, New-York, 1998.
2. D. Kapur E. Rodriguez-Carbonell. Automatic generation of polynomial invariants of bounded degree using abstract interpretation. *Science of Computer Programming*, 64(1):54–75, 2007.
3. J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.
4. G. Ge. *Algorithms related to multiplicative representations of algebraic numbers*. PhD thesis, U.C. Berkeley, 1993.
5. Joos Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.*, pages 239–277, 1983.
6. Manuel Kauers and Burkhard Zimmermann. Computing the algebraic relations of c-finite sequences and multisequences. *J. Symb. Comput.*, 43:787–803, November 2008.
7. Laura Kovács. Invariant generation for p-solvable loops with assignments. In *Proceedings of the 3rd international conference on Computer science: theory and applications*, CSR'08, pages 349–359, Berlin, Heidelberg, 2008. Springer-Verlag.
8. Marc Moreno Maza and Rong Xiao. Generating program invariants via interpolation. *CoRR*, abs/1201.5086, 2012.
9. Markus Müller-Olm and Helmut Seidl. Computing polynomial program invariants. *Inf. Process. Lett.*, 91(5):233–244, September 2004.
10. Markus Müller-Olm and Helmut Seidl. A Note on Karr's Algorithm. In Josep Díaz, Juhani Karhumäki, Arto Lepistö, and Donald Sannella, editors, *Automata, Languages and Programming*, volume 3142 of *Lecture Notes in Computer Science*, pages 1016–1028, Turku, Finland, July 2004. Springer.
11. Martin J. Osborne. Math tutorial: first-order difference equations, 2000.
12. E. Rodríguez-Carbonell and D. Kapur. An Abstract Interpretation Approach for Automatic Generation of Polynomial Invariants. In *International Symposium on Static Analysis (SAS 2004)*, volume 3148 of *Lecture Notes in Computer Science*, pages 280–295. Springer-Verlag, 2004.
13. E. Rodríguez-Carbonell and D. Kapur. Automatic generation of polynomial loop invariants: Algebraic foundations. ISSAC '04, pages 266–273. ACM, 2004.