



Cycle Detection for Affine Integer Linear Loops

Mishel Carelli^{1*} and Bernd Finkbeiner^{1,2†}

¹ CISP Helmholtz Center for Information Security, Germany
mishel.carelli@cispa.de
finkbeiner@cispa.de

² Technical University of Munich, Germany
bernd.finkbeiner@tum.de

Abstract

We study the cycle-detection problem for affine single-path linear-constrained loops over the integers. A cycle is a finite execution that returns to its initial state. Cycle detection is a natural relaxation of termination: every cycle witnesses non-termination, while an infinite execution need not contain a cycle.

We prove that cycle detection for affine integer loops belongs to Σ_2^P . The proof relies on the algebraic structure of periodic vectors of the update matrix. Using the cyclotomic factors of its characteristic polynomial, we obtain a polynomial representation of the periodic subspace and of exponentially distant states along a periodic orbit. We then apply a small-integer-solution theorem to show that, whenever a cyclic state exists, one exists with polynomial bit-length. Consequently, cycle existence can be expressed by existentially guessing such a state and universally quantifying over a polynomial-size binary encoding of a position in its orbit, with the resulting predicate decidable in polynomial time.

1 Introduction

Termination analysis is a classical problem in software verification. A particularly well-studied family of programs consists of *single-path linear-constrained loops* (SLCs) and their subclasses, such as affine SLCs, as well as their extensions to multipath linear-constrained loops [1].

A standard approach to proving termination is to search for a ranking function, i.e., a function that strictly decreases along every transition and takes values in a well-founded domain [10]. Linear ranking functions can be synthesized efficiently for many classes of linear loops, but the method is incomplete: the absence of a linear ranking function does not imply non-termination.

In this paper, we consider affine integer SLCs of the form

$$\text{while } (Cv \leq d) \text{ do } v' := Av + b,$$

where the program variables range over $\mathbb{Z}^n$ and the coefficients of A, b, C, d are rational.

*This work was supported by the European Research Council (ERC) Grant HYPER (No. 101055412).

†This work was supported by the European Research Council (ERC) Grant HYPER (No. 101055412).

The search for complete termination procedures for affine loops goes back at least to Tiwari [12], who proved decidability of termination for linear loops over the reals. Braverman subsequently established decidability over the rationals [2], while decidability over the integers was obtained only much later by Hosseini, Ouaknine, and Worrell [8]. The integer case is considerably more involved and requires substantial algebraic and number-theoretic machinery. Hosseini’s PhD thesis [7] gives a 2-EXPSPACE upper-bound analysis for the original decision procedure. A recent survey [1] modifies this algorithm and observes that the main decision procedure runs in exponential time in the size of the input loop. In the integer case, however, a preprocessing step used to eliminate degeneracy may generate exponentially many problem instances.

For important restricted classes, considerably lower complexity bounds are known. Hark, Frohn, and Giesl [6] show that termination of linear loops with rational spectrum is coNP-complete over the integers, rationals, algebraic reals, and reals.

A recent paper [3] considers the termination problem for general linear-constrained loops. One useful distinction is between *cyclic* executions, which revisit a previously visited state, and *self-avoiding* infinite executions, which never do so. For one-dimensional linear-constrained loops, cycle detection is decidable, whereas the existence of self-avoiding infinite executions is closely connected to long-standing open problems concerning generalized Collatz sequences. These results suggest that cycle detection may constitute a substantially more tractable problem than termination.

The distinction is fundamental. Every cycle yields an infinite execution, and hence non-termination, but the converse does not hold: a loop may admit an infinite execution while having no cycle. For example,

$$\textbf{while } (x \geq 0) \textbf{ do } x' := x + 1$$

has an infinite execution from every non-negative initial state, but no cyclic state.

Motivated by this distinction, we study the complexity of cycle detection for affine integer SLCs. Our main result shows that the problem belongs to Σ_2^P , the second level of the polynomial hierarchy. This gives a significantly lower known upper bound for detecting cyclic behaviour than the bounds arising from existing procedures for full termination, and provides further evidence that cycle detection can be more tractable than termination.

Our result is related to complexity bounds for flat affine counter systems with the finite-monoid property [9]. In such systems, the powers of the matrices occurring along loops range over a finite monoid. In contrast, we do not impose a finite-monoid assumption on the update matrix. Instead, we exploit the fact that any cyclic execution necessarily lies in the periodic subspace of the update matrix, on which the dynamics has finite order.

The main difficulty is that the period of this restricted dynamics can be exponentially large. We show that there exists a number G of polynomial bit-length such that the length of every elementary cycle divides G . Consequently, checking whether a candidate state is cyclic may require considering exponentially many positions of its orbit.

To overcome this difficulty, we first show that if a cyclic state exists, then one exists whose bit-length is polynomial in the input size. The proof represents cyclic states as the integer points of a rational polyhedron whose individual inequalities have polynomial bit-length and then applies a standard small-integer-solution theorem. The key algebraic ingredient is a polynomial representation of the periodic subspace using the cyclotomic factors of the characteristic polynomial of the update matrix.

Finally, after existentially guessing a polynomial-size cyclic-state candidate, we universally quantify over a polynomial-size binary encoding of a position in its orbit. Although the position

itself may be exponentially large, the corresponding iterate can be computed in polynomial time by reducing x^i modulo the cyclotomic product associated with the update matrix. This yields an $\exists\forall$ characterization with a polynomial-time predicate, and therefore establishes membership in Σ_2^P .

2 Preliminaries

2.1 Affine SLCs

An *affine single-path linear-constrained loop* (SLC) of dimension n over the integers is a loop

$$\text{while } (C\mathbf{v} \leq d) \text{ do } \mathbf{v}' := A\mathbf{v} + b,$$

where

$$A \in \mathbb{Q}^{n \times n}, \quad b \in \mathbb{Q}^n, \quad C \in \mathbb{Q}^{m \times n}, \quad d \in \mathbb{Q}^m.$$

Its state space is $\mathbb{Z}^n$. We write $\mathbf{v} \rightarrow \mathbf{v}'$ if $C\mathbf{v} \leq d$ and $\mathbf{v}' = A\mathbf{v} + b \in \mathbb{Z}^n$.

A *trace* is a finite or infinite sequence $\mathbf{v}_0, \mathbf{v}_1, \dots$ of integer states such that $\mathbf{v}_i \rightarrow \mathbf{v}_{i+1}$ whenever both states occur in the sequence.

A *cycle of length* $k \geq 1$ is a finite trace $\mathbf{v}_0, \dots, \mathbf{v}_k$ such that $\mathbf{v}_0 = \mathbf{v}_k$. It is *elementary* if $\mathbf{v}_0, \dots, \mathbf{v}_{k-1}$ are pairwise distinct. A state $\mathbf{v} \in \mathbb{Z}^n$ is called *cyclic* if it occurs in a cycle.

Cycle Detection Problem. Given an affine integer SLC, decide whether it has a cycle.

The existence of a cycle implies non-termination, since the cycle can be repeated indefinitely. An affine update can be homogenized into a linear one. Namely, let

$$\hat{A} = \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix}, \quad \hat{\mathbf{v}} = \begin{pmatrix} \mathbf{v} \\ 1 \end{pmatrix}.$$

Then

$$\hat{A}\hat{\mathbf{v}} = \begin{pmatrix} A\mathbf{v} + b \\ 1 \end{pmatrix}.$$

The original guard is equivalent to

$$(C \ -d)\hat{\mathbf{v}} \leq 0.$$

By additionally requiring that the last coordinate is equal to 1, cycles of the affine loop correspond exactly to cycles of the homogenized linear loop. Affine integer SLCs with $b = 0$ are called *linear integer SLCs*.

We call a vector $v \in \mathbb{C}^n$ *periodic vector of* A if $A^i v = v$ for some $i \geq 1$. The least such i is called the *period* of v . Note that for a linear SLC every cyclic vector is a periodic vector of A , but the converse is false in general, since the orbit of a periodic vector may violate the guard.

2.2 Bit-length and Small Solution Theorem

For $z \in \mathbb{Z}$, the bit-length of z is $\lceil \log(|z| + 1) \rceil + 1$. The bit-length of $\frac{p}{q} \in \mathbb{Q}$, where p and $q > 0$ are relatively prime, is the sum of the bit-lengths of p and q . The bit-length of a vector, matrix, or polynomial is the sum of the bit-lengths of its entries or coefficients.

A rational polyhedron $P \subseteq \mathbb{R}^n$ has *facet complexity* at most ϕ if it admits a representation

$$P = \{x \in \mathbb{R}^n : Ax \leq b\}$$

in which every individual inequality, i.e., every i -th row of A together with the i -th coordinate of b , has encoding length at most ϕ . Notice that the facet complexity bounds the size of each inequality, rather than the number of inequalities.

We use the following standard small-solution property of systems of linear integer inequalities [11].

Theorem 2.1 (Small integer solution). *Let $P \subseteq \mathbb{R}^n$ be a rational polyhedron of facet complexity at most ϕ . If*

$$P \cap \mathbb{Z}^n \neq \emptyset,$$

then there exists $z \in P \cap \mathbb{Z}^n$ whose encoding length is polynomial in n and ϕ .

2.3 Polynomials and Roots of Unity

For $A \in \mathbb{Q}^{n \times n}$, its *characteristic polynomial* is

$$\chi_A(x) = \det(xI - A) \in \mathbb{Q}[x].$$

A complex number λ is an eigenvalue of A if and only if $\chi_A(\lambda) = 0$.

For an algebraic number λ , its *minimal polynomial over $\mathbb{Q}$* is the unique monic irreducible polynomial $m_\lambda \in \mathbb{Q}[x]$ such that $m_\lambda(\lambda) = 0$. If $f \in \mathbb{Q}[x]$ satisfies $f(\lambda) = 0$, then $m_\lambda \mid f$.

A complex number λ is a *root of unity* if $\lambda^k = 1$ for some $k \geq 1$. Its *order* is the least such k ; equivalently, λ is a primitive k -th root of unity.

The k -th *cyclotomic polynomial* $\Phi_k(x)$ is the monic polynomial whose roots are precisely the primitive k -th roots of unity. We use the following standard properties of cyclotomic polynomials:

1. $\Phi_k(x) \in \mathbb{Z}[x]$ and Φ_k is irreducible over $\mathbb{Q}$;
2. $\Phi_k(x) = \prod_{\substack{1 \leq l \leq k \\ \gcd(l, k) = 1}} (x - e^{(2\pi i)l/k})$;
3. $x^N - 1 = \prod_{k \mid N} \Phi_k(x)$;
4. Distinct cyclotomic polynomials are relatively prime.

Consequently, if λ is a primitive k -th root of unity, then Φ_k is the minimal polynomial of λ over $\mathbb{Q}$.

2.4 Polynomial Remainders

Let $P(x) \in \mathbb{Z}[x]$ be monic and let $G(x) \in \mathbb{Z}[x]$. The remainder of G modulo P , denoted by $\text{rem}_P(x)(G(x))$, is the unique polynomial $R(x)$ satisfying

$$G(x) = S(x)P(x) + R(x), \quad \deg R < \deg P.$$

Since P is monic, both $S(x)$ and $R(x)$ have integer coefficients.

2.5 The Class Σ_2^P

The class Σ_2^P is the second level of the polynomial hierarchy, which is contained in PSPACE. A decision problem L belongs to Σ_2^P if there exists a polynomial p and a polynomial-time decidable predicate R such that

$$x \in L \iff \exists y \in \{0, 1\}^{p(|x|)} \forall z \in \{0, 1\}^{p(|x|)} R(x, y, z).$$

Equivalently, $\Sigma_2^P = \text{NP}^{\text{NP}}$.

3 Affine Single-path linear-constrained loops

Definition 3.1. Let $A \in \mathbb{Q}^{n \times n}$ be a matrix. The *maximal period* of A , denoted by $G \in \mathbb{N}$, is defined as

$$G = \text{lcm}\{g \mid A \text{ has an eigenvalue that is a primitive } g\text{-th root of unity}\}.$$

If A has no eigenvalues that are roots of unity, we set $G = 1$.

We use the following known result [5].

Lemma 3.2. *The space of periodic vectors of A is generated by eigenvectors of A that correspond to eigenvalues that are roots of unity.*

Lemma 3.3. *Let $A \in \mathbb{Q}^{n \times n}$ have maximal period G . Then the period of every periodic vector of A divides G .*

Proof. Let v be a periodic vector of A and let p be its period, i.e., p is the least positive integer such that $A^p v = v$.

By Lemma 3.2, v can be written as $v = v_1 + \dots + v_l$, where $v_1, \dots, v_l$ are non-zero eigenvectors of A corresponding to root-of-unity eigenvalues $\lambda_1, \dots, \lambda_l$. We may assume that $\lambda_1, \dots, \lambda_l$ are pairwise distinct (if $v = 0$, then $l = 0$). Let g_i be the order of λ_i , i.e., let λ_i be a primitive g_i -th root of unity.

Since eigenvectors corresponding to distinct eigenvalues are linearly independent, for every $t \geq 1$, $A^t v = v$ if and only if $\lambda_i^t = 1$ for every $1 \leq i \leq l$. Consequently, the least positive t such that $A^t v = v$ is $\text{lcm}(g_1, \dots, g_l)$, and hence $p = \text{lcm}(g_1, \dots, g_l)$. By the definition of G , every g_i divides G , and therefore $p \mid G$. $\square$

Definition 3.4. Let $A \in \mathbb{Q}^{n \times n}$, and let $g_1, \dots, g_k$ be the distinct orders of the root-of-unity eigenvalues of A . The *cyclotomic product* of A is the polynomial

$$P_A(x) = \prod_{i=1}^k \Phi_{g_i}(x),$$

If A has no root-of-unity eigenvalues, we set $P_A(x) = 1$.

Lemma 3.5. *Let $A \in \mathbb{Q}^{n \times n}$, and let $P_A(x)$ be its cyclotomic product.*

Then P_A is a monic, square-free polynomial in $\mathbb{Z}[x]$, $\deg P_A \leq n$, $P_A(x) \mid \chi_A(x)$, and

$$\ker(P_A(A)) = \{v \in \mathbb{C}^n \mid A^t v = v \text{ for some } t \geq 1\}.$$

Proof. Every cyclotomic polynomial is monic and belongs to $\mathbb{Z}[x]$, and distinct cyclotomic polynomials are relatively prime. Hence P_A is monic, square-free, and belongs to $\mathbb{Z}[x]$.

If λ is a primitive g_i -th root of unity and an eigenvalue of A , then Φ_{g_i} is the minimal polynomial of λ over $\mathbb{Q}$, and therefore $\Phi_{g_i} \mid \chi_A$. Since the factors Φ_{g_i} are pairwise relatively prime, $P_A \mid \chi_A$. Consequently, $\deg P_A \leq \deg \chi_A = n$.

Let v be periodic. By Lemma 3.2, v is a linear combination of eigenvectors corresponding to root-of-unity eigenvalues. If u is such an eigenvector with eigenvalue λ of order g , then Φ_g is a factor of P_A , and hence $P_A(A)u = P_A(\lambda)u = 0$. Therefore $P_A(A)v = 0$.

Conversely, G be a maximal period of A . Since every g_i divides G , $\Phi_{g_i}(x) \mid x^G - 1$ for every i . As these factors are pairwise relatively prime, $P_A(x) \mid x^G - 1$. Thus if $P_A(A)v = 0$, then $(A^G - I)v = 0$ so v is periodic. $\square$

For every $i \geq 0$, let $R_{A,i}(x) = \text{rem}_{P_A(x)}(x^i)$. We call $R_{A,i}$ the i -th *remainder polynomial* of A .

Lemma 3.6. *Let $r = \deg P_A$ and let v be a periodic vector of A . Then, for every $i \geq 0$, $A^i v = R_{A,i}(A)v$.*

Moreover, if $v, Av, \dots, A^{r-1}v$ are integer vectors, then $A^i v \in \mathbb{Z}^n$ for every $i \geq 0$.

Proof. By polynomial division, $x^i = S_i(x)P_A(x) + R_{A,i}(x)$ for some polynomial S_i . Since v is periodic, Lemma 3.5 gives $P_A(A)v = 0$, and therefore $A^i v = R_{A,i}(A)v$.

Since P_A is monic and has integer coefficients, the equality $P_A(A)v = 0$ expresses $A^r v$ as an integer linear combination of $v, Av, \dots, A^{r-1}v$. Multiplying this equality by successive powers of A shows inductively that every later iterate is an integer linear combination of the preceding r iterates. Hence $A^i v \in \mathbb{Z}^n$ for every $i \geq 0$. $\square$

Lemma 3.7. *Let $A \in \mathbb{Q}^{n \times n}$. The coefficients of $P_A(x)$ and of $R_{A,i}(x)$, for every $i \geq 0$, have bit-length polynomial in n .*

Proof. Bound for P_A . Let $r = \deg P_A \leq n$. Since P_A is a monic polynomial of degree r whose roots all have absolute value 1, it can be written as $P_A(x) = \prod_{j=1}^r (x - \sigma_j)$, where $|\sigma_j| = 1$. Hence, every coefficient of P_A has absolute value at most $\binom{r}{j} \leq 2^r \leq 2^n$. Since $P_A \in \mathbb{Z}[x]$, its coefficients have bit-length $O(n)$.

Bound for $R_{A,i}$. Fix $i \geq 0$ and write $R_{A,i}(x) = q_0 + q_1 x + \dots + q_{r-1} x^{r-1}$. Let $\sigma_1, \dots, \sigma_r$ be the distinct roots of P_A and consider the Vandermonde matrix

$$W = \begin{pmatrix} 1 & \sigma_1 & \sigma_1^2 & \dots & \sigma_1^{r-1} \\ 1 & \sigma_2 & \sigma_2^2 & \dots & \sigma_2^{r-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \sigma_r & \sigma_r^2 & \dots & \sigma_r^{r-1} \end{pmatrix}.$$

Since $P_A(\sigma_t) = 0$ and $R_{A,i}$ is the remainder of x^i modulo P_A , we have $R_{A,i}(\sigma_t) = \sigma_t^i$. Thus,

$$W \begin{pmatrix} q_0 \\ \vdots \\ q_{r-1} \end{pmatrix} = \begin{pmatrix} \sigma_1^i \\ \vdots \\ \sigma_r^i \end{pmatrix}.$$

By Cramer's rule, $q_j = \det(W_j) / \det(W)$, where W_j is obtained from W by replacing its j -th column by $(\sigma_1^i, \dots, \sigma_r^i)^T$. Every entry of W_j has absolute value 1, and therefore $|\det(W_j)| \leq r!$.

Moreover,

$$(\det W)^2 = \prod_{1 \leq s < t \leq r} (\sigma_s - \sigma_t)^2,$$

which is the discriminant of P_A . Since P_A is a square-free polynomial with integer coefficients, its discriminant is a non-zero integer [4, Sec. 3.3.2]. Hence $|\det W| \geq 1$.

Therefore $|q_j| \leq r! \leq n!$. Since $R_{A,i}(x) \in \mathbb{Z}[x]$, every coefficient of $R_{A,i}$ has bit-length $O(n \log n)$. $\square$

Lemma 3.8. *Let $\mathcal{R}$ be a linear integer SLC of dimension n and coefficients of bit-length at most Δ . If $\mathcal{R}$ has a cyclic state, it also has a cyclic state of bit-length polynomial in n and Δ .*

Proof. Let $\mathcal{R}$ be of the form

$$\textbf{while } (Cv \leq d) \textbf{ do } v' := Av.$$

Let P_A be the cyclotomic product of A , let $r = \deg P_A$, and let $R_{A,i}(x)$ be the i -th remainder polynomial of A .

If $r = 0$, then $P_A = 1$, and by Lemma 3.5 the only periodic vector is 0. Hence, if a cyclic state exists, then 0 is cyclic and the statement follows. Assume therefore that $r \geq 1$.

By Lemmas 3.3, 3.5 and 3.6, a vector $v \in \mathbb{Z}^n$ is cyclic if and only if $P_A(A)v = 0$, $v, Av, \dots, A^{r-1}v$ are integer vectors, and

$$CR_{A,i}(A)v \leq d$$

for every $0 \leq i < G$, where G is the maximal period of A .

We express these conditions as a system of linear constraints over integer vectors $v_0, \dots, v_{r-1}$. We require $v_{j+1} = Av_j$ for every $0 \leq j < r-1$, $P_A(A)v_0 = 0$, and

$$CR_{A,i}(A)v_0 \leq d$$

for every $0 \leq i < G$. Integer solutions of this system correspond exactly to cyclic states, with v_0 being the cyclic state.

By Lemma 3.7, the coefficients of P_A and of every $R_{A,i}$ have bit-length polynomial in n . Moreover, $\deg P_A \leq n$ and $\deg R_{A,i} < n$. Hence $P_A(A)$ and $R_{A,i}(A)$ involve only the powers $I, A, \dots, A^n$, whose entries have bit-length polynomial in n and Δ . Consequently, every individual equality or inequality in the system has bit-length polynomial in n and Δ .

The system has $nr \leq n^2$ integer variables. Although it may contain exponentially many guard inequalities, its facet complexity is polynomial in n and Δ . Therefore, by Theorem 2.1, if the system has an integer solution, then it has one of bit-length polynomial in n and Δ . In particular, v_0 has polynomial bit-length, which proves the claim. $\square$

Theorem 3.9. *Cycle detection for affine integer SLCs is in Σ_2^P .*

Proof. By homogenizing the affine update, it is enough to consider a linear integer SLC

$$\textbf{while } (Cv \leq d) \textbf{ do } v' := Av.$$

By Lemma 3.8, if the SLC has a cyclic state, then it has one whose bit-length is polynomial in the size of the input. We existentially guess such a vector $v \in \mathbb{Z}^n$.

Let P_A be the cyclotomic product of A , let $r = \deg P_A$, and let G be the maximal period of A . The polynomial P_A can be computed in polynomial time. Indeed, if $\Phi_g \mid \chi_A$, then

$\varphi(g) = \deg \Phi_g \leq n$, where φ is the Euler's totient function. Since $\varphi(g) \geq \sqrt{g/2}$, we have $g \leq 2n^2$. Hence it is enough to consider $1 \leq g \leq 2n^2$, construct Φ_g , and test whether $\Phi_g \mid \chi_A$. The maximal period G is then the least common multiple of the corresponding values of g .

Moreover, there are at most n such values of g , and therefore $G \leq (2n^2)^n$. In particular, G and every $i < G$ have bit-length polynomial in n .

We first check that v is periodic by testing $P_A(A)v = 0$. We also check that $A^j v \in \mathbb{Z}^n$ for every $0 \leq j < r$. These conditions are polynomial-time checkable, since $r \leq n$. By Lemma 3.6, they imply that every iterate $A^j v$ is an integer vector.

It remains to check the guard along the orbit. By Lemma 3.3, the period of v divides G , so it is enough to check the first G positions. For a given $0 \leq i < G$, let $R_{A,i}(x)$ be the i -th remainder polynomial of A . By Lemma 3.6, $A^i v = R_{A,i}(A)v$. Hence the guard at position i is equivalent to $CR_{A,i}(A)v \leq d$.

Given i in binary, $R_{A,i}$ can be computed in polynomial time by repeated squaring of x modulo P_A . By Lemma 3.7, all reduced polynomials occurring in this computation have coefficients of polynomial bit-length. Since $\deg R_{A,i} < r \leq n$, the value $R_{A,i}(A)v$ and the inequality $CR_{A,i}(A)v \leq d$ can therefore be computed and checked in polynomial time.

Consequently, there exists a polynomial-time predicate R such that

$$\mathcal{R} \text{ has a cycle} \iff \exists v \forall i R(\mathcal{R}, v, i),$$

where v has polynomial bit-length and i ranges over binary strings of length $\lceil \log_2(G+1) \rceil$. The predicate R checks the periodicity and integrality conditions above and the inequality $CR_{A,i}(A)v \leq d$.

Thus, by the $\exists\forall$ characterization of Σ_2^P , cycle detection belongs to Σ_2^P . $\square$

4 Conclusion

We studied cycle detection for affine single-path linear-constrained loops over the integers and showed that the problem belongs to Σ_2^P . The proof combines a characterization of periodic vectors through cyclotomic factors of the update matrix with a polynomial bound on the bit-length of cyclic witnesses. Although a cycle may have exponentially large period, its positions can be represented and checked using polynomial-size remainder polynomials.

These results provide further evidence that cycle detection can be more tractable than full termination. An important direction for future work is to determine whether the Σ_2^P upper bound is tight and to study cycle detection for more general classes of linear-constrained loops.

References

- [1] Amir M. Ben-Amram, Samir Genaim, Joël Ouaknine, and James Worrell. Termination analysis of linear-constraint programs, 2025.
- [2] Mark Braverman. Termination of integer linear programs. In Thomas Ball and Robert B. Jones, editors, *Computer Aided Verification*, pages 372–385, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
- [3] Mishel Carelli. Loop Termination and Generalized Collatz Sequences. In Sayan Bhattacharya, Danupon Nanongkai, Michael Benedikt, and Gabriele Puppis, editors, *53rd International Colloquium on Automata, Languages, and Programming (ICALP 2026)*, volume 374 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 175:1–175:21, Dagstuhl, Germany, 2026. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

- [4] Henri Cohen. A course in computational algebraic number theory. In *Graduate texts in mathematics*, 1993.
- [5] Karl-G. Grosse-Erdmann and Alfred Peris Manguillot. *Linear Chaos*. Universitext. Springer, 2011.
- [6] Marcel Hark, Florian Frohn, and Jürgen Giesl. Termination of triangular polynomial loops, 2024.
- [7] M Hosseini. *On termination and divergence of linear programs*. PhD thesis, University of Oxford, 2021.
- [8] Mehran Hosseini, Joël Ouaknine, and James Worrell. Termination of Linear Loops over the Integers. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, volume 132 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 118:1–118:13, Dagstuhl, Germany, 2019. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.
- [9] Radu Iosif and Arnaud Sangnier. How hard is it to verify flat affine counter systems with the finite monoid property? In Cyrille Artho, Axel Legay, and Doron Peled, editors, *Automated Technology for Verification and Analysis*, volume 9938 of *Lecture Notes in Computer Science*, pages 89–105. Springer, 2016.
- [10] Andreas Podelski and Andrey Rybalchenko. A complete method for the synthesis of linear ranking functions. In *Verification, Model Checking, and Abstract Interpretation, 5th International Conference, VMCAI 2004, Venice, Italy, January 11-13, 2004, Proceedings*, volume 2937, pages 239–251, 01 2004.
- [11] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, 1986.
- [12] A. Tiwari. Termination of linear programs. In R. Alur and D. Peled, editors, *Computer-Aided Verification, CAV*, volume 3114 of *LNCS*, pages 70–82. Springer, July 2004.