FROM POLYNOMIAL INVARIANTS TO LINEAR LOOPS

GEORGE KENISON[1], LAURA KOVÁCS[1], AND ANTON VARONKA[1]

ABSTRACT. Loop invariants are software properties that hold before and after every iteration of a loop. As such, invariants provide inductive arguments that are key in automating the verification of program loops. The problem of generating loop invariants; in particular, invariants described by polynomial relations (so called *polynomial invariants*), is therefore one of the hardest problems in software verification. In this paper we advocate an alternative solution to invariant generation. Rather than inferring invariants from loops, we synthesise loops from invariants. As such, we generate loops that satisfy a given set of polynomials; in other words, our synthesised loops are correct by construction.

Our work turns the problem of loop synthesis into a symbolic computation challenge. We employ techniques from algebraic geometry to synthesise loops whose polynomial invariants are described by *pure difference* binomials. We show that such complex polynomial invariants need "only" linear loops, opening up new venues in program optimisation. We prove the existence of non-trivial loops with linear updates for polynomial invariants generated by pure difference binomials. Importantly, we introduce an algorithmic approach that constructs linear loops from such polynomial invariants, by generating linear recurrence sequences that have specified algebraic relations among their terms.

1. INTRODUCTION

Loop invariants, or more simply *invariants* in the sequel, are software properties that hold before and after every iteration of a loop. Invariants are often key to inductive arguments for automating the verification of programs with loops, see, e.g. [25, 22, 23, 21, 14]. One challenging aspect in invariant synthesis is the derivation of *polynomial invariants* for loop programs over numeric data structures. Such invariants are defined by polynomial relations $P(x_1, \ldots, x_d) = 0$ among the program variables $x_1, \ldots, x_d$. A nice property of polynomial invariants is that they define a polynomial ideal, called a *polynomial invariant ideal* [25, 22]. As such, the problem of generating (all) polynomial invariants is reduced to generating a finite basis of the polynomial invariant ideal.

In this paper, we reverse engineer the problem of polynomial invariant generation and propose an alternative solution to invariant synthesis. Rather than generating polynomial invariants for a given loop, we synthesise loops for a given polynomial invariant. Assume the postcondition of some section of code with a loop is given by a conjunction of polynomial equalities. Instead of generating an invariant that implies the postcondition, our solution comprises the synthesis of a new loop, one that is correct with respect to the specification–and that by construction.

Linear Loop Synthesis. The key aspect of our work comes with considering *homogeneous linear loops*, hereafter simply linear loops. Linear loops are a class of single-path loops whose update assignments are determined by a homogeneous system of linear equations in the program variables. More specifically, a *linear loop* is a loop program of the form

$$\mathcal{L}: x \leftarrow s; \text{ while } \star \text{ do } x \leftarrow Mx,$$

where x is a d-dimensional column vector of program variables, s is a d-dimensional vector with rational entries, and M is a $d \times d$-matrix with rational entries. Herein we employ the notation $\star$, instead of using `true` as loop guard, as our focus is on loop synthesis rather than proving loop termination.

Linear loops are fundamental objects in the computational study of recurrence. On the one hand, this class of loops represents a restrictive computational model. On the other hand, fundamental problems such as the decidability of the Halting Problem are open for this class [24]. For the avoidance of doubt, we lose no generality by working over the class of linear loops rather than the class of *affine loops* (those single-path loop programs with update assignments of the form $x \leftarrow Mx + v$ where $v \in \mathbb{Q}^d$). Indeed, the problem of studying the functional behaviour of affine loops can be reduced to that of studying linear loops; admittedly the reduction step will, in general, increase the number of program variables [25, 22, 24].

Linear Loops and Recurrences. Given a (system of) polynomial relation(s), our work constructs a linear loop. By construction, each of the given polynomial relations is satisfied by the loop variables before and after each iteration; thus each relation is an invariant of the loop. (Specific details are given in the discussion on our contributions.) We employ techniques from algebraic geometry to synthesise loops whose polynomial invariants are described by *pure difference binomials*. For such polynomial invariants, the procedure in Section 3 shows that "only" linear loops are required, thus addressing challenging aspects of arithmetic reductions in program optimisation [2]. Further, we prove the existence of non-trivial loops with linear updates for polynomial invariants generated by pure difference binomials (see Section 5). Examples 1.1 and 1.2 showcase linear loops that are synthesised by our work. We note that the study of *pure difference ideals*, those ideals generated by pure difference binomials, and their respective linear loops is well motivated. The classes of lattice and toric ideals (defined in Section 2) are pure difference ideals. Pure difference ideals also appear in the encoding of random walks on Markov chains of the form $\mathbb{N}^d$ by way of the connected components of the underlying graph [6, 16].

(a) Loop $\mathcal{L}_1$.
```
(x, y, z) := (1, 1, 1);
while ⋆ do
    x := 2x;
    y := 4y;
    z := 8z;
end while
```

(b) Loop $\mathcal{L}_2$.
```
(x, y) := (1, 1);
while ⋆ do
    x := 2x;
    y := 2y;
end while
```

FIGURE 1. Synthesised linear loops $\mathcal{L}_1$ and $\mathcal{L}_2$

Example 1.1. Consider the input ideal $I_1 \subseteq \mathbb{Q}[x, y, z]$ generated by the polynomials $p_1 = x^2 - y$ and $p_2 = x^3 - z$. Note that p_1 and p_2 are pure difference binomials in x, y, z. The procedure of Section 3 outputs a linear loop $\mathcal{L}_1$ (see Fig. 1a).

Example 1.2. Given the input ideal $I_2 \subseteq \mathbb{Q}[x, y]$ generated by the polynomial $p = x^3y - xy^3$. The procedure of Section 3 outputs a linear loop $\mathcal{L}_2$ (see Fig. 1b). Note, I_1 is the invariant ideal of $\mathcal{L}_1$. Loop $\mathcal{L}_2$, in turn, satisfies all invariants in I_2; however, I_2 is a strict subset of the invariant ideal of $\mathcal{L}_2$.

Key to our work is modelling loops as linear recurrence sequences that have specified algebraic relations among their terms. Let x_n denote the value of a loop variable x at the nth loop iteration. Recall that for a linear loop, x_n is given by a linear recurrence sequence with constant coefficients, commonly known as a *C-finite* sequence [8]. C-finite sequences are therefore key to our loop synthesis procedure (Section 3): we model program loops as systems of recurrence equations. Indeed, we aim to synthesise a system of C-finite recurrence sequences, and hence a linear loop, that satisfies given polynomial relations.

Our Contributions.

(1) For a polynomial ideal, we consider the problem of synthesising a *non-parametrised* loop (i.e., synthesising both the loop body and concrete initial values) such that every polynomial in the ideal is an invariant of the loop. In particular, we demonstrate a procedure for synthesising loops from pure difference ideals. In fact,
   (a) Given a pure difference ideal I, we describe a process that synthesises a linear loop with invariant ideal I (Section 3).
   (b) Suppose that $I = \langle p_1, \ldots, p_k \rangle$ is a polynomial ideal not necessarily generated by binomials, for which, by a change of coordinates, there exists a generating set of pure difference binomials. We present a procedure that outputs a linear loop such that any polynomial $p \in \langle p_1, \ldots, p_k \rangle$ is an invariant of said loop (Section 4).

(2) Under reasonable assumptions about the input, the aforementioned generated loops are *non-trivial*. By non-trivial, we mean that the orbit (or trajectory) of the vector

$$\langle x(n) \rangle_{n=0}^{\infty} = \langle x_1(n), \ldots, x_d(n) \rangle_{n=0}^{\infty}$$

given by the values of the loop variables $x_1, \ldots, x_d$ at the nth loop iteration is infinite. That is to say, the loop program functions on an infinite-state system. We shall defer a formal definition of a non-trivial loop to Section 2.

In Section 5, we consider corollaries to our loop synthesis procedure from Section 3. In particular, we consider specialisations for restrictive classes of input ideals. One corollary, concerning *canonical pure difference binomials*, is as follows.

Corollary 1.3. *Suppose that $I = \langle p \rangle \subseteq \mathbb{Q}[x_1, \ldots, x_d]$ where p is an irreducible polynomial of the form $p = x_1^{\alpha_1} \cdots x_d^{\alpha_d} - x_1^{\beta_1} \cdots x_d^{\beta_d}$. Then the procedure in Section 3 synthesises a linear loop for which I is precisely the invariant ideal of the loop.*

We end this note with a conclusion that discusses related work and proposes directions for future research (Section 6).

2. Preliminaries

2.1. **Abstract Algebra.** Let $\mathbb{K}$ be a field and $\mathbb{K}^d$ the vector space of d-tuples in $\mathbb{K}$. A *monomial* in the indeterminates (or polynomial variables) $x_1, \ldots, x_d$ is an expression $x_1^{v_1} x_2^{v_2} \cdots x_d^{v_d}$ where each exponent v_j is a non-negative integer. We employ the shorthand x^v to denote such monomials. A *polynomial* is a finite linear combination of monomials. This can be extended to include the negative integer exponents, if needed. We shall explicitly refer to monomials x^v with $v \in \mathbb{Z}^d$ (or their linear combinations) as *Laurent monomials* (Laurent polynomials, respectively), whenever negative powers are considered.

Let $\mathbb{K}[x_1, \ldots, x_d]$ be a polynomial ring, for brevity $\mathbb{K}[x]$. For computability reasons, throughout $\mathbb{K}$ will be the field of algebraic numbers, so $\mathbb{K} := \overline{\mathbb{Q}}$. We employ the standard notation $\mathbb{K}^*$ to refer to the set $\mathbb{K} \setminus \{0\}$ of invertible elements of the field and denote by $\mathrm{GL}_d(\mathbb{K})$ the multiplicative group of $d \times d$ invertible matrices over $\mathbb{K}$.

2.2. **Algebraic Geometry.** We recall standard preliminary material and terminology from the field of algebraic geometry, and refer to [4, 3] for more details.

Ideals. A *polynomial ideal* is a subset $I \subseteq \mathbb{K}[x]$ that satisfies the following properties: $0 \in I$; I is closed under addition; and for each $p \in \mathbb{K}[x]$ and $q \in I$, necessarily $pq \in I$. For a set of polynomials $S \subseteq \mathbb{K}[x]$, the *ideal generated by S* is given by

$$I = \langle S \rangle := \{ s_1 q_1 + \cdots + s_\ell q_\ell : s_j \in S, q_j \in \mathbb{K}[x], \ell \in \mathbb{N} \}.$$

A polynomial ideal I is *proper* if I is not equal to $\mathbb{K}[x]$, I is *prime* if $p \cdot q \in I$ implies that $p \in I$ or $q \in I$, and I is *radical* if $p^n \in I$ implies that $p \in I$.

Key to our discussion will be the bases for polynomial ideals.

Theorem 2.1 (Hilbert's Basis Theorem). *Every ideal in $\mathbb{K}[x]$ has a finite basis.*

Seminal work by Buchberger introduced Gröbner bases for polynomial ideals, which permit the algorithmic computation of key properties of polynomial ideals [1, 3], including ideal membership, ideal union/intersection,

elimination ideals, and many more. A key property that we draw upon in our synthesis procedure is the computation of a basis for a *saturation* of an ideal. Given $q \in \mathbb{K}[x]$, we compute a basis for the *saturation of I with respect to q*

$$I : (q)^\infty := \{p \in \mathbb{K}[x] : q^n p \in I \text{ for some } n \in \mathbb{N}\}.$$

We also recall relevant structural properties for classes of polynomial ideals.

Theorem 2.2 ([3, Theorem 6, Chapter 4.6])**.** *Each radical polynomial ideal I in $\mathbb{K}[x]$ admits a unique decomposition as an intersection of finitely many prime ideals $I = p_1 \cap \cdots \cap p_r$ such that for each pair $p_i \not\subset p_j$. The decomposition is commonly referred to as the* minimal decomposition of a radical ideal.

Varieties. The notion of an algebraic variety generalises the concept of algebraic curves to d dimensions. An (affine) *algebraic* variety $V \subseteq \mathbb{K}^d$ is the locus of points satisfying a system of polynomial equations. In the sequel, we shall focus on the varieties associated with polynomial ideals. Let I be a polynomial ideal in $\mathbb{K}[x]$. The locus of points in $\mathbb{K}^d$ where the polynomials in I simultaneously vanish is called the *variety of the ideal* and denoted by $V(I)$. Specifically,

$$V(I) = \{x \in \mathbb{K}^d : p(x) = 0 \text{ for all } p \in I\}.$$

A *subvariety* is a subset of a variety that is, itself, a variety. A variety V is *irreducible* if when written as a union of subvarieties $V = V_1 \cup V_2$ then necessarily either $V_1 = V$ or $V_2 = V$. An affine variety is irreducible if and only if $I(V)$ is a prime ideal.

Let $V \subseteq \mathbb{K}^d$ be an affine variety. We endow V with the *Zariski topology* by declaring that the closed sets of V are precisely the subvarieties of V. In this way, we extend the definition of *Zariski closure* as follows. The *Zariski closure* of a subset $S \subseteq \mathbb{K}^d$ is defined to be the smallest affine variety containing S.

2.3. **C-finite Sequences.** The class of *C-finite* sequences [18] consists of the real-algebraic linear sequences $\langle u_n \rangle_{n=0}^\infty$ that satisfy recurrence relations

(1) $$u_{n+d} = a_{d-1} u_{n+d-1} + \cdots a_0 u_n,$$

with constant coefficients $a_{d-1}, \ldots, a_0$ such that $a_0 \neq 0$. A C-finite sequence $\langle u_n \rangle_n$ that satisfies (1) is entirely determined by its initial values $u_0, \ldots, u_{d-1}$. The *order* of $\langle u_n \rangle_n$ is the minimum length of the recurrence relations it satisfies.

Given a system of C-finite sequences $\langle x_1(n) \rangle_n, \ldots, \langle x_d(n) \rangle_n$, consider the ideal consisting of all polynomials $P \in \mathbb{K}[y_1, \ldots, y_d]$ such that the polynomial equality $P = 0$ is satisfied for all $n \geq 0$ after simultaneously setting $y_j := x_j(n)$ for all $j \in \{1, \ldots, d\}$. We call this ideal the *ideal of algebraic relations* over $\mathbb{K}$ associated with the aforementioned system.

2.4. **Loop Invariants.** Let $\mathcal{L}$ be a linear loop with variables $x = (x_1, \ldots, x_d)$. For each loop variable x_j, let $\langle x_j(n) \rangle_n$ denote the sequence whose nth term is given by the value of x_j after the nth loop iteration. A *polynomial invariant* of $\mathcal{L}$ is a polynomial $P \in \mathbb{K}[x]$ such that

$$P(x_1(n), \ldots, x_d(n)) = 0$$

holds for all $n \geq 0$. The set of polynomial invariants of $\mathcal{L}$ forms an ideal, called the *(polynomial) invariant ideal* of $\mathcal{L}$ [25, 22]. In other words, the invariant ideal of $\mathcal{L}$ is the ideal of algebraic relations over $\mathbb{K}$ among the sequences $\langle x_1(n) \rangle_n, \ldots, \langle x_d(n) \rangle_n$. We note that, in our setting, it is always possible to compute a finite basis for the invariant ideal using Gröbner bases computation [19, 22].

The invariant ideal I of $\mathcal{L}$ is radical. It can be equivalently described by its variety $V(I) \subseteq \mathbb{K}^d$. Let

$$O := \left\{ (x_1(n), \ldots, x_d(n)) \in \mathbb{K}^d : n \in \mathbb{N} \right\}$$

be the *orbit of the loop*. Informally speaking, O is the set of variable vectors that $\mathcal{L}$ can reach during its execution. The Zariski closure of O in $\mathbb{K}^d$ is precisely the variety $V(I)$ and, further, is the smallest algebraic variety that contains O. The Zariski closure of O is the *strongest algebraic invariant* of $\mathcal{L}$ [12]. We shall sometimes abuse terminology and refer to the Zariski closure of O as the *Zariski closure of $\mathcal{L}$*. A loop $\mathcal{L}$ is *trivial* if its orbit O is a finite set.

2.5. **Lattices.** Let $(G, +)$ be an additive abelian group. A set $X \subseteq G$ is *linearly independent* if for any $n_1, \ldots, n_k \in \mathbb{Z}$ and any pairwise distinct $a_1, \ldots, a_k \in X$ a linear combination $\sum_{i=1}^{k} n_i a_i = 0$ is zero only if $n_1 = \cdots = n_k = 0$. If $\langle X \rangle = G$, the set X is called a *basis* of G.

An abelian group that has a finite basis is referred to as *lattice*. It is known that a lattice has fixed basis size, called *rank* and, furthermore, every lattice of rank $r \geq 1$ is isomorphic to $\mathbb{Z}^r$ as a group. A *saturation* of a lattice $L \subseteq \mathbb{Z}^d$ is a sublattice of $\mathbb{Z}^d$ defined as

$$\text{Sat}(L) := \{ u \in \mathbb{Z}^d : cu \in L \text{ for some } c \in \mathbb{Z} \setminus \{0\} \}.$$

If $L = \text{Sat}(L)$, the lattice L is said to be *saturated*.

An important class of lattices are those that describe the multiplicative relations among algebraic numbers. The *exponent lattice* of $\zeta_1, \ldots, \zeta_k \in \mathbb{K}^*$ is given by

$$L_{\exp}(\zeta_1, \ldots, \zeta_k) := \left\{ (n_1, \ldots, n_k) \in \mathbb{Z}^k : \prod_{i=1}^{k} \zeta_i^{n_i} = 1 \right\}.$$

The *lattice ideal* $I_L \subset \mathbb{K}[x_1, \ldots, x_d]$ of a lattice $L \subseteq \mathbb{Z}^d$ is the ideal $I_L := \langle x^\alpha - x^\beta : \alpha, \beta \in \mathbb{N}^d, \alpha - \beta \in L \rangle$.

2.6. **Toric Ideals and Varieties.** Consider an integer $s \times d$-matrix

$$A := \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1d} \\ a_{21} & a_{22} & \ldots & a_{2d} \\ & & \ldots & \\ a_{s1} & a_{s2} & \ldots & a_{sd} \end{pmatrix}$$

with column set $\{a_1, \ldots, a_d\} \subset \mathbb{Z}^s$. The purpose of defining this matrix is twofold.

First, we can view A as a linear transformation $T_A \colon \mathbb{Z}^d \to \mathbb{Z}^s$ such that $T_A(x) = Ax$. Thus we define the *kernel of A* by $\ker A := \left\{ x \in \mathbb{Z}^d : T_A(x) = 0 \right\}$.

It is easy to see that $\ker A \subseteq \mathbb{Z}^d$ is a lattice. In particular, one can define a lattice ideal for $\ker A$. Moreover, $\ker A$ is saturated.

Second, we can consider the columns of A as Laurent monomials over the indeterminates $z_1, \ldots, z_s$. Formally, a column $\boldsymbol{a}_i$ of A defines a Laurent monomial as $\chi^i(z_1, \ldots, z_s) = z_1^{a_{1i}} \ldots z_s^{a_{si}}$. We define the ring homomorphism

$$\pi_A : \mathbb{K}[x_1, \ldots, x_d] \to \mathbb{K}[z_1^{\pm 1}, \cdots, z_s^{\pm 1}]$$

by mapping the variables $x_1, \ldots, x_d$ to $\chi^1, \ldots, \chi^d$. The codomain of the homomorphism is the ring of Laurent polynomials over $\mathbb{K}$ with s variables.

The *toric ideal* I_A associated with matrix A is the kernel of π_A. The ideal I_A is a pre-image of a prime ideal, and hence I_A is itself a prime ideal of $\mathbb{K}[x]$. As shown in [4, Proposition 1.1.9], a toric ideal has an equivalent definition as a lattice ideal

$$(2) \qquad I_A = \langle x^{\boldsymbol{u}} - x^{\boldsymbol{v}} : \boldsymbol{u}, \boldsymbol{v} \in \mathbb{N}^d, \boldsymbol{u} - \boldsymbol{v} \in \ker A \rangle;$$

that is, as an ideal of a lattice $\ker A$. We emphasise that not every lattice is a kernel of a linear transformation and respectively, lattice ideals are not necessarily toric. In fact, toric ideals are precisely the prime lattice ideals [4, Proposition 1.1.11].

The homomorphism of $\mathbb{K}$-algebras is naturally associated with a group homomorphism $\varphi_A \colon \mathbb{K}^s \to \mathbb{K}^d$, defined by

$$\varphi_A(z) = (\chi^1(z), \ldots, \chi^d(z)).$$

The vanishing set of a toric ideal I_A is the Zariski closure of $\varphi_A(\mathbb{K}^s)$. Such irreducible varieties of $\mathbb{K}^d$ are called *toric varieties*. They share a number of important properties and have been widely studied along with their ideals [4, 27].

We refer to binomials of the form $x^{\boldsymbol{u}} - x^{\boldsymbol{v}}$ as *pure difference binomials*. A *pure difference ideal* is generated by pure difference binomials. Note that lattice and, in particular, toric ideals are pure difference ideals. Let $p = x_1^{\alpha_1} \cdots x_d^{\alpha_d} - x_1^{\beta_1} \cdots x_d^{\beta_d}$ be a pure difference binomial. Its *exponent vector* is $(\alpha_1 - \beta_1, \ldots, \alpha_d - \beta_d) \in \mathbb{Z}^d$.

Remark 2.3. Clearly, there are infinitely many pairwise distinct pure difference binomials sharing the same exponent vector —the vector is invariant when we multiply a pure difference binomial by a monomial, e.g., $x^2 - y^2$ and $x^3 y - x y^3$. For a given exponent vector $v = (v_1, \ldots, v_d) \in \mathbb{Z}^d$, we define a unique *canonical (pure difference) binomial* as $p(x_1, \ldots, x_d) := x^{v_+} - x^{v_-}$, where

$$v_+ = (\max\{v_1, 0\}, \ldots, \max\{v_d, 0\}) \in \mathbb{N}^d$$

and $v_- = v_+ - v \in \mathbb{N}^d$. Note that $x^2 - y^2$ is the canonical binomial associated with the vector $(2, -2)$, whereas $x^3 y - x y^3$ (see also Example 1.2) is not canonical.

3. FROM PURE DIFFERENCE IDEALS TO LINEAR LOOPS

We now describe our loop synthesis approach, by restricting our input polynomials/ideals to pure difference binomials/ideals. Given a pure difference ideal I as an input, our procedure outputs a linear loop such that

each polynomial in I is an invariant of the loop. We thus show that *loop synthesis is decidable for pure difference polynomials/ideals*.

We next outline our loop synthesis procedure and illustrate its main steps in Table 1.

Loop Synthesis Procedure:

Input: A list $p_1, \dots, p_k \in \mathbb{K}[x_1, \dots, x_d]$ of pure difference binomials or, alternatively, a polynomial ideal I generated by pure difference binomials.
(Step 1) Construct the lattice L determined by the exponents associated with the generators of I.
(Step 2a) Analyse lattice ideals I_L and $I_{\mathrm{Sat}(L)}$; the ideal $I_{\mathrm{Sat}(L)}$ is prime, enabling Step 2b.
(Step 2b) Construct a matrix A with $\ker A = \mathrm{Sat}(L)$.
(Step 3) Synthesise a linear loop $\mathcal{L}$ with a diagonal update matrix M whose diagonal entries are determined by the columns of A. The ideal $I_{\mathrm{Sat}(L)}$ is the invariant ideal of $\mathcal{L}$.
Output: Linear loop $\mathcal{L}$ with invariants $p_1, \dots, p_k$.

TABLE 1. Loop synthesis for our running examples

	Example 1.1	Example 1.2
Input: I	$\langle x^2 - y, x^3 - z \rangle$	$\langle x^3 y - x y^3 \rangle$
Step 1: I_L	$\langle x^2 - y, x^3 - z \rangle$	$\langle x^2 - y^2 \rangle$
Step 2a: $I_{\mathrm{Sat}(L)}$	$\langle x^2 - y, x^3 - z \rangle$	$\langle x - y \rangle$
Step 2b: A	$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$

Step 3: $\mathcal{L}$	$(x, y, z) := (1, 1, 1);$
	 while $\star$ do
	 $(x, y, z) := (2x, 4y, 8z);$
	 end while
		$(x, y) := (1, 1);$
		 while $\star$ do
		 $(x, y) := (2x, 2y);$
		 end while

We further detail each component of our synthesis procedure, proving correctness of each step of the synthesis process.

Input. The input for the synthesis process is a (possibly empty) finite list $p_1, \dots, p_k$ of pure difference binomials. Let I denote the *pure difference polynomial ideal* $I := \langle p_1, \dots, p_k \rangle$ in $\mathbb{K}[x]$ generated by this finite set. Our goal is to synthesise a linear loop $\mathcal{L}$ for which I is an invariant.

Step 1: Lattice ideal I_L. We start by listing the k exponent vectors $\boldsymbol{b}_1, \dots, \boldsymbol{b}_k \in \mathbb{Z}^d$ of the pure difference binomials $p_1, \dots, p_k$. Let $B := \{\boldsymbol{b}_1, \dots, \boldsymbol{b}_k\}$ and L the lattice spanned by the exponent vectors B. If $k = 0$, our convention is $B := \{\boldsymbol{0}\}$ and $L = \{\boldsymbol{0}\} \subseteq \mathbb{Z}^d$. In order to meet our objective, we first show that the saturation of the ideal $I = \langle p_1, \dots, p_k \rangle$ with respect to $\prod_{i=1}^d x_i$ is precisely the lattice ideal I_L (Theorem 3.2). In this direction, we begin with an intermediate lemma.

Lemma 3.1. *Let I be an ideal generated by $p_1, \ldots, p_k$ with exponent vectors constituting the set $B = \{b_1, \ldots, b_k\}$. Let J be the ideal generated by the canonical binomials of B (as in Remark 2.3). Then*

$$I : \left(\prod_{i=1}^{d} x_i\right)^{\infty} = J : \left(\prod_{i=1}^{d} x_i\right)^{\infty}.$$

Proof. Since $I \subseteq J$, one inclusion is straightforward: namely,

$$I : \left(\prod_{i=1}^{d} x_i\right)^{\infty} \subseteq J : \left(\prod_{i=1}^{d} x_i\right)^{\infty}.$$

In the other direction, consider a polynomial $g \in J : \left(\prod_{i=1}^{d} x_i\right)^{\infty}$. Let $q_1, \ldots, q_k$ be the canonical binomials generating J. Then g admits a decomposition of the form

$$g \cdot \left(\prod_{i=1}^{d} x_i\right)^{n_1} = f_1 \cdot q_1 + \cdots + f_k \cdot q_k$$

for some polynomials $f_1, \ldots, f_k \in \mathbb{K}[x]$ and some $n_1 \geq 0$.

Each generator p_ℓ of the ideal I has the form $p_\ell = m_\ell q_\ell$, where $m_1, \ldots, m_k$ are monomials and so

$$\left(\prod_{i=1}^{d} m_i\right) \cdot g \cdot \left(\prod_{i=1}^{d} x_i\right)^{n_1} = \sum_{\ell=1}^{k} m_\ell q_\ell \cdot \left(f_\ell \cdot \prod_{i \neq \ell} m_i\right)$$
$$= \sum_{\ell=1}^{k} p_\ell \cdot \left(f_\ell \cdot \prod_{i \neq \ell} m_i\right)$$

lies in I. Finally, there exists $n_2 \geq 0$ such that $\left(\prod_{i=1}^{k} x_i\right)^{n_2}$ is a multiple of the monomial $\prod_{i=1}^{k} m_i$. Thus

$$\left(\prod_{i=1}^{k} x_i\right)^{n_2} \cdot g \cdot \left(\prod_{i=1}^{k} x_i\right)^{n_1} \in I,$$

and hence $g \in I : \left(\prod_{i=1}^{d} x_i\right)^{\infty}$. □

Theorem 3.2. *Let $I \subseteq \mathbb{K}[x_1, \ldots, x_d]$ be a pure difference ideal and $L \subseteq \mathbb{Z}^d$ the lattice spanned by the exponent vectors of its generators. Then $I : \left(\prod_{i=1}^{d} x_i\right)^{\infty} = I_L$ and the lattice ideal I_L is radical.*

Proof. Since $B = \{b_1, \ldots, b_k\}$ spans the lattice L, [11, Corollary 3.22] implies that $J : \left(\prod_{i=1}^{d} x_i\right)^{\infty} = I_L$. The desired equality $I : \left(\prod_{i=1}^{d} x_i\right)^{\infty} = I_L$ now follows from Lemma 3.1. The second assertion follows from [11, Theorem 3.23]. □

Note that I is contained in I_L and, in general, this inclusion is strict. In particular, $I \subsetneq I_L$ in Example 1.2, see also Table 1.

Step 2a: Saturated lattice ideal $I_{\text{Sat}(L)}$. Before we proceed with Step 2 of our loop synthesis process, we briefly reflect on the lattice ideals that contain I. Notice that in Step 1 we not only found one of them, I_L, but we also pointed out that its lattice L had already been computed. Indeed, the generating set $b_1, \ldots, b_k$ of L is obtained from the pure difference binomials directly. While the generating polynomials I_L can also be computed (e.g. by employing Gröbner bases techniques from [20, Section 5] to compute the

saturation of I), our computation proceeds with vectors and lattices rather than polynomials and ideals.

Since I_L is a radical ideal (Theorem 3.2), I_L admits a unique decomposition (see Theorem 2.2). We adjust a general result by Eisenbud and Sturmfels [7], which concerns decompositions of binomial ideals, to our setting.

Lemma 3.3 ([7, Corollary 2.5]). *Let $L \subseteq \mathbb{Z}^d$ be a sublattice and $\mathrm{Sat}(L) \subseteq \mathbb{Z}^d$ its saturation. The minimal decomposition of ideal I_L includes the lattice ideal $I_{\mathrm{Sat}(L)}$ so that $I_L = I_{\mathrm{Sat}(L)} \cap J_1 \cap \cdots \cap J_\ell$. Here $\ell \geq 0$ and $I_{\mathrm{Sat}(L)}, J_1, \ldots, J_\ell$ are prime ideals of $\mathbb{K}[x]$. In particular, $I_{\mathrm{Sat}(L)}$ is toric.*

As an aside, work by Grigoriev et al. [10] presents an alternative approach to this step. Therein those authors decompose a so-called *binomial variety* $V(I_L)$ into a finite union of irreducible varieties.

In the computational part of Step 2 that follows, we compute a *prime lattice ideal* $I_{\mathrm{Sat}(L)}$ that contains I.

Step 2b: Matrix A encoding $I_{\mathrm{Sat}(L)}$. As before, $\{b_1, \ldots, b_k\}$ is a set of vectors spanning L over $\mathbb{Z}$. Versions of the next proposition appear in the literature, see e.g. [11, Theorem 3.17].

Proposition 3.4. *Let $L \subseteq \mathbb{Z}^d$ be a sublattice of rank r. If $r < d$, then there exists an integer $(d - r) \times d$-matrix A such that $\mathrm{Sat}(L) = \ker A$. Otherwise, if $r = d$, the same holds for $A = 0 \in \mathbb{Z}^{1 \times d}$. Further, there is an effective process to construct the matrix A.*

Recall that for each $y := (y_1, \ldots, y_d) \in \mathrm{Sat}(L)$ there is an integer c such that $c \cdot y \in L$. Since L consists of integer linear combinations of $\{b_1, \ldots, b_k\}$, a vector of the form $c \cdot y$ lies in the $\mathbb{Z}$-span of the set $\{b_1, \ldots, b_k\}$. Let V denote a vector subspace of $\mathbb{Q}^d$ over the field $\mathbb{Q}$ spanned by $\{b_1, \ldots, b_k\}$. Thus elements of $\mathrm{Sat}(L)$ are the integer vectors in V.

Proposition 3.4 follows from the next technical lemma.

Lemma 3.5. *There is a computable integer matrix A such that the null space, $\mathrm{Null}(A) = \{v \in \mathbb{Q}^d : Av = 0\}$, is equal to V.[1]*

Proof. Let $B \in \mathbb{Z}^{k \times d}$ be the matrix with rows $b_1, \ldots, b_k$. The row space $\mathrm{Row}(B)$ over $\mathbb{Q}$ is thus equal to V. The orthogonal complement of $\mathrm{Row}(B)$ is $\mathrm{Row}(B)^\perp = \mathrm{Null}(B)$. It follows that $\mathrm{Null}(B)$ has a basis of $d - r$ linearly independent vectors, which we denote by $a_1, \ldots, a_{d-r}$, provided that $r < d$. On the other hand, if $r = d$, then V is not a proper subspace of $\mathbb{Q}^d$, from which it follows that $\mathrm{Null}(B) = \{0\}$. Let A be the matrix with rows $a_1, \ldots, a_{d-r}$ (and defined as a single row vector 0 in the case $r = d$). Then, by definition, $\mathrm{Row}(A) = \mathrm{Null}(B)$. The result follows by elementary properties of orthogonal decomposition in finite-dimensional vector spaces. Indeed, we have

$$\mathrm{Null}(A) = \mathrm{Row}(A)^\perp = \mathrm{Null}(B)^\perp = (\mathrm{Row}(B)^\perp)^\perp = \mathrm{Row}(B) = V.$$

---

[1]Herein we distinguish between a $\mathbb{Q}$-subspace of vectors orthogonal to the row space of a given integer matrix (commonly its *null space*) and a sublattice of orthogonal integer vectors (commonly its *kernel*).

Generally speaking, the matrix A constructed above has rational entries; however, multiplying the entries of a matrix by a scalar does not change the null space. Thus we can assume, without loss of generality, that A has integer entries and preserves the property $\mathrm{Null}(A) = V$, as desired. $\qquad\square$

Proof of Proposition 3.4. There are two statements to prove in Proposition 3.4 depending on the cases $r < d$ or $r = d$. Note that the latter statement, that $A = \mathbf{0} \in \mathbb{Z}^{1 \times d}$ if $r = d$, was dealt with in the proof of Lemma 3.5. Thus all that remains it to establish the former statement. To this end, we show that $\mathrm{Sat}(L) = \ker A$ for the matrix A constructed in the proof of Lemma 3.5. We note that $\mathrm{Sat}(L)$ is equal to

$$V \cap \mathbb{Z}^d = \mathrm{Null}(A) \cap \mathbb{Z}^d = \{v \in \mathbb{Q}^d : Av = 0\} \cap \mathbb{Z}^d$$

$$= \{v \in \mathbb{Z}^d : Av = 0\} = \ker A,$$

as desired. $\qquad\square$

Step 3: Synthesise linear loop $\mathcal{L}$. We take a brief pause and reflect on the combination of Lemma 3.3 and Proposition 3.4 together with the formal definitions presented in Section 2. The sum total is a threefold equivalence between i) toric ideals, ii) ideals of saturated lattices, and iii) ideals of lattices presented as $\ker A$. Our objective, to synthesise a loop with prescribed polynomial invariants, relies on the constructive aspect of each of the preceding steps. In this final step, we will use the matrix A, constructed in Proposition 3.4, to synthesise a linear loop with invariant ideal $I_{\mathrm{Sat}(L)}$.

In the proof of Theorem 3.7, we will employ the following result due to Kauers and Zimmermann [19, Proposition 5] concerning algebraic relations among C-finite sequences.

Proposition 3.6. *The ideal over $\overline{\mathbb{Q}}[x_0, x_1, \ldots, x_d]$ associated with the algebraic relations among the $d + 1$ bi-infinite C-finite sequences*

$$\langle n \rangle_{n \in \mathbb{Z}}, \; \langle \lambda_1^n \rangle_{n \in \mathbb{Z}}, \; \ldots, \; \langle \lambda_d^n \rangle_{n \in \mathbb{Z}}$$

is equal to the lattice ideal of the exponent lattice of $\lambda_1, \ldots, \lambda_d$.

We now turn to our main result in this step.

Theorem 3.7. *Let $p_1, \ldots, p_k \in \mathbb{K}[x_1, \ldots, x_d]$ be pure difference binomials and let $L \subset \mathbb{Z}^d$ be the lattice spanned by their exponent vectors. There exists a linear loop $\mathcal{L}$ with a diagonal update matrix $M \in \mathbb{Q}^{d \times d}$ such that $I_{\mathrm{Sat}(L)}$ is the invariant ideal of $\mathcal{L}$.*

Proof. Following Proposition 3.4, it remains to prove that the ideal of a saturated lattice $\mathrm{Sat}(L)$ can be realised as the ideal of all polynomial invariants of a linear loop. Our proof adapts the argument in [9, Proposition 3.7] due to Galuppi and Stanojkovski.

First, there exists an integer matrix $A \in \mathbb{Z}^{s \times d}$ such that $\ker A = \mathrm{Sat}(L)$ (by Proposition 3.4). As before (cf. Section 2), let $\{a_1, \ldots, a_d\}$ be the set of column vectors of A. Now let $p_1, \ldots, p_s$ be the first s prime numbers and define $\lambda_j := p_1^{a_{1j}} \cdots p_s^{a_{sj}}$. Note that for each $j \in \{1, \ldots, d\}$, λ_j is the evaluation of the monomial x^{a_j} at $p = (p_1, \ldots, p_s)$.

Since there are no non-trivial multiplicative relations among pairwise distinct primes, a vector $\boldsymbol{n} := (n_1, \ldots, n_d)$ is a member of the exponent lattice of $\{\lambda_1, \ldots, \lambda_d\}$ if and only if $\boldsymbol{n}$ simultaneously achieves unity; i.e., $p_i^{n_1 a_{i1} + \cdots + n_d a_{id}} = 1$ for each $i \in \{1, \ldots, s\}$. Specifically, $(n_1, \ldots, n_d) \in L_{\exp}(\lambda_1, \ldots, \lambda_d)$ if and only if for each $i \in \{1, \ldots, s\}$ we have that $n_1 a_{i1} + \cdots + n_d a_{id} = 0$. Thus it follows, by definition, that $L_{\exp}(\lambda_1, \ldots, \lambda_d) = \ker A = \text{Sat}(L)$.

Finally, let J be the ideal generated by the algebraic relations among the C-finite sequences $\langle \lambda_1^n \rangle_{n \in \mathbb{N}}, \ldots, \langle \lambda_d^n \rangle_{n \in \mathbb{N}}$. *Mutatis Mutandis*, the argument in Proposition 3.6 holds for natural-indexed sequences. Taken in combination with the above argument, it follows that $J = I_{\text{Sat}(L)}$.

The polynomial invariants of a linear loop $\mathcal{L}$ with initial vector $(1, \ldots, 1) \in \mathbb{Q}^d$ and update matrix $M = \text{diag}(\lambda_1, \ldots, \lambda_d)$ are exactly those in the ideal J, which concludes the proof. $\qquad\square$

Output. From our starting point of a pure difference ideal I, we constructed an integer matrix A such that $I_{\text{Sat}(L)}$ is a toric ideal associated with A, and $I \subseteq I_{\text{Sat}(L)}$.

We output the linear loop $\mathcal{L}$ with the invariant ideal $I_{\text{Sat}(L)}$. Since $I \subseteq I_{\text{Sat}(L)}$, the loop $\mathcal{L}$ meets our objective: each of the polynomials in I is invariant under the action of $\mathcal{L}$. Correctness of the procedure follows from Proposition 3.4 and Theorem 3.7.

The following corollary summarises our synthesis procedure.

Corollary 3.8. *Let $p_1, \ldots, p_k \in \mathbb{K}[x_1, \ldots, x_d]$ be a set of pure difference binomials and $I = \langle p_1, \ldots, p_k \rangle$. There exists a linear loop $\mathcal{L}$ with a diagonal update matrix $M \in \mathbb{Q}^{d \times d}$ such that any polynomial $p \in I = \langle p_1, \ldots, p_k \rangle$ is an invariant of $\mathcal{L}$. There is a procedure to effectively construct loop $\mathcal{L}$.*

4. Transformed pure difference ideals

The procedure in Section 3 synthesises linear loops from ideals generated by pure difference binomials. In this section, we demonstrate that, subject to certain assumptions on the input, we can also synthesise linear loops for non-binomial ideals.

We call a polynomial ideal $\langle p_1, \ldots, p_k \rangle \in \mathbb{K}[x]$ a *transformed pure difference ideal* if there exists an invertible linear change of coordinates for which each p_j in the generating set is a pure difference binomial after the coordinate change. Here, by an *invertible linear change of coordinates* we mean that the associated change-of-basis matrix S is an element of $\text{GL}_d(\mathbb{K})$.

Theorem 4.1. *Let I be a transformed pure difference ideal with associated change-of-basis matrix $S \in \text{GL}_d(\mathbb{K})$. Then there exists a computable linear loop $\mathcal{L}$ such that I is an invariant of $\mathcal{L}$.*

We take $I = \langle p_1, \ldots, p_k \rangle$ and S as above. Further, let $J := \langle q_1, \ldots, q_k \rangle$ be the associated pure difference ideal after the change of coordinates S. The synthesis procedure summarised in Corollary 3.8 outputs a loop $\mathcal{L}'$ for which the pure difference ideal $J = \langle q_1, \ldots, q_k \rangle$ is invariant. More specifically, $\mathcal{L}'$ is the loop with update assignments described by a diagonal update matrix M and initial vector $v_{\text{in}} = (1, \ldots, 1)$ such that each polynomial in ideal J is an invariant of $\mathcal{L}'$.

The proof of Theorem 4.1 is as an immediate corollary of the next lemma, which outputs the desired linear loop $\mathcal{L}$.

Lemma 4.2. *Let $\mathcal{L}$ be the linear loop with update assignment matrix $S^{-1}MS$ and initial vector $S^{-1}v_{in}$. Then every polynomial in I is an invariant of $\mathcal{L}$.*

Proof. Let $e_1, \ldots, e_d$ be the standard basis of $\mathbb{K}^d$. After the change of coordinates S, the new basis vectors are $S^{-1}e_1, \ldots, S^{-1}e_d$ and the coordinates of $a = x_1 e_1 + x_d e_d$ are $Sa = (x'_1, \ldots, x'_d)$. Clearly,

$$a \in \bigcap_{i=1}^{k} V(p_i) \Leftrightarrow Sa \in \bigcap_{i=1}^{k} V(q_i).$$

Hence, $v_{\text{in}} \in \bigcap_{i=1}^{k} V(q_i)$ implies that $S^{-1}v_{\text{in}} \in \bigcap_{i=1}^{k} V(p_i)$. Moreover, the matrix $S^{-1}MS$ encodes the linear update assignments of $\mathcal{L}'$ in the standard basis; thus $(S^{-1}MS)^n S^{-1}v_{\text{in}} \in \bigcap_{i=1}^{k} V(p_i)$ for all $n \geq 0$. Hence, each polynomial in I is an invariant of $\mathcal{L}$. $\square$

Example 4.3. Let $I = \langle p_1, p_2 \rangle$ be the ideal of $\mathbb{K}[x, y, z]$ generated by $p_1 = 4y^2 + y - x$ and $p_2 = 8y^3 - x + z$. The change of coordinates described by the invertible matrix $S := \begin{pmatrix} 0 & 2 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$ yields $q_1 = (x')^2 - y'$, $q_2 = (x')^3 - z'$. Thus I is a transformed pure difference ideal and, after a change of coordinates, we have arrived at the ideal in Example 1.1. In the new coordinate system, we synthesise a loop $\mathcal{L}'$ (Corollary 3.8 and Fig. 1a) for which each polynomial in the pure difference ideal $\langle q_1, q_2 \rangle$ is invariant. In the old coordinate system, we proceed as in Theorem 4.1. Our procedure synthesises the loop $\mathcal{L}$ with update matrix $S^{-1} \cdot \text{diag}(2, 4, 8) \cdot S$ and initial vector $S^{-1} \cdot (1, 1, 1)^T$ as follows:

$(x, y, z) := (3/2, 1/2, 1/2);$
while $\star$ **do**
  $x := 4x - 2y;$
  $y := 2y;$
  $z := -4x - 2y + 8z;$
end while

By construction, both polynomials p_1 and p_2 are invariants of $\mathcal{L}$, and thus so is any $p \in I = \langle p_1, p_2 \rangle$.

Remark 4.4. The approach of Theorem 4.1 relies on the existence of an appropriate change of coordinates that moves ideal I to a pure difference ideal J and further, that a change-of-basis matrix S is given explicitly. The problem of determining the existence of such S appears to be a challenging task.

A similar challenge is addressed by Katthän et al. [17]. Their algorithmic approach [17, Algorithm 4.5] can generate all matrices $S \in \text{GL}_d(\mathbb{K})$ that move an ideal I to a *unital* ideal J. Recall that unital ideals are those generated by pure difference binomials and monomials, and hence pure difference ideals are a strict subclass. A straightforward approach to transform an ideal to a pure difference ideal is to apply the procedure of [17] and to manually check whether any of the transformed ideals output has a basis

without monomials. If J is such an ideal, then Theorem 4.1 can be employed to synthesise a linear loop for the initial ideal I.

5. Further results

In this section, we gather together corollaries of our synthesis procedure from Section 3.

5.1. Existence of Non-Trivial Linear Loops.
Theorems 5.1 and 5.2 next show that, subject to certain restrictions on the input ideal, there are always non-trivial loops that witness a given input as an invariant.

Theorem 5.1. *Let I be an ideal generated by at most $d-1$ pure difference binomials in $\mathbb{K}[x_1, \ldots, x_d]$. There exists a non-trivial linear loop $\mathcal{L}$ such that any polynomial $p \in I$ is an invariant of $\mathcal{L}$.*

Proof. In light of Corollary 3.8, it suffices to show that $\mathcal{L}$ generated by the procedure described in Section 3 is non-trivial.

Recall that a linear loop $\mathcal{L}$ is trivial if the input vector has finite orbit. For such loops, the variable vector $(x_1, \ldots, x_d)$ is attained at two different iterations of $\mathcal{L}$. Since, by construction, the update matrix $M := \operatorname{diag}(\lambda_1, \ldots, \lambda_d)$, the loop $\mathcal{L}$ is trivial if and only if $\lambda_1^k = \cdots = \lambda_d^k = 1$ for some $k \geq 0$. This implies that all diagonal entries of the loop update matrix M are roots of unity. However, by construction, the entries $\lambda_1, \ldots, \lambda_d$ are positive rational numbers (see proof of Theorem 3.7). Therefore, $\lambda_1 = \cdots = \lambda_d = 1$ is a necessary condition for $\mathcal{L}$ to be trivial.

From the proof of Proposition 3.4, the matrix A has rank 0 if and only if the associated lattice L is spanned by $r = d$ linearly independent vectors. By assumption, L has rank at most $d-1$ because it is generated by at most $d-1$ exponent vectors. Thus $M \neq \operatorname{diag}(1, \ldots, 1)$ and so $\mathcal{L}$ is non-trivial. $\square$

The next theorem is a specialisation of Theorem 5.1 and follows from Step 3 of the synthesis procedure in Section 3.

Theorem 5.2. *Let $I_T \neq \langle x_1 - 1, \ldots, x_d - 1 \rangle$ be a toric ideal of $\mathbb{K}[x_1, \ldots, x_d]$. There exists a non-trivial linear loop $\mathcal{L}$ such that I_T is the invariant ideal of $\mathcal{L}$.*

Proof. We recall that toric ideals are precisely the lattice ideals of saturated lattices $\operatorname{Sat}(L) = \ker A$. Due to Theorem 3.7, a loop $\mathcal{L}$ with invariant ideal $I_{\operatorname{Sat}(L)}$ can be generated for an arbitrary saturated lattice $\operatorname{Sat}(L) = \ker A$. Observe that from the proof of Theorem 5.1, $\mathcal{L}$ is trivial if and only if $\operatorname{Sat}(L) = \mathbb{Z}^d$. This, in turn, is equivalent to $I_T = \langle x^\alpha - x^\beta : \alpha, \beta \in \mathbb{N}^d \rangle = \langle x_1 - 1, \ldots, x_d - 1 \rangle$. $\square$

Given polynomials $p_1, \ldots, p_k$, a necessary condition for a non-trivial loop to simultaneously satisfy $p_i = 0$ for all $i = 1, \ldots, k$, is the existence of infinitely many rational solutions to a system of equations $p_1 = 0 \wedge \cdots \wedge p_k = 0$. When $p_1, \ldots, p_k$ are pure difference binomials with $k \leq d-1$, the system indeed has infinitely many solutions–and this is utilised in Theorem 5.1. However, determining whether an arbitrary system of polynomial equations has infinitely many rational solutions is a highly non-trivial problem, as witnessed by the example below. Note that determining whether an equation has infinitely many integer solutions is undecidable [5].

Example 5.3. Here, $d = 2$ and $k = 1$. a) The equation $x^3 + y^3 = 1$ has precisely two rational solutions: $(x_1, y_1) = (1, 0)$ and $(x_2, y_2) = (0, 1)$. b) For comparison, the equation $x^3 + y^3 = 9$ has infinitely many rational solutions [26, Chapter 5.2].

5.2. **Modifications to the Synthesis Process.** A higher objective than that set in Section 3 is as follows: given a polynomial ideal I, construct a linear loop whose invariant ideal is precisely I. The invariant ideals are radical, and so, for this question, one may assume that the given ideal I is radical. Equivalently, the objective is to construct a linear loop whose Zariski closure is the variety $V(I)$. Our synthesis procedure does not generally achieve this goal because each inclusion in the chain of ideals

$$(3) \qquad\qquad I \subseteq J \subseteq I_L \subseteq I_{\text{Sat}(L)}$$

considered in Section 3 is, in general, strict. Here J stands for the ideal generated by the canonical binomials, as in e.g. Lemma 3.1.

Remark 5.4. On the one hand, $\ker A$ of any integer $s \times d$-matrix A is a sublattice of $\mathbb{Z}^d$. On the other hand, the converse statement is not true since there are lattices that cannot be represented as matrix kernels. For example, $L := \mathbb{Z}(2, -2) \subset \mathbb{Z}^2$ is not saturated and hence not a kernel of a matrix: $(2, -2) \in L$ but $(1, -1) \notin L$.

By Remark 5.4, we generally have $I_L \subsetneq I_{\text{Sat}(L)}$. An examination of Example 1.2 (see also Table 1), shows how most of the inclusions in (3) are strict; in this example, only the equality $J = I_L$ holds. Nevertheless, its (general) violation is witnessed elsewhere in the literature (cf. the discussion that follows [11, Corollary 3.21]).

In special cases, we can simplify the procedure of Section 3 by observing (introduced) redundancy. In this direction, we provide a list of sufficient conditions for equalities to hold in (3).

Proposition 5.5. *Let $I \subseteq \mathbb{K}[x_1, \ldots, x_d]$ be a pure difference ideal.*
  (1) *Suppose that $I = \langle p \rangle$ is a principal ideal for which p is a canonical pure difference binomial. Then $I = I_L$. If, in addition, p is irreducible, then $I = I_{\text{Sat}(L)}$ holds.*
  (2) *Suppose that I is generated by pure difference binomials and at least one of the generators $p_1, \ldots, p_k$ has a positive exponent vector $v_i \in \mathbb{Z}^d_{>0}$. Then, $J = I_L$.*

Proof. Regarding (1), we consider the principal ideal of $p = x^\alpha - x^\beta$ with $\gcd(x^\alpha, x^\beta) = 1$. Let I_L be the lattice ideal of $L := \mathbb{Z} \cdot (\alpha - \beta)$. This lattice ideal is generated by pure difference binomials. Each such generator takes the form $x^{n\alpha} - x^{n\beta}$ for some positive integer n, or $x^{-m\beta} - x^{-m\alpha}$ for some negative integer m. Polynomials of this form are divisible by $x^\alpha - x^\beta$. It quickly follows that $I_L \subseteq \langle p \rangle$ and hence $I_L = I$. If, in addition, p is irreducible, then p is prime ($\mathbb{K}[x_1, \ldots, x_d]$ is a unique factorisation domain). Thus $I_L = I = \langle p \rangle$ is prime and so L is saturated. Therefore $I = I_L = I_{\text{Sat}(L)}$.

Assertion (2), in turn, is a modification of [27, Lemma 12.4]. Without loss of generality, let J be an ideal generated by canonical pure difference binomials $q_1, \ldots, q_k$, where q_1's exponent vector v is positive. Then, $q_1 =$

$x^v - 1$ and every variable x_i, $1 \leq i \leq d$, has an inverse in the factor ring $\mathbb{K}[x]/J$. Hence there exists $g \in \mathbb{K}[x]$ such that $p := g \cdot \left(\prod_{i=1}^{d} x_i \right) - 1 \in J$. Let $f \in J : \left(\prod_{i=1}^{d} x_i \right)^{\infty}$; that is, assume there exists $n \geq 0$ such that $\left(\prod_{i=1}^{d} x_i \right)^{n} \cdot f \in J$. As a consequence, $g^n \cdot \left(\prod_{i=1}^{d} x_i \right)^{n} \cdot f \in J$. We rewrite the latter in the following form: $\left(g^n \left(\prod_{i=1}^{d} x_i \right)^{n} - 1 \right) \cdot f + f \in J$. Note that the expression wrapped by the outer parentheses is divisible by p. It follows immediately that $f \in J$. Thus $J = J : \left(\prod_{i=1}^{d} x_i \right)^{\infty}$ and, by way of Theorem 3.2, $I_L = J$. $\qquad \square$

Note that Corollary 1.3 follows from Proposition 5.5 (i): an irreducible pure difference binomial is clearly canonical. A loop synthesised for $I_{\mathrm{Sat}(L)}$ then has I as its invariant ideal by Theorem 3.7.

6. Discussion and Conclusions

Related Works. On the one hand, deriving polynomial invariants for the class of loops with (non-linear) polynomial arithmetic in their update assignments is, in general, undecidable [12]. On the other hand, for restricted classes of loops there are efficient procedures for synthesising invariants. Indeed, the restricted classes of polynomial arithmetic in so-called *solvable loops* [25]—loops with (blocks of) affine assignments, admit such procedures [22, 23, 14, 21].

Previous works synthesising linear loops from non-linear polynomial invariants include [13]. Their approach is also based on algebraic reasoning about the C-finite sequences generated by linear loops. Yet, the synthesis problem is translated into a constraint solving task in non-linear arithmetic, by relying on loop templates and using a conflict resolution procedure based on cylindrical algebraic decomposition/Gröbner basis computation [15]. Unlike [13], our synthesis procedure restricts to linear algebraic reasoning. The algorithm of [13] is relative complete as it generates all linear loops satisfying a given invariant of a bounded degree. As such, and in contrast to our results from Theorems 5.1 and 5.2, the work of [13] gives no sufficient conditions for the existence of at least one non-trivial loop satisfying the invariant.

The approach in [9] studies cyclic semigroups and sheds light on their geometry. In particular, irreducible components of Zariski closures for cyclic semigroups are shown to be isomorphic to toric varieties. Using the terminology in this note, their observation that toric ideals are precisely the invariant ideals of some linear loops is the key motivation for our synthesis procedure.

Conclusions and Future Directions. Using machinery from algebraic geometry, we identify classes of polynomial invariants for which synthesis becomes decidable. Our synthesis procedure can produce infinitely many different loops that, by construction, all have the same invariant. For a given input, the number of variables s of the procedurally generated output loops is equal to the number d of indeterminates in the input polynomials. Observe that linear loops with $s > d$ variables can still satisfy invariants

from $\mathbb{K}[x_1, \ldots, x_d]$ on a subset of their variables. The challenge of deriving an upper bound on the number of program variables s for the invariant, also raised in [13, Section 4.2], remains open.

We aim to analyse the bit complexity of our procedure in the future. Note that in Step 3, prime numbers are raised to the powers that are, in general, exponential in the number of variables d. Therefore, the generated update matrix might have entries with exponentially many (in D) bits, cf. the worst-case double exponential running time of Gröbner basis computation for the invariant ideal.

We intent to extend our synthesis approach to synthesise loops whose invariant ideals are non-prime lattice ideals. One challenge to be addressed is the classification of Zariski closures of the orbits O of linear loops, cf. [9]. In this direction, it is of interest whether loops with non-diagonalisable matrices have invariant ideals structurally different from those of loops synthesised in Sections 3 and 4.

We conclude this paper by highlighting the following limitation of our approach, which we intend to address in future work. The construction in Step 1, that introduces the lattice ideal I_L, entails that we can only synthesise loops whose invariant ideals are lattice ideals. Further, Theorem 3.2 implies that $V(I_L)$ is the Zariski closure of $V(I) \setminus V(\prod_{i=1}^{d} x_i)$, cf. [3, Chapter 4.4, Theorem 10]. Our procedure thus only synthesises loops whose orbits lie outside of the coordinate hyperplanes.

Example 6.1. We revisit the synthesis problem for an ideal $I = \left\langle x^3y - xy^3 \right\rangle$ of Example 1.2. The invariant ideal of a linear loop $\mathcal{L}'$ with update matrix

$$M := \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

and initial vector $v_{\text{init}} = (1, 0)$ is precisely the ideal I.

The loop $\mathcal{L}'$ in the example above stands in contrast to the synthesised loop $\mathcal{L}$ in Example 1.2 because $V(I)$ is the strongest algebraic invariant of $\mathcal{L}'$. In contrast, the strongest algebraic invariant of $\mathcal{L}$ is $V(x - y)$.

References

[1] B. Buchberger. "Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal". In: *J. Symb. Comput.* 41.3-4 (2006), pp. 475–511.

[2] K. D. Cooper, L. T. Simpson, and C. A. Vick. "Operator Strength Reduction". In: *ACM Trans. Program. Lang. Syst.* 23.5 (2001), pp. 603–625.

[3] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Fourth. Undergraduate Texts in Mathematics. An introduction to computational algebraic geometry and commutative algebra. Springer, Cham, 2015, pp. xvi+646. DOI: `10.1007/978-3-319-16721-3`.

[4] D. A. Cox, J. B. Little, and H. K. Schenck. *Toric varieties*. Vol. 124. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2011, pp. xxiv+841. DOI: `10.1090/gsm/124`.

[5] M. Davis. "On the Number of Solutions of Diophantine Equations". In: *Proceedings of the American Mathematical Society* 35.2 (1972), pp. 552–554.

[6] P. Diaconis, D. Eisenbud, and B. Sturmfels. "Lattice walks and primary decomposition". In: *Mathematical essays in honor of Gian-Carlo Rota (Cambridge, MA, 1996)*. Vol. 161. Progr. Math. Birkhäuser Boston, Boston, MA, 1998, pp. 173–193.

[7] D. Eisenbud and B. Sturmfels. "Binomial ideals". In: *Duke Math. J.* 84.1 (1996), pp. 1–45. DOI: `10.1215/S0012-7094-96-08401-X`.

[8] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence sequences*. Vol. 104. Math. Surveys Monogr. Amer. Math. Soc., Providence, RI, 2003, pp. xiv+318. DOI: `10.1090/surv/104`.

[9] F. Galuppi and M. Stanojkovski. "Toric varieties from cyclic matrix semigroups". In: *Rend. Istit. Mat. Univ. Trieste* (2021). DOI: `10.13137/2464-8728/33099`.

[10] D. Grigoriev, A. Iosif, H. Rahkooy, T. Sturm, and A. Weber. "Efficiently and Effectively Recognizing Toricity of Steady State Varieties". In: *Mathematics in Computer Science* 15 (2019), pp. 199–232.

[11] J. Herzog, T. Hibi, and H. Ohsugi. *Binomial ideals*. Vol. 279. Graduate Texts in Mathematics. Springer, Cham, 2018, pp. xix+321. DOI: `10.1007/978-3-319-95349-6`.

[12] E. Hrushovski, J. Ouaknine, A. Pouly, and J. Worrell. "On Strongest Algebraic Program Invariants". In: *J. of ACM* (2020). To appear.

[13] A. Humenberger, D. Amrollahi, N. Bjørner, and L. Kovács. "Algebra-Based Reasoning for Loop Synthesis". In: *Form. Asp. Comput.* 34.1 (July 2022). DOI: `10.1145/3527458`.

[14] A. Humenberger, M. Jaroschek, and L. Kovács. "Invariant Generation for Multi-Path Loops with Polynomial Assignments". In: *Proc. of VMCAI.* 2018, pp. 226–246.

[15] D. Jovanovic and L. de Moura. "Solving non-linear arithmetic". In: *ACM Commun. Comput. Algebra* 46.3/4 (2012), pp. 104–105.

[16] T. Kahle, J. Rauh, and S. Sullivant. "Positive margins and primary decomposition". In: *J. Commut. Algebra* 6.2 (2014), pp. 173–208. DOI: `10.1216/JCA-2014-6-2-173`.

[17] L. Katthän, M. Michalek, and E. Miller. "When is a Polynomial Ideal Binomial After an Ambient Automorphism?" In: *Found. Comput. Math.* 19.6 (2019), pp. 1363–1385. DOI: `10.1007/s10208-018-9405-0`.

[18] M. Kauers and P. Paule. *The Concrete Tetrahedron - Symbolic Sums, Recurrence Equations, Generating Functions, Asymptotic Estimates*. Texts & Monographs in Symbolic Computation. Springer, 2011.

[19] M. Kauers and B. Zimmermann. "Computing the algebraic relations of C-finite sequences and multisequences". In: *Journal of Symbolic Computation* 43.11 (2008), pp. 787–803. DOI: `https://doi.org/10.1016/j.jsc.2008.03.002`.

[20] D. Kesh and S. K. Mehta. "Generalized Reduction to Compute Toric Ideals". In: *Algorithms and Computation*. Ed. by Y. Dong, D.-Z. Du, and O. Ibarra. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 483–492.

[21] Z. Kincaid, J. Cyphert, J. Breck, and T. W. Reps. "Non-Linear Reasoning for Invariant Synthesis". In: *Proc. of POPL.* 2018, 54:1–54:33.

[22] L. Kovács. "Reasoning Algebraically About P-Solvable Loops". In: *Proc. of TACAS.* 2008, pp. 249–264.

[23] S. de Oliveira, S. Bensalem, and V. Prevosto. "Polynomial Invariants by Linear Algebra". In: *Proc. of ATVA.* 2016, pp. 479–494.

[24] J. Ouaknine and J. Worrell. "On Linear Recurrence Sequences and Loop Termination". In: *ACM SIGLOG News* 2.2 (Apr. 2015), pp. 4–13. DOI: `10.1145/2766189.2766191`.

[25] E. Rodríguez-Carbonell and D. Kapur. "Automatic Generation of Polynomial Loop Invariants: Algebraic Foundations". In: *Proc. of ISSAC.* 2004, pp. 266–273.

[26] J. H. Silverman and J. T. Tate. *Rational Points on Elliptic Curves*. 2nd. Springer Publishing Company, Incorporated, 2015.

[27] B. Sturmfels. *Gröbner bases and convex polytopes*. Vol. 8. University Lecture Series. American Mathematical Society, Providence, RI, 1996, pp. xii+162. DOI: `10.1090/ulect/008`.