University of Freiburg
Department of Computer Science
Chair of Software Engineering

Ranking Function Synthesis for Linear Lasso Programs

Master's Thesis[1]

Jan Leike

June 30, 2013

Supervisor:
Prof. Dr. Andreas Podelski

[1]This is an error-corrected version of the original thesis, updated last on November 6, 2013.

Abstract

The scope of this work is the constraint-based synthesis of termination arguments for the restricted class of programs called *linear lasso programs*. A termination argument consists of a ranking function as well as a set of supporting invariants.

We extend existing methods in several ways. First, we use Motzkin's Transposition Theorem instead of Farkas' Lemma. This allows us to consider linear lasso programs that can additionally contain strict inequalities. Existing methods are restricted to non-strict inequalities and equalities.

Second, we consider several kinds of ranking functions: affine-linear, piecewise and lexicographic ranking functions. Moreover, we present a novel kind of ranking function called *multiphase ranking function* which proceeds through a fixed number of phases such that for each phase, there is an affine-linear ranking function. As an abstraction to the synthesis of specific ranking functions, we introduce the notion *ranking function template*. This enables us to handle all ranking functions in a unified way.

Our method relies on non-linear algebraic constraint solving as a subroutine which is known to scale poorly to large problems. As a mitigation we formalize an assessment of the difficulty of our constraints and present an argument why they are of an easier kind than general non-linear constraints.

We prove our method to be complete: if there is a termination argument of the form specified by the given ranking function template with a fixed number of affine-linear supporting invariants, then our method will find a termination argument.

To our knowledge, the approach we propose is the most powerful technique of synthesis-based discovery of termination arguments for linear lasso programs and encompasses and enhances several methods having been proposed thus far [4, 18, 27].

Contents

Chapter 1

Introduction

Software verification as a branch of computer science studies the automatic derivation of correctness properties of computer programs. Termination is the property that no infinite program execution is possible. In this work we focus on the automatic discovery of a termination argument given a program of a specific form. Whether a given program terminates is undecidable according to the Halting Problem. Hence there is no algorithm that finds a termination argument for *every* terminating program. Because of this, we content ourselves with considering *linear lasso programs*. Linear lasso programs consist of a *stem* followed by a *loop*. Stem and loop each are boolean combinations of affine-linear constraints. For an example, see Figure 1.1.

$$
\begin{array}{l}
\textbf{assume}\,(\,y > 1\,)\,; \\
\textbf{while}\;\;(\,q \geq 0\,)\colon \\
\qquad q \;:=\; q - y\,; \\
\qquad y \;:=\; y + 1\,;
\end{array}
\qquad\qquad
\begin{aligned}
\textsc{stem}(q, y) &\equiv y > 1 \\
\textsc{loop}(q, y, q', y') &\equiv q \geq 0 \;\wedge\; q' = q - y \\
&\qquad\qquad \wedge\; y' = y + 1
\end{aligned}
$$

Figure 1.1: A linear lasso program given as program code (left) and its translation as stem and loop transition in linear arithmetic (right).

Lasso programs usually do not occur as stand-alone programs; rather, they are encountered when a finite representation of an infinite path in a control flow graph is needed. For example, in (potentially spurious) counter-examples in termination analysis [11, 16, 22, 23], non-termination analysis [15], stability analysis [10, 28], or cost analysis [1, 14].

In this work we build constraints from the given program code, such that a termination argument for this program can be computed via constraint solving. The method we propose is more powerful than any other constraint-based synthesis of termination arguments for linear lasso programs proposed thus far (see Section 1.1 for an assessment).

First, by using Motzkin's Transposition Theorem instead of Farkas' Lemma, we are able to handle lasso programs that contain both strict and non-strict inequalities. (For example, the program in Figure 1.1 contains the strict inequality $y > 1$ in the stem and only non-strict inequalities in the loop transi-

tion.) Existing methods disallowed strict inequalities or sometimes resorted to the workaround of replacing a strict inequality $a > b$ by $a \geq b + 1$, which only works for integer domains.

Second, instead of focusing on one type of ranking function, we use several templates for ranking functions (e.g., affine-linear or lexicographic ranking functions). For this, we introduce the notion of a *ranking function template* that enables formalization of ranking functions of various kinds, including the aforementioned ones. When given a linear lasso program, we can prove its termination by trying many different kinds of templates available by repeating our method for each of them.

Furthermore, we present a novel ranking function that we call *multiphase ranking function*. This ranking function proceeds through a fixed finite number of phases, before terminating. Each phase is ranked by an affine-linear function; when this function becomes non-positive, we transition to the next phase. These multiphase ranking functions can be seen to be orthogonal to lexicographic ranking functions: if a program has a lexicographic ranking function, it generally does not have a multiphase ranking function, or vice versa. We give various examples of programs that have a multiphase ranking function.

$$\begin{array}{l} \textbf{while}\ \ (q \geq 0):\\ \quad q\ :=\ q - y;\\ \quad y\ :=\ y + 1; \end{array} \qquad \begin{array}{l} f_1(q, y) = 1 - y\\ f_2(q, y) = q + 1 \end{array}$$

Figure 1.2: An execution of this linear lasso program can be split into two phases: first y increases until it is positive, then q decreases until the loop condition $q \geq 0$ is violated. We can discover the affine-linear functions f_1 and f_2. Together, they form a multiphase ranking function where f_1 corresponds to phase one and f_2 corresponds to phase two.

Our constraint-based synthesis method can be summarized as follows. The input is a linear lasso program as well as a linear ranking function template. The template yields a formula, which we augment by adding constraints for affine-linear inductive supporting invariants. These invariants contain information from the program stem that may be indispensable to the program's termination proof. Next, five equivalence transformations are applied to the constraints, the last of which is given by Motzkin's Theorem. The last transformation removes any universal quantifiers. The resulting constraints are then passed to an SMT solver which checks them for satisfiability; a positive result implies that the program terminates. Furthermore, a satisfying assignment will yield the supporting invariants and a ranking function. These form a termination argument for the given linear lasso program and thus can be used by another tool [1, 10, 14, 11, 15, 16, 22, 23, 28].

In addition to being sound, our method is complete in the following sense. If there is a termination argument in form of a fixed number of affine-linear supporting invariants and a ranking function of the form specified by the given ranking function template, then our method will discover a termination argument. In other words, the existence of a solution is never lost in the process of transforming the constraints.

Our method applies to linear lasso programs of rational and real variable domains. While it is feasible to use it for integer domains, it is not complete for integers. The main reason is that Motzkin's Theorem does not hold over the integers. In fact, the discovery of affine-linear ranking functions for lasso programs without stem is already co-NP-complete [2].

In contrast to some related methods [18, 27], which we extend in this work, the constraints we generate are not linear, but rather non-linear algebraic constraints. Solving these constraints is decidable, but requires exponential time and space [13]. Much progress on non-linear SMT solvers has been made and present-day algorithms routinely solve non-linear constraints of various sizes [21]. *Cylindrical algebraic decomposition* (CAD) seems to be the most successful practical method in these endeavors.

We will argue that the constraints we generate generally are not as wicked as non-linear constraints can possibly be. We assess the number of variables that need to be assigned to make the constraints linear. For this we introduce the notion of *suitable colorings* for ranking function templates. This is a criterion that states which of the Motzkin coefficients that occur in non-linear operations we can eliminate from the final constraints. Moreover, we provide several other optimizations that reduce the number of these variables. Additionally, for the CAD algorithm we exemplarily discuss why in practical cases, we can find assignments for invariants in polynomial time.

The contributions of this work can be summarized as follows.

- The use of Motzkin's Theorem instead of Farkas' Lemma enables strict inequalities in linear lasso programs.
- The novel multiphase ranking function is presented.
- We handle synthesis of different types of ranking functions in a unified way using our notion of ranking function templates.
- The number of variables occurring in non-linear operations in the generated constraints is assessed for every ranking function template we present.
- We argue why solving our non-linear constraints is not terribly difficult.

1.1 Related Work

Tiwari showed that termination is decidable for deterministic stem-free linear lasso programs of the form

$$\texttt{while}(Bx > b)\ \ x\texttt{:=}Ax + c\texttt{;}$$

where $Bx > b$ is a conjunction of affine-linear constraints and $Ax+c$ is an affine-linear transition function [33]. This result is based on eigenvector analysis of the involved matrix A. Braverman extends this result and proves the decidability of lasso programs of the following form [6]:

$$\texttt{while}(B_s x > b_s \wedge B_w x \geq b_w)\ \ x\texttt{:=}Ax + c\texttt{;}$$

where the matrices and vectors are rational and variables have rational or real domain. Moreover, this class of lasso programs also admits decidable termination analysis over integer domain for the homogeneous case where $b_s, b_w, c = 0$.

Ben-Amram et al. show that linear lasso programs with integer domain have undecidable termination if the loop's coefficients are from $\mathbb{Z} \cup \{r\}$ for an arbitrary irrational number r [3].

For constraint-based synthesis of termination arguments for various classes of linear lasso programs, Farkas' Lemma has been extensively used [4, 5, 9, 18, 27, 29, 30], although always in its affine form.

The first complete method of ranking function synthesis for linear lasso programs through constraint solving was due Podelski and Rybalchenko [27]. Their approach only considers lasso programs without stem and termination arguments in form of an affine-linear ranking function and requires only linear constraint solving.

The idea of generating affine-linear inductive invariants via Farkas' Lemma-transformed constraints is first presented by Colón et al. [9]. We will take the same approach when generating inductive supporting invariants. This method relies on non-linear constraint solving and some of the same authors explore an under-approximation technique for solving these [30].

Bradley, Manna and Sipma propose a similar approach for linear lasso programs [4]. They introduce affine-linear inductive supporting invariants to handle the stem. Their termination argument is a lexicographic ranking function with each component corresponding to one loop disjunct. This not only requires non-linear constraint solving, but also an ordering on the loop disjuncts. The authors extend this approach in [5] by the use of *template trees*. These trees allow each lexicographical component to have a ranking function that decreases not necessarily in every step, but *eventually*. This bears some resemblance to multiphase ranking functions.

Heizmann et al. extend the method of Podelski and Rybalchenko [18]. They are the first to introduce the notion of lasso programs. Utilizing supporting invariants analogously to Bradley et al., they synthesize affine-linear ranking functions. Due to their restriction to non-decreasing invariants, the generated constraints are linear.

A collection of example-based explanations of constraint-based verification techniques can be found in [29]. This includes the generation of ranking functions, interpolants, invariants, resource bounds and recurrence sets.

In [2] Ben-Amram and Genaim discuss the synthesis of linear ranking functions for integer lasso programs without stem. They prove that this problem is generally co-NP-complete and continue considering several special cases which admit a polynomial time complexity.

1.2 Structure

This work is divided into eight chapters. After this introductory chapter, in Chapter 2 we recapitulate the mathematical foundations for ordinal numbers, formal logic and linear arithmetic including Motzkin's Transposition Theorem. Following this, we formally define linear lasso programs, invariants and notions related to termination in Chapter 3. This chapter concludes with a proof that termination of linear lasso programs is undecidable.

In Chapter 4 we introduce the notion of linear ranking function templates and formalize a way for turning synthesized affine-linear functions into ranking

functions. We discuss the multiphase ranking function template and three other relevant templates and their properties.

Given a linear lasso program and a linear ranking function template, we describe in Chapter 5 how to build the constraints whose solutions are the termination argument. We analyze the difficulty of the generated constraints—the *non-linear dimension* in Chapter 6. We will prove a criterion that enables us to reduce the number of variables that occur in non-linear operations in the constraints. In Chapter 7 we discuss some methods for solving the constraints and their computational complexity. We motivate with help of the cylindrical algebraic decomposition of parts of the constraints that solving them is not necessarily difficult in practice, despite the poor worst-case time complexity of non-linear SMT solvers. Finally, our results are summarized in Chapter 8.

This work is meant to be read in a linear fashion, each chapter building on the results of the previous ones. Our most important results are stated in chapters 3, 4, 5 and 6.

Chapter 2

Preliminaries

In this chapter we introduce the required mathematical concepts from set theory, formal logic and selected results from linear programming. We also dedicate Section 2.4 to Motzkin's Transposition Theorem.

2.1 Well-orderings and Ordinal Numbers

The definitions and results of this section are standard knowledge in the mathematical branch of set theory [24].

Definition 2.1 (Well-ordered set)**.** A strict linear ordering $<$ on a set X is a *well-ordering* iff every non-empty subset of X has a $<$-minimal element.

Definition 2.2 (Ordinals)**.** A set α is called *ordinal number* or *ordinal* iff

- $\beta \in \alpha$ implies $\beta \subset \alpha$, and
- $\in$ (set membership) is a well-ordering on α.

We denote the collection of all ordinals with **On**.

Ordinal numbers are a method of counting indefinitely. The first ordinal is $\emptyset$ and for every ordinal α the successor is $\{\alpha\} \cup \alpha$. Furthermore, the union of a collection of ordinals is again an ordinal, therefore we can take the supremum of a collection of ordinals via set union.

Ordinals that are not successors are called *limit ordinals*. The first limit ordinal is ω. We can define addition, multiplication and exponentiation for ordinals coinciding with these operations on the natural numbers (however, in general addition and multiplication are not commutative). This yields

$$\omega + \omega = \omega \cdot 2, \qquad \sup\{\omega \cdot k \mid k \in \omega\} = \omega^2.$$

We get the sequence

$$0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \ldots, \omega^2, \omega^2 + 1, \ldots.$$

Note that there is such a vast number of ordinals that **On** cannot be a set[1]. Nevertheless, for purposes of computer science, we are content with the set of

[1] If **On** was a set, it would be an ordinal according to Definition 2.2 and hence contain itself. This is a contradiction to the well-foundedness of set theory.

countable ordinals. This justifies the usage of **On** like a set, for example as a codomain of functions.

Every well-ordered set is isomorphic to an ordinal number. In this sense the ordinals are the 'mothers of all well-orderings'. This motivates why we may consider ordinals instead of arbitrary well-ordered sets.

Lemma 2.3 (Well-orderings and ordinals)**.** *For every well-ordered set $(X, <)$ there is a unique ordinal α and a bijection $f : X \to \alpha$ such that $x < y$ iff $f(x) \in f(y)$ for every $x, y \in X$.*

Proof. See the literature on set theory, e.g. [24]. □

2.2 First-order Logic

We present a short introduction to first-order logic [12] and the notation we use in this work. Given a set S containing constants, function and relation symbols, we define *terms* and *formulae* of first order logic for S recursively. Every variable and constant is an S-term, and so is the application of an n-ary function symbol to a sequence of n terms. The application of an n-ary relation symbol to n S-terms constitute *atomary* S-formulae (atoms). Formulae can be joined together using boolean connectives $\neg, \wedge, \vee, \rightarrow$, and quantified using universal ($\forall$) and existential ($\exists$) quantifiers followed by the quantified variable. Variables that are not bound by quantifiers in a formula φ are called *free variables of* φ. We use the convention that quantifiers bind weakly (until the end of the line), and $\wedge$ and $\vee$ have precedence over $\rightarrow$; negation ($\neg$) is the strongest connective.

An S-structure $\mathfrak{A} = (A, (Z^{\mathfrak{A}})_{Z \in S})$ consists of a set A called the *universe of* $\mathfrak{A}$, and an interpretation $Z^{\mathfrak{A}}$ of every symbol Z in S. If an S-formula φ holds in a S-model $\mathfrak{A}$, we say $\mathfrak{A}$ *models* φ and write $\mathfrak{A} \models \varphi$. An S-formula φ is *satisfiable* iff an S-structure exists that models φ. If φ is modeled by all S-structures, we call φ *valid* and write $\models \varphi$. Given a set of S-formulae T, we write $T \models \varphi$ iff $\mathfrak{A} \models \varphi$ for every S-structure $\mathfrak{A}$ that models each $\psi \in T$. If two S-structures $\mathfrak{A}$ and $\mathfrak{B}$ model the same S-formulae, we call $\mathfrak{A}$ and $\mathfrak{B}$ *elementarily equivalent*.

In this work we entertain a special interest in *linear arithmetic* $S_{\text{linear}} = \{0, 1, +, -, \leq, =\}$ and *non-linear arithmetic* $S_{\text{non-linear}} = \{0, 1, +, -, \cdot, \leq, =\}$, where 0 and 1 are constants, $+$, $-$, $\cdot$ are binary function symbols and $\leq$, $=$ are binary relations. The usual axioms concerning ordered rings apply. Structures we consider are the rationals $\mathbb{Q}$ and the reals $\mathbb{R}$ together with the usual interpretations of 0, 1, $+$, $-$, $\cdot$, $\leq$ and $=$ as well as their elementary equivalents. Structures elementarily equivalent to the reals are called *real closed fields*; an example of a real closed field are the real algebraic numbers (the field of roots of rational polynomials).

Given an S-formulae φ, an *satisfiability modulo theory solver* (SMT solver) is a software tool that determines whether φ holds in an specific S-structure (e.g. $\mathbb{Q}$ or $\mathbb{R}$). If it does, the solver outputs a valuation to the free variables of φ. We call the input φ the *constraint* to the solution.

For notational simplicity, and if the structure $\mathfrak{A}$ is clear from context, we identify formulae with the sets they generate. A formula φ containing n free variables $x_1, \ldots, x_n$, is identified with the set

$$\{(x_1, \ldots, x_n) \in A^n \mid \mathfrak{A} \models \varphi(x_1, \ldots, x_n)\}.$$

For later use, we state the Compactness Theorem for first order logic [12].

Theorem 2.4 (Compactness)**.** *A set of formulae T is satisfiable if and only if every finite subset of T is satisfiable.*

2.3 Linear Arithmetic

For the remainder of this work, fix $\mathbb{K}$ to be the field of rational numbers $\mathbb{Q}$ or any real closed field, such as the real numbers $\mathbb{R}$. We use the vector x to denote the variables $x_1, \ldots, x_n$. By convention, all vectors are column vectors. For a vector v, the *transpose* will be denoted as v^T. A function $f : \mathbb{K}^n \to \mathbb{K}$ is called *affine-linear* (or simply *affine*) iff $f(x) = c^T x + d$ for some vector $c \in \mathbb{K}^n$ and some number $d \in \mathbb{K}$. We call inequalities of the form $a < b$ *strict inequalities* and inequalities of the form $a \leq b$ *non-strict inequalities*. When either comparison operator could apply to an equation, we use the symbol $\lhd$.

Given a matrix $A \in \mathbb{K}^{m \times n}$ and a vector $b \in \mathbb{K}^m$, the inequality $Ax \leq b$ denotes the conjunction of the linear inequalities

$$\bigwedge_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} x_j \leq b_i$$

where $a_{i,j}$ denotes the entry of the matrix A in row i and column j. If we understand these constraints as the set of vectors $\{x \in \mathbb{K}^n \mid Ax \leq b\}$, they form a convex subset of $\mathbb{K}^n$ called a *polyhedron*.

2.4 Motzkin's Transposition Theorem

Intuitively, Motzkin's Transposition Theorem states that a given system of linear inequalities has no solution if and only if a contradiction can be derived via a positive linear combination of the equations.

Motzkin's Theorem will be used in this work to equivalently transform universally quantified formulae into existential ones. Additionally, as a side effect, the number of non-linear multiplications (multiplications of two variables) will be greatly reduced.

Theorem 2.5 (Motzkin's Transposition Theorem [31])**.** *Let $A \in \mathbb{K}^{m \times n}$, $B \in \mathbb{K}^{\ell \times n}$, $b \in \mathbb{K}^m$, and $d \in \mathbb{K}^\ell$. (M1) and (M2) are equivalent.*

$$\forall x \in \mathbb{K}^n.\ \neg(Ax \leq b \ \wedge\ Bx < d) \tag{M1}$$

$$\begin{aligned} \exists \lambda \in \mathbb{K}^m\ \exists \mu \in \mathbb{K}^\ell.\ & \lambda \geq 0 \ \wedge\ \mu \geq 0 \\ & \wedge\ \lambda^T A + \mu^T B = 0 \ \wedge\ \lambda^T b + \mu^T d \leq 0 \\ & \wedge\ (\lambda^T b < 0 \ \vee\ \mu \neq 0) \end{aligned} \tag{M2}$$

Note that the formula (M2) contains the disjunction $(\lambda^T b < 0 \vee \mu \neq 0)$. We call the case where $\mu = 0$ and $\lambda^T b < 0$ the *classical case*, because the formula coincides with the one of the classical version of Farkas' Lemma (Lemma 2.8). The other case will be called the *non-classical case*. Note that the equation $\mu \neq 0$ can equivalently be written as $\sum_i \mu_i > 0$ since μ is already constraint to non-negative entries.

The remainder of this section is dedicated to the proof of Motzkin's Theorem. We motivate this proof with two versions of Farkas' Lemma which easily follow from the strong duality theorem of linear programming [31]: an affine version (Lemma 2.7) and a classical version (Lemma 2.8). However, note that the literature typically takes the opposite route and uses Farkas' Lemma to prove the duality theorem [31].

Theorem 2.6 (Strong duality theorem)**.** *Let $A \in \mathbb{K}^{m\times n}$, $b \in \mathbb{K}^m$, and $c \in \mathbb{K}^n$. Define the linear programming problem $P = \{c^T x \mid Ax \leq b\}$ and its dual $D = \{b^T y \mid A^T y = c, y \geq 0\}$. If either of P or D is non-empty, then $\sup P = \inf D$.*

Proof. See the literature on linear programming, e.g. [31]. □

The duality theorem holds over the theory of the reals as well as the rationals. This is because a polyhedron defined by inequalities involving only rational coefficients has only rational vertices. If a linear programming problem (or its dual respectively) has an optimal solution, it always has a vertex as an optimal solution; hence there is a rational optimum [31].

Motzkin's Theorem states that a given system of linear inequalities has no solution (M1) if and only if a contradiction can be derived via a positive linear combination of the equations (M2). The two cases distinguished in the disjunction (M2) correspond to a contradiction derived using only non-strict inequalities (classical case) and a contradiction derived using at least one strict inequality (non-classical case).

The following affine version of Farkas' Lemma is usually applied instead of Motzkin's Theorem in the context of lasso programs [4, 5, 9, 18, 27, 29, 30]. Motzkin's Theorem can be seen as an adaption of Farkas' Lemma to allow for strict inequalities. Conversely, the classic Farkas' Lemma is a included in Motzkin's Theorem as the special case where $B = 0$ and $d = 0$.

Lemma 2.7 (Affine Farkas' Lemma)**.** *Let $A \in \mathbb{K}^{m\times n}$, $b \in \mathbb{K}^m$, $c \in \mathbb{K}^n$, and $\delta \in \mathbb{K}$ such that $Ax \leq b$ has a solution. Then the following two formulae are equivalent.*

$$\forall x \in \mathbb{K}^n.\ Ax \leq b \to c^T x \leq \delta$$
$$\exists \lambda \in \mathbb{K}^m.\ \lambda \geq 0\ \wedge\ \lambda^T A = c^T\ \wedge\ \lambda^T b \leq \delta$$

Proof. We reformulate Lemma 2.7 in terms of linear programming. Let P and D be as in Theorem 2.6.

$$\text{Let } P \neq \emptyset. \text{ Then } \sup P \leq \delta \text{ iff } \inf D \leq \delta.$$

If P is bounded, then D is feasible and by the strong duality theorem their solutions are equal. Conversely, if $\inf D \leq \delta$, then D is feasible and the strong duality theorem asserts that $\sup P \leq \delta$. □

Lemma 2.8 (Classic Farkas' Lemma)**.** *For all $A \in \mathbb{K}^{m\times n}$ and $b \in \mathbb{K}^m$ the following two formulae are equivalent.*

$$\forall x \in \mathbb{K}^n.\ \neg Ax \leq b$$
$$\exists \lambda \in \mathbb{K}^m.\ \lambda \geq 0\ \wedge\ \lambda^T A = 0\ \wedge\ \lambda^T b < 0$$

Proof. We proceed analogously to the proof of Lemma 2.7. Here P is infeasible, consequently its dual D is unbounded and thus attains some negative value. □

The following Lemma is of technical nature. We require it for the proof of Theorem 2.5.

Lemma 2.9 (Closure of polyhedra)**.** *Let* $X = \{x \in \mathbb{K}^n \mid Ax \leq b, Bx < d\} \neq \emptyset$. *The smallest closed set containing* X *is* $Y = \{x \in \mathbb{K}^n \mid Ax \leq b, Bx \leq d\}$.

Proof. Y contains X and is the finite intersection of closed half-spaces and therefore closed. We need to show that every point in $Y \setminus X$ is the limit of a sequence of points in X. Let $y \in Y \setminus X$ and since X is not empty, we can pick an $x \in X$. For $0 < t \leq 1$,

$$A(tx + (1-t)y) = tAx + (1-t)Ay \leq tb + (1-t)b = b,$$
$$B(tx + (1-t)y) = tBx + (1-t)By < td + (1-t)d = d.$$

We conclude that $tx + (1-t)y \in X$ for all $0 < t \leq 1$. But

$$\lim_{t \to 0} \big(tx + (1-t)y\big) = y,$$

therefore y is in the closure of X. □

Proof of Theorem 2.5. Either $Ax \leq b$ is inconsistent, then Lemma 2.8 states the equivalence of (M1) to the classical case (first disjunct) in (M2). Otherwise write

$$Bx \leq d \equiv \bigwedge_{i=1}^{\ell} b_i^T x \leq d_i.$$

There is a subset $S \subseteq \{b_i^T x < d_i \mid 1 \leq i \leq \ell\}$ such that $S \cup \{Ax \leq b\}$ is satisfiable, but $S \cup \{Ax \leq b\} \cup \{b_{i_0}^T x < d\}$ is not for some i_0. Write S as $B'x < d'$ for a submatrix B' of B and a subvector d' of d. (M1) is then equivalent to

$$\forall x.\ Ax \leq b \ \wedge\ B'x < d' \to -b_{i_0}^T x \leq -d_{i_0}. \tag{2.1}$$

This can be formulated as

$$X := \{x \mid Ax \leq b, B'x < d'\} \subseteq \{x \mid -b_{i_0}^T x \leq -d_{i_0}\} =: Z.$$

Z is a closed set, hence X is contained in Z iff the closure of X is. By Lemma 2.9, the closure of X is $\{x \mid Ax \leq b, B'x \leq d'\}$, we can therefore replace $B'x < d'$ with $B'x \leq d'$ in (2.1). $Ax \leq b \wedge B'x \leq d'$ is satisfiable by assumption, hence by Lemma 2.7, we get equivalently

$$\exists \lambda, \mu \geq 0.\ \lambda^T A + \mu^T B' = -b_{i_0}^T \ \wedge\ \lambda^T b + \mu^T d' \leq -d_{i_0}.$$

This yields an assignment for the non-classical case (second disjunct) in (M2).

Conversely, a contradiction derived from the inequalities makes $Ax \leq b \ \wedge$ $Bx < d$ unsatisfiable. Assume the non-classical case of (M2) holds and we have an $x^* \in \mathbb{K}^n$ such that $Ax^* \leq b$ and $Bx^* < d$. Then

$$\lambda^T Ax^* \leq \lambda^T b, \qquad \mu^T Bx^* < \mu^T d$$

since λ and μ have only non-negative entries. This yields the following contradiction.

$$0 \cdot x^* = (\lambda^T A + \mu^T B)x^* = \lambda^T Ax^* + \mu^T Bx^* < \lambda^T b + \mu^T d \leq 0 \qquad \square$$

Chapter 3

Lasso Programs

In Section 3.1 we introduce the notion of lasso programs and, more relevant to this work, linear lasso programs. Invariants and inductive invariants are presented in Section 3.2, as well as the motivation to stick to the latter when building the constraints. Finally, in Section 3.3 we define termination and ranking functions and conclude this chapter with a related undecidability result.

3.1 Definition

Definition 3.1 (Lasso program [18])**.** A *lasso program* $\mathbf{P} = (\text{STEM}, \text{LOOP})$ over the *domain* Σ consists of a set of initial states $\text{STEM} \subseteq \Sigma$ and a binary relation $\text{LOOP} \subseteq \Sigma \times \Sigma$.

Definition 3.2 (Semantics of lasso programs)**.** Let $\mathbf{P} = (\text{STEM}, \text{LOOP})$ be a lasso program over the domain Σ. A *state* of $\mathbf{P}$ is an element $\sigma \in \Sigma$. An *execution* of $\mathbf{P}$ is a (possibly infinite) sequence of states $\sigma_0\sigma_1 \ldots$ such that $\sigma_0 \in \text{STEM}$ and $(\sigma_i, \sigma_{i+1}) \in \text{LOOP}$ for all $i \geq 0$.

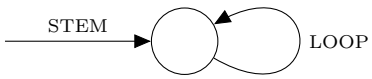


Figure 3.1: The name 'lasso program' is motivated by the shape of their transition graph.

In this work, we consider the following special case of lasso programs, namely those that have a linear specification for their stem and loop transitions, as in the following example.

Example 3.3. Consider the following lasso program $\mathbf{P}_{y \geq 1}$.

$$
\begin{array}{l}
\textbf{assume}\,(\,y = 1\,)\,; \\
\textbf{while}\,(\,q \geq 0\,)\,: \\
\qquad q \;:=\; q - y\,; \\
\qquad y \;:=\; y + 1\,;
\end{array}
$$

We can represent the stem and loop transition of $\mathbf{P}_{y\geq 1}$ with the following formulae.

$$
\begin{aligned}
\textsc{stem}(q, y) &\equiv y = 1 \\
\textsc{loop}(q, y, q', y') &\equiv q \geq 0 \;\wedge\; q' = q - y \;\wedge\; y' = y + 1
\end{aligned}
$$

An execution of $\mathbf{P}_{y\geq 1}$ is $\sigma_0\sigma_1\sigma_2$ where

$$
\begin{aligned}
&\sigma_0 : y \mapsto 1, q \mapsto 2, \\
&\sigma_1 : y \mapsto 2, q \mapsto 1, \text{ and} \\
&\sigma_2 : y \mapsto 3, q \mapsto -1.
\end{aligned}
$$

Since q is negative in σ_2, there is no possible successor state to σ_2.

Definition 3.4 (Linear lasso program)**.** A *linear lasso program* is a lasso program $\mathbf{P} = (\textsc{stem}, \textsc{loop})$ such that STEM and LOOP are defined by quantifier-free formulae of linear arithmetic. A linear lasso program is called *conjunctive*, iff STEM and LOOP contain no disjunctions and negations occur only before atoms.

Lemma 3.5 (Linear lasso program normal form)**.** *For all* linear lasso programs $\mathbf{P} = (\textsc{stem}, \textsc{loop})$*, the formulae* STEM *and* LOOP *can be written in the following normal form.*

$$
\begin{aligned}
\textsc{stem}(x) &\equiv \bigvee_{n\in N} \left(B_n x \leq b_n \;\wedge\; B'_n x < b'_n\right) \\
\textsc{loop}(x, x') &\equiv \bigvee_{m\in M} \left(A_m \tbinom{x}{x'} \leq c_m \;\wedge\; A'_m \tbinom{x}{x'} < c'_m\right)
\end{aligned}
$$

B_n, B'_n, A_m, and A'_m are matrices, b_n, b'_n, c_m, and c'_m are vectors, and N and M suitable finite index sets. The program $\mathbf{P}$ is conjunctive if and only if it has a normal form with $\#N = \#M = 1$.

Proof. We transform the formulae STEM and LOOP in negation normal form such that negations occur only before atoms. Then we rewrite negated atoms using the following identities.

$$
\neg a \leq b \equiv -b < -a \qquad \neg a < b \equiv -b \leq -a \qquad a \neq b \equiv a < b \;\vee\; a > b
$$

Additionally, *true* can be rewritten as $0 \leq 0$ and *false* as $0 \leq -1$. Finally, we transform obtained the formulae in disjunctive normal form. □

According to Lemma 3.5, STEM and LOOP correspond geometrically to a union of convex polyhedra (see Figure 3.2).

Example 3.6. The program $\mathbf{P}_{y\geq 1}$ from Example 3.3 is a conjunctive linear lasso program. Its normal form is

$$
\begin{aligned}
\textsc{stem}(q, y) &\equiv y \leq 1 \;\wedge\; -y \leq -1, \\
\textsc{loop}(q, y, q', y') &\equiv -q \leq 0 \;\wedge\; q' - q + y \leq 0 \;\wedge\; -q' + q - y \leq 0 \\
&\qquad \wedge\; y' - y - 1 \leq 0 \;\wedge\; -y' + y + 1 \leq 0.
\end{aligned}
$$

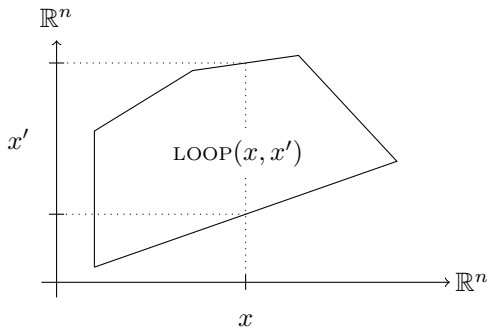


Figure 3.2: The loop transition of a conjunctive linear lasso program geometrically corresponds to a polyhedron. The n-dimensional state spaces $\mathbb{R}^n$ of x and x' are shown compactly as either axis. The successor state x' to a state x is chosen non-deterministically from the possible pairs $(x, x') \in \text{LOOP}$.

3.2 Invariants

Informally, an invariant is a property that always holds during program execution. Although our primary goal is to prove termination, the inference of invariants can uncover information critical to this goal. In Section 5.1 we will discuss how we involve invariants in the ranking function discovery process.

Definition 3.7 (Invariant)**.** A state $\sigma \in \Sigma$ of a lasso program $\mathbf{P}$ is *reachable* iff there is an execution of $\mathbf{P}$ containing σ. A formula ψ is called an *invariant* of $\mathbf{P}$ iff $\models \psi(\sigma)$ for all reachable states σ of $\mathbf{P}$.

Definition 3.8 (Affine-linear invariant)**.** An invariant $\psi(x)$ is an *affine-linear invariant* if it is of the form

$$\psi(x) \equiv s^T x + t \rhd 0$$

for some vector $s \in \mathbb{K}^n$, some value $t \in \mathbb{K}$, and $\rhd \in \{>, \geq\}$. If $\rhd = >$, the invariant $\psi(x)$ is called *strict* invariant; if $\rhd = \geq$, the invariant $\psi(x)$ is called *non-strict* invariant.

Definition 3.9 (Inductive invariant)**.** A formula ψ is called an *inductive invariant* for a linear lasso program $\mathbf{P}$ iff the following two formulae hold.

$$\forall \sigma \in \Sigma.\ \text{STEM}(\sigma) \to \psi(\sigma) \tag{II}$$
$$\forall \sigma, \sigma' \in \Sigma.\ \psi(\sigma) \wedge \text{LOOP}(\sigma, \sigma') \to \psi(\sigma') \tag{IC}$$

Example 3.10. $\mathbf{P}_{y \geq 1}$ from Example 3.3 has the affine-linear inductive invariant $y \geq 1$, since it is implied by the stem and

$$\mathbb{K} \models \forall q, y, q', y'.\ y \geq 1 \ \wedge\ (q \geq 0 \ \wedge\ q' = q - y \ \wedge\ y' = y + 1) \to y' \geq 1.$$

Remark 3.11. *Every inductive invariant is an invariant.*

Proof. By induction using (II) and (IC). □

Invariants, that are not inductive invariants are called *non-inductive* invariants.

Example 3.12. The converse to Remark 3.11 does not hold: non-inductive invariants exist. Consider the program $\mathbf{P}_{\text{inv}}$:

$$\textsc{stem}(y, z) \equiv y \geq 0 \ \wedge \ z \geq 0$$
$$\textsc{loop}(y, z, y', z') \equiv y' = z \ \wedge \ z' = y$$

$y \geq 0$ and $z \geq 0$ are invariants of $\mathbf{P}_{\text{inv}}$: initially y and z are non-negative and their values do not decrease in the loop transition. However, neither of the two invariants is inductive since

$$y \geq 0 \ \wedge \ y' = z \ \wedge \ z' = y \to y' \geq 0$$

is false for $y = z' = 1$, and $z = y' = -1$ (and analogously for $z \geq 0$). Intuitively, the conclusion $y' \geq 0$ depends on the information that $z \geq 0$ and vice versa, so neither invariant can be proven inductively on their own.

3.3 Termination and Ranking Functions

Definition 3.14 (Termination)**.** A lasso program *terminates* iff it has no execution of infinite length.

Definition 3.15 (Ranking function)**.** Let α be a set with well-ordering relation $<_\alpha$. A *ranking function* f for a lasso program $\mathbf{P} = (\textsc{stem}, \textsc{loop})$ on domain Σ is a function $f : \Sigma \to \alpha$ such that for all reachable states σ and σ'

$$\textsc{loop}(\sigma, \sigma') \to f(\sigma') <_\alpha f(\sigma). \tag{RF}$$

If Σ is countable, we can always make α countable by choosing the image of f together with the induced well-ordering on this subset of α. By Lemma 2.3 there is always an ordinal β and an isomorphism $h : \alpha \to \beta$ such that $h \circ f$ is a ranking function on β. Without loss of generality we can therefore assume that we are ranking over ordinals.

Example 3.16. The linear lasso program $\mathbf{P}_{y \geq 1}$ from Example 3.3 has the ranking function $f(q, y) = q+1$ mapping all but the last state of every execution to a non-negative integer. From Example 3.10 we know that $y \geq 1$ is an invariant of $\mathbf{P}_{y \geq 1}$, hence we can conclude that $f(q, y)$ is well-defined and decreases for every loop transition. The ordinal isomorphic to the non-negative integers is ω, the first infinite ordinal.

The next lemma illuminates the relationship between termination and ranking functions and justifies our search for the latter for the goal of proving termination.

Lemma 3.17. *A lasso program* $\mathbf{P}$ *has a ranking function if and only if it terminates.*

Proof. The image of the states in every execution of $\mathbf{P}$ under f is a strictly decreasing sequence in α with respect to $<_\alpha$ by (RF). Because $<_\alpha$ is a well-ordering on α, this sequence cannot be infinite.

Conversely, for reachable states $\Sigma' \subseteq \Sigma$, the graph $G = (\Sigma', \textsc{loop})$ is acyclic by assumption. Hence the ranking function $f : \Sigma \to \mathbf{On}$ that assigns every state an ordinal number such that $f(\sigma) = \sup\{f(\sigma') \mid (\sigma, \sigma') \in \textsc{loop}\} + 1$ is well-defined. □

Even though every terminating lasso program has a ranking function, in general they can be arbitrarily complicated and their existence is undecidable according to the following theorem. Consequently, in this work we want to restrict ourselves to the proper subclass of lasso programs which are linear as well as consider only specific classes of ranking functions.

Theorem 3.18 (Halting problem for lasso programs [33])**.** *Termination of linear lasso programs is undecidable.*

Proof. We reduce the halting problem for Minsky counter machines [25] to lasso programs. These counter machines have a finite number of registers (each holding one non-negative integer) and a programming in form of a finite sequence of statements. Possible statements are

- $\mathrm{INC}(r_k)$: increment register k by one,
- $\mathrm{DEC}(r_k)$: decrement register k by one, and
- $\mathrm{JZ}(r_k, s_\ell)$: if register k is zero, jump to instruction s_ℓ, otherwise continue.

Let M be such an n-counter machine and let its sequence of statements be $s_0, \ldots, s_m$. We define a linear lasso program $\mathbf{P} = (\textsc{stem}, \textsc{loop})$ over the variables $s, r_1, \ldots, r_n$ as follows.

$$\textsc{stem} \equiv s = 0 \wedge \bigwedge_{j=1}^{n} r_j = 0$$

The loop transition $\textsc{loop}$ is a large disjunction composed of the following disjuncts constructed from the program instructions of M.

$$\begin{aligned}
s_i = \mathrm{INC}(r_k): \quad & \big(s = i \ \wedge\ s' = s+1 \ \wedge\ r'_k = r_k + 1 \ \wedge \bigwedge_{j \neq k} r'_j = r_j\big) \\
s_i = \mathrm{DEC}(r_k): \quad & \big(s = i \ \wedge\ s' = s+1 \ \wedge\ r_k \geq 1 \ \wedge\ r'_k = r_k - 1 \ \wedge \bigwedge_{j \neq k} r'_j = r_j\big) \\
& \vee\ \big(s = i \ \wedge\ s' = s+1 \ \wedge\ r_k < 1 \ \wedge\ r'_k = 0 \ \wedge \bigwedge_{j \neq k} r'_j = r_j\big) \\
s_i = \mathrm{JZ}(r_k, s_\ell): \quad & \big(s = i \ \wedge\ s' = \ell \ \wedge\ r_k = 0 \ \wedge \bigwedge_{j} r'_j = r_j\big) \\
& \vee\ \big(s = i \ \wedge\ s' = s+1 \ \wedge\ r_i \neq 0 \ \wedge \bigwedge_{j} r'_j = r_j\big)
\end{aligned}$$

Given a run for the counter machine M starting with empty registers at instruction 0, we can construct an execution for the lasso program $\mathbf{P}$ by assigning the current program position to s and the register content to $r_1, \ldots, r_n$. Conversely, given an execution of $\mathbf{P}$, we conclude inductively that in every state the program counter s and the registers $r_1, \ldots, r_n$ contain only integers. Hence we can define a run of M such that every execution step of M is given by a state of $\mathbf{P}$. □

Because of this fundamental undecidability, any method trying to prove termination of a given lasso program must be incomplete. However, Braverman showed the decidability of the termination of deterministic linear lasso programs that have an affine-linear function as loop transition [6], extending the work of Tiwari [33]. We conjecture that the termination of general, conjunctive linear lasso programs is also decidable. The critical property here seems to be the convexity of the loop transition. Like linear functions, polyhedral transitions tend to move variables into a particular direction (e.g. $y' \geq y + 1$) or rotate them about (e.g. $y' = -y$); see Example 4.16. If one could eliminate the rotating behavior, any terminating linear lasso program should have a multiphase ranking function (see Section 4.2 for its definition): since it is terminating, there must be an inequality $a^T x + b \geq 0$ that is eventually violated. Hence the loop implies $a^T x' \leq c^T x + e$ for some c, e and we can proceed to argument about $(c - a)^T x + e \geq 0$ recursively.

Conjecture 3.19. *Termination of conjunctive linear lasso programs over rational and real variable domain is decidable.*

Decidability of termination does hold for integer domains if the lasso program's coefficients allow real numbers [3].

Chapter 4

Ranking Function Templates

This chapter is centered around the notion of *ranking function templates*. The concept is introduced in Section 4.1 together with the auxiliary concept of transforming affine-linear functions to functions with ordinals as image. We then discuss three important examples of linear ranking function templates, multiphase in Section 4.2, piecewise in Section 4.3 and lexicographic in Section 4.4. An overview over the results on our ranking function templates is given in Section 6.4.

4.1 Definition

Definition 4.1 (Ranking function template)**.** A quantifier-free formula $\textsc{t}(x, x')$ containing function symbols and variables is called a *ranking function template* iff for every lasso program $\mathbf{P} = (\textsc{stem}, \textsc{loop})$, the satisfiability of

$$\forall \sigma, \sigma' \in \Sigma.\ \textsc{loop}(\sigma, \sigma') \to \textsc{t}(\sigma, \sigma') \tag{4.1}$$

implies that $\mathbf{P}$ terminates. If (4.1) holds for a program $\mathbf{P}$, we say that $\mathbf{P}$ *instantiates the template* $\textsc{t}$.

The ranking function template is our instrument for proving termination. An assignment to the function symbols and variables gives rise to a ranking function. Together with a set of supporting invariants, this constitutes a termination argument. All ranking function templates we consider can be encoded in linear arithmetic.

We use the term *affine-linear function symbol* $f(x)$ as a shorthand for $s^T x + t$ for a vector $s \in \mathbb{K}^n$ and a variable $t \in \mathbb{K}$.

Definition 4.2 (Linear ranking function template)**.** Let D be a finite set of variables and let F be a finite set of affine-linear function symbols. A *linear ranking function template* $\textsc{t}(x, x')$ over F and D is a ranking function template that can be written as a boolean combination of atoms of the form

$$\sum_{f \in F} \big(\alpha_f \cdot f(x) + \beta_f \cdot f(x')\big) + \sum_{d \in D} \gamma_d \cdot d \rhd 0,$$

where $\alpha_f, \beta_f, \gamma_d \in \mathbb{K}$ are constants and $\rhd \in \{\geq, >\}$. A variable $f \in F$ (respectively $d \in D$) *occurs in an atom* A of $\textsc{t}(x, x')$ iff it has a non-zero coefficient α_f or β_f (respectively γ_d) in A.

For brevity we will also write *template* instead of ranking function template and *linear template* instead of linear ranking function template. Moreover, we disallow empty atoms of the form $0 \rhd 0$ for notational convenience.

In order to establish that a formula conforming to the syntactic requirements is indeed a ranking function template, (4.1) must entail termination of the linear lasso program $\mathbf{P}$. According to Lemma 3.17, we can equally well show that the satisfiability of (4.1) implies the existence of a ranking function for $\mathbf{P}$.

Example 4.3. The formula $false$ is a ranking function template:

$$\forall \sigma, \sigma' \in \Sigma.\ \textsc{loop}(\sigma, \sigma') \to false$$

is satisfiable iff $\textsc{loop} \equiv false$ and hence there can be no execution of length greater than 1 and therefore $\mathbf{P}$ terminates. $false$ is even a linear template; it can be written as $\delta > 0 \ \wedge\ -\delta > 0$ with variables $D = \{\delta\}$.

The following linear template is applied by Podelski and Rybalchenko in [27].

Definition 4.4. We define the *affine ranking function template* (affine template) over the function symbols $F = \{f\}$ and variables $D = \{\delta\}$ as

$$\delta > 0 \ \wedge\ f(x) > 0 \ \wedge\ f(x') < f(x) - \delta. \qquad (\textsc{t}_{\text{affine}})$$

We will argue in Lemma 4.10 that the affine template is indeed a ranking function template; let us now check the additional syntactic requirements for $\textsc{t}_{\text{affine}}$ to be a *linear* ranking function template.

$$\begin{aligned} \delta > 0 &\equiv \big(0 \cdot f(x) + 0 \cdot f(x')\big) + 1 \cdot \delta > 0 \\ f(x) > 0 &\equiv \big(1 \cdot f(x) + 0 \cdot f(x')\big) + 0 \cdot \delta > 0 \\ f(x') < f(x) - \delta &\equiv \big(1 \cdot f(x) + (-1) \cdot f(x')\big) + (-1) \cdot \delta > 0 \end{aligned}$$

Thus we can write every atom of $\textsc{t}_{\text{affine}}$ in the required form.

Example 4.5. Consider the program $\mathbf{P}_{y \geq 1}$ from Example 3.3. We check if $\mathbf{P}_{y \geq 1}$ instantiates the affine template $\textsc{t}_{\text{affine}}$:

$$\begin{aligned} \forall q, y, q', y'.\ (q \geq 0 \ \wedge\ q' = q - y \ \wedge\ y' = y + 1) \\ \to (\delta > 0 \ \wedge\ f(q, y) > 0 \ \wedge\ f(q', y') < f(q, y) - \delta) \end{aligned}$$

This formula is not satisfiable; essentially because it cannot be inferred that y is positive. However, in Example 3.10 we showed that $y \geq 1$ is an invariant of $\mathbf{P}_{y \geq 1}$ and hence we can regard the semantically equivalent loop transition

$$\begin{aligned} \textsc{loop}'(q, y, q', y') &\equiv y \geq 1 \ \wedge\ \textsc{loop}(q, y, q', y') \\ &\equiv y \geq 1 \ \wedge\ q \geq 0 \ \wedge\ q' = q - y \ \wedge\ y' = y + 1. \end{aligned}$$

Now $\textsc{t}_{\text{affine}}$ can be instantiated for $f(q, y) = q + 1$ and $\delta = \frac{1}{2}$ from Example 3.16 yielding the following valid formula.

$$\begin{aligned} \forall q, y, q', y'.\ (y \geq 1 \ \wedge\ q \geq 0 \ \wedge\ q' = q - y \ \wedge\ y' = y + 1) \\ \to \left(1 > 0 \ \wedge\ q + 1 > 0 \ \wedge\ q' + 1 < q + 1 - \frac{1}{2}\right) \end{aligned}$$

Example 4.6. Why do we need the positive variable δ in $\mathrm{T}_{\text{affine}}$? Assume we use the following template:

$$f(x) > 0 \ \wedge \ f(x') < f(x) \tag{4.2}$$

The formula (4.2) does not imply termination as required by Definition 4.1: f could exhibit zeno behavior by attaining the sequence of positive values

$$1, \ \frac{1}{2}, \ \frac{1}{4}, \ \frac{1}{8}, \ \ldots$$

and hence permit infinite executions.

Because our ranking function templates are constructed from affine-linear function symbols, we define a conversion to functions with the ordinal ω as image. Transforming affine-linear functions in this fashion yields a well ordering on their image (the well-ordering $\in$ on ordinals). From these 'elementary' ranking functions we will construct the ranking functions associated with the templates.

Definition 4.7. Given an affine-linear function f and a number $\delta > 0$ called the *step size of* f, we define the *ordinal ranking equivalent* of f as

$$\widehat{f}(x) = \begin{cases} \lceil \frac{f(x)}{\delta} \rceil, & \text{if } f(x) > 0, \text{ and} \\ 0 & \text{otherwise.} \end{cases} \tag{Rk}$$

$\lceil \cdot \rceil$ denotes the ceiling function that assigns to every real number r the smallest natural number that is larger or equal to r. Since the natural numbers coincide with the finite ordinals, we can use $\lceil \cdot \rceil$ to convert a real number into an ordinal. Ordinal ranking equivalents are well-defined; $\frac{f(x)}{\delta}$ is positive for $f(x) > 0$ since $\delta > 0$. Although ordinal ranking equivalents depend on the step size, for notational simplicity we do not explicitly denote it in $\widehat{f}$.

Example 4.8. Consider the ranking function $f(q, y) = q + 1$ of step size $\delta = \frac{1}{2}$ from Example 4.5. Its ordinal ranking equivalent is

$$\widehat{f}(q, y) = \begin{cases} \lceil 2(q+1) \rceil, & \text{if } q + 1 > 0, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

A formula T is a ranking function template if its satisfiability gives rise to a ranking function. We use ordinal ranking equivalents to transform the assignment to the function symbols from T to functions over ordinals. From these we build the ranking function; the image of this ranking function is itself an ordinal and we call this ordinal the *ranking structure of* T.

Lemma 4.9. *Let f be an affine-linear function of step size $\delta > 0$ and let x and x' be two states. If $f(x) > 0$ and $f(x) - f(x') > \delta$, then $\widehat{f}(x) > 0$ and $\widehat{f}(x) > \widehat{f}(x')$.*

Proof. From $f(x) > 0$ follows that $\widehat{f}(x) > 0$. Hence $\widehat{f}(x) > \widehat{f}(x')$ in the case $\widehat{f}(x') = 0$. For $\widehat{f}(x') > 0$, we use the fact that $f(x) - f(x') > \delta$ to conclude that $\frac{f(x)}{\delta} - \frac{f(x')}{\delta} > 1$ and hence $\widehat{f}(x') > \widehat{f}(x)$. □

We can immediately apply this lemma to show that $\mathrm{T}_{\text{affine}}$ is indeed a ranking function template.

Lemma 4.10. *$\mathrm{T}_{\text{affine}}$ is a linear ranking function template.*

Proof. If $\mathrm{T}_{\text{affine}}$ is implied by the loop, the assignment to f and δ satisfies the requirements of Lemma 4.9. Consequently, $\widehat{f}$ is a ranking function for $\mathbf{P}$ of step size δ. □

Example 4.11. Consider the simple non-conjunctive program $\mathbf{P}_{\text{disj}}$.

```
while (q ≥ 0):
    if (y > 0):
        q := q − y − 1;
    else:
        q := q + y − 1;
```

Written as a linear lasso program, the stem and loop transitions are

$$\begin{aligned} \text{STEM} \equiv \quad & \mathit{true}, \\ \text{LOOP} \equiv \quad & (q \geq 0 \ \wedge \ y > 0 \ \wedge \ y' = y \ \wedge \ q' = q - y - 1) \\ & \vee (q \geq 0 \ \wedge \ y \leq 0 \ \wedge \ y' = y \ \wedge \ q' = q + y - 1). \end{aligned}$$

As $\mathrm{T}_{\text{affine}}$ is implied by the loop: it has the assignment $f(q, y) = q+1$ and $\delta = \frac{1}{2}$. This corresponds to the ordinal ranking equivalent

$$r(q, y) = \widehat{f}(q, y) = \lceil q + 1 \rceil.$$

4.2 Multiphase Template

The multiphase ranking function template is targeted at programs that go through different phases in their execution. Each phase is ranked with an affine-linear ranking function and the phase is considered to be completed once this ranking function becomes non-positive. This yields a ranking structure of $\omega \cdot k$ as an ω-ranking is performed for each of the k phases.

Example 4.12. Consider the program $\mathbf{P}_{2-\text{phase}}$ from Figure 1.2.

```
while (q ≥ 0):
    q := q − y;
    y := y + 1;
```

Every execution of $\mathbf{P}_{2-\text{phase}}$ can be partitioned into two phases; first y increases until it is positive and then q decreases until the loop condition $q \geq 0$ is violated. Depending on the initial values of y and q, either phase might be skipped altogether.

Definition 4.13. We define the *k-phase ranking function template* (k-phase template) over the functions $F = \{f_1, \ldots, f_k\}$ and variables $D = \{\delta_1, \ldots, \delta_k\}$

as follows.

$$\begin{aligned} & \bigwedge_{i=1}^{k} \delta_i > 0 \\ \wedge\ & \bigvee_{i=1}^{k} f_i(x) > 0 \qquad (\mathrm{T}_{k-\mathrm{phase}}) \\ \wedge\ & \bigwedge_{i=1}^{k} \Big(f_i(x') < f_i(x) - \delta_i \ \vee \bigvee_{j=1}^{i-1} f_j(x) > 0 \Big) \end{aligned}$$

The multiphase ranking function given by an assignment to the template $f_1, \ldots, f_k$ to $\mathrm{T}_{k-\mathrm{phase}}$ is in phase i if $f_i(x) > 0$ and $f_j(x) \leq 0$ for all $j < i$. Line 2 in $\mathrm{T}_{k-\mathrm{phase}}$ states that the multiphase ranking function is always in some phase i. Line 3 states that if we are in a phase $\geq i$, then f_i has to be decreasing by at least $\delta_i > 0$.

Note that the 1-phase template coincides with the affine template.

Lemma 4.14. $\mathrm{T}_{k-\mathrm{phase}}$ *is a linear ranking function template.*

Proof. It is clear that $\mathrm{T}_{k-\mathrm{phase}}$ conforms to the syntactic requirements to be a linear template. Consider the following ranking function on $\omega \cdot k$.

$$r(x) = \begin{cases} \omega \cdot (k-i) + \widehat{f}_i(x) & \text{if } f_j(x) \leq 0 \text{ for all } j < i \text{ and } f_i(x) > 0, \\ 0 & \text{otherwise.} \end{cases} \tag{4.3}$$

Let $(x, x') \in \textsc{loop}$. We need to show that $r(x') < r(x)$. From line 2 in $\mathrm{T}_{k-\mathrm{phase}}$ follows that $r(x) > 0$ for any x, and there is an i such that $f_i(x) > 0$ and $f_j(x) \leq 0$ for all $j < i$. By line 3, $f_j(x') \leq 0$ for all $j < i$ because $f_j(x') < f_j(x) - \delta_j \leq 0 - \delta_j \leq 0$ since $f_\ell(x) \leq 0$ for all $\ell < j$.

If $f_i(x') \leq 0$, then $r(x') \leq \omega \cdot (k-i) < \omega \cdot (k-i) + \widehat{f}_i(x) = r(x)$. Otherwise $f_i(x') > 0$ and from line 3 follows $f_i(x') < f_i(x) - \delta_i$. By Lemma 4.9, $\widehat{f}_i(x) > \widehat{f}_i(x')$ for the ordinal ranking equivalent f_i with step size δ_i. Hence

$$r(x') = \omega \cdot (k-i) + \widehat{f}_i(x') < \omega \cdot (k-i) + \widehat{f}_i(x) = r(x). \qquad \square$$

Example 4.15. Consider the program $\mathbf{P}_{2-\mathrm{phase}}$ from Example 4.12. From the 2-phase template we get an assignment $f_1(q, y) \mapsto 1 - y$ and $f_2(q, y) \mapsto q + 1$, each with step size 1. Thus $\mathbf{P}_{2-\mathrm{phase}}$ has the ranking function

$$r(q, y) = \begin{cases} \omega + \lceil 1 - y \rceil, & \text{if } y < 1, \\ \lceil q + 1 \rceil, & \text{if } y \geq 1 \ \wedge\ q + 1 > 0, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Example 4.16. There are terminating conjunctive linear lassos that do not have a multi-phase ranking function:

$$\begin{array}{l} \textbf{assume}\,(\,z \geq y + 1\,)\,; \\ \textbf{while}\,(\,q \geq 0\,)\,: \\ \qquad q \ := \ q + z - y - 1\,; \\ \qquad y \ := \ -y\,; \\ \qquad z \ := \ -z\,; \end{array}$$

Here y and z are both subject to a rotation of 180 degrees. The function $f(q, y, z) = q + 1$ is eventually decreasing in the sense that after a finite number of iterations, its value will have decreased. However, during one step its value might increase. If we consider the loop transition $\textsc{loop}' = \textsc{loop} \circ \textsc{loop}$ such that the loop body is executed twice, then f is indeed a ranking function since y and z remain constant. However, concatenating the loop does not work in general since a variables y and z can do a rotation by an arbitrary irrational angle α (even over the theory of the rationals):

$$y' = \cos(\alpha) \cdot y - \sin(\alpha) \cdot z \ \wedge \ z' = \sin(\alpha) \cdot y + \cos(\alpha) \cdot y$$

Consequently, there is not necessarily a finite number of concatenations of $\textsc{loop}$ that make y remain constant.

Example 4.17. Although every phase has a linear ranking function, we cannot use this to state a complexity result about the program in question. The reason is the non-determinism of linear lasso programs. Consider the following linear lasso program.

$$\begin{aligned} \textsc{stem}(q, y) &\equiv y = 1 \\ \textsc{loop}(q, y, q', y') &\equiv (q \geq 0 \ \wedge \ y \geq 1 \ \wedge \ y' = 0) \vee \\ &\quad\ (q \geq 0 \ \wedge \ y \leq 0 \ \wedge \ y' = y - 1 \ \wedge \ q' = q - 1) \end{aligned} \qquad (\mathbf{P}_{\text{runtime}})$$

The runtime of $\mathbf{P}_{\text{runtime}}$ does not depend on the input at all: after the first loop execution y is set to 0 and q is set to *some arbitrary value*. In particular, this value does not depend on the initial value of q. The remainder of the loop execution then takes $\lceil q \rceil + 1$ iterations to terminate.

However, $\mathbf{P}_{\text{runtime}}$ instantiates the 2-phase template: it has the 2-phase ranking function $f_1(q, y) = y$ and $f_2(q, y) = q + 1$. It provably terminates, there is just no a priori bound on the execution steps.

4.3 Piecewise Template

The piecewise ranking function template formalizes an affine-linear ranking function that is defined piecewise using affine-linear predicates to discriminate the different pieces. This discrimination need not be unambiguous; if two predicates overlap, their corresponding affine-linear functions are both ranking functions. Piecewise ranking functions have a ranking structure of ω.

Definition 4.18. We define the *k-piece ranking function template* (k-piece template) over the functions $F = \{f_1, \ldots, f_k, g_1, \ldots, g_k\}$ and variables $D = \{\delta\}$ as follows.

$$\begin{aligned} &\delta > 0 \\ \wedge \ &\bigwedge_{i=1}^{k} \bigwedge_{j=1}^{k} \Big(g_i(x) < 0 \ \vee \ g_j(x') < 0 \ \vee \ f_j(x') < f_i(x) - \delta \Big) \\ \wedge \ &\bigwedge_{i=1}^{k} f_i(x) > 0 \\ \wedge \ &\bigvee_{i=1}^{k} g_i(x) \geq 0 \end{aligned} \qquad (\mathrm{T}_{k-\text{piece}})$$

We call the function symbols $\{g_i \mid 1 \leq i \leq k\}$ *discriminating predicates* and the function symbols $\{f_i \mid 1 \leq i \leq k\}$ *ranking pieces*.

Line 4 of $\mathrm{T}_{k-\mathrm{piece}}$ states that the predicates cover all states; in other words, the piecewise defined ranking function is not just a partial function. Given the the k different pieces $f_1, \ldots, f_k$ and a state x, we use f_i as a ranking function only if $g_i(x) \geq 0$. This choice need not be unambiguous—the discriminating predicates may overlap. If they do, we can use any one of their ranking pieces. According to line 3 in $\mathrm{T}_{k-\mathrm{piece}}$, all ranking pieces are positive-valued and by line 2 piece transitions are well-defined: the rank of the new state is always less than the rank any of the ranking pieces assigned to the old state. We formally prove this in the following lemma.

Lemma 4.19. $\mathrm{T}_{k-\mathrm{piece}}$ *is a linear ranking function template.*

Proof. It is clear that $\mathrm{T}_{k-\mathrm{piece}}$ conforms to the syntactic requirements to be a linear template. Consider the following ranking function on ω.

$$r(x) = \max\{\widehat{f}_i(x) \mid g_i(x) \geq 0\} \tag{4.4}$$

The function r is well-defined because according to line 4 in ($\mathrm{T}_{k-\mathrm{piece}}$), the set $\{\widehat{f}_i(x) \mid g_i(x) \geq 0\}$ is not empty. Let $(x, x') \in \textsc{loop}$ and let i and j be indices such that $r(x) = \widehat{f}_i(x)$ and $r(x') = \widehat{f}_j(x')$. By definition of r, we have that $g_i(x) \geq 0$ and $g_j(x) \geq 0$ and line 2 then implies $f_j(x') < f_i(x) - \delta$. According to Lemma 4.9 and line 3, this entails $\widehat{f}_j(x') < \widehat{f}_i(x)$ and thus $r(x') < r(x)$. □

Example 4.20. Consider the following program $\mathbf{P}_{\mathrm{gcd}}$ adapted from [4].

```
assume(y1 ≥ 1 ∧ y2 ≥ 1);
while(y1 − y2 ≥ 1 ∨ y2 − y1 ≥ 1):
    if (y1 > y2):
        y1 := y1 − y2;
    else:
        y2 := y2 − y1;
```

Given two positive integers y_1 and y_2, the program $\mathbf{P}_{\mathrm{gcd}}$ computes the greatest common denominator. Note that $y_1 - y_2 \geq 1 \vee y_2 - y_1 \geq 1$ is the integer equivalent of $y_1 \neq y_2$.

The program $\mathbf{P}_{\mathrm{gcd}}$ instantiates the 2-piece template for the ranking pieces $f_1(y_1, y_2) = y_1$ and $f_2(y_1, y_2) = y_2$ with step size $\delta = 1$ and discriminating predicates $g_1(y_1, y_2) = y_1 - y_2$ and $g_2(y_1, y_2) = y_2 - y_1$, given the two inductive invariants $y_1 \geq 1$ and $y_2 \geq 1$.

4.4 Lexicographic Template

Lexicographic ranking functions are used frequently and have been adopted to lasso programs by Bradley, Manna and Sipma [4]. They consist of lexicographically ordered components of affine-linear functions. Hence they have a ranking structure of ω^k. A state is mapped to a tuple of values such that the loop transition leads to a decrease with respect to the lexicographic ordering for this tuple. Therefore no function may increase unless a function of a lower index

decreases. Additionally, at every step there must be at least one function that decreases.

Definition 4.21. We define the *k-lexicographic ranking function template* (k-lexicographic template) over the functions $F = \{f_1, \ldots, f_k\}$ and variables $D = \{\delta_1, \ldots, \delta_k\}$ as follows.

$$\begin{aligned} & \bigwedge_{i=1}^{k} \delta_i > 0 \\ \wedge\ & \bigwedge_{i=1}^{k} f_i(x) > 0 \\ \wedge\ & \bigwedge_{i=1}^{k-1} \left(f_i(x') \leq f_i(x) \ \vee \bigvee_{j=1}^{i-1} f_j(x') < f_j(x) - \delta_j \right) \\ \wedge\ & \bigvee_{i=1}^{k} f_i(x') < f_i(x) - \delta_i \end{aligned} \tag{$\mathrm{T}_{k-\mathrm{lex}}$}$$

Consider the formula $\mathrm{T}_{k-\mathrm{lex}}$. Line 2 establishes that all lexicographic entries $f_1, \ldots, f_k$ are positive-valued. In every step, at least one component must decrease according to line 4. All functions corresponding to indexes smaller than the decreasing function may increase by line 3.

Example 4.22. Consider the program $\mathbf{P}_{\mathrm{gcd}}$ from Example 4.20. $\mathbf{P}_{\mathrm{gcd}}$ has the lexicographic ranking function with first index $f_1(y_1, y_2) = y_2$ and second index $f_2(y_1, y_2) = y_1$ provided the two inductive invariants $y_1 \geq 1$ and $y_2 \geq 1$.

Lemma 4.23. *$\mathrm{T}_{k-\mathrm{lex}}$ is a linear ranking function template.*

Proof. It is clear that $\mathrm{T}_{k-\mathrm{lex}}$ conforms to the syntactic requirements to be a linear template. Consider the following ranking function on ω^k.

$$r(x) = \sum_{j=1}^{k} \omega^{k-j} \cdot \widehat{f_j}(x) \tag{4.5}$$

Let $(x, x') \in \textsc{loop}$. From line 2 in $\mathrm{T}_{k-\mathrm{lex}}$ follows $f_j(x) > 0$ for all j, so $r(x) > 0$. By line 4 and Lemma 4.9, there is a minimal i such that $\widehat{f_i}(x') < \widehat{f_i}(x)$. Line 3 implies that $\widehat{f_1}(x') \leq \widehat{f_1}(x)$ and hence inductively $\widehat{f_j}(x') \leq \widehat{f_j}(x)$ for all $j < i$ since i was minimal.

$$\begin{aligned} r(x') &= \sum_{j=1}^{k} \omega^{k-j} \cdot \widehat{f_j}(x') \\ &\leq \sum_{j=1}^{i-1} \omega^{k-j} \cdot \widehat{f_j}(x) + \sum_{j=i}^{k} \omega^{k-j} \cdot \widehat{f_j}(x') \\ &< \sum_{j=1}^{i-1} \omega^{k-j} \cdot \widehat{f_j}(x) + \omega^{k-i} \cdot \widehat{f_i}(x) \\ &\leq r(x) \end{aligned}$$

□

Chapter 5

Building the Constraints

In this chapter we discuss an automatic procedure for the instantiation of ranking function templates. Given a linear lasso program $\mathbf{P}$ and a linear ranking function template $\textsc{t}$, we set up constraints whose solution is a termination argument for $\mathbf{P}$. With the help of Motzkin's Transposition Theorem, this will be a purely existentially quantified formula. We first discuss the addition of supporting invariants in Section 5.1. The step-by-step transformations involved in building the constraints are the subject in Section 5.2. In Section 5.3 we show that this procedure is sound and complete. We conclude this chapter with a discussion of lasso programs that contain integer variables in Section 5.4.

5.1 Loop Augmentation with Invariants

Ranking function templates are checked for implication by the loop transition. As this transition is independent of the lasso program's stem, information critical to the program's termination proof might be missed. We address this issue by augmenting the loop transition with inductive invariants similar to [9]. The following lemma formalizes this process.

Lemma 5.1 (Loop augmentation with invariants)**.** *Let* $\textsc{t}$ *be a ranking function template,* $\mathbf{P} = (\textsc{stem}, \textsc{loop})$ *be a lasso program, and* $(\psi_\ell)_{\ell \in L}$ *a finite number of invariants of* $\mathbf{P}$*. If the formula*

$$\forall x, x'.\ \big(\textsc{loop}(x, x') \wedge \bigwedge_{\ell \in L} \psi_\ell(x)\big) \to \textsc{t}(x, x') \tag{5.1}$$

is satisfiable, then $\mathbf{P}$ *terminates.*

Proof. Because every ψ_ℓ holds at all reachable states of $\mathbf{P}$, so does $\bigwedge_{\ell \in L} \psi_\ell$. Consider the transition

$$\textsc{loop}'(x, x') \equiv \Big(\bigwedge_{\ell \in L} \psi_\ell(x)\Big) \ \wedge\ \textsc{loop}(x, x').$$

The two programs $\mathbf{P} = (\textsc{stem}, \textsc{loop})$ and $\mathbf{P}' = (\textsc{stem}, \textsc{loop}')$ are semantically equivalent: they have the same executions. Therefore $\mathbf{P}$ terminates iff $\mathbf{P}'$ terminates, and the latter is equivalent to the satisfiability of (5.1) by Definition 4.1. □

In addition to solving the constraints (5.1), we need to encode that all ψ_ℓ are invariants. We use inductive invariants and add the conditions (II) and (IC) to our constraint system for every inductive invariant ψ_ℓ.

$$\bigwedge_{\ell \in L} \forall x.\ \textsc{stem}(x) \to \psi_\ell(x) \tag{II0}$$

$$\bigwedge_{\ell \in L} \forall x, x'.\ \psi_\ell(x)\ \wedge\ \textsc{loop}(x, x') \to \psi_\ell(x') \tag{IC0}$$

$$\forall x, x'.\ \big(\textsc{loop}(x, x')\ \wedge\ \bigwedge_{\ell \in L} \psi_\ell(x)\big) \to \textsc{t}(x, x') \tag{TI0}$$

We call (II0) *invariant initiation*, (IC0) *invariant consecution* and (TI0) the *template implication*.

The following lemma asserts that a finite number of inductive invariants is sufficient to entail the ranking function template, if it is entailed by all inductive invariants.

Lemma 5.2. *Let I be the set of all inductive invariants of* loop *and φ be a formula. Then $I, \textsc{loop} \models \varphi$ iff there is a finite subset $I' \subseteq I$ such that $I', \textsc{loop} \models \varphi$.*

Proof. If $I, \textsc{loop} \models \varphi$, then the set $T := I \cup \{\textsc{loop}, \neg\varphi\}$ is unsatisfiable. By the Compactness Theorem, there is a finite subset $T' \subseteq T$ that is unsatisfiable, and hence $T'' = T' \cup \{\textsc{loop}, \neg\varphi\}$ is also unsatisfiable. Therefore we can conclude for the finite set $I' = T'' \cap I$ that $I', \textsc{loop} \models \varphi$. □

5.2 The Constraints

In this section we will sequentially apply five equivalence transformations to the constraints (II0), (IC0) and (TI0) to make them more easily solvable by an SMT solver. The reason for this is that the result (1) has only existential quantification instead of universal and (2) has a significantly reduced number of non-linear operations (multiplications of variables). In Section 5.3 we argue that each transformation is indeed an equivalence transformation; this method is sound and complete.

We fix a linear ranking function template over F in conjunctive normal form,

$$\textsc{t}(x, x') \equiv \bigwedge_{i \in I} \bigvee_{j \in J_i} \textsc{t}_{i,j}(x, x') \equiv \bigwedge_{i \in I} \bigvee_{j \in J_i} d_{i,j}^T \tbinom{x}{x'} \rhd_{i,j} e_{i,j}, \tag{5.2}$$

where the vectors d and the numbers e are linear combinations of the uninterpreted function symbols in F and $\rhd_{i,j} \in \{\geq, >\}$. We partition every J_i in $J_i^{\geq}$ and $J_i^{>}$ such that $\rhd_{i,j} = \geq$ for all $j \in J_i^{\geq}$ and $\rhd_{i,j} = >$ for all $j \in J_i^{>}$.

Furthermore, we fix a linear lasso program $\mathbf{P} = (\textsc{stem}, \textsc{loop})$. According to Lemma 3.5, we can write $\mathbf{P}$ in normal form:

$$\textsc{stem}(x) \equiv \bigvee_{n \in N} \textsc{stem}_n(x) \equiv \bigvee_{n \in N} \big(B_n x \leq b_n\ \wedge\ B'_n x < b'_n\big) \tag{5.3}$$

$$\begin{aligned} \textsc{loop}(x, x') &\equiv \bigvee_{m \in M} \textsc{loop}_m(x, x') \\ &\equiv \bigvee_{m \in M} \big(A_m \tbinom{x}{x'} \leq c_m\ \wedge\ A'_m \tbinom{x}{x'} < c'_m\big) \end{aligned} \tag{5.4}$$

Let $\{\psi_\ell \mid \ell \in L\}$ denote the inductive invariants; every invariant is an inequality of the form $s^T x + t \rhd 0$ for a vector s, a number t, and $\rhd \in \{\geq, >\}$.

Transformation 1: Remove disjunctions in stem and loop. The disjunction in the stem and loop formulae are moved outside the quantifiers' scope in (II0), (IC0) and (TI0).

$$\bigwedge_{\ell\in L}\bigwedge_{n\in N} \forall x.\ \textsc{stem}_n(x) \to \psi_\ell(x) \tag{II1}$$

$$\bigwedge_{\ell\in L}\bigwedge_{m\in M} \forall x, x'.\ \psi_\ell(x) \wedge \textsc{loop}_m(x, x') \to \psi_\ell(x') \tag{IC1}$$

$$\bigwedge_{m\in M} \forall x, x'.\ \textsc{loop}_m(x, x') \wedge \bigwedge_{\ell\in L} \psi_\ell(x) \to \textsc{t}(x, x') \tag{TI1}$$

Transformation 2: Remove template conjunctions. The conjunctions in the ranking function template are moved outside the quantifiers' scope.

$$\bigwedge_{\ell\in L}\bigwedge_{n\in N} \forall x.\ \textsc{stem}_n(x) \to \psi_\ell(x) \tag{II2}$$

$$\bigwedge_{\ell\in L}\bigwedge_{m\in M} \forall x, x'.\ \psi_\ell(x) \wedge \textsc{loop}_m(x, x') \to \psi_\ell(x') \tag{IC2}$$

$$\bigwedge_{i\in I}\bigwedge_{m\in M} \forall x, x'.\ \textsc{loop}_m(x, x') \wedge \bigwedge_{\ell\in L} \psi_\ell(x) \to \bigvee_{j\in J_i} \textsc{t}_{i,j}(x, x') \tag{TI2}$$

Transformation 3: Replicate supporting invariants. We supply different supporting invariants to every template implication. This will later enable us to get rid of a number of non-linear variables. In order to achieve this, we introduce invariants for every $\ell \in L$, $i \in I$ and $m \in M$; therefore let $L' = L \times I \times M$.

$$\bigwedge_{\ell\in L'}\bigwedge_{n\in N} \forall x.\ \textsc{stem}_n(x) \to \psi_\ell(x) \tag{II3}$$

$$\bigwedge_{\ell\in L'}\bigwedge_{m\in M} \forall x, x'.\ \psi_\ell(x) \wedge \textsc{loop}_m(x, x') \to \psi_\ell(x') \tag{IC3}$$

$$\bigwedge_{i\in I}\bigwedge_{m\in M} \forall x, x'.\ \textsc{loop}_m(x, x') \wedge \bigwedge_{\ell\in L} \psi_{(\ell,i,m)}(x) \to \bigvee_{j\in J_i} \textsc{t}_{i,j}(x, x') \tag{TI3}$$

Transformation 4: Write as negated conjunctions. In order to make Motzkin's Theorem applicable, we write the implications equivalently as negated conjunctions.

$$\bigwedge_{\ell\in L'}\bigwedge_{n\in N} \forall x.\ \neg(\textsc{stem}_n(x)\ \wedge\ \neg\psi_\ell(x)) \tag{II4}$$

$$\bigwedge_{\ell\in L'}\bigwedge_{m\in M} \forall x, x'.\ \neg(\psi_\ell(x)\ \wedge\ \textsc{loop}_m(x, x')\ \wedge\ \neg\psi_\ell(x')) \tag{IC4}$$

$$\bigwedge_{i\in I}\bigwedge_{m\in M} \forall x, x'.\ \neg\Big(\textsc{loop}_m(x, x') \wedge \bigwedge_{\ell\in L} \psi_{(\ell,i,m)}(x) \wedge \bigwedge_{j\in J_i} \neg\,\textsc{t}_{i,j}(x, x')\Big) \tag{TI4}$$

Transformation 5: Apply Motzkin's Transposition Theorem. For simplicity we assume that no involved invariants are non-strict inequalities (strict inequalities are processed analogously). We rewrite the invariants

$$\psi_{\ell,i,m}(x) \equiv s_{\ell,i,m}^T x + t_{\ell,i,m} \geq 0$$

where $s_{\ell,i,m} \in \mathbb{K}^n$ and $t_{\ell,i,m} \in \mathbb{K}$ are variables. Similarly, we use (5.2), (5.3), and (5.4) to rewrite $\textsc{t}_{i,j}$, $\textsc{stem}_n$ and $\textsc{loop}_m$ as linear inequalities. Next, we apply Motzkin's Transposition Theorem to every universally quantified subformula and obtain the following equivalent constraints.

$$\begin{aligned}
&\bigwedge_{\ell\in L'}\bigwedge_{n\in N} \exists \lambda,\mu,\xi \geq 0.\\
&\qquad \lambda^T B_n + \mu^T B'_n + \xi \tbinom{s_\ell}{0}^T = 0\\
&\qquad \wedge\ \lambda^T b_n + \mu^T b'_n + \xi t_\ell \leq 0\\
&\qquad \wedge\ \big(\lambda^T b_n < 0\ \vee\ \xi + \textstyle\sum \mu > 0\big)
\end{aligned} \tag{II5}$$

$$\begin{aligned}
&\bigwedge_{\ell\in L'}\bigwedge_{m\in M} \exists \lambda,\chi_1,\mu,\chi_2 \geq 0.\\
&\qquad \lambda^T A_m + \mu^T A'_m + \chi_2 \tbinom{0}{s_\ell}^T - \chi_1 \tbinom{s_\ell}{0}^T = 0\\
&\qquad \wedge\ \lambda^T c_m + \mu^T c'_m + (\chi_2 - \chi_1) t_\ell \leq 0\\
&\qquad \wedge\ \big(\lambda^T c_m - \chi_1 t_\ell < 0\ \vee\ \chi_2 + \textstyle\sum \mu > 0\big)
\end{aligned} \tag{IC5}$$

$$\begin{aligned}
&\bigwedge_{i\in I}\bigwedge_{m\in M} \exists \lambda,(\xi_\ell)_{\ell\in L},(\zeta_j)_{j\in J_i},\mu \geq 0.\\
&\qquad \lambda^T A_m + \mu^T A'_m + \sum_{\ell\in L} \xi_\ell \tbinom{s_{\ell,i,m}}{0}^T + \sum_{j\in J_i} \zeta_j d_{i,j}^T = 0\\
&\qquad \wedge\ \lambda^T c_m + \mu^T c'_m + \sum_{\ell\in L} \xi_\ell t_{\ell,i,m} + \sum_{j\in J_i} \zeta_j e_{i,j} \leq 0\\
&\qquad \wedge\ \big(\lambda^T c_m + \sum_{\ell\in L} \xi_\ell t_{\ell,i,m} + \sum_{j\in J_i^{\geq}} \zeta_j e_{i,j} < 0\\
&\qquad\qquad \vee \sum_{j\in J_i^{>}} \zeta_j + \textstyle\sum \mu > 0\big)
\end{aligned} \tag{TI5}$$

An explanation to the coefficients introduced by Motzkin's Transposition Theorem is in order. For every inequality in (M1), a new existentially quantified variable is added in (M2). We call these new existentially quantified variables *Motzkin coefficients*.

In the invariant initiation (II5), the stem's non-strict inequalities correspond to the vector of variables λ, the stem's strict inequalities correspond to the vector of variables μ. The invariant has the Motzkin coefficient ξ. In the invariant consecution (IC5) and the template implication (TI5), the loop's non-strict inequalities correspond to the vector of variables λ and the loop's strict inequalities to the vector of variables μ. In (IC5) the Motzkin coefficient χ_1 corresponds to the premise $\psi_\ell(x)$, while the Motzkin coefficient χ_2 corresponds to $\psi_\ell(x')$.

Lastly, the Motzkin coefficients ξ_ℓ in (TI5) correspond to the invariants $\psi_\ell(x)$ in the template implication and the Motzkin coefficients ζ_j correspond to the ranking function template's inequalities.

5.3 Soundness and Completeness

It is clear that step 1, 2 and 4 are equivalence transformations; they are simple syntactic modifications that preserve semantics. Step 3 introduces a number of new invariants, hence the constraints potentially gain new solutions, but retain all old solutions. However, adding more invariants is still sound; by Lemma 5.1 we might just as well have started out with the larger number of invariants. Finally, transformation 5 also retains equivalence by Motzkin's Transposition Theorem.

We can now state the soundness and completeness of our method: solving the constraint (II5) $\wedge$ (IC5) $\wedge$ (TI5) is equivalent to solving the constraint (II0) $\wedge$ (IC0) $\wedge$ (TI0), which according to Lemma 5.1 is satisfiable only if **P** terminates.

Theorem 5.3 (Soundness)**.** *If the constraint* (II5) $\wedge$ (IC5) $\wedge$ (TI5) *is satisfiable, then* **P** *terminates.*

Theorem 5.4 (Completeness)**.** *If the constraint* (II0) $\wedge$ (IC0) $\wedge$ (TI0) *is satisfiable, then so is the constraint* (II5) $\wedge$ (IC5) $\wedge$ (TI5)*.*

We get even more than just termination guarantee the soundness theorem suggests. The resulting variable assignment gives rise to a termination argument in form of a ranking function together with a set of supporting invariants. This serves as a termination proof that can be verified by an independent theorem prover.

5.4 Integer Lasso Programs

In Section 5.2 we built the constraints for rational or real variable domains. In this section we want to motivate that the same procedure can be applied to integer or mixed integer variable domains.

Definition 5.5. A lasso program is said to have *mixed integer domain*, iff it contains some variables whose domain is the integers.

The soundness of this method for integers is trivial—the integers are a subset of the rationals and hence every execution of a program of mixed integer domain is also an execution of the program with the larger domain. Therefore the mixed integer program has no infinite execution if the program with larger domain has none. We are interested in the completeness. Note that even the instantiation of the affine template for lasso programs without stem is co-NP-complete in the integer case [2].

We introduce the notion of *integral polyhedra*. A polyhedron is integral, if it contains all inequalities that do not follow over the rationals, but are entailed over the integers. This will enable the use of Motzkin's Theorem for integer polyhedra. We give an equivalent definition.

Definition 5.6. A polyhedron $Ax \leq b$ is *integral* iff it coincides with the convex hull of the integer solutions of $Ax \leq b$.

For a given polyhedron, we can compute its *integral hull* (the corresponding integral polyhedron) using Hartmann's algorithm [7]. However, the number of inequalities needed can grow exponentially [17]. If we fix the dimension n, the running time is polynomial in the number of inequalities m and their descriptive size.

Lemma 5.7 (Integral polyhedra)**.** *A integral polyhedron contains no integer points if and only if it is empty.*

Proof. If the polyhedron is empty, it cannot contain integer points. Conversely, assume the integral polyhedron is not empty. Using the terminology of the proof of Lemma 2.7, we know that the primal problem P is integral and thus has an integer optimal solution [31]. This integer optimal solution is an integer point in the polyhedron. □

According to Lemma 5.7, if we manage to make the polyhedron in (M1) integral, we can equivalently transform an integer universally quantified statement into a rational existentially quantified one using Motzkin's Theorem. However, this is not applicable for our method because the polyhedra in (II4), (IC4), and (TI4) contain free variables. Making just the stem and loop transitions integral does preserve more solutions; however, we cannot obtain completeness by this approach, as the following example illustrates.

Example 5.8. Consider the following program $\mathbf{P}_{\text{int}}$.

$$\begin{array}{l} \textbf{assume}\,(\,2y \geq z\,)\,; \\ \textbf{while}\,(\,q \geq 0 \;\wedge\; z = 1\,)\colon \\ \qquad q \;:=\; q - 2y + 1\,; \end{array}$$

Clearly, $f(q, y, z) = q + 1$ is a ranking function for $\mathbf{P}_{\text{int}}$, hence we use the affine template. The only inductive invariant is $2y - z \geq 0$ since inductive invariants have to be implied by the stem. These invariants are not sufficient to prove that $f(q, y, z)$ is indeed a ranking function:

$$\begin{aligned} & f(q, y, z) - f(q', y', z') - \mu \cdot (2y - z) \\ = \; & q - (q - 2y + 1) - (2y - z) \\ = \; & z - 1 = 0, \text{ but should be positive.} \end{aligned}$$

The invariant $2y \geq z$ and the loop condition $z = 1$ imply over the integers that $y \geq 1$ and hence

$$\forall x, x' \in \mathbb{Z}^n.\ \textsc{loop}(x, x') \wedge 2y - z \geq 0 \to f(x) - f(x') \geq 1$$

is valid. Computing the integral hull of $\textsc{loop} \wedge 2y - z \geq 0$ yields $y \geq 1$ and with this inequality the ranking function can be discovered.

Chapter 6

Non-linearity in the Constraints

In this chapter we discuss the constraints generated in Section 5.2. We asses the number of variables that occur in non-linear operations in these constraints using formal notions introduced in Section 6.1. Furthermore, we give a theorem that enables us to eliminate some of the Motzkin coefficients from the constraints in Section 6.2. We apply this technique to our ranking function templates in Section 6.3 and give a summarizing overview of the results in Section 6.4.

6.1 Definitions

Definition 6.1 (Dependency graph)**.** Let T be a linear ranking function template with variables D and function symbols F. The template's *dependency graph* is a graph $G_{\mathrm{T}} = (D \cup F, E)$ with the set of nodes $D \cup F$ and the edges

$$E = \{(f_1, f_2) \in (D \cup F)^2 \mid \mathrm{T} \text{ has an atom where both, } f_1 \text{ and } f_2 \text{ occur}\}.$$

It follows from the definition that the dependency graph G_{T} of a ranking function template T is reflexive and symmetric (undirected). Given a variable or function symbol $f \in D \cup F$, we denote by $[f]$ the connected component[1] that contains f.

Example 6.2. The following table lists the set of connected components in the dependency graph for the ranking function templates introduced in Chapter 4. See Figure 6.1 for a visualization.

$\mathrm{T}_{\mathrm{affine}}$	$\big\{\{f, \delta\}\big\}$
$\mathrm{T}_{k-\mathrm{phase}}$	$\big\{\{f_i, \delta_i\} \mid 1 \leq i \leq k\big\}$
$\mathrm{T}_{k-\mathrm{piece}}$	$\big\{\{f_1, \ldots, f_k, \delta\}\big\} \cup \big\{\{g_i\} \mid 1 \leq i \leq k\big\}$
$\mathrm{T}_{k-\mathrm{lex}}$	$\big\{\{f_i, \delta_i\} \mid 1 \leq i \leq k\big\}$

[1] A connected component is a maximal subset of nodes such that these nodes are pairwise connected by paths.

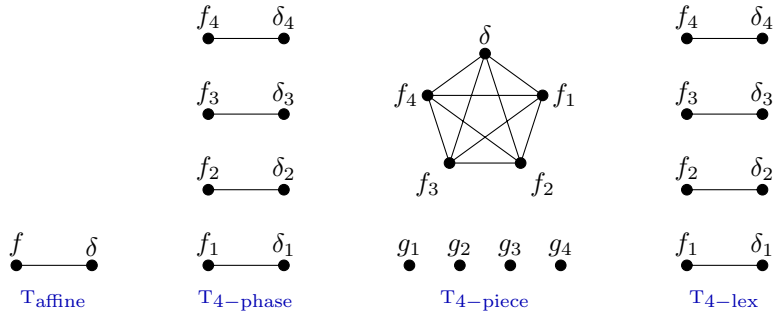


Figure 6.1: The dependency graph of the affine, 4-phase, 4-piece and 4-lexicographic template. The number of connected components is 1, 4, 5, and 4 respectively. The graphs' reflexive edges are not shown.

Next, we define colorings, coloring graphs and suitable colorings for a template T. A suitable coloring selects the occurrences of atoms of the template whose Motzkin coefficient we can eliminate in the constraint (II5) $\wedge$ (IC5) $\wedge$ (TI5) (see Section 6.2).

Definition 6.3 (Coloring)**.** Let $\mathrm{T} = \bigwedge_{i \in I} \bigvee_{j \in J_i} \mathrm{T}_{i,j}$ be a linear ranking function template in CNF and let D be the variables and F be the function symbols of T. A *coloring* η *of* T is mapping from occurrences of atoms of T to $\{\bigcirc, \color{red}\bullet, \color{blue}\bullet\}$. The occurrence of an atom $\mathrm{T}_{i,j}$ is called *red* iff it is mapped to $\color{red}\bullet$, *blue* iff it is mapped to $\color{blue}\bullet$, and uncolored otherwise.

In Definition 6.3 we consider occurrences of atoms rather than atoms because an atom may occur multiple times in the same template and we want to be able to distinguish these occurrences. For simplicity, we will sometimes write that an atom is red, blue or uncolored respectively, if it is clear from context which occurrence we mean. Moreover, by stating f occurs in a red atom, we mean f occurs in an atom which has an occurrence that is colored red.

Definition 6.4 (Coloring graph)**.** Let $\mathrm{T} = \bigwedge_{i \in I} \bigvee_{j \in J_i} \mathrm{T}_{i,j}$ be a linear ranking function template in CNF with variables D and function symbols F, and let η be a coloring for T. The *coloring graph* is a directed graph $G_\eta = (\mathcal{K}, E)$ such that the following holds.

- The set of nodes $\mathcal{K}$ is the set of connected components of G_{T}.
- For all $f_1, f_2 \in D \cup F$, there is an edge from the connected component of f_1 to the connected component of f_2, i.e., $([f_1], [f_2]) \in E$, if and only if f_1 occurs in an red atom T_{i_1,j_1} and f_2 occurs in a blue atom T_{i_2,j_2} and $i_1 = i_2$, i.e., T_{i_1,j_1} and T_{i_2,j_2} occur in the same conjunct.

Definition 6.5 (Suitable coloring)**.** Let T be a linear ranking function template in CNF and let F be the function symbols and D be the variables of T. A coloring η is *suitable for* T iff the following holds.

a) Every conjunct of T contains exactly one red atom.

b) For every $f_1, f_2 \in D \cup F$ that occur in two different blue atoms, there is no path between f_1 and f_2 in the dependency graph G_{T}.

c) The coloring graph G_η is acyclic.

See Figure 6.2 on page 46 for a visualization of some suitable colorings for our ranking function templates. We also give two detailed examples in the following.

Example 6.6. Consider the linear template $\mathrm{T}_{\mathrm{affine}}$ from Definition 4.4. Since $\mathrm{T}_{\mathrm{affine}}$ does not contain any disjunctions in CNF, every conjunct contains exactly one atom. Therefore the only suitable coloring for $\mathrm{T}_{\mathrm{affine}}$ is one that colors all occurrences of atoms red according to Definition 6.5 (a). As no atoms are colored blue, conditions of Definition 6.5 (b) and (c) are trivially satisfied.

According to Definition 6.5 (a), occurrences of atoms in a conjunct that contains only one atom have to be colored red.

Example 6.7. Consider the 3-phase template.

$$\begin{aligned} &\delta_1 > 0 \ \wedge\ \delta_2 > 0 \ \wedge\ \delta_3 > 0 \\ \wedge\ &\big(f_1(x) > 0 \ \vee\ f_2(x) > 0 \ \vee\ f_3(x) > 0\big) \\ \wedge\ &f_1(x') < f_1(x) - \delta_1 \\ \wedge\ &\big(f_2(x') < f_2(x) - \delta_2 \ \vee\ f_1(x) > 0\big) \\ \wedge\ &\big(f_3(x') < f_3(x) - \delta_3 \ \vee\ f_2(x) > 0 \ \vee\ f_1(x) > 0\big) \end{aligned} \tag{$\mathrm{T}_{3-\mathrm{phase}}$}$$

We construct a coloring η for $\mathrm{T}_{3-\mathrm{phase}}$, given in CNF. The following atoms have to be colored red according to Definition 6.5 (a).

$$\delta_1 > 0, \qquad \delta_2 > 0, \qquad \delta_3 > 0, \qquad f_1(x') < f_1(x) - \delta_1.$$

The remaining candidates are the atoms for blue coloring are

$$\begin{aligned} f_1(x) > 0 \ \vee\ f_2(x) > 0 \ \vee\ f_3(x) > 0, \\ f_2(x') < f_2(x) - \delta_2 \ \vee\ f_1(x) > 0, \\ f_3(x') < f_3(x) - \delta_3 \ \vee\ f_2(x) > 0 \ \vee\ f_1(x) > 0. \end{aligned}$$

Recall that although $f_1(x) > 0$ occurs three times in this list, we consider it as three different occurrences of the atom in $\mathrm{T}_{3-\mathrm{phase}}$. By Example 6.2, the dependency graph $G_{\mathrm{T}_{3-\mathrm{phase}}}$ has three connected components. We color the following two atoms blue.

$$f_2(x') < f_2(x) - \delta_2 \text{ and } f_3(x') < f_3(x) - \delta_3.$$

We complete our coloring by choosing the color red for the three occurrences of the atoms $f_1(x) > 0$. Note that this choice for η is not the only possibility. We visualize the coloring η:

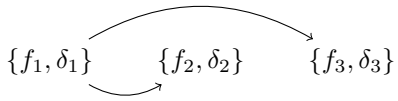
$$\begin{aligned} &\delta_1 > 0 \ \wedge\ \delta_2 > 0 \ \wedge\ \delta_3 > 0 \\ \wedge\ &\big(f_1(x) > 0 \ \vee\ f_2(x) > 0 \ \vee\ f_3(x) > 0\big) \\ \wedge\ &f_1(x') < f_1(x) - \delta_1 \\ \wedge\ &\big(f_2(x') < f_2(x) - \delta_2 \ \vee\ f_1(x) > 0\big) \\ \wedge\ &\big(f_3(x') < f_3(x) - \delta_3 \ \vee\ f_2(x) > 0 \ \vee\ f_1(x) > 0\big) \end{aligned}$$

Let us check the conditions of Definition 6.5:

a) We colored exactly one atom in each conjunct red.

b) The two sets of variables and function symbols $\{f_2, \delta_2\}$ and $\{f_3, \delta_3\}$ that occur in blue colored atoms are different connected components of the dependency graph of $\mathrm{T}_{3-\mathrm{phase}}$.

c) The coloring graph G_η is acyclic:



Hence η is a suitable coloring for the ranking function template $\mathrm{T}_{3-\mathrm{phase}}$.

Lemma 6.8. *Let* T *be a ranking function template, let* G_T *be the dependency graph of* T *and let* η *be a suitable coloring for* T*. If* G_T *has* c *connected components, then the number of occurrences of atoms colored blue is at most* $c - 1$*.*

Proof. Let M be the function assigning to every blue atom A the connected component of the variables and function symbols occurring in A. The function M is injective: if there are two blue atoms A_1, A_2 such that $M(A_1) = M(A_2)$, then from Definition 6.5 (b) follows that $A_1 = A_2$.

Assume there are c or more blue atoms, and let K_1 be some connected component in G_T. Consider the conjunct of $A_1 = M^{-1}(K_1)$. By Definition 6.5 (a), there is a red atom A_2 in this conjunct; let $K_2 = M(A_2)$. We have that (K_2, K_1) is an edge in the coloring graph G_η.

Consequently, every node in the finite coloring graph G_η has an incoming edge, and thus the graph must contain a cycle. This contradicts Definition 6.5 (c). □

Definition 6.9 (Degree of a template)**.** Let T be a linear ranking function template. We define the *degree of a coloring* η of T as

$$\deg_\mathrm{T}(\eta) = \#\,\eta^{-1}(\{\circ\}),$$

the number of occurrences of atoms that are uncolored. The *degree of* T is the minimal degree of all suitable colorings of T.

As we will show in Section 6.2, the degree of T is the number of non-linear Motzkin coefficients of atoms of T that we are not going to eliminate from our constraints.

Example 6.10. By Example 6.6, the only suitable coloring for $\mathrm{T}_\mathrm{affine}$ is a coloring η such that all atoms are colored red. The template $\mathrm{T}_\mathrm{affine}$ has a degree of at most

$$\deg_{\mathrm{T}_\mathrm{affine}}(\eta) = 0.$$

The number of connected components in the dependency graph of a template T gives rise to a lower bound on the degree of T according to Lemma 6.8.

Lemma 6.11. *Let* T *be a ranking function template, let* G_{T} *be the dependency graph of* T *and let* η *be a suitable coloring for* T*. If* G_{T} *has* c *connected components and* $c-1$ *occurrences of atoms are colored blue by* η*, then the degree of* T *is* $\deg_{\mathrm{T}}(\eta)$*.*

Proof. By Definition 6.5 (a), in every coloring the same number of occurrences of atoms is colored red. Moreover, by Lemma 6.8, no more than $c-1$ atoms may be colored blue, therefore there is no coloring that such that less atoms are uncolored and thus $\deg_{\mathrm{T}}(\eta)$ is minimal. □

Example 6.12. Recall the linear ranking function template $\mathrm{T}_{3-\mathrm{phase}}$ and its suitable coloring η from Example 6.7.

$$\deg_{\mathrm{T}_{3-\mathrm{phase}}}(\eta) = 3.$$

The dependency graph of $\mathrm{T}_{3-\mathrm{phase}}$ has three components. By Lemma 6.11 coloring two atoms blue implies that $\deg_{\mathrm{T}_{3-\mathrm{phase}}}(\eta)$ is minimal and therefore $\mathrm{T}_{3-\mathrm{phase}}$ has degree 3.

Definition 6.13 (Non-linear dimension)**.** Let φ be a formula in non-linear arithmetic containing the free or existentially quantified variables V. The *non-linear dimension* of φ is the size of the smallest subset of variables $V' \subseteq V$ such that φ becomes a formula in linear arithmetic when assigning a value to each variable in V' (removing their quantifiers).

A formula φ in non-linear arithmetic is also a formula in linear arithmetic if it uses no non-linear operations (multiplication of variables).

Example 6.14. Consider the formula in non-linear arithmetic

$$\varphi(y) \equiv \exists x.\, x \cdot y = 1.$$

We have one non-linear operation in φ: the multiplication $x \cdot y$. The formula φ becomes linear after the assignment to the variable x or the variable y.

$$\begin{aligned} \varphi_1 &\equiv \exists x.\, x \cdot 3 = 1 \equiv \exists x.\, x + x + x = 1 \\ \varphi_2(y) &\equiv \frac{1}{2} \cdot y = 1 \equiv y = 2 \end{aligned}$$

Here we used the assignment $x \mapsto \frac{1}{2}$ and $y \mapsto 3$ respectively. Consequently, φ has non-linear dimension 1.

6.2 Non-linear dimension of the Constraints

In this section we examine the non-linear dimension of the constraints generated in Section 5.2. First we show that the constraints (II5) $\wedge$ (IC5) $\wedge$ (TI5) can be simplified. We eliminate quantifiers by fixing the value of the quantified variables: a variable v is fixed to a finite set of values $\{u_1, \ldots, u_m\}$ by replacing $\exists v.\, \varphi(v)$ with $\varphi(u_1) \vee \ldots \vee \varphi(u_m)$.

Theorem 6.15 (Omitting quantifiers)**.** *Let* η *be a suitable coloring for the linear ranking function template* T *according to Definition 6.5. If for* every

existentially-quantified subformula in (II5)*,* (IC5) *and* (TI5)*, we eliminate quantifiers by fixing Motzkin coefficients to a finite set of values as described below, then we obtain* equivalent *constraints.*

I. The Motzkin coefficient ξ *in the invariant initiation* (II5) *is fixed to* $\{0,1\}$*.*

II. The Motzkin coefficient χ_2 *in the invariant consecution* (IC5) *is fixed to* $\{0,1\}$*.*

III. The Motzkin coefficients ζ_j *in* (TI5) *of every atom* $\mathrm{T}_{i,j}(x,x')$ *colored red or blue by* η *is fixed to* $\{0,1\}$*.*

IV. The Motzkin coefficients ξ_ℓ *in* (TI5) *of strict invariants are fixed to* $\{0,1\}$*, Motzkin coefficients of non-strict invariants are fixed to* $\{1\}$*.*

Applying the quantifier eliminations I, II and IV from Theorem 6.15 to (II5), (IC5), and (TI5) yields the following constraints (elimination III is omitted for clarity).

$$\begin{aligned}\bigwedge_{\ell\in L'}\bigwedge_{n\in N}\bigvee_{\xi\in\{0,1\}} \exists\lambda,\mu\geq 0.\\ \lambda^T B_n+\mu^T B'_n+\xi\tbinom{s_\ell}{0}^T=0\\ \wedge\ \lambda^T b_n+\mu^T b'_n+\xi t_\ell\leq 0\\ \wedge\ \big(\lambda^T b_n<0\ \vee\ \xi+\textstyle\sum\mu>0\big)\end{aligned}\tag{II6}$$

$$\begin{aligned}\bigwedge_{\ell\in L'}\bigwedge_{m\in M}\bigvee_{\chi_2\in\{0,1\}} \exists\lambda,\chi_1,\mu\geq 0.\\ \lambda^T A_m+\mu^T A'_m+\chi_2\tbinom{0}{s_\ell}^T-\chi_1\tbinom{s_\ell}{0}^T=0\\ \wedge\ \lambda^T c_m+\mu^T c'_m+(\chi_2-\chi_1)t_\ell\leq 0\\ \wedge\ \big(\lambda^T c_m-\chi_1 t_\ell<0\ \vee\ \chi_2+\textstyle\sum\mu>0\big)\end{aligned}\tag{IC6}$$

$$\begin{aligned}\bigwedge_{i\in I}\bigwedge_{m\in M}\bigvee_{(\xi_\ell)_{\ell\in L'}\in\{0,1\}^{L'}} \exists\lambda,(\zeta_j)_{j\in J_i},\mu\geq 0.\\ \lambda^T A_m+\mu^T A'_m+\sum_{\ell\in L}\xi_\ell\tbinom{s_{\ell,i,m}}{0}^T+\sum_{j\in J_i}\zeta_j d_{i,j}^T=0\\ \wedge\ \lambda^T c_m+\mu^T c'_m+\sum_{\ell\in L}\xi_\ell t_{\ell,i,m}+\sum_{j\in J_i}\zeta_j e_{i,j}\leq 0\\ \wedge\ \big(\lambda^T c_m+\sum_{\ell\in L}\xi_\ell t_{\ell,i,m}+\sum_{j\in J_i^{\geq}}\zeta_j e_{i,j}<0\\ \vee\ \sum_{j\in J_i^{>}}\zeta_j+\textstyle\sum\mu>0\big)\end{aligned}\tag{TI6}$$

Proof of Theorem 6.15. We need to show that if there is a solution to (II5) $\wedge$ (IC5) $\wedge$ (TI5), then there is also a solution to (II6) $\wedge$ (IC6) $\wedge$ (TI6); the

converse is clear. The four variables fixed to specific values, I–IV, are discussed independently in the following.

I. Let λ, μ and ξ be a solution for the invariant initiation (II5):

$$\begin{aligned} &\lambda^T B_n + \mu^T B'_n + \xi \tbinom{s_\ell}{0}^T = 0 \\ \wedge\ &\lambda^T b_n + \mu^T b'_n + \xi t_\ell \leq 0 \\ \wedge\ &\left(\lambda^T b_n < 0 \ \vee\ \xi + \sum \mu > 0\right) \end{aligned} \tag{6.1}$$

If $\xi = 0$, there is nothing to show. Otherwise we can pick an assignment to the corresponding constraints in (II6),

$$\begin{aligned} &\lambda'^T B_n + \mu'^T B'_n + \tbinom{s_\ell}{0}^T = 0 \\ \wedge\ &\lambda'^T b_n + \mu'^T b'_n + t_\ell \leq 0 \\ \wedge\ &\left(\lambda'^T b_n < 0 \ \vee\ 1 + \sum \mu' > 0\right) \end{aligned} \tag{6.2}$$

by setting $\lambda' = \frac{\lambda}{\xi}$ and $\mu' = \frac{\mu}{\xi}$, since λ and μ only occur in these three atoms. Thus (6.1) is satisfiable iff (6.2) is.

II. Analogously to I, if $\chi_2 \neq 0$, we can divide the solution to the invariant consecution (IC5) by χ_2.

III. Let $\mathcal{K}$ denote the set of connected components in the ranking function template's dependency graph G_{T}. Furthermore, let $G_\eta = (\mathcal{K}, E)$ be the coloring graph according to Definition 6.4. This graph is finite and acyclic, therefore we find a connected component $K \in \mathcal{K}$ that has no incoming edges in G_η. We will show that fixing the values of the Motzkin coefficients of atoms where variables and function symbols from K occur is equivalent, and then remove K from the coloring graph G_η. We do this iteratively for all nodes of the coloring graph. Every atom of T contains variables or function symbols, and thus we cover all described quantifier eliminations.

First, for every red atom T_{i,j^*} where variables or function symbols from K occur, we divide the conjunct's Motzkin coefficients by the Motzkin coefficient of T_{i,j^*} analogously to I and II.

Second, the variables and function symbols of K occur in at most one blue colored atom T_{i_0,j_0} according to Definition 6.5 (b). Let ζ be the Motzkin coefficient of T_{i_0,j_0} in (TI5) as assigned by Motzkin's Theorem in transformation step 5. We assume $\zeta > 0$.

Let $\mathrm{T}_{i_0,j_{\mathrm{red}}}$ be the red atom of the conjunct $\bigvee_{j \in J_{i_0}} \mathrm{T}_{i_0,j}$ which contains T_{i_0,j_0} and let ζ_{red} be the Motzkin coefficient of $\mathrm{T}_{i_0,j_{\mathrm{red}}}$ in (TI5). We know that we already handled the $\mathrm{T}_{i_0,j_{\mathrm{red}}}$ in an earlier step, otherwise there would be an incoming edge to K in the coloring graph G_η. Thus we have divided the conjunct by ζ_{red} if $\zeta_{\mathrm{red}} \neq 0$.

For every function symbol $f \in K$ and every variable $d \in K$, we pick $\frac{\zeta}{\zeta_{\mathrm{red}}} \cdot f$ as a new assignment to f and $\frac{\zeta}{\zeta_{\mathrm{red}}} \cdot d$ as a new assignment to d ($\zeta \cdot f$ for f and $\zeta \cdot d$ for d in case $\zeta_{\mathrm{red}} = 0$). By Definition 4.2, $\mathrm{T}_{i,j}$ can be written as

$$\sum_{f \in F_{i,j}} (\alpha_f f(x) + \beta_f f(x')) + \sum_{d \in D_{i,j}} \gamma_d d \rhd 0,$$

and this is equivalent to the following by multiplication with $\frac{\zeta}{\zeta_{\text{red}}} > 0$.

$$\sum_{f \in F_{i,j}} \left(\alpha_f \Big(\frac{\zeta}{\zeta_{\text{red}}} \cdot f \Big)(x) + \beta_f \Big(\frac{\zeta}{\zeta_{\text{red}}} \cdot f \Big)(x') \right) + \sum_{d \in D_{i,j}} \gamma_d \Big(\frac{\zeta}{\zeta_{\text{red}}} \cdot d \Big) \rhd 0$$

IV. For every inductive invariant $\psi \equiv s^T x + t \rhd 0$, the multiple

$$\psi' \equiv (\xi \cdot s^T)x + \xi \cdot t \rhd 0$$

is also an inductive invariant for every $\xi > 0$ if ψ is a strict invariant ($\rhd = >$) and for all $\xi \geq 0$ if ψ is a non-strict invariant ($\rhd = \geq$). The variables of every invariant $\psi_{\ell,i,m}$ occur only in its initiation (II5), its consecution (IC5) and in exactly one template implication in (TI5) (due to the transformation step 3). Hence for every solution to (II5) $\wedge$ (IC5) we can pick $\frac{s_\ell}{\xi_\ell}$, $\frac{t_\ell}{\xi_\ell}$ as a solution to (II6) and (IC6). □

The proof of Theorem 6.15 motivates why we need the complicated restrictions to suitable colorings in Definition 6.5. These are the weakest requirements to a coloring such that we can eliminate the Motzkin coefficients of the colored atoms. We get the elimination of red atoms 'for free'—we remove these by dividing the assignments of all other Motzkin coefficients by this value. We remove blue atoms by rescaling the assignment to the template's variables and function symbols. However, we have to avoid cyclic dependencies, otherwise the rescaling operation never terminates. That is why we need to define the notion of a coloring graph in Definition 6.4.

Next, let us assess the non-linear dimension of the constraints (II0) $\wedge$ (IC0) $\wedge$ (TI0) before our transformations in Section 5.2. We want to compare this to the non-linear dimension of the constraints (II6) $\wedge$ (IC6) $\wedge$ (TI6), the output of our method.

Theorem 6.16. *Let L be the index set of invariants, let F and D be the function symbols and variables of the ranking function template T respectively. Let n denote the number of lasso program variables. The constraints* (II0) $\wedge$ (IC0) $\wedge$ (TI0) *have non-linear dimension*

$$(n+1)\#L + (n+1)\#F + \#D.$$

Proof. Non-linear operations occur only with the invariants $\psi(x)$ and the ranking function template's atoms $\mathrm{T}_{i,j}(x, x')$. Because we cannot choose x or x' since they are universally quantified, we have to choose as the set of variables that occur in non-linear operations

$$V = \{s_\ell, t_\ell \mid \ell \in L\} \cup D \cup F.$$

The vectors s_ℓ and the affine-linear function symbols $f \in F$ have a total number of n and $n+1$ variables respectively. □

Theorem 6.17. *Let T be a linear ranking function template and let $L' = L \times I \times M$ as in Section 5.2: L is the index set of invariants, M is the index set of the loop transition's disjunctions in CNF and I is the index set of conjunctions in the ranking function template's DNF. Let η be a suitable coloring for T. The constraint* (II6) $\wedge$ (IC6) $\wedge$ (TI6) *has non-linear dimension at most*

$$\#M \cdot \deg_{\mathrm{T}}(\eta) + \#L'.$$

Proof. We first count the number of Motzkin's Theorem applications in transformation step 5:

- $\#L \cdot \#M \cdot \#I \cdot \#N$ from (II4),
- $\#L \cdot (\#M)^2 \cdot \#I$ from (IC4), and
- $\#I \cdot \#M$ from (TI4).

Let n_{STEM} be the total number of inequalities in the stem transition and n_{LOOP} be the total number of inequalities in the loop transition. Thus the constraint (II6) $\wedge$ (IC6) $\wedge$ (TI6) has a total number of

$$\#L \cdot \#M \cdot \#I \cdot n_{\text{STEM}} + \#L \cdot \#M \cdot \#I \cdot n_{\text{LOOP}} + \#I \cdot n_{\text{LOOP}}$$

Motzkin coefficients λ and μ, as well as $\#L'$ Motzkin coefficients χ_1 for invariants $\#M \cdot \deg_{\text{T}}(\eta)$ Motzkin coefficients ζ for the ranking function template. □

In order to eliminate more variables in our constraints, we introduce non-decreasing invariants [18], as a restricted class of inductive invariants.

Definition 6.18 (Non-decreasing invariant)**.** An affine-linear inductive invariant $\psi(x) \equiv s^T x + t \geq 0$ is *non-decreasing* iff

$$\models \forall x, x'.\ \text{LOOP}(x, x') \to s^T x' - s^T x \geq 0.$$

Restricting the inductive invariants to non-decreasing invariants is equivalent to fixing their Motzkin coefficients χ_1 in the invariant consecution (IC6) to the value 1. This enables the following corollary to Theorem 6.17.

Corollary 6.19. *Let* T*, M and η as in Theorem 6.17. When using only non-decreasing invariants, the constraint* (II6) $\wedge$ (IC6) $\wedge$ (TI6) *has non-linear dimension at most* $\#M \cdot \deg_{\text{T}}(\eta)$*.*

Example 6.20. The inductive invariant $y \geq 1$ from Example 3.10 is in fact non-decreasing:

$$\models \forall q, y, q', y'.\ q \geq 0 \ \wedge\ q' = q - y \ \wedge\ y' = y + 1 \ \to\ y' - y \geq 0$$

Example 6.21. Consider the program $\mathbf{P}_{\text{diff42}}$ [18].

$$\begin{array}{l} q \ := \ y + 42\,; \\ \textbf{while} \ \ (q \geq 0)\,: \\ \qquad y \ := \ 2 \cdot y - q\,; \\ \qquad q \ := \ (y + q)/2\,; \end{array}$$

$\mathbf{P}_{\text{diff42}}$ instantiates the affine template with the ranking function $f(q, y) = q + 1$ and the non-decreasing supporting invariant $q - y \geq 42$:

$$q' - y' = \frac{y+q}{2} - (2y - q) = \frac{3}{2}(q - y) \geq \frac{3}{2} \cdot 42 \geq 42$$

Non-decreasing inductive invariants are weaker in expressiveness, however they still cover a wide range of practical cases. An inductive invariant is non-decreasing if

- the invariant involves only variables that are not modified by the loop transition, or

- the invariant is an equality.

Example 6.22. The variable χ_1 in the invariant consecution (IC5) cannot be generally restricted to any finite set of values analogously to Definition 6.18 without losing solutions. Let $\alpha > 1$ be some fixed constant and consider the following linear lasso program $\mathbf{P}_\alpha$:

$$\begin{aligned}&\textbf{assume}(\,y := \alpha\,);\\ &\textbf{while}\ \ (\,q \geq 0\,):\\ &\qquad q\ :=\ q - y\,;\\ &\qquad y\ :=\ \tfrac{1}{\alpha}(y + \alpha - 1)\,;\end{aligned}$$

The program $\mathbf{P}_\alpha$ terminates, because $y \geq 1$ is an invariant of $\mathbf{P}_\alpha$. Furthermore, the invariant is inductive: the stem $y = \alpha$ implies $y \geq 1$, and

$$y' = \frac{y + \alpha - 1}{\alpha} = \frac{y}{\alpha} + \frac{\alpha - 1}{\alpha} \geq \frac{1}{\alpha} + \frac{\alpha - 1}{\alpha} = 1.$$

However, $y \geq 1$ is not a non-decreasing invariant:

$$y' - y = \frac{y + \alpha - 1}{\alpha} - y = \frac{\alpha - 1}{\alpha} \cdot (1 - y). \tag{6.3}$$

We are stuck, because (6.3) cannot be inferred to be non-negative: there is no lower bound on $-y$. We have to choose $\chi_1 = \frac{1}{\alpha}$ in (IC6) because

$$y' - \frac{1}{\alpha} \cdot y = \frac{y + \alpha - 1}{\alpha} - \frac{1}{\alpha} \cdot y = \frac{\alpha - 1}{\alpha} \geq 0.$$

In fact, every value $\chi_1 > \frac{1}{\alpha}$ will not work for the same reason as in (6.3).

Corollary 6.23. *If the linear ranking function template* T *has degree* ≤ 0 *and we consider only non-decreasing invariants, then the constraint* (II6) $\wedge$ (IC6) $\wedge$ (TI6) *is linear.*

Proof. According to Corollary 6.19, the constraints have non-linear dimension at most $\#M \cdot \deg_{\mathrm{T}}(\eta)$ for a suitable coloring η of T. Consequently, for $\deg_{\mathrm{T}}(\eta) = 0$, we have no non-linear operations. Since there is no universal quantification, the generated constraint is linear by Definition 6.9. □

The constraints generated by $\mathrm{T}_{\mathrm{affine}}$ are due Podelski and Rybalchenko [27]. In [18] this template is extended to incorporate non-decreasing inductive invariants, and the generated template coincides with the one generated here, if we restrict ourselves to non-decreasing invariants and conjunctive linear lasso programs.

6.3 Application to our Templates

In this section we assess the degree of the ranking function templates introduced in Chapter 4. See Figure 6.2 on page 46 for a visualization.

Lemma 6.24. *The ranking function template* $\mathrm{T}_{k-\mathrm{phase}}$ *has degree* $\frac{1}{2}k(k-1)$.

Proof. Consider the following coloring η.

$$\begin{aligned}
&\bigwedge_{i=1}^{k} \delta_i > 0 \\
\wedge\ &\Big(f_1(x) > 0 \ \vee\ \bigvee_{i=1}^{k} f_i(x) > 0\Big) \\
\wedge\ &f_1(x') < f_1(x) - \delta_1 \\
\wedge\ &\bigwedge_{i=2}^{k} \Big(f_i(x') < f_i(x) - \delta_i \ \vee\ f_1(x) > 0 \ \vee\ \bigvee_{j=2}^{i-1} f_j(x) > 0\Big)
\end{aligned}$$

We check the requirements of Definition 6.5:

a) Every conjunct contains exactly one red atom.

b) The sets $\{f_i, \delta_i\}$ are the connected components of $\mathrm{T}_{k-\mathrm{phase}}$ according to Example 6.2.

c) The coloring graph G_η has the edges $([f_1], [f_i])$ for $i = 2, \dots, k$. Hence it is acyclic.

We conclude that η is a suitable coloring of $\mathrm{T}_{k-\mathrm{phase}}$.

$$\deg_{\mathrm{T}_{k-\mathrm{phase}}}(\eta) = \frac{k(k+5)}{2} - (k-1) - (2k+1) = \frac{k(k-1)}{2}.$$

The number of blue colored atoms is $k-1$ and the number of connected components is k, therefore, by Lemma 6.11, this degree is minimal. □

Example 6.25. Consider the 2-phase template defined in Definition 4.13. It has degree $\frac{1}{2} \cdot 2(2-1) = 1$. When considering only non-decreasing supporting invariants, Corollary 6.19 states that the generated constraints have non-linear dimension at most $\#M$, where $\#M$ is number of disjunctions in the normal form of the linear lasso program's loop transition. If we build constraints for the lasso program $\mathbf{P}_{2-\mathrm{phase}}$ from Example 4.12, we have only one non-linear variable according to Theorem 6.17 when considering non-decreasing supporting invariants.

Lemma 6.26. *The ranking function template* $\mathrm{T}_{k-\mathrm{piece}}$ *has degree* $2k^2 - 1$.

Proof. Consider the following coloring η.

$$\begin{aligned}
&\delta > 0 \\
\wedge\ &\bigwedge_{i=1}^{k} \Big(g_i(x) < 0 \ \vee\ g_i(x') < 0 \ \vee\ f_i(x') < f_i(x) - \delta\Big) \\
\wedge\ &\bigwedge_{i=1}^{k} \bigwedge_{j \neq i} \Big(g_i(x) < 0 \ \vee\ g_j(x') < 0 \ \vee\ f_j(x') < f_i(x) - \delta\Big) \\
\wedge\ &\bigwedge_{i=1}^{k} f_i(x) > 0 \\
\wedge\ &\Big(g_1(x) \geq 0 \ \vee\ \bigvee_{i=2}^{k} g_i(x) \geq 0\Big)
\end{aligned}$$

We check the requirements of Definition 6.5:

a) Every conjunct contains exactly one red atom.

b) The sets $\{g_i\}$ and $\{\delta, f_1, \dots, f_k\}$ are the connected components of $\mathrm{T}_{k-\mathrm{piece}}$ according to Example 6.2.

c) The coloring graph G_η has the edges $([\delta], [g_i])$ for all i and $([g_i], [g_1])$ for $i > 1$. Hence it is acyclic.

We conclude that η is a suitable coloring of $\mathrm{T}_{k-\mathrm{piece}}$.

$$\deg_{\mathrm{T}_{k-\mathrm{piece}}}(\eta) = (3k^2 + 2k + 1) - k - (k^2 + k + 2) = 2k^2 - 1.$$

The number of blue colored atoms is k and the number of connected components is $k + 1$, therefore, by Lemma 6.11, this degree is minimal. □

Lemma 6.27. *The ranking function template* $\mathrm{T}_{k-\mathrm{lex}}$ *has degree* $\frac{1}{2}(k-1)(k-2)$.

Proof. This proof is similar to the proof of Lemma 6.24 since the lexicographic termination has the same dependency graph as the multiphase template. Consider the following coloring η.

$$\begin{aligned}
&\bigwedge_{i=1}^{k} \delta_i > 0 \\
\wedge\ &\bigwedge_{i=1}^{k} f_i(x) > 0 \\
\wedge\ &f_1(x') \le f_1(x) \\
\wedge\ &\bigwedge_{i=2}^{k-1} \Big(f_i(x') \le f_i(x) \ \vee\ f_1(x') < f_1(x) - \delta_1 \ \vee \bigvee_{j=2}^{i-1} f_j(x') < f_j(x) - \delta_j \Big) \\
\wedge\ &\Big(f_k(x') < f_k(x) - \delta_k \ \vee\ f_1(x') < f_1(x) - \delta_1 \ \vee \bigvee_{i=2}^{k-1} f_i(x') < f_i(x) - \delta_i \Big)
\end{aligned}$$

We check the requirements of Definition 6.5:

a) Every conjunct contains exactly one red atom.

b) $\{f_i, \delta_i\}$ are the connected components of $\mathrm{T}_{k-\mathrm{lex}}$ according to Example 6.2.

c) The coloring graph G_η has the edges $([f_i], [f_1])$ for all $i > 1$. Hence it is acyclic.

We conclude that η is a suitable coloring of $\mathrm{T}_{k-\mathrm{lex}}$.

$$\deg_{\mathrm{T}_{k-\mathrm{lex}}}(\eta) = \frac{k(k+5)}{2} - (k-1) - 3k = \frac{(k-1)(k-2)}{2}.$$

The number of blue colored atoms is $k - 1$ and the number of connected components is k, therefore, by Lemma 6.11, this degree is minimal. □

Example 6.28. The program $\mathbf{P}_{\text{gcd}}$ from Example 4.22 instantiates the 2-lexicographic template. The two invariants $y_1 \geq 1$ and $y_2 \geq 1$ are non-decreasing. The coloring η from Lemma 6.27 has degree

$$\deg_{\mathrm{T}_{2-\text{lex}}}(\eta) = \frac{1}{2} \cdot 1 \cdot 0 = 0.$$

Consequently, by Corollary 6.23, the generated constraints are linear if we are considering non-decreasing invariants, and otherwise

$$\#L' = \#L \cdot \#I \cdot \#M = 1 \cdot 6 \cdot 2 = 12$$

by Theorem 6.17.

6.4 Overview

Linear ranking function templates use affine-linear function variables to synthesize a termination argument. When constructing a ranking function from the assignment to these function variables, the ordinal ranking equivalents (Definition 4.7) of these linear functions turn out to be central components. The image of the ranking functions constructed from the ordinal ranking equivalents is an ordinal, namely the *ranking structure* of T.

The following table gives an overview of the presented ranking function templates: the affine template, the k-phase template, the k-piece template and the k-lexicographic template. We state the number of conjuncts and atoms when written in CNF, the number of connected components in their dependency graph, their ranking structure and degree (as proven in Section 6.3).

	$\mathrm{T}_{\text{affine}}$	$\mathrm{T}_{k-\text{phase}}$	$\mathrm{T}_{k-\text{piece}}$	$\mathrm{T}_{k-\text{lex}}$
Conjuncts	3	$2k+1$	k^2+k+2	$3k$
Atoms	3	$\frac{1}{2}k(k+5)$	$3k^2+2k+1$	$\frac{1}{2}k(k+5)$
Connected comp.	1	k	$k+1$	k
Ranking structure	ω	$\omega \cdot k$	ω	ω^k
Degree	0	$\frac{1}{2}k(k-1)$	$2k^2-1$	$\frac{1}{2}(k-1)(k-2)$

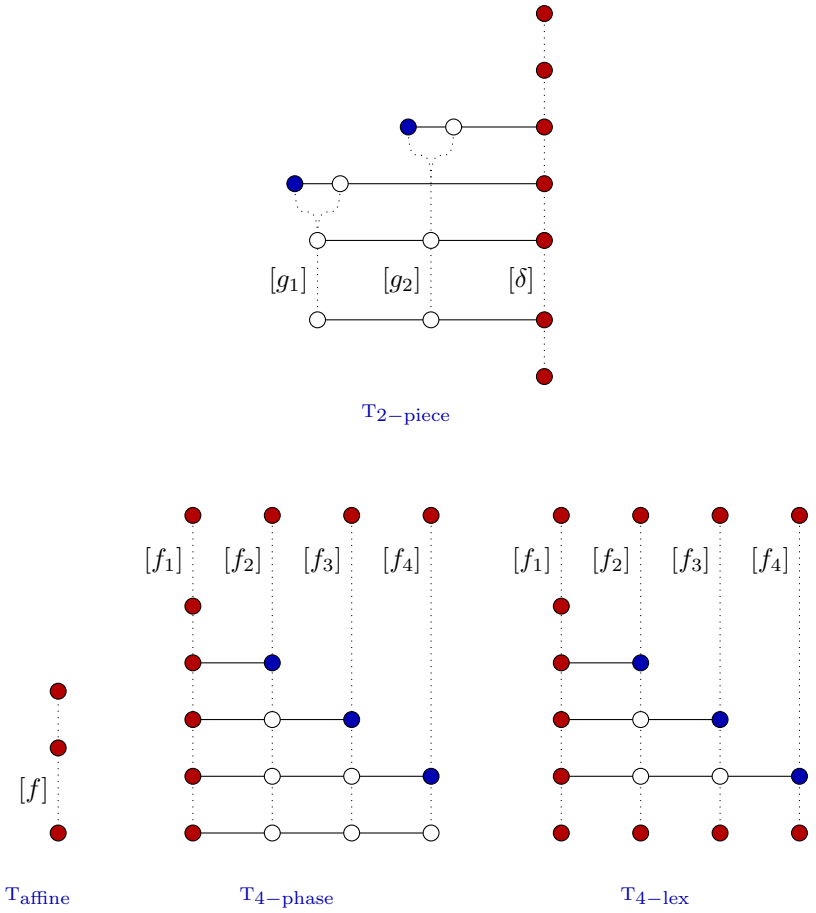


Figure 6.2: Visualization of suitable colorings for the 2-piece, affine, 4-phase and 4-lexicographic ranking function template. Every circle represents an occurrence of an atom; its color is determined by η. Two circles are connected with a solid line if they occur together in one conjunct. Every connected component of the coloring graph is represented by a dotted line that connects all atoms where these variable and function symbols occur. We can now easily check the conditions of Definition 6.5: every solid line connects exactly one red circle (a), every dotted line connects at most one blue circle (b). We can extract the coloring graph by drawing a directed edge between two connected components if there is a solid line connecting a red circle with a blue one (c). The degree of the templates is the number of white circles (uncolored atoms).

Chapter 7

Solving the Constraints

In Chapter 5 we constructed constraints that are satisfiable for a given linear lasso program only if there exists a ranking function of a specialized form. These constraints are of the existential fragment of non-linear real arithmetic. In this chapter we want to discuss strategies available for solving these constraints.

Since Tarski published the first decision procedure for the first order theory of the reals [32], several other algorithms have been proposed (an overview can be found in Grant Passmore's PhD thesis [26]). The Grigor'ev–Vorobjov–Theorem states that, in theory, the existential fragment of non-linear real arithmetic can be solved in single exponential time [13]. However, this bound seems to be only of limited practical relevance [19]. *Cylindrical algebraic decomposition* (CAD) is most successful in practice, despite its doubly exponential worst case complexity bound. This is still an active area of research and recently significant progress has been achieved in terms of running time [21].

For Farkas' Lemma based constraints, specialized solving algorithms have been thought out, e.g. under-approximation using heuristics [9, 30] and bisection search combined with linear constraint solving [4]. However, we found it is both feasible and practical to utilize an off-the-shelf SMT solver to find a solution to small and medium-sized examples. Nonetheless, in this section we want to examine the CAD algorithm for our case in detail and discuss some possible runtime mitigation. The goal is to motivate that while the generated constraints are indeed non-linear, for most practical cases they are still not vastly more difficult to solve than a linear constraint.

After a brief introduction to cylindrical algebraic decomposition in Section 7.1, we exemplary solve the constraints corresponding to one invariant consecution in Section 7.2. We show that invariants that depend only on a constant number of loop inequalities correspond to solutions of the non-linear system that can be discovered in polynomial time.

7.1 Introduction to CAD

Cylindrical algebraic decomposition was first presented by Collins [8]. We give a brief introduction by example based on Jirstrand's technical report [20].

The goal is to find a partition of $\mathbb{R}^n$ such that the given set of polynomials have constant sign on each component. These components are finitely repre-

sented by single points; satisfiability of the non-linear constraints can be decided by checking these representative points.

Example 7.1. Consider the following system of polynomial equations in the two variables x and y.

$$\begin{aligned} x^2 + y^2 - 2 &< 0 \\ x^3 - y^2 &= 0 \end{aligned} \tag{7.1}$$

The two involved polynomials are $p_1(x, y) = x^2 + y^2 - 2$ and $p_2(x, y) = x^3 - y^2$.

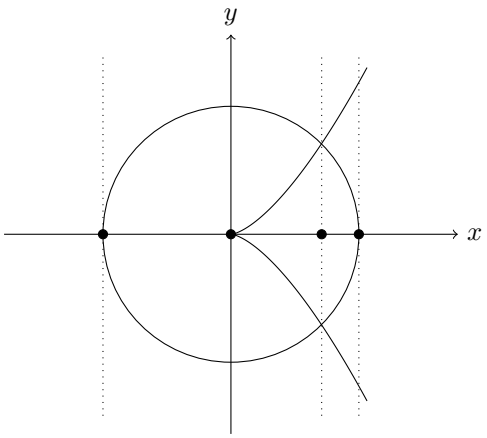


Figure 7.1: The zero sets of the polynomials in (7.1) and some projections on the x-axis (solid dots).

The algorithm works in three phases:

1. *The projection phase:* all points of zero sets corresponding to vertical tangents, singularities and intersections are projected to the lower dimension eliminating one variable.
2. *The base phase:* For mono-variant polynomials, all roots can be enumerated and we thus get a sign-invariant decomposition of $\mathbb{R}^1$.
3. *The extension phase:* The technique of the base phase is applied recursively to lift the sign invariant decomposition from $\mathbb{R}^i$ to $\mathbb{R}^{i+1}$.

In Example 7.1, projection to the x-axis yields the solid dots as depicted in Figure 7.1. These are the two points $(-\sqrt{2}, 0)$ and $(\sqrt{2}, 0)$ corresponding to vertical tangents of p_1, as well as $(0, 0)$, the singularity of p_2, and finally $(1, 0)$, the projection of the intersection points $(1, 1)$ and $(1, -1)$ of p_1 and p_2. This gives us the decomposition on the x-axis defined by these four points as well as the intervals inbetween them. We can evaluate the signs of the polynomials p_1 and p_2 on these regions:

x	$(-\infty, -\sqrt{2})$	$-\sqrt{2}$	$(-\sqrt{2}, 0)$	0	$(0, 1)$	1	$(1, \sqrt{2})$	$\sqrt{2}$	$(\sqrt{2}, \infty)$
$\text{sign}(p_1(x))$	$+$	0	$-$	$-$	$-$	$-$	$-$	0	$+$
$\text{sign}(p_2(x))$	$-$	$-$	$-$	0	$+$	$+$	$+$	$+$	$+$

Over each region, we can calculate recursively the decomposition of $\mathbb{R}^2$ and check for points that satisfy the system of inequalities (7.1); in our example, the point $(0, 0)$ is a possible solution.

For the precise definition of the projection phase, along with the required notion of *principal subresultant coefficients* (psc) used in the proof of Lemma 7.2, we reference Jirstrand's report [20] as this would go far beyond the scope of this work.

7.2 Solving with CAD

As an illustration we discuss the CAD of the invariant consecution. In theory the arguments offered here also apply to the complete constraints, although admittedly additional difficulties arise due to the simultaneous presence of more than one variable that occurs in non-linear operations.

We start with a single invariant consecution (IC4):

$$\forall x, x'.\ \psi_\ell(x) \wedge \textsc{loop}_m(x, x') \to \psi_\ell(x') \tag{7.2}$$

For clarity, we drop the indices m of LOOP and ℓ of ψ. Recall that we write

$$\begin{aligned} \textsc{loop}(x, x') &\equiv Ax \leq b \ \wedge\ A'x < b', \\ \psi(x) &\equiv s^T x + t \geq 0. \end{aligned}$$

After applying Motzkin's Theorem in transformation step 5, we get (IC5) and fixing the value of χ_2 according to Theorem 6.15, the constraints (IC6) corresponding to (7.2) are

$$\begin{aligned} \exists \lambda, \chi, \mu \geq 0.\ & \lambda^T A + \mu^T A' + \tbinom{0}{s}^T - \chi \tbinom{s}{0}^T = 0 \\ & \wedge\ \lambda^T c + \mu^T c' + (1 - \chi)t \leq 0 \\ & \wedge\ (\lambda^T c - \chi t < 0\ \vee\ \sum \mu > 0) \end{aligned} \tag{7.3}$$

We are solving for the vectors $\lambda, \mu,\ s \in \mathbb{K}^n$, and the variables $\chi \in \mathbb{K}$ and $t \in \mathbb{K}$. The matrices A, A' and vectors c, c' are constant. Hence the only non-linear terms are $\chi \binom{s}{0}^T$ and χt. If we find an assignment for χ, the constraints become linear and thus can be solved using an SMT solver for linear arithmetic, which have polynomial runtime complexity [31].

For simplification, we focus on the first disjunct in (7.3) (classical case), since the other case is structurally very similar. Let $A = (a_{i,j})$, $\lambda = (\lambda_1 \dots \lambda_m)^T$, and $s = (s_1 \dots s_n)^T$. We write (7.3) explicitly:

$$\chi \geq 0 \tag{7.4}$$

$$\lambda_i \geq 0, \qquad \text{for } 1 \leq i \leq m \tag{7.5}$$

$$\sum_{i=1}^{m} a_{i,j}\lambda_i - \chi s_j = 0, \qquad \text{for } 1 \leq j \leq n \tag{7.6}$$

$$\sum_{i=1}^{m} a_{i,n+j}\lambda_i + s_j = 0, \qquad \text{for } 1 \leq j \leq n \tag{7.7}$$

$$\sum_{i=1}^{m} c_i\lambda_i - (1 - \chi)t < 0 \tag{7.8}$$

We solve (7.7) for s_j and eliminate s_j from (7.6) yielding the following system of equations.

$$\chi \geq 0 \tag{7.9}$$

$$\lambda_i \geq 0, \qquad \text{for } 1 \leq i \leq m \tag{7.10}$$

$$\sum_{i=1}^{m}(a_{i,j} + a_{i,n+j}\chi)\lambda_i = 0, \qquad \text{for } 1 \leq j \leq n \tag{7.11}$$

$$\sum_{i=1}^{m} c_i\lambda_i - (1-\chi)t \leq 0 \tag{7.12}$$

We ignore the constraint (7.12) because in the case where $\chi \neq 1$, we can always assign t such that this inequality holds. For the projection we choose the ordering $\lambda_1, \ldots, \lambda_m, \chi$. The set of polynomials for the CAD is

$$P = \{\chi, \lambda_i \mid 0 \leq i \leq m\} \cup \Big\{ \sum_{i=1}^{m}(a_{i,n+j}\chi + a_{i,j})\lambda_i \mid 0 \leq j \leq n \Big\}. \tag{7.13}$$

In particular, the coefficient polynomials to λ_i in (7.13) are linear in χ.

Lemma 7.2. *In every projection step k in the CAD of (7.13), the set of polynomials*

$$P_k = \{\lambda_i \mid k \leq i \leq m\} \;\cup\; \Big\{ \sum_{i=k}^{m} p_{i,j}(\chi)\lambda_i \mid j \in J_k \Big\} \;\cup\; \{q_\ell(\chi) \mid \ell \in L_k\} \tag{7.14}$$

for suitable index sets J and L. The polynomials $p_{i,j}$ and q_ℓ only involve the variable χ.

Proof. We proceed inductively. Clearly (7.13) satisfies this criterion. Consider the projection of λ_k.

- For every polynomial $p \in P_k$, we take $p(\lambda_k = 0)$. This yields $\lambda_{k+1}, \ldots, \lambda_m$, $\sum_{i=k+1}^{m} p_{i,j}(\chi)\lambda_i$ and preserves $q_\ell(\chi)$.
- For every polynomial $p \in P_k$, we calculate $\operatorname{psc}_{\lambda_k}(p, \frac{\partial p}{\partial \lambda_k})$. Since p is linear in λ_k, this yields the same results as the previous step.
- For every pair of polynomials $p_{j_1}, p_{j_2} \in P_k$, we calculate

$$\begin{aligned} &\operatorname{psc}_{\lambda_k}(p_1, p_2) \\ &= \operatorname{psc}_{\lambda_k}\Big(\sum_{i=k}^{m} p_{i,j_1}(\chi)\lambda_i, \sum_{i=k}^{m} p_{i,j_2}(\chi)\lambda_i\Big) \\ &= \sum_{i=k+1}^{m} \Big(\frac{\operatorname{lcm}(p_{k,j_1}, p_{k,j_2})}{p_{k,j_1}} p_{i,j_1}(\chi) - \frac{\operatorname{lcm}(p_{k,j_1}, p_{k,j_2})}{p_{k,j_2}} p_{i,j_2}(\chi)\Big)\lambda_i. \end{aligned}$$

  This is again of the form given in (7.14). □

According to Lemma 7.2, after m projection steps we are left with a set of polynomials $P_m = \{q_\ell(\chi) \mid \ell \in L_m\}$ dependent only on the variable χ.

Lemma 7.3. *The following holds for P_m.*

I. The degree of any $q_\ell \in P_m$ is at most 2^m.

II. $\#P_m \leq n^{2^m}$.

III. The number of distinct roots of all $q_\ell \in P_m$ *is bounded by* $2^m n^{2^m}$.

Proof.

I. Initially, all polynomials are linear. In every projection step, the maximum degree of polynomials can at most double as the least common multiple's degree is less or equal to the degree of the product.

II. Since each polynomial is connected with every other polynomial, the number of distinct new polynomials is at most squared in every projection step.

III. Follows directly from I and II. □

More importantly, the number of projection steps depend on the number of λ-variables m. Motzkin's Theorem introduces one λ-variable for every inequality in (M1). Therefore the runtime scales with the number of statements relevant to prove the invariant consecution. We assume that in practice, only a small (maybe even constant) number of inequalities is required to prove an invariant. This greatly reduces the bound in Lemma 7.3 III.

Theorem 7.4. *Invariants that depend only on a constant number of loop inequalities can be discovered in polynomial time.*

Proof. Let e be the bound on the required loop inequalities. There are $\binom{m}{e} \leq m^e$ possibilities to select e of the m inequalities. We search for a solution to (7.2) by applying CAD to (7.10) and (7.11). The result is described by Lemma 7.2 and Lemma 7.3 states the bound $2^e n^{2^e}$ for distinct values of χ. Given possible assignments to χ, we plug every one of these into the constraints (7.3) and solve using a solver for linear arithmetic. Satisfiability for linear arithmetic is decidable in polynomial time [31] and we only have polynomially many values for χ to try since e is constant. □

Although Theorem 7.4 gives a polynomial algorithm for solving the constraints, it is not practical. It would be a great deal more efficient to follow the CAD algorithm in constructing the solution, which has been omitted here for simplicity of presentation. Additionally, there is no good reason not to enlarge e to take more loop inequalities into consideration until a predefined time limit runs out.

Chapter 8

Conclusion

The scope of this work is a new method for synthesizing termination arguments for linear lasso programs. This method generalizes existing methods and extends them in various ways. In Section 1.1 we elaborated on how our method relates to existing research.

We introduced the notion of *ranking function templates* in Chapter 4 and discussed the affine, multiphase, piecewise and lexicographic templates in detail. For the affine-linear functions used in the ranking function templates, we introduced the notion of *ordinal ranking equivalent* in order to naturally build ranking functions using ordinal arithmetic from assignments for the template's variables and functions symbols.

The *multiphase ranking function* is a novel type of ranking function and received some more detailed investigation. We showed that there are conjunctive linear lasso programs that do not have a multiphase ranking function (Example 4.16) and we showed that the existence of a multiphase ranking function does not entail information about the program's complexity (Example 4.17).

Notable formal results in this work are the undecidability proof for termination of linear lasso programs (Theorem 3.18) and the theorem regarding the removal of quantifiers in our constraints (Theorem 6.15).

Other contributions include the soundness and completeness statements for our method (Theorem 5.3 and Theorem 5.4), the discourse about the treatment of mixed integer variable domains (Section 5.4), the assessment of the non-linear dimension before and after our transformations to the constraints (Theorem 6.16, Theorem 6.17, Corollary 6.19 and Corollary 6.23) and the motivation why solving the resulting constraints is not necessarily very difficult (Section 7.2). An overview over the ranking function templates we consider and their properties can be found in Section 6.4, including their non-linear dimension and their ordinal ranking structure.

8.1 Future Work

For future work, it would be interesting to see new ranking function templates. There certainly are more types of ranking functions that can be formalized by ranking function templates. One could investigate the use of affine-linear, multiphase, piecewise and lexicographic templates as a 'construction kit'. For

example, they could be combined to more general templates by replacing single affine-linear functions in the lexicographic template by a piecewise or multiphase ranking function.

Furthermore, it seems vital to implement our method and try it on real world examples. Only experimental evaluation will tell which ranking function templates are both computationally feasible and practically relevant. Ideally, our method would be used in conjunction with a tool that is able to combine termination arguments for lasso programs to a termination argument for a complex program.

Moreover, the selection of a ranking function template is not part of our method. A heuristic could be devised that intelligently suggests a template by looking at the program code. This could reduce required human interaction and/or speed up the termination argument synthesis.

Our method is not complete on integer lasso programs as discussed in Section 5.4. Possibly there is a way of making the polyhedra integral even though they contain free variables. Otherwise, a different approach for integers needs to be developed. As integer variables are extremely common in real life code, this topic requests further attention.

The complexity of our method is centrally determined by the complexity of non-linear algebraic constraint solving. Any progress being made in this field improves the applicability of our method. Non-linear constraint solving is an active area of research and recent progress [21] suggests that algorithmic improvements are not yet exhausted.

Another plot line unfinished is the decidability of the termination of conjunctive linear lasso programs. We conjectured in Conjecture 3.19 that this is decidable, but a proof remains due.

Acknowledgements

I would like to thank my supervisor Matthias Heizmann for all his patience and support. The dialogue with him and his continued encouragement was invaluable to this work. Furthermore, I extend my gratitude to Fabian Reiter and Pascal Raiola for their very helpful corrections and suggestions.

Errata

This is an error corrected version of the original thesis, updated last on November 6, 2013. The most important changes are:

- Removed Lemma 3.13 because its statement was false. Thanks go to Amir Ben-Amram for pointing this out.
- Added missing ξ_ℓ in item TI6.
- Fixed step size in Example 4.8.
- Corrected the coloring of $\tau_{k-\text{lex}}$ in Lemma 6.27.
- Fixed Typos

Bibliography

[1] E. Albert, P. Arenas, S. Genaim, and G. Puebla. Closed-form upper bounds in static cost analysis. *J. Autom. Reasoning*, 46(2):161–203, 2011.

[2] A. M. Ben-Amram and S. Genaim. On the linear ranking problem for integer linear-constraint loops. In *POPL*, pages 51–62, New York, NY, USA, 2013. ACM.

[3] A. M. Ben-amram, S. Genaim, and A. N. Masud. On the termination of integer loops. In *VMCAI*, pages 72–87. Springer, 2012.

[4] A. R. Bradley, Z. Manna, and H. B. Sipma. Linear ranking with reachability. In *CAV*, pages 491–504. Springer, 2005.

[5] A. R. Bradley, Z. Manna, and H. B. Sipma. The polyranking principle. In *ICALP*, pages 1349–1361. Springer, 2005.

[6] M. Braverman. Termination of integer linear programs. In *CAV*, pages 372–385. Springer, 2006.

[7] P. J. Charles, J. M. Howe, and A. King. Integer polyhedra for program analysis. In *AAIM*, pages 85–99. Springer, 2009.

[8] E. G. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata Theory and Formal Languages*, volume 33, pages 134–183. Springer, 1975.

[9] M. A. Colón, S. Sankaranarayanan, and H. B. Sipma. Linear invariant generation using non-linear constraint solving. In *CAV*, pages 420–432. Springer, 2003.

[10] B. Cook, J. Fisher, E. Krepska, and N. Piterman. Proving stabilization of biological systems. In *VMCAI*, pages 134–149, 2011.

[11] B. Cook, A. Podelski, and A. Rybalchenko. Terminator: Beyond safety. In *CAV*, pages 415–418, 2006.

[12] H.-D. Ebbinghaus, J. Flum, and W. Thomas. *Mathematical Logic*. Springer, 1984.

[13] D. Y. Grigor'ev and J. N. N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *Journal of Symbolic Computation*, 5(1-2):37–64, 1988.

[14] S. Gulwani and F. Zuleger. The reachability-bound problem. In *PLDI*, pages 292–304, 2010.

[15] A. Gupta, T. A. Henzinger, R. Majumdar, A. Rybalchenko, and R.-G. Xu. Proving non-termination. In *POPL*, pages 147–158, 2008.

[16] W. R. Harris, A. Lal, A. V. Nori, and S. K. Rajamani. Alternation for termination. In *SAS*, pages 304–319, 2010.

[17] M. Hartmann. Cutting planes and the complexity of the integer hull. Technical report, Ithaca, NY, USA, 1988.

[18] M. Heizmann, J. Hoenicke, J. Leike, and A. Podelski. Linear ranking for linear lasso programs. In *ATVA*, 2013.

[19] H. Hong and C. L. Comparison of several decision algorithms for the existential theory of the reals. Technical report, 1991.

[20] M. Jirstrand. Cylindrical algebraic decomposition – an introduction. Technical report, S-581 83 Linköping, Sweden, 1995.

[21] D. Jovanović and L. D. Moura. Solving non-linear arithmetic. In *IJCAR*, pages 339–354. Springer, 2012.

[22] D. Kroening, N. Sharygina, S. Tonetta, A. Tsitovich, and C. M. Wintersteiger. Loop summarization using abstract transformers. In *ATVA*, pages 111–125, 2008.

[23] D. Kroening, N. Sharygina, A. Tsitovich, and C. M. Wintersteiger. Termination analysis with compositional transition invariants. In *CAV*, pages 89–103, 2010.

[24] K. Kunen. *Set Theory*. Elsevier, 1980.

[25] M. Minsky. Recursive unsolvability of post's problem of 'tag'. *Annals of Mathematics*, 74(3):437–455, 1961.

[26] G. O. Passmore. *Combined Decision Procedures for Nonlinear Arithmetics, Real and Complex*. PhD thesis, University of Edinburgh, 2011.

[27] A. Podelski and A. Rybalchenko. A complete method for the synthesis of linear ranking functions. In *VMCAI*, pages 239–251. Springer, 2004.

[28] A. Podelski and S. Wagner. A sound and complete proof rule for region stability of hybrid systems. In *HSCC*, pages 750–753, 2007.

[29] A. Rybalchenko. Constraint solving for program verification theory and practice by example. In *CAV*, pages 57–71. Springer, 2010.

[30] S. Sankaranarayanan, H. B. Sipma, and Z. Manna. Constraint-based linear-relations analysis. In *SAS*, pages 53–68. Springer, 2004.

[31] A. Schrijver. *Theory of linear and integer programming*. Wiley-Interscience series in discrete mathematics and optimization. Wiley, 1999.

[32] A. Tarski. A decision method for elementary algebra and geometry. Technical report, RAND Corporation, 1951.

[33] A. Tiwari. Termination of linear programs. In *CAV*, pages 70–82. Springer, 2004.