When Less Is More: Consequence-Finding in a Weak Theory of Arithmetic

ZACHARY KINCAID∗, Princeton University, United States
NICOLAS KOH∗, Princeton University, United States
SHAOWEI ZHU∗, Princeton University, United States

This paper presents a theory of non-linear integer/real arithmetic and algorithms for reasoning about this theory. The theory can be conceived of as an extension of linear integer/real arithmetic with a weakly-axiomatized multiplication symbol, which retains many of the desirable algorithmic properties of linear arithmetic. In particular, we show that the conjunctive fragment of the theory can be effectively manipulated (analogously to the usual operations on convex polyhedra, the conjunctive fragment of linear arithmetic). As a result, we can solve the following consequence-finding problem: given a ground formula $F$, find the strongest conjunctive formula that is entailed by $F$. As an application of consequence-finding, we give a loop invariant generation algorithm that is monotone with respect to the theory and (in a sense) complete. Experiments show that the invariants generated from the consequences are effective for proving safety properties of programs that require non-linear reasoning.

CCS Concepts: • Theory of computation → Automated reasoning; Program analysis; Invariants; • Mathematics of computing → Gröbner bases and other special bases.

Additional Key Words and Phrases: Decision procedures, theory of arithmetic, convex polyhedra, polynomial ideals, program analysis, nonlinear invariant generation

ACM Reference Format:

1 INTRODUCTION

The theory of linear integer/real arithmetic possesses characteristics that make it useful across a range of applications. Foremost, it is a decidable theory, with practical decision procedures based on (integer) linear programming. Beyond decidability, the conjunctive fragments of linear real and integer arithmetic (corresponding to convex polyhedra and the integer points within them, respectively) can be manipulated effectively. This fact has been leveraged, for instance, for invariant generation [Colón et al. 2003; Cousot and Halbwachs 1978], termination analysis [Podelski and Rybalchenko 2004], optimization [Bjørner et al. 2015; Li et al. 2014; Sebastiani and Tomasi 2012], and program transformation [Feautrier 1996; Lengauer 1993].

Including multiplication in the language of arithmetic has a dramatic effect on the resulting theory. Non-linear (integer) arithmetic is not even recursively axiomatizable, let alone decidable. As a result,

∗The authors are listed in alphabetical order.

Authors’ addresses: Zachary Kincaid, Princeton University, Princeton, NJ, United States, zkincaid@cs.princeton.edu; Nicolas Koh, Princeton University, Princeton, NJ, United States, ekoh@cs.princeton.edu; Shaowei Zhu, Princeton University, Princeton, NJ, United States, shaoweiz@cs.princeton.edu.

This work is licensed under a Creative Commons Attribution 4.0 International License.

© 2023 Copyright held by the owner/author(s).

2473-1421/2023/1-ART44

https://doi.org/10.1145/3571237
solvers for non-linear arithmetic rely on heuristic reasoning techniques [Borrilleras et al. 2019, 2009; Fuhs et al. 2007; Jovanović 2017; Kremer et al. 2016], and algorithms for manipulating the conjunctive fragment (e.g., [Bagnara et al. 2005; Kincaid et al. 2017]) are imprecise. The use of such heuristics precludes clients of non-linear solvers and abstract domains from satisfying desirable properties— for instance, there are no non-trivial complete ranking function synthesizers or monotone invariant generation schemes for non-linear integer arithmetic. And while heuristics are often effective in practice, they can also be unpredictable. For instance, Hawblitzel et al. [2014] reports “we found Z3’s theory of nonlinear arithmetic to be slow and unstable; small code changes often caused unpredictable verification failures,” which prompted the authors to develop information-hiding techniques to avoid triggering non-linear heuristics.

This paper develops the theory of linear integer/real rings (LIRR)—commutative rings extended with an order relation and an “integer” predicate that obey certain axioms from the theory of linear integer/real arithmetic. While all axiomatizable theories of non-linear arithmetic are incomplete, LIRR is weak by design (relative to say Peano arithmetic), trading power for tractable automated reasoning:

- LIRR is decidable. Furthermore, LIRR does not lose any of the reasoning power of linear integer/real arithmetic (in a sense made precise in Theorems 1 and 8).
- The conjunctive fragment of LIRR can be manipulated effectively, analogously to convex polyhedra. This enables some clients of linear arithmetic (for instance, recurrence-based loop invariant generation—see Section 5) to be “lifted” to non-linear arithmetic.
- LIRR is axiomatized by Horn clauses. This implies existence of minimal models [Van Emden and Kowalski 1976], which simplifies consequence-finding. It also ensures that the theory is convex [Tinelli 2003] (and stably infinite), so LIRR can be combined with other theories via the Nelson-Oppen protocol [Nelson and Oppen 1979].

The key technical contribution of this paper is a suite of algorithms for manipulating algebraic cones—a set of polynomials that can be represented as the sum of a polynomial ideal and a polyhedral cone. Algebraic cones can be seen as a representation of a system of polynomial equalities and inequalities (analogous to the constraint representation of a convex polyhedron). Similarly, congruence constraints can be represented by an algebraic lattice—a sum of a polynomial ideal and a point lattice. Algebraic cones and lattices are the basis of our decision procedure for the problem of testing satisfiability of a ground formula modulo LIRR, wherein they serve as a representation of a Herbrand model. We show that algebraic cones can be effectively manipulated like convex polyhedra: membership and emptiness are decidable, and algebraic cones are closed under intersection, sum, projection, inverse homomorphism, and cutting plane closure with respect to an algebraic lattice (analogous to computing the convex hull of the integer points within a convex polyhedron).

Algorithms for algebraic cones arise as a marriage of techniques between polynomial ideals (based on Gröbner bases) and convex polyhedra. Such combinations have been investigated in prior work (e.g., [Bagnara et al. 2005; Kincaid et al. 2017; Tiwari 2005]), in the context of incomplete heuristics for reasoning about real or integer arithmetic. This paper investigates the strength of this combination through the lens of a first-order theory of arithmetic. The critical finding is that these methods enable complete consequence-finding (modulo LIRR). We present an algorithm that, given a ground formula $F$, computes the set of all polynomials $p$ such that $F$ entails that $p$ is non-negative, modulo LIRR (analogous to computing the convex hull of $F$, modulo linear arithmetic). Such consequence-finding has a wide range of applications in program analysis [Reps et al. 2004]. As a case study, we give one application to non-linear invariant generation, and show that the technique has good practical performance on top of theoretical guarantees.
The paper is organized as follows. Section 2 presents background on logic, commutative algebra, and polyhedral theory. The theory of linear/integer rings is presented in two steps. Section 3 presents the theory of linear real rings, LRR, which is essentially the theory of linear integer/real rings excluding the integer predicate and its associated axioms. The full theory LIRR is given in Section 4. An invariant generation algorithm that demonstrates the use of consequence-finding is given in Section 5. Section 6 evaluates the decision procedure for LIRR and the invariant generation algorithm experimentally. The LIRR decision procedure is not empirically competitive with state-of-the-art heuristic solvers. On the other hand, the experimental results for the invariant generation procedure are positive, establishing the value of consequence-finding modulo LIRR. Related work is discussed in Section 7. Proofs for all statements in this paper can be found in Kincaid et al. [2022b].

2 BACKGROUND

2.1 First-Order Logic

A signature $\sigma = (F, R, ar)$ consists of a set of function symbols $F$ and a set of relation symbols $R$ that are mutually disjoint, and a function $ar : (F \cup R) \rightarrow \mathbb{Z}_{\geq 0}$ mapping each symbol to its arity. For any set of symbols $X$ (presumed disjoint from $F$ and $R$), we use $\sigma(X)$ to denote the extension of $\sigma$ with the constant symbols $X$. A $\sigma$-structure $\mathfrak{A}$ consists of a set $U^\mathfrak{A}$ (the universe of $\mathfrak{A}$) along with an interpretation $f^\mathfrak{A} : (U^\mathfrak{A})^{\sigma(f)} \rightarrow U^\mathfrak{A}$ of each function symbol $f \in F$ and an interpretation $r^\mathfrak{A} \subseteq (U^\mathfrak{A})^{\sigma(r)}$ of each relation symbol $r \in R$. The set of $\sigma$-terms and $\sigma$-formulas are defined in the usual way. A formula is said to be a sentence if it has no free variables, and ground if it has neither free nor bound variables. A $\sigma$-structure $\mathfrak{A}$ is a model of a set of sentences $T$ if for all $F \in T$, $\mathfrak{A}$ satisfies $F$ (written $\mathfrak{A} \models F$). A $\sigma$-theory $T$ is a set of sentences closed under entailment (for any sentence $F$, if $F$ is satisfied by every model of $T$, then $F$ belongs to $T$). For any $\sigma$-structure $\mathfrak{A}$, $Th(\mathfrak{A})$ denotes the $\sigma$-theory consisting of all sentences $F$ such that $\mathfrak{A} \models F$. If $T$ is a $\sigma$-theory and $F$ is a $\sigma(X)$-formula, we say that $F$ is satisfiable modulo $T$ if there exists a $\sigma(X)$-structure $\mathfrak{A}$ that satisfies $F$ along with each formula in $T$. If $F$ and $G$ are $\sigma(X)$-formulas, we say that $F$ entails $G$ modulo $T$ (written $F \models_T G$) if every $\sigma(X)$-structure that satisfies $F$ and each sentence in $T$ also satisfies $G$.

2.2 Commutative Algebra

This section recalls some basic facts about commutative algebra (see [Cox et al. 2015]). Let $\sigma_{or}$ be the signature of ordered rings, consisting of a binary addition ($+$) and multiplication ($\cdot$) operators, the constants 0 and 1, equality, and a binary relation $\preceq$.

The commutative ring axioms, CR, are as follows:
- $\forall x, y, z. x + (y + z) = (x + y) + z$ and $\forall x, y, z. x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (Associativity)
- $\forall x, y. x + y = y + x$ and $\forall x, y, x \cdot y = y \cdot x$ (Commutativity)
- $\forall x. x + 0 = x$ and $\forall x. x \cdot 1 = x$ (Identity)
- $\forall x, y, z. x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (Distributivity)
- $\forall x, \exists y. x + y = 0$ (Additive inverse)

A model of these axioms is called a commutative ring. Examples of commutative rings include the integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, and the reals $\mathbb{R}$. For any commutative ring $R$ and finite set of variables $X$, let $R[X]$ denote the set of polynomials over $X$ with coefficients in $R$; this too forms a commutative ring.

Modules are a generalization of linear spaces in which the scalars form a ring rather than a field. If $R$ is a commutative ring, an $R$-module is a commutative group $(M, 0, +)$ equipped with a scalar multiplication operation $\cdot : R \times M \rightarrow M$ satisfying the usual axioms of linear spaces $(a \cdot (m + n) = a \cdot m + a \cdot n, (a + b) \cdot m = a \cdot m + b \cdot m, (a \cdot b) \cdot m = a \cdot (b \cdot m), and 1 \cdot m = m)$. For instance,
R is itself an R-module where scalar multiplication is the usual ring multiplication; \( R[X] \) is both an R-module and an \( R[X] \)-module.

Let \( R \) be a commutative ring and \( N \) be an \( R \)-module. For \( L, M \subseteq N \) and \( S \subseteq R \) we use \( L + M \) to denote the set of sums of elements in \( L \) and \( M \), and \( S(M) \) to denote the set of weighted sums of elements of \( M \) with coefficients in \( S \):

\[
L + M \triangleq \{ \ell + m : \ell \in L, m \in M \}
\]

\[
S(M) \triangleq \{ s_1m_1 + \cdots + s_nm_n : n \in \mathbb{Z}_{\geq 0}^+, s_1, \ldots, s_n \in S, m_1, \ldots, m_n \in M \}
\]

For instance, if \( V \) is a linear space over \( \mathbb{Q} \) and \( G \subseteq V \) then \( \mathbb{Q}(G) \) is the span of \( G \)—the smallest linear subspace of \( V \) containing \( G \). Note that \( S(M) \) always contains zero (since we may take \( n = 0 \)). We omit braces for finite sets, and write \( S(\{m_1, \ldots, m_k\}) \) for \( S(\langle m_1, \ldots, m_k \rangle) \).

Let \( R \) be a commutative ring. An ideal \( I \subseteq R \) is a sub-module of \( R \) (considered as an \( R \)-module); i.e., a set that (1) contains zero, (2) is closed under addition, and (3) is closed under multiplication by arbitrary elements of \( R \). An ideal \( I \) defines a congruence relation \( \equiv_I \), where \( p \equiv_I q \) if and only if \( p - q \in I \). (The notation \( p - q \) abbreviates \( p + (-q) \), where \( -q \) is the unique additive inverse of \( q \).) One may think of an ideal as a set of elements that are congruent to zero with respect to some congruence relation, with the closure conditions of ideals corresponding to the idea that the sum of two zero-elements is zero, and the product of a zero-element with anything is again zero. We use \( R/I \) to denote the quotient ring in which the elements are sets of the form \( r + I \) for some \( r \in R \) (that is, equivalence classes of \( \equiv_I \)), and sum and product are defined as \( (r + I) + (s + I) = (r + s) + I \) and \( (r + I) \cdot (s + I) = (r \cdot s) + I \). Note that any subset \( P \subseteq R \) generates an ideal (the smallest with respect to inclusion order containing \( P \)), which is exactly \( R/P \). When \( R \) is clear from context, we will write \( P \) for the ideal \( R/P \) generated by the set \( P \).

Fix a set of variables \( X \). We use \( [X] \) to denote the set of monomials over \( X \). A monomial ordering \( \preceq \) is a total order on \([X]\) such that (1) \( 1 \preceq m \) for all \( m \), and (2) for any \( m \preceq n \) and any monomial \( v \), we have \( mv \preceq nv \). Applications often require fixing a monomial order, but the choice of which is irrelevant. A reasonable default is degree reverse lexicographic order: first compare monomials by their total degree, then break using a reverse lexicographic order. (Assuming a fixed monomial ordering) the leading monomial \( \text{LM}(p) \) of a polynomial \( p = a_1m_1 + \cdots + a_nm_k \in \mathbb{Q}[X] \), \( a_1, \ldots, a_n \neq 0 \), is the greatest monomial among \( m_1, \ldots, m_k \). The leading monomial of the zero polynomial is undefined.

Fix a monomial ordering \( \preceq \). Let \( p \) be a non-zero polynomial in \( \mathbb{Q}[X] \). Then \( p \) can be written as \( p = am + q \) where \( m = \text{LM}(p) \), \( a \) is the coefficient of \( m \) in \( p \), and \( q = p - am \), and interpret \( p \) as a rewrite rule \( m \rightarrow -\frac{1}{a}q \). Intuitively, if \( p \) is in some ideal \( I \), then \( p \equiv_I 0 \), and \( m \equiv_I -\frac{1}{a}q \). For instance, the polynomial \( \frac{1}{2}x^2 - y \) can be interpreted as a rewrite rule \( x^2 \rightarrow 2y \), and using this rule we may rewrite \( x^3 + x^2 \rightarrow 2xy + x^2 \rightarrow 2xy + 2y \). Observe that if \( I = \langle \frac{1}{2}x^2 - y \rangle \), \( x^3 + x^2 \equiv_I 2xy + 2y \). Applying a rewrite rule to a polynomial replaces one of its monomials with a smaller polynomial (in the sense that the polynomial is zero or its leading monomial is smaller than the one it replaced). A set of polynomials \( G \) is a Gröbner basis (with respect to \( \preceq \)) if its associated rewrite system is confluent. Assuming that \( G \) is a Gröbner basis, we use \( \text{red}_G : \mathbb{Q}[X] \rightarrow \mathbb{Q}[X] \) to denote the function that maps any polynomial to its normal form under the rewrite system \( G \). Equivalently, \( \text{red}_G(p) \) is the unique polynomial \( q \) such that (1) \( p - q \in \langle G \rangle \), and (2) no monomial in \( q \) is divisible by \( \text{LM}(g) \) for any \( g \in G \). We note some important properties of \( \text{red}_G \):

- (Membership) For all \( p \in \mathbb{Q}[X] \), \( \text{red}_G(p) = 0 \) if and only if \( p \in \langle G \rangle \)
- (Linearity) If \( a_1, \ldots, a_n \in \mathbb{Q} \) and \( p_1, \ldots, p_n \in \mathbb{Q}[X] \), then \( \text{red}_G(\sum_{i=1}^n a_i p_i) = \sum_{i=1}^n a_i \text{red}_G(p_i) \)
- (Ordering) For all \( p \in \mathbb{Q}[X] \), \( p = q_1g_1 + \cdots + q_ng_n + \text{red}_G(p) \) for some \( q_1, \ldots, q_n \in \mathbb{Q}[X] \), \( g_1, \ldots, g_n \in G \), and \( \text{LM}(q_ig_i) \leq \text{LM}(p) \) for all \( i \).
(Representation independence) If \( G_1 \) and \( G_2 \) are Gröbner bases with respect to the same monomial ordering and \( \langle G_1 \rangle = \langle G_2 \rangle \), then \( \text{red}_{G_1}(p) = \text{red}_{G_2}(p) \) for all \( p \).

For any finite set of polynomials \( P \) and monomial ordering \( \preceq \), we may compute a Gröbner basis for the ideal generated by \( P \) (e.g., using Buchberger’s algorithm [Buchberger 1976]). We use \( \text{GröbnerBasis}_{\preceq}(P) \) to denote this basis.

### 2.3 Polyhedral Theory

This section recalls some basic facts about polyhedral theory (see for example [Schrijver 1999]). In the following, we use \text{linear space} to refer to a linear space over the field \( \mathbb{Q} \). We use \( \mathbb{Q}^n \) to denote the linear space of rational vectors of length \( n \). Note that for any set of variables \( X \), \( \mathbb{Q}[X] \) is an (infinite-dimensional) linear space. We use \( \mathbb{Q}[X]^1 \) to denote the \(|X|+1\)-dimensional linear space of polynomials of degree at most one (i.e., polynomials of the form \( a_1 x_1 + \ldots + a_n x_n + b \), with \( a_1, \ldots, a_n, b \in \mathbb{Q} \) and \( x_1, \ldots, x_n \in X \)).

Let \( V \) be a linear space. A set \( C \subseteq V \) is called \text{convex} if for every \( u, v \in C \), the line segment between \( u \) and \( v \) is contained in \( C \) (i.e., for every \( \lambda \in [0, 1] \), we have \( \lambda u + (1 - \lambda) v \in C \)). For a set \( G \subseteq V \), we use \( \text{conv}(G) \) to denote the \text{convex hull} of \( G \)—the smallest convex set that contains \( G \):

\[
\text{conv}(G) \triangleq \left\{ \lambda_1 g_1 + \cdots + \lambda_n g_n : \lambda_1, \ldots, \lambda_n \in \mathbb{Q}^\geq 0, g_1, \ldots, g_n \in G, \sum_{i=1}^n \lambda_i = 1 \right\}
\]

where \( \mathbb{Q}^\geq 0 \) denotes the set of non-negative rational numbers. A set \( C \subseteq V \) is called a (convex) \text{cone} if it contains zero and is closed under addition and multiplication by non-negative scalars. For a set \( G \subseteq V \), the \text{conical hull} of \( G \) is the smallest convex cone containing \( G \); it is precisely \( \mathbb{Q}^\geq 0 \langle G \rangle \).

Let \( V \) be a linear space and \( C \subseteq V \) be a cone. We say that \( v \in C \) is an \text{additive unit} if both \( v \) and \( -v \) belong to \( C \), and denote the set of additive units as \( \mathcal{U}(C) \) (\( \mathcal{U}(C) \) is also known as the \text{lineality space} of \( C \)—the largest linear space contained in \( C \)). We say that \( C \) is \text{salient} if \( \mathcal{U}(C) = 0 \). We say that \( C \) is \text{finitely generated} (or polyhedral) if \( C = \mathbb{Q}^\geq 0 \langle G \rangle \) for some finite set \( G \).

Let \( X \) be a finite set of variables. The set of functions \( \mathbb{Q}^X \) mapping variables to rationals is a linear space (of dimension \( |X| \)). A \text{polyhedron} in \( \mathbb{Q}^X \) is of the form \( P = \{ x \in \mathbb{Q}^X : p_1(x) \geq 0, \ldots, p_n(x) \geq 0 \} \) for some linear polynomials \( p_1, \ldots, p_n \in \mathbb{Q}[X]^1 \). We say that inequality \( p(x) \geq 0 \) is \text{valid} for a polyhedron \( P \) if it is satisfied by every point in \( P \). The set of valid inequalities of a polyhedron \( P \) is \( \mathcal{P}(1) \). That is, we may “shift” the halfspace to eliminate some real solutions while keeping all integer points. A set \( C \subseteq \mathbb{Q}[X]^1 \) is \text{closed under cutting planes} iff for any \( n, m \in \mathbb{Z} \) with \( n > 0 \) and any \( p \in \mathbb{Z}[X] \) such that \( np + m \in C \), we have \( p + [m/n] \in C \). We use \( \text{cp}(C) \) to denote the cutting plane closure of a cone \( C \)—the smallest cone that contains \( C \) and which is closed under cutting planes.

Let \( V \) be a linear space. We say that a subset \( L \subseteq V \) is a \text{point lattice} if there exists some \( v_1, \ldots, v_n \in V \) such that \( L = \mathbb{Z}\langle v_1, \ldots, v_n \rangle \). We call a set of generators \( \{v_1, \ldots, v_n\} \) for a point lattice...
a basis for \( L \) if it is linearly independent. A basis for a point lattice can be computed as the Hermite normal form of its generators in polynomial time [Schrijver 1999, Ch. 4].

3 LINEAR REAL RINGS

In this section, we develop the theory of linear real rings, LRR. Linear real rings are a common extension of the theory of commutative rings and the positive fragment of the theory of linear real arithmetic. Section 3.1 presents the axioms of the theory and introduces regular and algebraic cones. Regular cones correspond to models of the theory, and algebraic cones correspond to effective structures; cones that are both regular and algebraic correspond to a class of effective models of LRR. Section 3.2 presents a decision procedure for satisfiability of ground formulas modulo LRR. Section 3.3 gives a procedure that discovers all implied inequalities of a ground formula modulo LRR, represented as a (regular) algebraic cone.

3.1 Linear Real Rings

Define LRR to be the \( \sigma_{or} \)-theory axiomatized by the axioms of commutative rings CR as well as the following theorems of LRA:

\[
\begin{align*}
\forall x. x &\leq x & \text{(Reflexivity)} \\
\forall x, y, z. x \leq y \land y \leq z &\Rightarrow x \leq z & \text{(Transitivity)} \\
\forall x, y, z. x \leq y \land y \leq x &\Rightarrow x = y & \text{(Antisymmetry)} \\
\forall x, y, z. (x \leq y &\Rightarrow x + z \leq y + z) & \text{(Compatibility)} \\
0 \leq 1 &\land 0 \neq 1 & \text{(Non-triviality)} \\
\text{for all } n \in \mathbb{Z}^{\geq 1}, \exists x. x + \cdots + x &= 1 & \text{(Divisibility)} \\
\text{for all } n \in \mathbb{Z}^{\geq 0}, \forall x. 0 &\leq x + \cdots + x \Rightarrow 0 \leq x & \text{(Perforation-freeness)}
\end{align*}
\]

Note that divisibility and perforation-freeness are axiom schemata, with one axiom for each natural number (\( \exists x. x = 1, \exists x. x + x = 1, \exists x. x + x + x = 1 \), and so on). Equivalently, LRR is the theory consisting of all \( \sigma_{or} \)-sentences that hold in all structures \( \mathfrak{U} \) where \( (U, 0^U, 1^U, +^U, \cdot^U) \) forms a commutative ring and \( (U^\mathbb{Q}, 0^U, 1^U, +^U, \cdot^U, \leq^U) \) forms an unperforated partially ordered divisible group. We regard the real numbers \( \mathbb{R} \) as the “standard” model of LRR; other models include the rationals, the complex numbers (where complex numbers with the same imaginary part are ordered by their real part) and, as we shall see shortly, more exotic interpretations. The signature of ordered rings should be regarded as a “minimal” signature for LRR, but models of LRR can be lifted to richer languages. In the following, we will make use of an extended language that includes atomic formulas \( p \leq q \) and \( p = q \) where \( p \) and \( q \) are polynomials with rational coefficients; any such atom can be translated into the language of ordered rings by scaling and re-arranging terms (for example, the formula \( 0 \leq \frac{1}{2} x - y \) can be translated to the \( \sigma_{or}(\{x, y\}) \) formula \( (1 + 1) \cdot y \leq x \).

The axioms that LRR adds onto commutative rings are a subset of the axioms of LRA. Naturally we might ask if the subset is “enough.” Notably, totality of the order (an axiom of linear real arithmetic) is independent of LRR (e.g., \( \leq \) is non-total for the complex numbers). Nevertheless, LRR is at least as strong as LRA, in the sense that satisfiability modulo LRA can be reduced to satisfiability modulo LRR (noting that every formula in the language of LRA is equisatisfiable to a negation-free formula modulo LRA).

Theorem 1. Let \( F \) be a ground negation-free formula in the language of LRA. Then \( F \) is satisfiable modulo LRA iff it is satisfiable modulo LRR.
PROOF. The ⇒ direction is trivial, since the reals are a model of \( LRR \). For the ⇐ direction, we show the contrapositive: suppose that \( F \) is unsatisfiable modulo \( LRA \), and show that it is unsatisfiable modulo \( LRR \).

First observe that for any \( LRR \)-model \( \mathcal{A} \), and any terms \( c_1, d_1, c_2, d_2 \) such that \( \mathcal{A} \models c_1 \leq d_1 \) and \( \mathcal{A} \models c_2 \leq d_2 \), we have \( \mathcal{A} \models c_1 + c_2 \leq d_1 + d_2 \). Hence, since \( \mathcal{A} \models c_1 \leq d_1 \), we have \( \mathcal{A} \models c_1 + c_2 \leq d_1 + c_2 \) by compatibility; since \( \mathcal{A} \models c_2 \leq d_2 \), we have \( F \models d_1 + c_2 \leq d_1 + d_2 \) by compatibility and commutativity. Finally, by transitivity we have \( \mathcal{A} \models c_1 + c_2 \leq d_1 + d_2 \).

Without loss of generality, we may suppose that \( F \) is conjunction of inequalities. For convenience, we first assume that all inequalities are non-strict. Thus \( F \) can be written in the form \( Ax \leq b \). Since this system is unsatisfiable modulo \( LRA \), then by Farkas’ lemma there is some \( \vec{y} \geq 0 \) such that \( \vec{y}^T A = 0 \) and \( \vec{y}^T b < 0 \). Without loss of generality, we may suppose that \( \vec{y} \) is an integer vector. It follows from the observation above that \( F \models_{LRR} 0 \leq b \). Since \( \leq \) is unperforated, we have \( F \models_{LRR} 0 < -1 \), and by non-triviality and antisymmetry we have \( F \models_{LRR} false \); i.e., \( F \) is unsatisfiable modulo \( LRR \).

Now consider the case of disequalities (and thus formulas with strict inequalities, treating \( p < q \) as an abbreviation for \( p \leq q \land p \neq q \)). In this case, we may suppose without loss of generality that \( F \) is conjunction of inequalities and disequalities, which can be written in the form \( Ax \leq b \land \bigwedge_{i=1}^n c_i^T \vec{x} \neq d_i \) (with at least one disequality, or else we fall into the case above). Since \( F \) is unsatisfiable, we must have \( Ax \leq b \models_{LRA} \bigvee_{i=1}^n c_i^T \vec{x} = d_i \). Since \( LRA \) is a convex theory, we must have \( Ax \leq b \models_{LRR} c_i^T \vec{x} = d_i \) for some \( i \). We may then argue as above that \( Ax \leq b \models_{LRR} c_i^T \vec{x} \leq d_i \) and \( Ax \leq b \models_{LRR} d_i \leq c_i^T \vec{x} \), and so by antisymmetry \( Ax \leq b \models_{LRR} c_i^T \vec{x} = d_i \), and thus \( F \) is unsatisfiable modulo \( LRR \).

In the remainder of this section, we develop a model theory of \( LRR \), based on regular cones. For any set of variables \( X \), we say that a set \( C \subseteq \mathbb{Q}[X] \) is a regular cone if it is a cone (closed under addition and multiplication by non-negative rationals), \( 1 \in C \), and \( \mathcal{U}(C) \) forms an ideal in \( \mathbb{Q}[X] \). We say that \( C \) is consistent if \( C \neq \mathbb{Q}[X] \); in the case that \( C \) is regular, \( C \) is consistent iff \( -1 \not\in C \). Consistent cones and regular cones are both closed under intersection, the latter is because ideals are closed under intersection.

Let \( X \) be a set of symbols, and let \( \mathcal{A} \) be a \( \sigma_{or}(X) \)-structure satisfying the axioms of \( LRR \). Define \( C(\mathcal{A}) = \{ p \in \mathbb{Q}[X] : \mathcal{A} \models 0 \leq p \} \) to be its non-negative consequences. Naturally, \( C(\mathcal{A}) \) forms a consistent regular cone. We now show that, conversely, any consistent regular cone can be associated with a model of \( LRR \).

Let \( X \) be a set of variables, let \( C \subseteq \mathbb{Q}[X] \) be a regular cone. Define a \( \sigma_{or}(X) \)-structure \( \mathcal{M}(C) \) where

- The universe and function symbols \( 0, 1, +, \cdot \) are interpreted as in the quotient ring \( R = \mathbb{Q}[X]/I \), where \( I \) is the ideal of additive units \( \mathcal{U}(C) \). Thus, elements of the universe are sets of polynomials with rational coefficients of the form \( p + I \), where \( p \in \mathbb{Q}[X] \).
- Each constant symbol \( x \in X \) is interpreted as \( x + I \).
- \( \leq \) is interpreted as the relation \( \{(p + I, q + I) : q - p \in C\} \).

Observe that \( \mathcal{M}(C) \models 0 \leq q \iff q \in C \), and \( \mathcal{M}(C) \models 0 = q \iff q \in \mathcal{U}(C) \).

**Lemma 1.** Let \( X \) be a set of variables, and let \( C \subseteq \mathbb{Q}[X] \) be a consistent regular cone. Then \( \mathcal{M}(C) \) is a model of \( LRR \).

**Proof.** Clearly \( R = \mathbb{Q}[X]/\mathcal{U}(C) \) is a commutative ring and satisfies the divisibility axioms. Since \( C \) is a cone, it follows that \( \leq \) is reflexive, transitive, compatible with addition, and perforation-free; furthermore since \( C \) is regular we have that \( \leq \) is antisymmetric. Non-triviality follows from the fact that \( C \) is consistent.
While regular cones give us a “standard form” in which LRR models can be represented, they cannot be manipulated effectively. For this purpose, we introduce algebraic cones, which are (not necessarily regular) cones that admit a finite representation.

We say that a cone \( C \subseteq \mathbb{Q}[X] \) is algebraic if there is an ideal \( I \) and a finitely-generated cone \( D \) such that \( C = I + D \). An algebraic cone can be represented as a pair \((Z, P)\) (with \( Z, P \subseteq \mathbb{Q}[X] \)) where \( Z = \{z_1, \ldots, z_m\} \) (“zeros”) is a basis for an ideal and \( P = \{p_1, \ldots, p_n\} \) (“positives”) is a basis for a cone; the algebraic cone represented by \((Z, P)\) is denoted by

\[
\text{alg.cone}_X(Z, P) = (Z) + \mathbb{Q}^{\geq 0}(P) = \left\{ \sum_{i=1}^m q_iz_i + \sum_{j=1}^n \lambda_jp_j : q_1, \ldots, q_m \in \mathbb{Q}[X], \lambda_1, \ldots, \lambda_n \in \mathbb{Q}^{\geq 0} \right\}
\]

We will omit the \( X \) subscript when it is clear from context. Say that the pair \((Z, P)\) is oriented (with respect to a monomial ordering \( \leq \)) if:

1. \( Z \) is a Gröbner basis for \((Z)\) (with respect to \( \leq \)), and
2. Each \( p_i \in P \) is reduced with respect to \( Z \) (i.e., \( \text{red}_Z(p_i) = p_i \) for all \( i \)).

The following shows that the problem of checking membership in an algebraic cone can be reduced to checking membership in a finitely-generated cone (which can be checked in polytime using linear programming). It comes in two parts: (1) checking membership assuming an oriented representation (Lemma 2) and (2) computing an oriented representation (Lemma 3).

**Lemma 2** (Membership). Let \( X \) be a set of variables, and \( Z, P \subseteq \mathbb{Q}[X] \) be finite sets of polynomials such that \((Z, P)\) is oriented. For any polynomial \( q \in \mathbb{Q}[X] \), we have \( q \in \text{alg.cone}_X(Z, P) \) iff \( \text{red}_Z(q) \in \mathbb{Q}^{\geq 0}(P) \).

**Proof.** \((\Leftarrow)\) If \( \text{red}_Z(q) \in \mathbb{Q}^{\geq 0}(P) \) then since \((q - \text{red}_Z(q)) \in (Z) \) we have \( q = (q - \text{red}_Z(q)) + \text{red}_Z(q) \in (Z) + \mathbb{Q}^{\geq 0}(P) = \text{alg.cone}_X(Z, P) \).

\((\Rightarrow)\) Suppose \( q \in \text{alg.cone}_X(Z, P) \). Then we have \( q = z + p \) for some \( z \in (Z) \) and \( p \in \mathbb{Q}^{\geq 0}(P) \). Since \( z \in (Z) \), we have \( \text{red}_Z(z) = 0 \), and since \( p \) is a (non-negative) linear combination of polynomials that are reduced w.r.t. \( Z \), we have \( \text{red}_Z(p) = p \). It follows that \( \text{red}_Z(q) = \text{red}_Z(z) + \text{red}_Z(p) = p \), and so \( \text{red}_Z(q) \in \mathbb{Q}^{\geq 0}(P) \). \( \square \)

For any set of variables \( X \), finite sets of polynomials \( Z, P \subseteq \mathbb{Q}[X] \), and monomial ordering \( \leq \), define \( \text{orient}_\leq(Z, P) = (G, \{\text{red}_G(p) : p \in P, \text{red}_G(p) \neq 0\}) \) where \( G = \text{GröbnerBasis}_\leq(Z) \) is a Gröbner basis for \((Z)\) with respect to the order \( \leq \).

**Lemma 3** (Orientation). Let \( X \) be a set of variables, \( Z, P \subseteq \mathbb{Q}[X] \) be finite sets of polynomials, and \( \leq \) be a monomial ordering. Then \( \text{orient}_\leq(Z, P) \) is oriented with respect to \( \leq \) and \( \text{alg.cone}(Z, P) = \text{alg.cone}(\text{orient}_\leq(Z, P)) \).

**Proof.** Let \( G = \text{GröbnerBasis}_\leq(Z) \) and \( P' = \{\text{red}_G(p) : p \in P, \text{red}_G(p) \neq 0\} \). Since \( \text{red}_G \) is idempotent, \( \text{orient}_\leq(G, P') \) is oriented w.r.t. \( \leq \). Clearly, \((Z) = (G)\). Since algebraic cones are closed under addition and multiplication by non-negative rationals, it is sufficient to prove that \( P \subseteq (G) + \mathbb{Q}^{\geq 0}(P') \) and \( P' \subseteq (Z) + \mathbb{Q}^{\geq 0}(P) \).

- \( P \subseteq (G) + \mathbb{Q}^{\geq 0}(P') \): Suppose \( p \in P \). Since \( p - \text{red}_G(p) \in (G) \) and \( \text{red}_G(p) \in \mathbb{Q}^{\geq 0}(P') \) (since it either belongs to \( P' \) or it is zero), we have \( p = (p - \text{red}_G(p)) + \text{red}_G(p) \in (G) + \mathbb{Q}^{\geq 0}(P') \).

- \( P' \subseteq (Z) + \mathbb{Q}^{\geq 0}(P) \): Suppose \( p' \in P \). Then \( p' = \text{red}_G(p) \) for some \( p \in P \). It follows that \( p' - p \in (G) = (Z) \), and so \( p' = (p' - p) + p \in (Z) + \mathbb{Q}^{\geq 0}(P) \). \( \square \)

As a consequence of decidability of membership in algebraic cones, we have a model checking procedure for models associated to algebraic cones. Given a ground formula \( F \) and generators \( Z, P \) for an algebraic cone, checking \( \mathcal{M}(\text{alg.cone}(Z, P)) \models F \) is decidable.
We first observe an invariant of the algorithm: for all \(u\),

\[
\text{Algorithm 1: Saturation}
\]

3.2 Satisfiability Modulo LRR
This section presents a decision procedure for testing satisfiability of ground \(\sigma_{or}(X)\)-formulas modulo the theory LRR. As usual, it is sufficient to develop a theory solver, which can test satisfiability of the conjunctive fragment; formulas with disjunctions can be accommodated using DPLL(\(T\)) [Ganzinger et al. 2004].

Without loss of generality, a ground conjunctive \(\sigma_{or}(X)\)-formula \(F\) can be written in the form

\[
F = \left( \bigwedge_{p \in P} 0 \leq p \right) \land \left( \bigwedge_{q \in Q} \neg (0 \leq q) \right) \land \left( \bigwedge_{r \in R} \neg (0 = r) \right)
\]

where \(P, Q,\) and \(R\) are finite sets of polynomials (noting the equivalences \(x \equiv y \equiv 0 \leq y - x\) and \(x = y \equiv 0 \leq x - y \land 0 \leq y - x\)). In the following, we will first show that it is possible to compute a finite representation of the least regular cone \(C\) that contains all of the non-negative polynomials \(P\) (Theorem 3), and then show that \(F\) is satisfiable if and only if \(C\) is consistent and \(\mathcal{M}(C) \models F\) (Theorem 4). Since \(C\) is algebraic and computable from \(P\), and checking that \(C\) is consistent and that \(\mathcal{M}(C) \models F\) is decidable, this yields a sound and complete procedure for checking satisfiability of ground \(\sigma_{or}(X)\)-formulas modulo LRR.

We first show that we can compute the sum of two algebraic cones by combining their bases for the zeros and the positives, before proving the correctness of Algorithm 1.

**Theorem 2** (Sum). Let \(Z_1, P_1, Z_2, P_2 \subseteq \mathbb{Q}[X]\) be finite sets of polynomials. Then

\[
\text{alg.cone}(Z_1, P_1) + \text{alg.cone}(Z_2, P_2) = \text{alg.cone}(Z_1 \cup Z_2, P_1 \cup P_2).
\]

**Theorem 3.** Let \(X\) be a finite set of variables. For any finite sets of polynomials \(Z, P \subseteq \mathbb{Q}[X]\), \(\text{regularize}(Z, P)\) (Algorithm 1) returns a pair \((Z', P')\) such that \(\mathbb{Q} \geq 0\langle P'\rangle\) is salient and \(\text{alg.cone}(Z', P')\) is the least regular cone that contains \(\text{alg.cone}(Z, P)\).

Proof. Let \(Z_i, P_i,\) and \(t_i\) denote the values of \(Z, P,\) and \(t\) after \(i\) iterations of the loop in Algorithm 1. We first observe an invariant of the algorithm: for all \(i\), we have

\[
\text{alg.cone}(Z_{i+1}, P_{i+1}) = \text{alg.cone}(\text{orient}_{\leq}(Z_i \cup \{t_i\}, P_i))
\]

Definition

\[
= \text{alg.cone}(Z_i \cup \{t_i\}, P_i)
\]

Lemma 3

\[
= \text{alg.cone}(Z_i, P_i) + \langle t \rangle
\]

Theorem 2

We first prove that the algorithm terminates. For iteration \(i + 1\), we have \(\langle Z_{i+1} \rangle \equiv \langle Z_i \rangle + \langle t_i \rangle\). Since \(t_i\) is a conic combination of polynomials in \(P_i\) which are reduced with respect to \(Z_i\), we have \(\text{red}_{Z_i}(t_i) = t_i \neq 0\) and so \(t_i \notin \langle Z_i \rangle\). Hence we have \(\langle Z_{i+1} \rangle \not\equiv \langle Z_i \rangle\). For a contradiction, suppose that the algorithm does not terminate. Then we have an infinite strictly ascending chain of ideals...
Theorem 4. Let \( (by \text{Lemma } 44:10 \text{ Zachary Kincaid, Nicolas Koh, and Shaowei Zhu} \text{ Proc. ACM Program. Lang., Vol. 7, No. POPL, Article } 44. \text{ Publication date: January } 2023. \)

\[
\begin{array}{|c|c|c|}
\hline
\text{Iteration} & \text{Z} & \text{P} & \text{Additive unit} \\
\hline
0 & \emptyset & \{1 \cup Q\} & x^2 - xy \\
1 & \{xy - x^2\} & \{1, x^3 - z, w - x^3, z - w, w^3\} & x^3 - z \\
2 & \{xy - x^2, x^3 - z, yz - xz\} & \{1, w - z, z - w, w^3\} & w - z \\
3 & \{xy - x^2, x^3 - z, yz - xz, w - z\} & \{1, z^3\} & - \\
\hline
\end{array}
\]

\([Z_0] \subseteq [Z_1] \subseteq \ldots \text{ in } \mathbb{Q}[X], \) which contradicts the fact that \( \mathbb{Q}[X] \) is a Noetherian ring [Cox et al. 2015, Ch. 2 §5].

Suppose that the loop terminates after \( n \) iterations—we must show that \( \text{alg.cone}(\text{regularize}(Z_n, P_n)) \) is the least regular cone that contains \( \text{alg.cone}(Z, P) \). Since \( Z_0 = Z \) and \( P_0 = P \cup \{1\} \), and we have \( \text{alg.cone}(Z_i, P_i) \subseteq \text{alg.cone}(Z_{i+1}, P_{i+1}) \) for all \( i \), we have that \( \text{alg.cone}(\text{regularize}(Z_n, P_n)) \) must contain \( \text{alg.cone}(Z, P) \) and 1. By the termination condition, we have that \( \mathbb{Q}^\geq 0 \langle P_n \rangle \) is salient, and therefore \( \text{alg.cone}(Z_n, P_n) \) is regular. It remains to show that it is the least such regular cone. Suppose that there is another regular cone \( C \) with \( \text{alg.cone}(Z, P) \subseteq C \). We show that for all iterations \( i, \text{alg.cone}(Z_i, P_i) \subseteq C \) by induction on \( i \). Initially this is true since \( Z_0 = Z \) and \( P_0 = Q \cup \{1\} \), and \( C \) contains \( \text{alg.cone}(Z, P) \) (by assumption) and 1 (since \( C \) is regular). For the inductive step, we

\[
\text{Example 3.1. Table 1 illustrates Algorithm 1 on the set of polynomials}
\]

\[
Q = \{x^2 - xy, xy - x^2, x^2y - z, w - xy^2, z - w, w^3\}.
\]

Each row \( i \) gives the set of zero polynomials \( Z \) and set of positive polynomials \( P \) at the beginning of iteration \( i \), along with the selected additive unit \( t \). Intuitively, each round selects an additive unit from the positives, removes it from the positives and adds it to the zeros. The algorithm terminates at iteration 3: the positive cone is salient, and so there is no additive unit to select. \( \square \)

The following theorem is the basis of our decision procedure for \( \text{LRR} \): it shows that to test satisfiability of \( F \), we only need to check whether the least cone \( C \) that agrees with all positive atoms of \( F \) is consistent and other atoms do not contradict the consequences of \( C \).

**Theorem 4.** Let \( F \) be the ground conjunctive formula

\[
F = \left( \bigwedge_{p \in P} 0 \leq p \right) \land \left( \bigwedge_{q \in Q} \neg(0 \leq q) \right) \land \left( \bigwedge_{r \in R} \neg(0 = r) \right).
\]

Let \( C \) be the least regular cone that contains \( P \). Then \( F \) is satisfiable modulo \( \text{LRR} \) iff \( C \) is consistent and \( \mathfrak{M}(C) \models F \).

**Proof.** If \( C \) is consistent and \( \mathfrak{M}(C) \models F \), then \( F \) is satisfiable modulo \( \text{LRR} \) \((\mathfrak{M}(C) \text{ is a model of } F \text{ (by Lemma 1) of } \text{LRR}) \). We thus only need to prove the other direction.

Suppose that \( F \) is satisfiable modulo \( \text{LRR} \). Then there is some model \( \mathfrak{A} \) of \( \text{LRR} \) with \( \mathfrak{A} \models F \). We have that \( C \subseteq C(\mathfrak{A}) \), since \( C(\mathfrak{A}) \) is a regular cone that contains \( P \) (since \( \mathfrak{A} \models F \))\), and \( C \) is the least such cone. It follows that \( C \) is consistent, since if \( \neg 1 \in C \) then \( \neg 1 \in C(\mathfrak{A}) \), which is not possible because \( C(\mathfrak{A}) \) is consistent. It remains to show that \( \mathfrak{M}(C) \models F \). Clearly \( \mathfrak{M}(C) \models 0 \leq p \) for all \( p \in P \), since \( P \subseteq C \). For any \( q \in Q \) we have \( \mathfrak{A} \models \neg(0 \leq q) \), since \( \mathfrak{A} \models F \). Thus \( q \notin C(\mathfrak{A}) \) and so \( q \notin C \).
since \( C \subseteq C(\mathcal{M}) \). Hence \( \mathcal{M}(C) \models \neg (0 \leq q) \). Similarly, we have that \( \mathcal{M}(C) \models \neg (0 = r) \) for all \( r \in R \). Combining the above, we have \( \mathcal{M}(C) \models F \).

**Decision Procedure for LRR.** Summarizing, we have the following decision procedure for satisfiability of ground conjunctive \( \sigma_{\alpha r}(X) \)-formulas modulo LRR. Let \( F \) be of the form in Theorem 4. First compute a representation \((Z', P')\) of the least regular cone containing \( P \) using Algorithm 1. If \( \text{red}_Z(1) = 0 \), then \( F \) is unsatisfiable (\( \text{alg.cone}(Z', P') \) is inconsistent). Otherwise, check whether \( \mathcal{M}(\text{alg.cone}(Z', P')) \models F \) by testing whether there is some \( q \in Q \) with \( \text{red}_Z(q) \in \mathbb{Q}^+ \langle P' \rangle \) (Lemma 2), or some \( r \in R \) with \( \text{red}_Z(r) = 0 \); if such a \( q \) or \( r \) exists, then \( F \) is unsatisfiable (Theorem 4), otherwise, \( \mathcal{M}(\text{alg.cone}(Z', P')) \) satisfies \( F \).

### 3.3 Consequence-finding modulo LRR

This section describes an algorithm that computes all polynomial inequalities that are entailed by a ground formula modulo LRR. Let \( X \) be a set of symbols and let \( F \) be a \( \sigma_{\alpha r}(X) \)-formula. Define the **non-negative cone** \( C_X(F) \) of \( F \) as follows:

\[
C_X(F) \triangleq \{ p \in \mathbb{Q}[X] : F \models_{\text{LRR}} 0 \leq p \}.
\]

It is easy to verify that for any formula \( F \), \( C_X(F) \) is a regular cone. We will omit the \( X \) subscript when it can be understood from the context.

A simple “eager” strategy for computing non-negative cones operates as follows. Suppose that \( F \) is a ground \( \sigma_{\alpha r}(Y) \)-formula and that \( X \subseteq Y \). First, we place \( F \) in disjunctive normal form; i.e., we compute a formula that is equivalent to \( F \) and takes the form \( \bigvee_{i=1}^n G_i \) where each \( G_i \) is a conjunctive formula. Observe that

\[
C_X(F) = C_X \left( \bigcup_{i=1}^n G_i \right) = \bigcap_{i=1}^n C_X(G_i) = \bigcap_{i=1}^n (C_Y(G_i) \cap \mathbb{Q}[X])
\]

since a disjunctive formula entails that a polynomial is non-negative exactly when each disjunct does. Thus, the problem of computing \( C_X(F) \) can be reduced to three sub-problems: (1) computing the (regular and algebraic) non-negative cone of a conjunctive formula, (2) projection of an algebraic cone onto a subset of symbols (i.e., the intersection of an algebraic cone with \( \mathbb{Q}[X] \)), and the intersection of algebraic cones. In the following, we show how to solve each sub-problem, and then present a “lazy” variant of the consequence-finding procedure that avoids (explicit) DNF computation.

#### 3.3.1 Non-Negative Cones of Conjunctive Formulas

This section addresses the following problem: given a ground \( \sigma_{\alpha r}(Y) \)-formula \( F \), compute a representation of the cone \( C_Y(F) \). In fact, the solution to this problem is immediate: \( C_Y(F) \) coincides with the least regular cone that contains the non-negative atoms of \( F \), which can be computed by the **regularize** procedure (Algorithm 1):

**Lemma 4.** Let \( Y \) be a set of symbols and let

\[
F = \left( \bigcap_{p \in P} 0 \leq p \right) \land \left( \bigcap_{q \in Q} \neg (0 \leq q) \right) \land \left( \bigcap_{r \in R} \neg (0 = r) \right)
\]

be a ground \( \sigma_{\alpha r}(Y) \)-formula. Then \( \text{alg.cone}_Y(\text{regularize}(\emptyset, P)) = C_Y(F) \).

**Proof.** Let \( C = \text{alg.cone}_Y(\text{regularize}(\emptyset, P)) \). By Theorem 3, \( C \) is the least regular cone that contains \( P \). Since \( C_Y(F) \) is a regular cone that contains \( P \), we have \( C \subseteq C_Y(F) \). It remains only to show that \( C_Y(F) \subseteq C \). If \( C \) is inconsistent (i.e., \( C = \mathbb{Q}[Y] \)), then \( C_Y(F) \subseteq C \) is immediate. Otherwise, \( \mathcal{M}(C) \models F \) by Theorem 4. For any \( q \in C_Y(F) \), we have \( F \models_{\text{LRR}} 0 \leq q \) and so \( \mathcal{M}(C) \models 0 \leq q \) and therefore \( q \in C \). \( \square \)
3.3.2 Projection of Algebraic Cones. This section addresses the following problem: given finite sets $Z, P \subseteq \mathbb{Q}[Y]$ and a subset $X \subseteq Y$, compute $Z', P' \subseteq \mathbb{Q}[X]$ such that $\text{alg.cone}(Z', P') = \text{alg.cone}(Z, P) \cap \mathbb{Q}[X]$. First, we review standard methods for solving this problem for polynomial ideals and finitely-generated cones (that is, the case when $P$ is empty, and the case where $Z$ is empty). The algorithm for algebraic cones is a combination of the two.

Any monomial $m$ over variables $Y$ can be regarded as the product of two monomials $m_X m_{\overline{X}}$ where $m_X$ is a monomial over $X$ and $m_{\overline{X}}$ is a monomial over $Y \setminus X$. For any monomial ordering $\preceq$, we may define an elimination ordering $\preceq_X$ where $m_X m_{\overline{X}} \preceq_X n_X n_{\overline{X}}$ iff $m_X < n_X$ or $m_{\overline{X}} = n_{\overline{X}}$ and $m_X \preceq n_X$. The classical algorithm for ideal projection computes a basis for $\mathbb{Q}[Y]\langle Z \rangle \cap \mathbb{Q}[X]$ by computing a Gröbner basis $G$ for $Z$ with respect to the order $\preceq_X$, and then taking $G \cap \mathbb{Q}[X]$ [Cox et al. 2015, Ch. 3]. By the ordering and membership properties of Gröbner bases, if $p \in \mathbb{Q}[Y]\langle Z \rangle = \mathbb{Q}[Y]\langle G \rangle$, then $p = q_1 g_1 + \cdots + q_n g_n$ for some $q_1, \ldots, q_n \in \mathbb{Q}[Y]$ and $g_1, \ldots, g_n \in G$ with $\text{Lm}(q_i g_i) \preceq_X \text{Lm}(p)$ for all $i$. Supposing that $p$ is also in $\mathbb{Q}[X]$, each $q_i$ and $g_i$ must also be in $\mathbb{Q}[X]$.

We now turn to the case of finally-generated cones. Since $P$ is a finite collection of polynomials, there is a finite set of monomials that appear in any polynomial in $P$, which we call $M$. Then we can see $\mathbb{Q}^{\geq 0}(P) \cap \mathbb{Q}[X] = \mathbb{Q}^{\geq 0}(P) \cap \mathbb{Q}(M \cap [X])$; and so our problem is to compute the intersection of a cone and a linear space—this is the dual view of the problem solved by polyhedral projection, for which there are several known algorithms. For the sake of completeness, we will describe how to apply Fourier-Motzkin elimination, which is one such algorithm. Suppose that we wish to compute $\mathbb{Q}^{\geq 0}(P) \cap \mathbb{Q}(N)$ for some set of monomials $N$. Fourier-Motzkin elimination proceeds by eliminating one dimension, a monomial $m \in M \setminus N$, at a time. First, we may normalize $P$ so that every polynomial in $P$ takes the form $p + am$, where $m$ does not appear in $p$, and $a$ is either 0, 1, or -1 (by multiplying each polynomial with an appropriate non-negative scalar). Then, take $Q = \{ p : p + 0m \in P \} \cup \{ p + q : p + m \in P, q - m \in P \}$. $\mathbb{Q}^{\geq 0}(Q)$ is precisely $\mathbb{Q}^{\geq 0}(P) \cap \mathbb{Q}(M \setminus m)$, since any non-negative combination of elements of $Q$ that results in a coefficient of 0 for $m$ is also a non-negative combination of elements of $Q$. Repeating this process for each monomial in $M \setminus N$, we get a finite set of polynomials that we denote $\text{proj}_X(P)$, with $\mathbb{Q}^{\geq 0}(\text{proj}_X(P)) = \mathbb{Q}^{\geq 0}(P) \cap \mathbb{Q}(N)$.

Finally, we put the two pieces together, by observing that we can project an algebraic cone $\text{alg.cone}(Z, P)$ by separately projecting the ideal $\langle Z \rangle$ and cone $\mathbb{Q}^{\geq 0}(P)$, provided that $(Z, P)$ is oriented with respect to the elimination ordering. That is, we define

$$\text{proj}_X(Z, P) = \{ G \cap \mathbb{Q}[X], \text{proj}_X((\text{red}_G(p) : p \in P)) \}$$

where $G$ is a Gröbner basis for $\langle Z \rangle$ w.r.t. the elimination order $\preceq_X$.

**Theorem 5 (Projection).** Let $Z, P \subseteq \mathbb{Q}[Y]$ be finite sets of polynomials, and let $X \subseteq Y$. Then $\text{alg.cone}_X(\text{proj}_X(Z, P)) = \text{alg.cone}_Y(Z, P) \cap \mathbb{Q}[X]$.

**Proof.** Let $G$ be a Gröbner basis for $\mathbb{Q}[Y]\langle Z \rangle$ w.r.t. the elimination order $\preceq_X$, let $Z' = G \cap \mathbb{Q}[X]$, and let $P' = \text{proj}_X(\text{red}_G(P))$, where $\text{red}_G(P)$ denotes the set $\{ \text{red}_G(p) : p \in P \}$. By Lemma 3, we have $\text{alg.cone}_X(Z, P) = \text{alg.cone}_Y(G, \text{red}_G(P))$. We only need to show that $\text{alg.cone}_X(Z', P') = \text{alg.cone}_Y(G, \text{red}_G(P)) \cap \mathbb{Q}[X]$. We know that $\text{alg.cone}_X(Z', P') \subseteq \text{alg.cone}_Y(G, \text{red}_G(P)) \cap \mathbb{Q}[X]$ since $Z' = G \cap \mathbb{Q}[X]$ is a basis for $\mathbb{Q}[Y]\langle G \rangle \cap \mathbb{Q}[X]$ and $\mathbb{Q}^{\geq 0}(P') = \mathbb{Q}^{\geq 0}(\text{proj}_X(\text{red}_G(P))) = \mathbb{Q}^{\geq 0}(\text{red}_G(P)) \cap \mathbb{Q}[X]$. Thus we only need to show the other direction.

Suppose that $q \in \text{alg.cone}_X(G, \text{red}_G(P)) \cap \mathbb{Q}[X]$. Since $q \in \mathbb{Q}[X]$ and $\text{Lm}(\text{red}_G(q)) \preceq_X \text{Lm}(q)$, we have $\text{red}_G(q) \in \mathbb{Q}[X]$. Since $q \in \text{alg.cone}_X(G, \text{red}_G(P))$, we have $\text{red}_G(q) \in \mathbb{Q}^{\geq 0}(\text{red}_G(P))$ by the membership lemma (Lemma 2). It follows that $\text{red}_G(q) \in \text{red}_G(P) \cap \mathbb{Q}[X] = \mathbb{Q}^{\geq 0}(P')$. Since $q, \text{red}_G(q) \in \mathbb{Q}[X]$ we have $q - \text{red}_G(q) \in \mathbb{Q}[X]$ and thus $q - \text{red}_G(q) \in \mathbb{Q}[Y]\langle G \rangle \cap \mathbb{Q}[X] = \mathbb{Q}[X]\langle Z' \rangle$. Thus we have $q = (q - \text{red}_G(q)) + \text{red}_G(q) \in \mathbb{Q}[X]\langle Z' \rangle + \mathbb{Q}^{\geq 0}(P') = \text{alg.cone}_X(Z', P')$. □
3.3.3 Intersection of Algebraic Cones. This section addresses the following problem: given finite sets $Z_1, P_1, Z_2, P_2 \subseteq \mathbb{Q}[X]$, compute $Z, P \subseteq \mathbb{Q}[X]$ such that $\text{alg.cone}(Z, P) = \text{alg.cone}(Z_1, P_1) \cap \text{alg.cone}(Z_2, P_2)$. The essential idea is to reduce the problem to a projection problem—essentially the same idea as the standard algorithm for ideal intersection [Cox et al. 2015, Ch. 4 §3] and the constraint-based algorithm for polyhedral join [Benoy et al. 2005].

The essential idea is to introduce a parameter $t$ that does not belong to $X$, and to “tag” each element of a cone $C_1 = \text{alg.cone}(Z_1, P_1)$ by multiplying by $t$, and to tag elements of $C_2 = \text{alg.cone}(Z_2, P_2)$ by multiplying by $1 - t$. If $p$ is a polynomial that belongs to $C_1$ and $C_2$, then $tp + (1 - t)p = p$ belongs to their “tagged sum.” This yields the following definition:

$$\text{intersect}(Z_1, P_1, Z_2, P_2) \triangleq \text{project}_X(tZ_1 \cup (1 - t)Z_2, tP_1 \cup (1 - t)P_2)$$

where the notation $pQ \triangleq \{pq : q \in Q\}$ (for a polynomial $p$ and set of polynomials $Q$) denotes the “tagging” operation.

Example 3.2. Consider the regular cones

$$C_1 = C(X = 1 \land y \leq 1) = \text{alg.cone}([x - 1], \{1, 1 - y\})$$
$$C_2 = C(y = 2 \land 2 \leq x^2) = \text{alg.cone}([y - 2], \{1, x^2 - 2\})$$

To intersect $C_1$ and $C_2$, form the “tagged sum” $(Z, P)$ where

$$Z = \{t(x - 1), (1 - t)(y - 2)\} = \{tx - t, -ty + 2t + y - 2\}$$
$$P = \{t, t(1 - y), (1 - t), (1 - t)(x^2 - 2)\} = \{t, t - y, t + 1, -tx^2 + 2t + x^2 - 2\}$$

Then project $(Z, P)$ onto the variables $(x, y)$, in two steps. First orient $(Z, P)$ w.r.t $\leq_{(x,y)}$ $G = \text{GröbnerBasis}_{\leq_{(x,y)}}(Z) = \{tx - t, -ty + 2t + y - 2, xy - 2x - y + 2\}$

red$_C(P) = \{t, -t - y + 2, -t + 1, t + x^2 - 2\}$

and then intersect $G$ with $\mathbb{Q}[x, y]$ and project the monomial $t$ out of red$_C(P)$ using Fourier-Motzkin elimination. The resulting cone is

$$C_1 \cap C_2 = \text{alg.cone}([xy - 2x - y + 2], \{1, -y + 2, x^2 - y, x^2 - 1\})$$

which is the non-negative cone of the formula $(x - 1) \cdot (y - 2) = 0 \land y \leq 2 \land y \leq x^2 \land 1 \leq x^2$. \hfill \blacksquare

To prove correctness of this construction, we need the following technical lemma relating cones to their “tagged” counterparts:

Lemma 5. Let $X$ be a set of variables and $t \notin X$. Let $Z, P \subseteq \mathbb{Q}[X]$ be finite sets of polynomials, and let $f \in \mathbb{Q}[t]$ be a polynomial in $t$. Then for all $a \in \mathbb{Q}$ such that $f(a) \geq 0$, and for all $q \in \text{alg.cone}_{X,t}(fZ, fP)$, we have $q[t \mapsto a] \in \text{alg.cone}_{X}(Z, P)$ (where $q[t \mapsto a]$ denotes substitution of all occurrences of $t$ in $q$ with $a$).

Proof. Let $Z = \{z_1, \ldots, z_m\}$ and $P = \{p_1, \ldots, p_n\}$. For any $q \in \text{alg.cone}_{X,t}(fZ, fP)$ we can write

$$q = \sum_{i=1}^{m} g_i f_i z_i + \sum_{j=1}^{n} \lambda_j f_p p_j \quad (\forall i. q_i \in \mathbb{Q}[X, t], \lambda_i \in \mathbb{Q}_{\geq 0})$$

$$q[t \mapsto a] = \sum_{i=1}^{m} (g_i f(a)) z_i + \sum_{j=1}^{n} (\lambda_j f(a)) p_j \in \text{alg.cone}(Z, P)$$

since each $g_i f(a)$ is a polynomial in $X$ and each $\lambda_j f(a)$ is a non-negative rational. \hfill \Box

\footnote{Recalling that cones are dual to polyhedra, cone intersection corresponds to polyhedral join, and cone sum to polyhedral meet.}
**Theorem 6** (Intersection). Let $Z_1, P_1, Z_2, P_2 \subseteq \mathbb{Q}[X]$ be finite sets of polynomials over some set of variables $X$. Then

$$\text{alg.cone(}\text{intersect}(Z_1, P_1, Z_2, P_2)) = \text{alg.cone}(Z_1, P_1) \cap \text{alg.cone}(Z_2, P_2).$$

**Proof.** We prove each side of the equation is included in the other:

$\subseteq:$ Let $q \in \text{alg.cone(}\text{intersect}(Z_1, P_1, Z_2, P_2))$. Since $\text{intersect}(Z_1, P_1, Z_2, P_2) = \text{project}_X(tZ_1 \cup (1-t)Z_2, tP_1 \cup (1-t)P_2)$, we have $q \in \text{alg.cone}(tZ_1 \cup (1-t)Z_2, tP_1 \cup (1-t)P_2) \cap \mathbb{Q}[X]$ by Theorem 5. Then $q$ can be written as $q_1 + q_2$ for some $q_1 \in \text{alg.cone}(tZ_1, tP_1)$ and $q_2 \in \text{alg.cone}((1-t)Z_2, (1-t)P_2)$. Then we have

$$q = q[t \mapsto 0], \quad q \in \mathbb{Q}[X]$$

$$= q_1[t \mapsto 0] + q_2[t \mapsto 0], \quad q = q_1 + q_2, \text{ linearity of substitution}$$

$$\in \text{alg.cone}(Z_1, P_1) \cap \text{alg.cone}(Z_2, P_2).$$

Symmetrically, we have $q = q[t \mapsto 1] = q_1[t \mapsto 1] \in \text{alg.cone}(Z_1, P_1)$, and so $q$ belongs to the intersection $\text{alg.cone}(Z_1, P_1) \cap \text{alg.cone}(Z_2, P_2)$.

$\supseteq:$ Let $q \in \text{alg.cone}(Z_1, P_1) \cap \text{alg.cone}(Z_2, P_2)$. We have $tq \in \text{alg.cone}(tZ_1, tP_1)$ and $(1-t)q \in \text{alg.cone}((1-t)Z_2, (1-t)P_2)$, and therefore

$$q = tq + (1-t)q \in \text{alg.cone}_X(tZ_1, tP_1) + \text{alg.cone}_X((1-t)Z_2, (1-t)P_2)$$

$$= \text{alg.cone}_X(tZ_1 \cup (1-t)Z_2, tP_1 \cup (1-t)P_2) \quad \text{Theorem 2}$$

Since $q$ also belongs to $\mathbb{Q}[X]$, we have $q \in \text{alg.cone}_X(tZ_1 \cup (1-t)Z_2, tP_1 \cup (1-t)P_2) \cap \mathbb{Q}[X] = \text{alg.cone(}\text{intersect}(Z_1, P_1, Z_2, P_2)). \quad \square$

3.3.4 Lazy Consequence-Finding. We conclude with a consequence-finding algorithm that avoids the (explicit) computation of disjunctive normal incurred by the eager strategy presented at the beginning of this section. Algorithm 2 operates by iteratively selecting a cube from the DNF of $F$, computing its non-negative cone (Lemma 4), and adding blocking clauses so that the same cube would not be selected again in future iterations.

**Algorithm 2: Lazy consequence finding**

```plaintext
1 Function consequence(F, X)
2   Input : Ground $\sigma_{or}(Y)$-formula $F$ and set of symbols $X \subseteq Y$
3   Output: Oriented pair $(Z, P)$ with $\text{alg.cone}_X(Z, P) = C_X(F)$.
4
5   G ← F;
6   (Z, P) ← ({1}, 0);  /* Invariant: $C_X(F) \subseteq \text{alg.cone}(Z, P)$ */
7   while G is satisfiable do
8       /* $\text{alg.cone}(Z', P') = C_Y(G_i)$ for some cube $G_i$ of the DNF of $F$ (Lemma 4) */
9       (Z', P') ← get-model(G);
10      (Z', P') ← project(Z', P', X);
11      (Z, P) ← intersect(Z, P, Z', P');
12      /* Block any model $\mathcal{M}$ with $C_X(\mathcal{M}) \subseteq \text{alg.cone}(Z, P)$ */
13      G ← G ∧ (\$z \in \mathbb{Z}, z = 0 \land (\$p \in \mathbb{P}, 0 \leq p) \}$
14   return (Z, P)
```

**Theorem 7.** Given a ground $\sigma_{or}(Y)$-formula $F$ and $X \subseteq Y$, $\text{consequence}(F, X)$ returns an oriented pair $(Z, P)$ such that $\text{alg.cone}_X(Z, P) = C_X(F)$. 

When Less Is More: Consequence-Finding in a Weak Theory of Arithmetic

PROOF. Say that a regular cone $C$ is a cube cone of formula $H$ if $C = C_X(H)$ for some cube in the DNF of $H$, and $C$ is consistent. Let $\text{cube.cones}(H)$ denote the (finite) set of cube cones of $H$.

We first prove termination. Let $G_i$ denote the formula $G$ on the $i$th iteration of the loop, and let $B_i$ denote the $i$th blocking clause, so for each $i$ we have $G_{i+1} = G_i \land \neg B_i$. By Theorem 4 and Lemma 4, we have that

$$\text{cube.cones}(G_{i+1}) = \text{cube.cones}(G_i \land \neg B_i) = \{ Q \in \text{cube.cones}(G_i) : \mathfrak{M}(Q) \models \neg B_i \}.$$ 

Since the model returned by get-model is always in $\text{cube.cones}(G_i)$ (Theorem 4 and Lemma 4) and that model always satisfies $B_i$, we have a strictly descending sequence $\text{cube.cones}(G_0) \supsetneq \text{cube.cones}(G_1) \supsetneq \text{cube.cones}(G_2) \supsetneq \ldots$. Since $\text{cube.cones}(G_0)$ is a finite set, this sequence must have finite length and therefore the algorithm terminates.

Next we show that $\text{alg.cone}_X(Z, P) = C_X(F)$, where $(Z, P)$ is the pair returned by the algorithm. Suppose that the while loop exits after $N$ iterations. We show that $\text{alg.cone}_X(Z, P) = C_X(F)$ that by proving each side is included in the other:

$\subseteq$ : Since the while loop exists after $N$ iterations, we have that $G_N = F \land \neg B_1 \land \ldots \land \neg B_N$ is unsatisfiable modulo LRR. Since $B_i \models_{\text{LRR}} B_N$, and therefore $\text{alg.cone}_X(Z, P) = C_X(B_N) \subseteq C_X(F)$.

$\supseteq$ : By Theorems 5 and 6, $\text{alg.cone}_X(Z, P) = \mathbb{Q}[X] \cap \bigcap_{i=1}^N C_i$ where each $C_i \in \text{cube.cone}(F)$, thus $\text{alg.cone}_X(Z, P) \supseteq \mathbb{Q}[X] \cup \bigcap_{C \in \text{cube.cone}(F)} C = C_X(F)$. \hfill $\square$

4 INTEGER ARITHMETIC

Let $\sigma^Z_{or}$ be the signature of ordered rings extended with an additional unary relation symbol $\text{Int}$. Define the theory of linear integer real rings LRR to be the $\sigma^Z_{or}$-theory axiomatized by the axioms of LRR along with the following:

$$\forall x, y. \text{Int}(x) \land \text{Int}(y) \Rightarrow \text{Int}(x + y) \quad \text{(Int closure +)}$$

$$\forall x, y. \text{Int}(x) \land x + y = 0 \Rightarrow \text{Int}(y) \quad \text{(Int closure -)}$$

for all $n \in \mathbb{Z}^{\geq 1}$ and $m \in \mathbb{Z}, \forall x. \text{Int}(x) \land 0 \leq nx + m \Rightarrow 0 \leq x + \left[\frac{m}{n}\right] \quad \text{(Cutting plane)}$

The cutting plane axiom is an axiom schema, with one axiom for each choice of positive integer $n$ and integer $m$. Intuitively, $\text{Int}$ identifies a set of elements as "integers", and an inequality $0 \leq nx + m$ can be strengthened to $0 \leq x + \left[\frac{m}{n}\right]$ whenever $x$ is an "integer", as is the case for integers in $\mathbb{R}$. LRR is thus the theory consisting of all $\sigma^Z_{or}$-sentences that hold in all structures $\mathfrak{M}$ where $(U^\mathfrak{M}, 0^\mathfrak{M}, 1^\mathfrak{M}, +^\mathfrak{M}, \cdot^\mathfrak{M}, \leq^\mathfrak{M})$ is a model of LRR, $\text{Int}^\mathfrak{M}$ is an additive subgroup of $(U^\mathfrak{M}, 0^\mathfrak{M}, +^\mathfrak{M})$ that contains $1^\mathfrak{M}$ (identifying the "integers"), and "integers" behave like integers with regards to $\leq$. We regard $\mathbb{R}$ as the standard model of LRR, with $\text{Int}$ identifying the subset of integers; $\text{Th}^Z(\mathbb{R})$ refers to the theory consisting of all $\sigma^Z_{or}$-sentences satisfied by $\mathbb{R}$. We can extend $\sigma^Z_{or}$-structures to interpret $\text{Int}(p)$ for $p \in \mathbb{Q}[X]$ by translating $\text{Int}(p)$ to the formula $\exists x. \text{Int}(x) \land p = x$, where $x$ is a fresh symbol and $p = x$ is translated into a $\sigma_{or}$-formula as described in Section 3. For example, the formula $\text{Int}\left(\frac{1}{2}x - y\right)$ is translated to $\exists x. \text{Int}(z) \land (1 + 1) \cdot z + (1 + 1) \cdot y = x$.

An induction axiom is conspicuously absent from LRR. Nevertheless, the axiomatization is sufficient for positive linear formulas.

**Theorem 8.** Let $F$ be a ground $\sigma^Z_{or}(X)$-formula that is free of negation and multiplication. Then $F$ is satisfiable modulo LRR iff $F$ is satisfiable modulo $\text{Th}^Z(\mathbb{R})$.

**Proof.** The $\Leftarrow$ direction is trivial, since any model of $\text{Th}^Z(\mathbb{R})$ is a model of LRR.

For the $\Rightarrow$ direction, we prove that if $F$ is unsatisfiable modulo $\text{Th}^Z(\mathbb{R})$, then it is unsatisfiable modulo LRR. We may assume without loss of generality that $F$ takes the form $\bigwedge_{p \in P} 0 \leq p \land \bigwedge_{s \in S} \text{Int}(s)$. We may also assume that $S \subseteq X$: if $F = G \land \text{Int}(t)$ for some non-constant term $t$, then...
$F$ is equisatisfiable with $G \land \text{Int}(y) \land y \leq t \land t \leq y$ for a fresh constant $y$ (modulo $Th^Z(\mathbb{R})$ and also modulo LIRR). Furthermore, we may assume that $S = X$ (i.e., all symbols are integers), since if some symbol is not constrained to be an integer, it can be projected by Fourier-Motzkin elimination, resulting in an equisatisfiable formula (again modulo both theories).

Suppose that $F$ is unsatisfiable modulo $Th^Z(\mathbb{R})$—i.e., the polyhedron defined by $\bigwedge_{p \in P} 0 \leq p$ has no integer points. Then there is a cutting-plane proof of $0 \leq -1$ from $\bigwedge_{p \in P} 0 \leq p$ [Chvátal 1973; Schrijver 1980]. Since each inference step of a cutting-plane proof is valid modulo LIRR, $F$ is unsatisfiable modulo LIRR.

We now extend models of LRR to LIRR. Let $X$ be a set of variables. For sets $C, L \subseteq \mathbb{Q}[X]$, say that $C$ is closed under cutting planes with respect to $L$ if for any $n, m \in \mathbb{Z}, n > 0, p \in L$, if $np + m \in C$, then $p + \left\lfloor \frac{m}{n} \right\rfloor \in C$. Define the cutting plane closure of $C$ with respect to $L$, denoted $cpl(C)$, to be the least cone that contains $C$ and is closed under cutting planes with respect to $L$. If $C$ is a regular cone, define $\mathcal{M}(C, L)$ to be the extension of $\mathcal{M}(C)$ that interprets $\text{Int}$ as $\{p + \mathcal{U}(C) : p \in L\}$. Observe that when $\mathcal{U}(C) \subseteq L$, $\mathcal{M}(C, L) \models \text{Int}(p)$ iff $p \in L$, for all $p \in \mathbb{Q}[X]$.

Say that the pair $(C, L)$ is regular if $C$ is a regular cone, $L$ is an additive subgroup of $\mathbb{Q}[X]$ that contains 1 and $\mathcal{U}(C)$, and $C$ is closed under cutting planes with respect to $L$. $(L, C)$ is an additive subgroup if $0 \in L$ and $x - y \in L$ whenever $x, y \in L$. If $(C_1, L_1)$ and $(C_2, L_2)$ are regular, we consider $(C_1, L_1)$ to be smaller than $(C_2, L_2)$ if $C_1 \subseteq C_2$ and $L_1 \subseteq L_2$.

Let $X$ be a set of symbols, and let $\mathcal{A}$ be a $\sigma_{or}$ structure satisfying the axioms of LIRR. Define $L(\mathcal{A}) \doteq \{p \in \mathbb{Q}[X] : \mathcal{A} \models \text{Int}(p)\}$ to be the set that $\mathcal{A}$ identifies as “integers”. Naturally, $(C(\mathcal{A}), L(\mathcal{A}))$ is regular. For the converse, we have the following.

**Lemma 6.** Let $X$ be a set of variables and $C, L \subseteq \mathbb{Q}[X]$. If $(C, L)$ is regular and $C$ is consistent, $\mathcal{M}(C, L)$ is a model of LIRR.

Analogously with regular and algebraic cones for LRR, regular $(C, L)$ give us a “standard form” in which LIRR models can be represented, but they lack a finite representation and cannot be manipulated effectively—we will define algebraic $(C, L)$ for this purpose.

We begin with algebraic lattices, which serve as a finite representation (certain) additive subgroups of $\mathbb{Q}[X]$. Call a set $L \subseteq \mathbb{Q}[X]$ an algebraic lattice if $L = I + L_0$ for an ideal $I$ and a point lattice $L_0$. For sets $Z, B \subseteq \mathbb{Q}[X]$, define $\text{alg.lattice}_Z(Z, B) = \mathbb{Q}[X](Z) + \mathbb{Z}(B)$. If $(Z, B)$ is oriented (with respect to $\leq$) and $B$ is linearly independent, say that $(Z, B)$ is independently oriented (with respect with $\leq$). Assuming $Z$ is a Gröbner basis, an independently oriented representation of $\text{alg.lattice}(Z, B)$ can be computed by

\[ \text{indep.orient}_Z(B) \doteq \text{int.basis}(\{\text{red}_Z(b) : b \in B\}) \]

where $\text{int.basis}$ denotes a function that computes a basis for a point lattice (this can be done in polytime using a Hermite Normal Form computation [Schrijver 1999, Ch. 4]).

**Lemma 7** (Orientation). Let $X$ be a set of variables, $Z, B \subseteq \mathbb{Q}[X]$ be finite sets of polynomials such that $Z$ is a Gröbner basis. Then $(Z, \text{indep.orient}_Z(B))$ is independently oriented, and $\text{alg.lattice}(Z, B) = \text{alg.lattice}(Z, \text{indep.orient}_Z(B))$.

Note that membership in a point lattice can be checked in polytime (to check $t \in \mathbb{Z}(b_1, \ldots, b_n)$, first solve $a_1b_1 + \cdots + a_nb_n = t$ and then check whether each $a_1, \ldots, a_n$ in the solution is an integer). Thus, by the following lemma we have that checking membership in an algebraic lattice is decidable.

**Lemma 8** (Membership). Let $X$ be a set of variables, and $Z, B \subseteq \mathbb{Q}[X]$ be finite sets of polynomials such that $(Z, B)$ is independently oriented. For any polynomial $p \in \mathbb{Q}[X]$, we have $p \in \text{alg.lattice}(Z, B)$ iff $\text{red}_Z(p) \in \mathbb{Z}(B)$.
Lastly, we develop a notion of algebraic cone/lattice pairs, which will serve as effective \( \sigma^Z_{op} \) structures. For \( C, L \subseteq \mathbb{Q}[X] \), say that \( (C, L) \) is **algebraic** if there exists finite sets \( Z, P, B \subseteq \mathbb{Q}[X] \) such that \( C = \text{alg.cone}_X(Z, P) \) and \( L = \text{alg.lattice}_X(Z, B) \). We denote this by \( (C, L) = \text{alg.cone}_X(Z, P, B) \), and drop the subscript \( X \) when the context is clear. Say that \( (Z, P, B) \) is **oriented** (with respect with \( \preceq \)) if \( (Z, P) \) is oriented and \( (Z, B) \) is independently oriented (both with respect with \( \preceq \)). If an algebraic \( (C, L) \) is also regular, it can be represented by an oriented triple \( (Z, P, B) \) such that \( \mathbb{Q}^{\geq 0}(P) \) is salient: first compute an oriented \( (Z, P) \) with \( \mathbb{Q}^{\geq 0}(P) \) salient such that \( C = \text{alg.cone}(Z, P) \) (Theorem 3), and then \( B \) such that \( (Z, B) \) is oriented and \( L = \text{alg.lattice}(Z, B) \) (Lemma 7). Under this condition, we have \( \mathcal{U}(\text{alg.cone}(Z, P)) = (Z) \subseteq \text{alg.lattice}(Z, B) \), and thus \( \mathfrak{M}(\text{alg.cone}(Z, P, B)) \models \text{Int}(p) \) iff \( p \in \text{alg.lattice}(Z, B) \). Since membership in an algebraic cone and lattice are both decidable, it follows that checking whether \( \mathfrak{M}(\text{alg.cone}(Z, P, B)) \models F \) for a ground formula \( F \) is decidable, provided that \( (Z, P, B) \) is oriented and \( P \) is salient.

### 4.1 Satisfiability Modulo LIRR

This section presents a decision procedure for testing satisfiability of ground conjunctive \( \sigma^Z_{op}(X) \)-formulas modulo LIRR. Without loss of generality, a ground conjunctive formula \( F \) can be written in the form

\[
F = \bigwedge_{p \in P} (0 \leq p) \land \bigwedge_{q \in Q} \neg (0 \leq q) \land \bigwedge_{r \in R} \neg (0 = r) \land \bigwedge_{s \in S} \text{Int}(s) \land \bigwedge_{t \in T} \neg \text{Int}(t),
\]

where \( P, Q, R, S, T \) are all finite sets of polynomials. In the following, we show that it is possible to compute a finite representation of the least regular \( (C, L) \) such that \( C \) contains \( P \) and \( L \) contains \( S \) (Theorem 10). Then we show that \( F \) is satisfiable modulo LIRR if and only if \( C \) is consistent and \( \mathfrak{M}(C, L) \models F \), and moreover that \( C = C(F) \) (Theorem 11). Since checking consistency of \( C \) and \( \mathfrak{M}(C, L) \models F \) is decidable, this yields a decision procedure for ground LIRR-formulas, as well as an algorithm for computing the non-negative cone of a ground formula.

#### 4.1.1 Cutting Plane Closure

This section addresses the following problem: given finite sets \( Z, P, B \subseteq \mathbb{Q}[X] \), compute \( Z', P' \) such that \( \text{alg.cone}(Z', P') \) contains \( \text{alg.cone}(Z, P) \) and is closed under cutting planes with respect to the algebraic lattice \( \text{alg.lattice}(Z, B) \). This is the key operation needed to compute the least regular pair \( (C, L) \) containing a given pair, which will be addressed in Section 4.1.2. Our strategy for computing cutting plane closure is to reduce it to the problem of computing the integer hull of a polyhedron.

First, we show that the cutting plane closure of a cone \( \text{alg.cone}(Z, P) \) with respect to the algebraic lattice \( \text{alg.lattice}(Z, B) \) coincides with the cutting plane closure of \( \text{alg.cone}(Z, P) \) with respect to the point lattice \( \mathbb{Z}(B) \):

**Lemma 9.** Let \( C, L \subseteq \mathbb{Q}[X] \) be such that \( C \) is a cone. Then \( cp_{\mathcal{U}(C)+L}(C) = cp_{L}(C) \).

**Proof.** Let \( L' = \mathcal{U}(C) + L \). Since \( L \subseteq L' \), \( cp_{L'}(C) \supseteq cp_{L}(C) \). For \( cp_{L'}(C) \subseteq cp_{L}(C) \), first observe that \( cp_{L}(C) \) is a cone that contains \( C \), so it suffices to show that it is closed under cutting planes with respect to \( L' \).

Let \( np + m \in cp_{L}(C) \), where \( n, m \in \mathbb{Z}, n > 0 \), and \( p \in L' \). Then \( p = z + v \) for some \( z \in \mathcal{U}(C) \) and \( v \in L \). Since \( np + m \in cp_{L}(C) \) and \( nz \in \mathcal{U}(cp_{L}(C)) \), we have \( (np + m) - nz \in cp_{L}(C) \) and so

\[
np + m = nv + m + nz - nz = n(z + v) + m - nz = (np + m) - nz \in cp_{L}(C).
\]

Since \( cp_{L}(C) \) is closed under cutting planes with respect to \( L \) and \( v \in L, v + \left\lfloor \frac{m}{n} \right\rfloor \in cp_{L}(C) \). Then \( p + \left\lfloor \frac{m}{n} \right\rfloor = z + v + \left\lfloor \frac{m}{n} \right\rfloor \in cp_{L}(C) \). Thus, \( cp_{L'}(C) \subseteq cp_{L}(C) \). 

\[\square\]
Next, we show that computing the cutting plane closure of an algebraic cone with respect to a point lattice can be reduced to computing the cutting plane closure of the cone of inequalities defining a (finite-dimensional) polyhedron.

**Lemma 10.** Let $B = \{b_1, \ldots, b_k\} \subseteq \mathbb{Q}[X]$, and let $C \subseteq \mathbb{Q}[X]$ be a cone. Let $Y = \{y_1, \ldots, y_k\}$ be a set of symbols disjoint from $X$ and define a linear map $f : \mathbb{Q}[Y]^1 \to \mathbb{Q}[X]$ by

$$f(a_0 + a_1 y_1 + \cdots + a_k y_k) = a_0 + a_1 b_1 + \cdots + a_k b_k.$$  

Then $cp_{\mathbb{Z}(B)}(C) = C + f(cp_{\mathbb{Z}(Y)}(f^{-1}(C)))$.

**Proof.** (⊆) Let $D = f(cp_{\mathbb{Z}(Y)}(f^{-1}(C)))$. Since $cp_{\mathbb{Z}(B)}(C)$ is the least cone that contains $C$ and is closed under cutting planes with respect to $\mathbb{Z}(B)$, it is sufficient to prove the following:

1. $C + D$ is a cone: it is the sum of two cones and is thus a cone.
2. $C + D$ contains $C$: since $C$ is non-empty we have $0 \in D$, so $C \subseteq C + D$.
3. $C + D$ is closed under cutting planes with respect to $\mathbb{Z}(B)$. Suppose $np + m \in C + D$, with $n, m \in \mathbb{Z}$, $n > 0$, and $p \in \mathbb{Z}(B)$; we must show that $p + \lfloor \frac{m}{n} \rfloor \in C + D$.

Without loss of generality, we may suppose $np + m \in D$—the argument is as follows. Since $np + m \in C + D$, we have $np + m = g + h$ for some $g \in C$ and $h \in D$. Since $np + m \in \mathbb{Z}(B) + \mathbb{Z}[Y] = f(\mathbb{Q}[Y]^1)$, we have $g = (np + m) - h \in f(\mathbb{Q}[Y]^1)$ since the image of $f$ is a subspace of $\mathbb{Q}[X]$ containing both $(np + m)$ and $h$. So $g \in C \cap f(\mathbb{Q}[Y]^1)$, and thus $g \in f(f^{-1}(C))$. Since $cp_{\mathbb{Z}(Y)}(\cdot)$ is extensive (i.e., $S \subseteq cp_{\mathbb{Z}(Y)}(S)$ for all $S$) and $f$ is linear, we have $np + m = g + h \in D$.

We now prove that $p + \lfloor \frac{m}{n} \rfloor \in C + D$. Since $p \in \mathbb{Z}(B)$, there exists $p' \in \mathbb{Z}(Y)$ such that $f(p') = p$. Then $f(np' + m) = np + m \in D$. Since $f$ is a linear map, $np' + m + g \in cp_{\mathbb{Z}(Y)}(f^{-1}(C))$ for some $g \in \ker(f)$ and $f^{-1}(0)$. This is a subspace, so $-g \in \ker(f)$. Since $0 \in C$, $\ker(f) = f^{-1}(0) \subseteq f^{-1}(C) \subseteq cp_{\mathbb{Z}(Y)}(f^{-1}(C))$. So $-g \in cp_{\mathbb{Z}(Y)}(f^{-1}(C))$, and since $cp_{\mathbb{Z}(Y)}(f^{-1}(C))$ is a cone, $np' + m + g - g \in cp_{\mathbb{Z}(Y)}(f^{-1}(C))$. Since $p' \in \mathbb{Z}(Y)$, $p' + \lfloor \frac{m}{n} \rfloor \in cp_{\mathbb{Z}(Y)}(f^{-1}(C))$. So $p + \lfloor \frac{m}{n} \rfloor = f(p' + \lfloor \frac{m}{n} \rfloor) \in C + D$.

(⊇) First note that $C \subseteq cp_{\mathbb{Z}(B)}(C)$, and since $cp_{\mathbb{Z}(B)}(C)$ is closed under addition, it suffices to show that $f(cp_{\mathbb{Z}(Y)}(f^{-1}(C))) \subseteq cp_{\mathbb{Z}(B)}(C)$. In turn, it suffices to show $cp_{\mathbb{Z}(Y)}(f^{-1}(C)) \subseteq f^{-1}(cp_{\mathbb{Z}(B)}(C))$. Let $D = f^{-1}(cp_{\mathbb{Z}(B)}(C))$. As before, it suffices to show that $D$ is a cone, $f^{-1}(C) \subseteq D$ and $D$ is closed under cutting planes with respect to $\mathbb{Z}(Y)$.

It is easy to verify that $D$ is a cone, and since $cp_{\mathbb{Z}(B)}(\cdot)$ is extensive, $f^{-1}(C) \subseteq D$. Suppose that $np + m \in f^{-1}(cp_{\mathbb{Z}(B)}(C))$, with $p \in \mathbb{Z}(Y)$, $n, m \in \mathbb{Z}$, and $n > 0$; we must show that $p + \lfloor \frac{m}{n} \rfloor \in D$. By linearity of $f$, $nf(p) + m = f(np + m) \in cp_{\mathbb{Z}(B)}(C)$. Since $f(p) \in \mathbb{Z}(B)$, and $cp_{\mathbb{Z}(B)}(C)$ is closed under cutting planes with respect to $\mathbb{Z}(B)$, $f(p) + \lfloor \frac{m}{n} \rfloor \in cp_{\mathbb{Z}(B)}(C)$. Thus, $f(p + \lfloor \frac{m}{n} \rfloor) \in cp_{\mathbb{Z}(B)}(C)$, and $p + \lfloor \frac{m}{n} \rfloor \in D$. □

It remains to show that the reduction in Lemma 10 is effective. The only non-trivial operation involved in the reduction that we have not already seen is computing the inverse image of an algebraic cone $C \subseteq \mathbb{Q}[X]$ under a linear map with finite-dimensional domain $f : \mathbb{Q}[Y]^1 \to \mathbb{Q}[X]$. This can be accomplished by extending the linear map to a ring homomorphism $\tilde{f} : \mathbb{Q}[Y] \to \mathbb{Q}[X]$, taking the inverse image of $C$ under $\tilde{f}$, and intersecting it with $\mathbb{Q}[Y]^1$.

For disjoint finite sets of variables $X$ and $Y$, a ring homomorphism $f : \mathbb{Q}[Y] \to \mathbb{Q}[X]$, and finite $Z, P \subseteq \mathbb{Q}[X]$, define

$$\text{inverse-hom}(Z, P, f, Y) \doteq \text{project}_Y(\{y - f(y) : y \in Y\} \cup Z, P).$$
Theorem 9 (Inverse image). Let $Z, P \subseteq \mathbb{Q}[X]$ be finite sets, $Y$ be a finite set of variables distinct from $X$, and $f : \mathbb{Q}[Y] \rightarrow \mathbb{Q}[X]$ be a ring homomorphism. Then

$$\text{alg.cone}_Y(\text{inverse-hom}(Z, P, f, Y)) = f^{-1}(\text{alg.cone}_X(Z, P)).$$

Note that $\mathbb{Q}[Y]^1$ is an algebraic (in fact, polyhedral) cone in $\mathbb{Q}[Y]$, so we can intersect an algebraic cone with $\mathbb{Q}[Y]^1$ using the procedure of Section 3.3.3. Precisely, let $Y \subseteq X$ be sets of variables. Define

$$\text{intersect-subspace}(Z, P, Y) = \text{second}(\text{intersect}(Z, P, \emptyset, P_{\mathbb{Q}[Y]^1})).$$

where $P_{\mathbb{Q}[Y]^1} = Y \cup -Y \cup \{1, -1\}$, and second returns the second component of the pair. Note that the first component is always $\emptyset$ (or equivalently, $\{0\}$) since it is a Gröbner basis for the ideal $\langle Z \rangle \cap \langle \emptyset \rangle = \{0\}$.

Let $\text{cut}(P, Y)$ be a procedure that computes the cutting plane closure of the cone generated by $P \subseteq \mathbb{Q}[Y]^1$, with respect to $\mathbb{Z}(Y)$. That is, $\mathbb{Q}^\infty(\text{cut}(P, Y)) = \text{cp}_{\mathbb{Z}(Y)}(\mathbb{Q}^\infty(P))$. This may be done by e.g., the iterated Gomory-Chvátal closure.\(^2\)

We now arrive at an effective implementation of the reduction in Lemma 10. Define an operation $\text{cut}(Z, P, B)$ by:

$$\text{cut}(Z, P, B) \triangleq \text{substitute}(f, \text{cut}(\text{intersect-subspace}(\text{inverse-hom}(Z, P, f, Y), Y))),$$

where $Y = \{y_1, \ldots, y_n\}$ is a set of fresh variables corresponding to $B = \{v_1, \ldots, v_n\}$ generating a point lattice, $f : \mathbb{Q}[Y] \rightarrow \mathbb{Q}[X]$ is the ring homomorphism defined by $f(y_i) = v_i$, and substitute$(f, P')$ applies $f$ to each polynomial in $P'$. By linearity of $f$, substitute$(f, P')$ computes the image of the polyhedral cone generated by $P'$.

Lemma 11. Let $Z, P, B \subseteq \mathbb{Q}[X]$ be finite subsets. Then we have

$$\text{cp}_{\mathbb{Z}(B)}(\text{alg.cone}(Z, P)) = \text{alg.cone}(Z, P \cup \text{cut}(Z, P, B)).$$

Example 4.1. We illustrate $\text{cut}(Z, P, B)$ with $Z = \emptyset$, $P = \{x_1 - 2x_2 + 1, x_1 + 2x_2, -x_1, x_2^2\}$ and $B = \{2x_1, 2x_2\}$.

Let $f : \mathbb{Q}[y_1, y_2]^1 \rightarrow \mathbb{Q}[x_1, x_2]$ be the function mapping $f(y_1) = 2x_1$ and $f(y_2) = 2x_2$, and let $\hat{f}$ denote its extension to a ring homomorphism $\mathbb{Q}[y_1, y_2] \rightarrow \mathbb{Q}[x_1, x_2]$. First, we compute $\text{inverse-hom}(Z, P, \hat{f}, \{y_1, y_2\})$, yielding the pair $(0, P')$ with $P' = \left\{\frac{1}{2}y_1 - y_2 + 1, \frac{1}{2}y_1 + y_2, -\frac{1}{2}y_1, \frac{1}{4}y_2^2\right\}$ (representing the algebraic cone $\hat{f}^{-1}(\text{alg.cone}(Z, P))$ which, in this case, happens to be polyhedral). Next, we compute generators for the polyhedral cone $\hat{f}^{-1}(\text{alg.cone}(Z, P)) \cap \mathbb{Q}[y_1, y_2]^1$ via $\text{intersect-subspace}(\emptyset, P', \{y_1, y_2\})$, yielding $P'' = \left\{\frac{1}{2}y_1 - y_2 + 1, \frac{1}{2}y_1 + y_2, -\frac{1}{2}y_1\right\}$.

Next, we compute generators for $\text{cp}(\mathbb{Q}^\infty(P''))$. Consider the polyhedron $Q$ that is defined by $P'':$

$$Q = \left\{(y_1, y_2) \in \mathbb{Q}^2 : 0 \leq \frac{1}{2}y_1 - y_2 + 1, 0 \leq \frac{1}{2}y_1 + y_2, 0 \leq \frac{1}{2}y_1\right\}$$

This polyhedron has vertices $\{0, 0\}$, $(0, 1)$ and $(-1, \frac{1}{2})$, so its integer hull is defined by $y_1 = 0, 0 \leq y_2$, and $y_2 \leq 1$. Hence, the cutting plane closure is $\text{cut}(P'') = \{y_1, -y_1, y_2, -y_2 + 1\}$.

---

\(^2\)When $1 \in P$, this can also be done by any algorithm that computes integer hulls. Precisely, $\text{cp}_{\mathbb{Z}(Y)}(\mathbb{Q}^\infty(P)) = \text{cp}(\mathbb{Q}^\infty(P))$, where the latter is the cutting plane closure of the (cone of) valid inequalities for $Q = \{x \in \mathbb{Q}^n : p(x) \geq 0 \text{ for all } p \in P\}$, which is also the cone of inequalities defining $Q_1$. The discrepancy arises because $1 \geq 0$ is always a valid inequality, and is contained in the latter; $\text{cp}_{\mathbb{Z}(Y)}(\cdot)$ generalizes cutting plane closure to cones that may not contain 1.
We now prove termination. By Theorem 10, \( \text{alg.cone}(Z, P, B) \) is the least regular \((C, L)\) satisfying \( \text{alg.cone}(Z, P) \subseteq C \) and \( \text{alg.lattice}(Z, B) \subseteq L \).

\[ \text{alg.cone}(Z', P', B') \leftarrow \text{regularize}(Z, P); \]
\[ B' \leftarrow \text{indep.orient}_Z(B \cup \{1\}); \]
\[ \text{cut}(Z', P', B'); \]
\[ \text{regularize}(Z', P' \cup Q); \]
\[ B' \leftarrow \text{indep.orient}_Z(B'); \]
\[ \text{alg.cone}(Z', P') = \text{alg.cone}(Z, P); \]
\[ \text{return} (Z', P', B'); \]

**Algorithm 3:** Regular cutting plane closure of a cone

Finally, applying substitute gives \( \text{cut}(Z, P, B) = \{2x_1, -2x_1, 2x_2, -2x_2 + 1\} \). By Lemma 11,

\[ \text{cp}_{Z(B)}(\text{alg.cone}(Z, P)) = \text{alg.cone}(Z, P) + \mathbb{Q}^{\geq 0}\langle 2x_1, -2x_1, 2x_2, -2x_2 + 1 \rangle. \]

### 4.1.2 Regular Cutting Plane Closure

This section addresses the following problem: given finite sets \( Z, P, B \subseteq \mathbb{Q}[X] \), compute \( Z', P', B' \) such that \( \text{alg.cone.lattice}(Z', P', B') \) is the least regular pair containing \( \text{alg.cone.lattice}(Z, P, B) \) (component-wise). Regularity of \((Z, P, B)\) requires that (1) \( \text{alg.cone}(Z, P) \) is a regular cone and (2) \( \text{alg.cone}(Z, P) \) is closed under cutting planes with respect to \( \text{alg.lattice}(Z, P) \). The regularize and \( \text{cp} \) procedures achieve (1) and (2) respectively, so the essential problem is to achieve both conditions simultaneously. Algorithm 3 accomplishes this by iterating regularize and \( \text{cp} \) until a fixed point is reached.

**Theorem 10** (Regular cutting plane closure). Let \( X \) be a finite set of variables, and \( Z, P, B \subseteq \mathbb{Q}[X] \) be finite sets. Then \( \text{cp}(Z, P, B) \) terminates, and \( \text{alg.cone.lattice}(\text{cp}(Z, P, B)) \) is the least regular \((C, L)\) satisfying \( \text{alg.cone}(Z, P) \subseteq C \) and \( \text{alg.lattice}(Z, B) \subseteq L \).

**Proof.** Assume that \((Z, P, B)\) is oriented. Let \( Z_i, P_i, B_i, Q_i \) be \( Z', P', B', Q \) at the end of the \( i \)th iteration respectively. Define \( C_i = \text{alg.cone}(Z_i, P_i) \) and \( L_i = \text{alg.lattice}(Z_i, B_i) \). When \( i = 0 \), these values are the values just before entry to the loop. For any cone \( C \subseteq \mathbb{Q}[X] \), let \( R(C) \) denote the least regular cone containing \( C \).

Define \( D_{i+1} = \text{cp}_{Z(B_i)}(C_i) \). By Theorem 11, \( D_{i+1} = \text{alg.cone}(Z_i, P_i \cup Q_i) \). By Theorem 3, \( C_{i+1} = R(D_{i+1}) = R(\text{cp}_{Z(B_i)}(C_i)) \). First note the following properties.

(P1) \( \mathcal{U}(C_i) = \mathcal{U}(\text{alg.cone}(Z_i, P_i)) = \langle Z_i \rangle \), because the output \((Z_i, P_i)\) of regularize is oriented and \( \mathbb{Q}^{\geq 0}\langle P_i \rangle \) is salient (Theorem 3).

(P2) \( C_i \) is an increasing sequence of regular cones by subset ordering, because \( C_{i+1} = R(\text{cp}_{Z(B_i)}(C_i)) \).

(P3) For all \( i, 1 \in C_i, \text{alg.cone}(Z, P) \subseteq C_i, 1 \in L_i, \) and \( \text{alg.lattice}(Z, B) \subseteq L_i \); By Theorem 3 and (P2), \( 1 \in C_i \) and \( \text{alg.cone}(Z, P) \subseteq C_i \) for all \( i \). By Lemma 7, \( 1 \in L_0 \) and \( L \subseteq L_0 \). By (P1) and (P2), \( \langle Z_i \rangle = \mathcal{U}(C_i) \subseteq \mathcal{U}(C_{i+1}) = \langle Z_{i+1} \rangle \). Then \( \text{alg.lattice}(Z_i, B_i) \subseteq \text{alg.lattice}(Z_{i+1}, B_i) \). Hence, \( 1 \in L_i \) and \( \text{alg.lattice}(Z, B) \subseteq L_i \) for all \( i \).

We now prove termination. By (P2), \( (\mathcal{U}(C_i))_i \) is an ascending chain of ideals. Since \( \mathbb{Q}[X] \) is Noetherian, \( \mathcal{U}(C_n) = \mathcal{U}(C_{n+1}) \) for some \( n \geq 0 \). Since \( C_i \subseteq D_{i+1} \subseteq C_{i+1} \) for all \( i \), \( \mathcal{U}(C_n) \subseteq \mathcal{U}(D_{n+1}) \subseteq \mathcal{U}(C_{n+1}) = \mathcal{U}(C_n) \).
\( \mathcal{U}(C_n) \), so \( \mathcal{U}(D_{n+1}) = \mathcal{U}(C_n) \) is an ideal. Since \( C_i \subseteq D_{i+1} \) and \( 1 \in C_i \) for all \( i \) (P3), \( 1 \in D_{n+1} \). So \( D_{n+1} \) is a regular cone. Since \( C_{n+1} \) is the least regular cone containing \( D_{n+1} \), we have \( C_{n+1} = D_{n+1} \).

We show that \( C_{n+1} \) is closed under cutting planes with respect to \( \mathbb{Z}(B_{n+1}) \), so that \( C_{n+2} = D_{n+1} = C_{n+1} \) and the algorithm terminates. By (P1), \( \langle Z_n \rangle = \mathcal{U}(C_n) = \mathcal{U}(C_{n+1}) = \langle Z_{n+1} \rangle \). Note that \( Z_n \) and \( Z_{n+1} \) are Gröbner bases with respect to the same monomial ordering, so by the representation independence property of Gröbner bases, \( \text{red}_{Z_n}(b) = \text{red}_{Z_n}(b) \) for all \( b \in \mathbb{Q}[X] \). Also, note that \( (Z_i, B_i) \) is independently oriented, by Lemma 7 and noting that the output of \( \text{regularize} \) is oriented. So \( \text{red}_{Z_i}(b) = b \) for all \( b \in B_i \).

\[
\mathcal{Z}(B_{n+1}) = \mathcal{Z}(\text{int.basis}(\{ \text{red}_{Z_n}(b) : b \in B_n \}))
= \mathcal{Z}(\{ \text{red}_{Z_n}(b) : b \in B_n \}) = \mathcal{Z}(\{ \text{red}_{Z_n}(b) : b \in B_n \}) = \mathcal{Z}(B_n)
\]

Hence,

\[
\text{cp}_{\mathcal{Z}(B_{n+1})}(C_{n+1}) = \text{cp}_{\mathcal{Z}(B_n)}(C_{n+1}) = \text{cp}_{\mathcal{Z}(B_n)}(D_{n+1}) = \text{cp}_{\mathcal{Z}(B_n)}(\text{cp}_{\mathcal{Z}(B_n)}(C_n)) = \text{cp}_{\mathcal{Z}(B_n)}(C_n) = C_{n+1},
\]

where the last equality follows from the definition of \( D \) and noting \( C_{n+1} = D_{n+1} \). Then \( C_{n+2} = R(\text{cp}_{\mathcal{Z}(B_{n+1})}(C_{n+1})) = R(C_{n+1}) = C_{n+1} \), and the algorithm terminates.

Now let \( N \) be the last iteration of the algorithm. We show that \( \text{alg.cone.lattice}(Z_N, P_N, B_N) = (C_N, L_N) \) is the least regular \((C, L)\) satisfying \( \text{alg.cone}(Z, P) \subseteq C \) and \( \text{alg.lattice}(Z, B) \subseteq L \).

We first show that \( \text{alg.cone.lattice}(Z_N, P_N, B_N) \) is regular. Since \( N \geq 1 \), \( \text{alg.cone}(Z_N, P_N) = C_N = R(\text{cp}_{\mathcal{Z}(B_{n+1})}(C_{n+1})) \) is regular. By (P1), \( \mathcal{U}(\text{alg.cone}(Z_N, P_N)) = \langle Z_N \rangle \subseteq \text{alg.lattice}(Z_N, B_N) = L_N \). By (P3), \( 1 \in L_N \). By the proof of termination, \( \text{cp}_{\mathcal{Z}(B_n)}(C_n) = C_n \). By (P1) and Lemma 9, \( C_N \) is closed under cutting planes with respect to \( L_N \). Thus, \( \text{alg.cone.lattice}(Z_N, P_n, B_N) \) is regular.

Finally, note that (1) \( \text{alg.cone}(Z, P) \subseteq C_N \) and (2) \( \text{alg.lattice}(Z, B) \subseteq L_N \) by (P3). We may show that \( (C_N, L_N) \) is the least regular pair satisfying (1) and (2) by supposing that \( (C', L') \) is regular and satisfies (1) and (2), and proving \( C_i \subseteq C' \) and \( L_i \subseteq L' \) by induction on \( i \).

\[\square\]

### 4.1.3 Satisfiability and Consequence-Finding modulo LIRR

Since we have a procedure for computing the regular cutting plane closure of an algebraic cone with respect to a point lattice, the following theorem yields both a decision procedure for \( \text{LIRR} \) and an algorithm for consequence-finding modulo \( \text{LIRR} \):

**Theorem 11.** Let \( F \) be the ground conjunctive formula

\[
F = \left( \bigwedge_{p \in P} 0 \leq p \right) \land \left( \bigwedge_{q \in Q} -(0 \leq q) \right) \land \left( \bigwedge_{r \in R} -(0 = r) \right) \land \left( \bigwedge_{s \in S} \text{Int}(s) \right) \land \left( \bigwedge_{t \in T} \neg\text{Int}(t) \right).
\]

Let \((C, L)\) be the least regular pair such that \( P \subseteq C \) and \( S \subseteq L \). Then we have the following:

1. \( F \) is satisfiable iff \( C \) is consistent and \( \mathfrak{M}(C, L) \models F \).
2. \( C = C(F) \).

Summarizing, we have the following decision procedure for satisfiability of conjunctive \( \sigma^Z_{op}(X) \)-formulas modulo \( \text{LIRR} \). Let \( F \) be a ground conjunctive formula of the form in Theorem 11. First compute \((Z', P', B') = rcp(\emptyset, P, B)\). If \( \text{red}_{Z'}(1) = 0 \), then \( F \) is unsatisfiable (\( \text{alg.cone}(Z', P') \) is inconsistent). Otherwise, we check whether \( \mathfrak{M} = \mathfrak{M}(\text{alg.cone.lattice}(Z', P', B')) \) satisfies \( F \) by testing whether there is some \( q \in Q \) with \( \text{red}_{Z'}(q) \in \mathbb{Q}^\geq\langle P' \rangle \) (Lemma 2), or some \( r \in R \) with \( \text{red}_{Z'}(r) = 0 \), or some \( t \in T \) with \( \text{red}_{Z'}(r) \in \mathbb{Z}\langle B' \rangle \) (Lemma 8); if such a \( q, r, \) or \( t \) exists, then \( F \) is unsatisfiable (Theorem 4), otherwise, \( \mathfrak{M} \) satisfies \( F \).

Consequence-finding modulo \( \text{LIRR} \) operates in the same way as Algorithm 2. The only difference is that \( \text{get-model} \) returns a triple \((Z', P', B')\) instead of pair \((Z', P')\)—but the point lattice basis \( B' \) is simply ignored by the rest of the algorithm.
In this section, we describe an application of consequence-finding modulo LIRR to the problem of computing loop invariants. The method is based on extracting recurrence relations (of a particular form) from the body of a loop, and using their closed forms to summarize loop dynamics. The key property of our loop-invariant generation procedure is that it is monotone: if more information about the program’s behavior is given to the procedure, then it may only compute invariants that are more precise (modulo LIRR). Monotonicity is achieved due to the fact that it is possible to find and manipulate the set of all implied inequalities of a formula modulo LIRR. Section 5.1 provides background on summarization and the loop summarization procedure presented in Section 5.2.

5.1 Program Summarization

Loop summarization is the problem of over-approximating the reflexive transitive closure of a transition formula (a notion that will be made precise in the following). One might think of a transition formula as a logical summary of the action of a program through one iteration of the body of some loop, and an approximation of its reflexive transitive closure as a summary for (an unbounded number of iterations of) the loop. Using the algebraic program analysis framework, a loop summarization procedure can be “lifted” to a whole-program analysis [Farzan and Kincaid 2015; Kincaid et al. 2021; Zhu and Kincaid 2021], allowing us to focus our attention on this relatively simple logical sub-problem.

Fix a finite set of symbols $X$ (corresponding to the variables in a program of interest) and a set of “primed copies” $X' = \{x' : x \in X\}$. Define a transition formula $F$ to be an existential $\sigma_{or}^Z(X \cup X')$-formula. A transition formula represents a relation over program states, where the unprimed variables correspond to the pre-state and the primed variables correspond to the post-state. For any pair of transition formulas $F[X, X']$ and $G[X, X']$, define their sequential composition as $F \circ G \equiv \exists X''. F[X' \mapsto X''] \land G[X' \mapsto X'']$ where $X'' = \{x'' : x \in X\}$ is a set of variable symbols disjoint from $X$ and $X'$ (representing the intermediate state between a computation of $F$ and a computation of $G$). Define the $t$-fold composition of a transition formula $F$ as $F^t \equiv F \circ \ldots \circ F$ ($t$ times). The problem of over-approximating reflexive transitive closure is, given a transition formula $F$, find a transition formula $F^*$ such that $F^t \models_{LIRR} F^*$ for all $t \in \mathbb{Z}_{\geq 0}$.

Our approach to this problem is based on the one in [Ancourt et al. 2010; Farzan and Kincaid 2015]. Given a transition formula $F$, this approach computes an over-approximation of its reflexive transitive closure $F^*$ in two steps. In the first step, it extracts a system of recurrences $F \models_{LRA} \land_{i=1}^n r_i' \leq r_i + a_i$ where each $r_i$ denotes a linear term over $X$, each $r_i'$ denotes a corresponding linear term over $X'$ and each $a_i$ is a rational number (for instance $(x' + y') \leq (x + y) + 2$, indicating that the sum of $x$ and $y$ increases by at most two). In the second step, it computes their closed forms $F^* \equiv \exists t. t \geq 0 \land \land_{i=1}^n r_i' \leq r_i + t a_i$. In the following, we generalize this strategy to the non-linear setting by considering recurrences where $a_i$ is not a rational number but rather an invariant of the loop—a polynomial in $X$ that does not change under the action of $F$.

5.2 A Loop Summarization Operator

This section describes the class of recurrences that we wish to compute (Section 5.2.1), a method to compute them (Section 5.2.2), and then defines a loop summarization operator and shows that it is monotone and (in a sense) complete modulo LIRR (Section 5.2.3).

5.2.1 Invariant-Bounded Differences. Lift the mapping from symbols in $X$ to their primed counterpart in $X'$ into a ring homomorphism of polynomial terms $(-)' : \mathbb{Q}[X] \rightarrow \mathbb{Q}[X']$ (so, e.g., $(xy + 3z)'$ denotes the polynomial $(x'y' + 3z')$). Define the space of linear invariant functionals $\text{LinInv}(F)$
of a formula \( F \) to be those linear terms over \( X \) that are invariant under the action of \( F \):

\[
\text{LinInv}(F) \triangleq \{ k \in \mathbb{Q}(X) : F \models_{\text{LIRR}} k' = k \}.
\]

Define the space of invariant polynomials \( \text{Inv}(F) \) to be the subring of \( \mathbb{Q}[X] \) generated by \( \text{LinInv}(F) \). Clearly, for any \( p \in \text{Inv}(F) \) we have \( F \models_{\text{LIRR}} p' = p \) (but the reverse does not hold). Finally, we define the class of recurrences of interest, the invariant-bounded differences of \( F \), to be

\[
diff{F} \triangleq \{ (r, a) \in \mathbb{Q}(X) \times \text{Inv}(F) : F \models_{\text{LIRR}} r' \leq r + a \}.
\]

Note that for any \( (r, a) \in \diff{F} \) and any \( t \in \mathbb{Z}^+ \), we have \( F^t \models_{\text{LIRR}} r' \leq r + ta \).

**Example 5.1.** Consider the program

\[
\text{while}(\ast) \{ \text{if } (\ast) \{ w = w + 1; \} \text{ else } \{ w = w + 2; \} \}
\]

\[
x = x + z; \quad y = y + z; \quad z = (x - y)(x - y);
\]

where \(*\) denotes non-deterministic choice. The transition formula for the loop body is

\[
F = (w' = w + 1 \lor w' = w + 2) \land x' = x + z \land y' = y + z \land z' = z + (x' - y')^2.
\]

Notice that the linear polynomial \( x - y \) is an invariant of the loop; \( \text{LinInv}(F) \) is the linear space spanned by \( (x - y) \). The polynomial \( (x - y)^2 \) is thus an invariant polynomial in the subring \( \text{Inv}(F) \). The invariant-bounded differences \( \diff{F} \) includes (but is not limited to) \(-w, -1\) \((w \text{ increases by at least 1}), (w, 2) \((w \text{ increases by at most 2})\), as well as \((z, (x - y)^2) \) and \((-z, -(x - y)^2) \) \((z \text{ is always set to } z + (x - y)^2 \text{ at each iteration})\).

**Example 5.2.** Consider the program while \((\ast) \{ w = -w; \}\). The transition formula \( F \) of the loop body is \(w' = -w\). The polynomial \( w^2 \) is an invariant polynomial of the loop; \( F \models_{\text{LIRR}} (w')^2 = w^2 \).

However, \( F \) has no linear invariants, so \( \text{LinInv}(F) = \{0\} \) and \( \text{Inv}(F) = \{0\} \).

5.2.2 Computing Invariant-Bounded Differences. We proceed in three steps, showing how to represent and compute \( \text{LinInv}(F) \), \( \text{Inv}(F) \), and finally \( \diff{F} \).

Since \( \text{LinInv}(F) \) is a linear space it can be represented by a basis, which we compute as follows. Let \( D \triangleq \{ d_x : x \in X \} \) denote a set of variables distinct from those in \( X, X' \). Define a ring homomorphism \( \delta : \mathbb{Q}[D] \to \mathbb{Q}[X \cup X'] \) by \( \delta(d_x) \triangleq x - x' \) and a second ring homomorphism \( \text{pre} : \mathbb{Q}[D] \to \mathbb{Q}[X] \) by \( \text{pre}(d_x) = x \). Then \( \text{LinInv}(F) = \text{pre}(\delta^{-1}(\mathcal{L}(C(F)))) \cap (D) : F \models_{\text{LIRR}} k' = k \text{ if } F \models_{\text{LIRR}} k' - k = 0 \text{ if } k' - k \in \text{LIRR} \text{ is a unit in the nonnegative cone of } F \); since \( k \) is linear, \( k' - k = \delta(d) \) for some linear term \( d \in \mathbb{Q}(D) \). A basis for \( \text{LinInv}(F) \) can be computed using the primitives we have developed in the preceding (consequence-finding, cone intersection, and inverse image).

Let \( \{a_1, \ldots, a_n\} \) be a basis for \( \text{LinInv}(F) \). The subring \( \text{Inv}(F) \) of \( \mathbb{Q}[X] \) can be represented as the elements of the polynomial ring \( \mathbb{Q}[K] \), where \( K = \{k_1, \ldots, k_n\} \) is a set of fresh variables, one for each basis element of \( \text{LinInv}(F) \). Let \( \text{inv} \) denote the (injective, since \( \{a_1, \ldots, a_n\} \) is linearly independent) ring homomorphism \( \mathbb{Q}[K] \to \mathbb{Q}[X] \) that sends \( k_i \) to \( a_i \) for each \( i \). Then the image of \( \text{inv} \) is precisely \( \text{Inv}(F) \) (i.e., \( \mathbb{Q}[K] \) and \( \text{Inv}(F) \) are isomorphic).

Finally, we show how to represent and compute \( \diff{F} \). Each element of \( \diff{F} \) is a pair \((r, a)\) consisting of a linear term \( r \in \mathbb{Q}(X) \) and a polynomial \( a \in \text{Inv}(F) \). As a technical convenience, we can represent such a pair as a polynomial in \( \mathbb{Q}(D) + \mathbb{Q}[K] \). Since \( D \) and \( K \) are disjoint, there exist (unique) linear maps \( \pi_D : \mathbb{Q}(D) + \mathbb{Q}[K] \to \mathbb{Q}(D) \) and \( \pi_K : \mathbb{Q}(D) + \mathbb{Q}[K] \to \mathbb{Q}[K] \) such that for all \( p \in \mathbb{Q}(D) + \mathbb{Q}[K] \) we have \( p = \pi_D(p) + \pi_K(p) \). Then we may define a bijection \( \text{rep} : \mathbb{Q}(D) + \mathbb{Q}[K] \to \mathbb{Q}(X) \times \text{Inv}(F) \) by \( \text{rep}(p) = (\text{pre}(\pi_D(p)), \text{inv}(\pi_K(p))) \). Define \( \diff{F} \) to be the inverse image of \( \diff{F} \) under \( \text{rep} \) (i.e., an exact representation of \( \diff{F} \) in the space \( \mathbb{Q}(D) + \mathbb{Q}[K] \)).

Thus, it suffices to show how to compute \( \diff{F} \). Define a ring homomorphism \( \delta_{\text{inv}} : \mathbb{Q}[D, K] \to \mathbb{Q}[X \cup X'] \) by \( \delta_{\text{inv}}(d_x) = x - x' \) and \( \delta_{\text{inv}}(k_i) = a_i \) (i.e., the common extension of \( \delta \) and \( \text{inv} \)). Then we see that \( \diff{F} \triangleq \delta_{\text{inv}}^{-1}(\mathcal{L}(C(F)) \cap (D) + \mathbb{Q}[K]) \); that is, the invariant-bounded differences of \( F \).
Algorithm 4: Linear restriction

correspond exactly to the members of $\delta_{inv}^{-1}(\mathcal{C}(F))$ that are linear in the $D$ variables. We illustrate this with an example.

**Example 5.3.** We continue Example 5.1. The nonnegative cone of $F$ is $\mathcal{C}(F) = \text{alg.cone}(Z, P)$, where $Z$ and $P$ are:

$$Z = \{(w-w'+1)(w-w'+2), x-x'+z, y-y'+z, z-z'+(x-y)^2\}$$

$$P = \{-w+w'-1, w-w'+2\}$$

Applying $\delta^{-1}$ to the units of this cone gives $Q[D]\langle (d_w+1)(d_w+2), d_x-d_y \rangle$ (to see why the inverse image contains $d_x - d_y$, observe that $\delta(d_x - d_y) = (x-x') - (y-y') = (x-x'+z) - (y-y'+z) \in \langle Z \rangle$). Intersecting this with $Q(D)$ yields $Q[d_x-d_y]$. Hence, $\text{LinInv}(F) = Q(x-y)$.

The subring $\text{Inv}(F)$ generated by these linear invariants is represented by $Q[k_1]$ (with $\text{inv}(k_1) = x-y$). We have the following corresponding elements in $\text{diff}(F)$ and $\overline{\text{diff}}(F)$:

$$(-w,-1) \sim -d_w-1, (w,2) \sim d_w+2, (z,(x-y)^2) \sim d_z + k_z^2, \text{ and } (-z,-(x-y)^2) \sim -d_z - k_z^2$$

Notice how $-d_w-1$ and $d_w+2$ correspond to $P$, and how $d_z + k_z^2$ and $-d_z - k_z^2$ correspond to the last polynomial $(z-z') + (x-y)^2 \in Z$.

We now continue with showing how to compute $\overline{\text{diff}}(F)$. Since we already saw how to compute inverse images of algebraic cones, it remains only to show that we can compute the intersection of an algebraic cone over $Q[D,K]$ with $Q(D) + Q[K]$; i.e., the set of polynomials in cone that are linear in the set of variables $D$, but may contain arbitrary monomials in $K$. This is nearly solved by the intersection algorithm in Section 3.3.3, since $Q(D) + Q[K]$ is the sum of a finitely-generated cone $Q(D) = Q^{\geq 0}(D \cup -D)$ and an ideal $Q[K]$; however, $Q(D) + Q[K]$ is not an algebraic cone because $Q[K]$ is not an ideal in $Q[D,K]$. However, the essential process behind cone intersection carries over, which yields Algorithm 4.

**Lemma 12.** Let $D, K$ be disjoint finite sets of variables and $Z, P \subseteq Q[D,K]$ be finite sets of polynomials over $D$ and $K$. Let $(V, R) = \text{lin}(Z, P, D, K)$. Then

$$Q[K](V) + Q^{\geq 0}(R) = \text{alg.cone}(Z, P) \cap (Q[K] + Q(D))$$

5.2.3 Loop Summarization. The core logic of our loop summarization operator appears in Algorithm 5, which computes an over-approximation $\exp(F, t)$ of the $t$-fold composition of $F$ (symbolic
Theorem 13 (Monotonicity). If \( F \models_{\text{LIRR}} G \), then \( F^* \models_{\text{LIRR}} G^* \).

### 6 EXPERIMENTAL EVALUATION

We consider two experimental questions raised by the relatively weak strength of LRR/LIRR.

1. (Section 6.2): Are the theories LRR/LIRR strong enough to prove unsatisfiability of formulas that are unsatisfiable modulo \( \text{Th}(\mathbb{R})/\text{Th}(\mathbb{Z}) \)? How does the performance of the decision procedures for LRR/LIRR compare with state-of-the-art SMT solvers?

2. (Section 6.3): Is the theory LIRR strong enough to enable client applications that rely on consequence-finding, such as the invariant generation algorithm presented in Section 5? How does LIRR-supported invariant generation compare with state-of-the-art automated program verification tools?
6.1 Experimental Setup

**Implementation.** We implemented an SMT solver for LRR and LIRR, which we call Chilon\(^3\). Our implementation relies on Z3 (as a SAT solver)\(^{[de Moura and Björner 2008]}\) Apron/NewPolka\(^{[Jeannet and Miné 2009]}\) for polyhedral operations, FLINT\(^{[Hart et al. 2021]}\) for lattice operations, and Normaliz\(^{[Bruns et al. 2021]}\) for Hilbert basis computation (a sub-procedure of iterated Gomory-Chvátal closure). Based on Chilon, we implemented the consequence-finding procedure as well as the approximate transitive closure operator for invariant generation. We have also integrated the invariant generation procedure into a static analysis framework that facilitates evaluation on software verification benchmarks, which is used as a proxy to evaluate the quality of the generated invariants.

**Environment.** We ran all experiments on an Oracle VirtualBox virtual machine with Lubuntu 22.04 LTS (Linux kernel version 5.15 LTS), with a two-core Intel Core i5-5575R CPU @ 2.80 GHz and 4 GB of RAM. All tools were run with the benchexec\(^{[Wendler and Beyer 2022]}\) tool under a time limit of 2 minutes on all benchmarks. Reported times are total aggregate, measured in seconds and averaged across 5 runs.

**SMT Benchmarks and Solvers.** SMT tasks are taken from the quantifier-free nonlinear real arithmetic and nonlinear integer arithmetic (QF_NRA and QF_NIA) divisions of SMT-COMP 2021\(^{[Barbosa et al. 2022]}\). For each division, we randomly draw the same number of tasks from each directory, resulting in about 100 tasks. We compare the performance of Chilon on these tasks against other solvers for standard theories of arithmetic, including Z3 4.8.13, MathSAT 5.6.5, CVC4 1.8, and Yices 2.6.4.

**Program Verification Benchmarks and Tools.** The program verification tasks are the safe, integer-only\(^4\) benchmarks from the c/ReachSafety-Loops subcategory of SV-COMP 2022\(^{[Beyer 2022]}\). Tasks from the nla-digbench and nla-digbench-scaling directories constitute the nonlinear benchmark suite, while all other tasks form the Linear suite. We compare against CRA (or Compositional Recurrence Analysis\(^{[Farzan and Kincaid 2015]}\)), another invariant generation tool based on analyzing recurrence relations; VeriAbs 1.4.2, the winner for the ReachSafety category of SV-COMP; and Ultimate Automizer 0.2.2, which performed best on the nla-digbench suite.

6.2 How Does Chilon Perform on SMT Tasks?

Table 2 records the results of running the five solvers on nonlinear SMT benchmarks. Since the reals are a model of LRR, if a formula is unsatisfiable modulo LRR then it is unsatisfiable modulo NRA, but the converse does not hold i.e., using a LRR-solver on NRA tasks can give false SAT results, but not false UNSAT results). The same holds for LIRR and NIA.

Chilon does not appear to be competitive for either QF_NRA or QF_NIA. It proves UNSAT for 6 out of 40 and 14 out of 41 tasks in the QF_NRA and QF_NIA suites, respectively, lower than other SMT solvers we compared against. Chilon reports false positives on 23 out of 40 UNSAT tasks in QF_NRA and 15 out of 41 UNSAT tasks in QF_NIA. It performs poorly on crafted tasks, in which the unsatisfiability proof often requires reasoning about the interaction between multiplication and the order relation, which is not axiomatized by our theories. It performs particularly well on verification tasks (e.g., the hycomp suite in QF_NRA, and the LassoRanker and UltimateLassoRanker suites in QF_NIA), but all other solvers we tested also performed well on these tasks. Chilon is competitive with other solvers in terms of running time. We note that there is substantial room for improving

---

\(^3\)The famous ancient Greek proverb "less is more", is attributed to Chilon of Sparta, one of the Seven Sages of Greece.

\(^4\)That is, the error location is unreachable, and all variables are integer-typed.
the performance of Chilon; in particular, it does not tightly integrate the theory solver with the underlying SAT solver as do most modern SMT solvers.

The experimental results suggest that the theories of linear integer / real rings is not generically suitable as an alternative to the theory of integers / reals for applications that only require a SAT or UNSAT answer.

Table 2. Comparison of Chilon with other SMT solvers on SMT-COMP benchmarks. The “#P” column denotes the number of proved tasks, and the “#E” column denotes the number of tasks on which a solver times out / runs out of memory. The max standard deviation in runtime across all benchmarks is Chilon: 25.58, Z3: 18.71, MathSat: 2.03, CVC4: 6.10, Yices: 4.29.

<table>
<thead>
<tr>
<th>suite</th>
<th>label</th>
<th>#task</th>
<th>Chilon</th>
<th>Z3</th>
<th>MathSAT</th>
<th>CVC4</th>
<th>Yices</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>#P</td>
<td>#E</td>
<td>time</td>
<td>#P</td>
<td>#E</td>
</tr>
<tr>
<td>SAT</td>
<td>QF_NRA</td>
<td>38</td>
<td>10/0</td>
<td>1215.9</td>
<td>15/20</td>
<td>2603.4</td>
<td>9</td>
</tr>
<tr>
<td>UNSAT</td>
<td>QF_NIA</td>
<td>40</td>
<td>11/0</td>
<td>1368.9</td>
<td>30</td>
<td>9/1</td>
<td>1193.4</td>
</tr>
<tr>
<td>?</td>
<td>?</td>
<td>27</td>
<td>12/0</td>
<td>1495.3</td>
<td>18/0</td>
<td>2224.6</td>
<td>12</td>
</tr>
<tr>
<td>SAT</td>
<td>QF_NRA</td>
<td>29</td>
<td>13/0</td>
<td>1595.9</td>
<td>26</td>
<td>3/0</td>
<td>535.9</td>
</tr>
<tr>
<td>UNSAT</td>
<td>QF_NIA</td>
<td>41</td>
<td>11/0</td>
<td>1347.2</td>
<td>36</td>
<td>5/0</td>
<td>662.2</td>
</tr>
<tr>
<td>?</td>
<td>?</td>
<td>28</td>
<td>16/1</td>
<td>2241.1</td>
<td>11/0</td>
<td>1361.1</td>
<td>12</td>
</tr>
</tbody>
</table>

6.3 How Does Chilon-inv Perform on Program Verification Tasks?

In this subsection, we evaluate the strength of consequence-finding modulo LIRR via the invariant generation scheme described in Section 5, implemented in the tool Chilon-inv. We compare with two similar recurrence-based invariant generation techniques, both of which rely on consequence-finding: CRA-lin [Farzan and Kincaid 2015] uses a complete consequence-finding procedure modulo linear arithmetic; and CRA [Kincaid et al. 2017] uses a heuristic consequence-finding procedure modulo non-linear arithmetic. We also evaluate a second configuration of Chilon-inv, which uses a refinement algorithm from [Cyphert et al. 2019] to improve analysis precision; this is guaranteed because the analysis that Chilon-inv implements is monotone.

Table 3 compares the performance of invariant generation using Chilon with other methods that utilize consequence-finding. Results show that Chilon-inv indeed performs strictly better than CRA-lin on both suites (particularly on the nonlinear suite). This is expected, since Chilon-inv’s consequence-finding algorithm is more powerful than that of CRA-lin, and Chilon-inv considers a larger class of recurrences. Chilon-inv outperforms CRA on the nonlinear suite, but CRA dominates the linear suite. This can be attributed to CRA’s control-flow refinement techniques that are not implemented in the base analysis in Chilon-inv (with refinement, Chilon-inv matches the performance of CRA on the linear suite—see Table 4).

Table 3. Comparison of recurrence-based invariant generation schemes. Timeouts are reported in parentheses. The max standard deviation in runtime across all benchmarks is Chilon: 1.89, CRA-lin: 0.08, CRA: 0.63.

<table>
<thead>
<tr>
<th>#tasks</th>
<th>Chilon-inv</th>
<th>CRA-lin</th>
<th>CRA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#tasks</td>
<td>time</td>
<td>#tasks</td>
</tr>
<tr>
<td>linear</td>
<td>178</td>
<td>117</td>
<td>955.9</td>
</tr>
<tr>
<td>nonlinear</td>
<td>290</td>
<td>232</td>
<td>2259.5</td>
</tr>
</tbody>
</table>
Table 4. Comparison of Chilon (with and without refinement) against leading SV-COMP competitors. Timeouts are reported in parentheses. The max standard deviation in runtime across all benchmarks is Chilon: 1.89, Chilon-inv + Refine: 0.11, UAutomizer: 9.08, VeriAbs: 0.00.

<table>
<thead>
<tr>
<th></th>
<th>Chilon-inv</th>
<th>Chilon-inv + Refine</th>
<th>UAutomizer</th>
<th>VeriAbs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#tasks</td>
<td>#correct</td>
<td>time</td>
<td>#correct</td>
</tr>
<tr>
<td>linear</td>
<td>178</td>
<td>117</td>
<td>955.9 (6)</td>
<td>140</td>
</tr>
<tr>
<td>nonlinear</td>
<td>290</td>
<td>232</td>
<td>2259.5 (15)</td>
<td>233</td>
</tr>
</tbody>
</table>

Table 4 provides context by comparing with state-of-the-art program verification tools. VeriAbs is a portfolio verifier that employs a variety of techniques, such as bounded model checking, k-induction, and loop summarization [Darke et al. 2021]. Notably, VeriAbs can summarize a numeric loops by accelerating linear recurrences involving only constants or variables that are unmodified within the loop [Darke et al. 2015]; the technique presented in Section 5.1 generalizes this scheme. Ultimate Automizer implements a counterexample-guided abstraction refinement algorithm following the trace abstraction paradigm [Heizmann et al. 2009]. Chilon-inv is competitive on the linear suite (particularly with refinement enabled) and outperforms the other tools on the nonlinear suite.

7 RELATED WORK

Real Arithmetic. The decidability of the theory of real closed fields is a classical result due to Tarski [1949] and Seidenberg [1954]. Practical (complete) algorithms for this theory are based on cylindrical algebraic decomposition (CAD) [Collins 1975; Jovanović and de Moura 2013; Kremer and Ábrahám 2020]. Due to the high computational complexity of decision procedures for the reals, a number of (incomplete) heuristic techniques have been devised [Tiwari 2005; Tiwari and Lincoln 2014; Zankl and Middeldorp 2010]. Similar to our approach, Tiwari [2005]’s method combines techniques from Gröbner bases and linear programming; however, the result of the combination is a semi-decision procedure for the existential theory of the reals, whereas we achieve a decision procedure for a weaker theory.

The \( \delta \)-complete decision procedure for the existential theory of the reals presented in [Gao et al. 2012] is similar in spirit to our work, in that the method gives up completeness in the classical sense while retaining a weaker version of it. Rather than using a standard model of the reals and relaxing the definition of satisfaction (each constraint is “within \( \delta \)” of being satisfied), we take the approach of using classical first-order logic, but admit non-standard models.

Positivestellensätze are a class of theorems that characterize sets of positive polynomial consequences of a system of inequalities over the reals (or a real closed field) [Krivine 1964]. Lemma 4 might be thought of as an analogue of a Positivestellensatz for LRR. Putinar’s Positivestellensatz [Putinar 1993] bears particular resemblance to our results: it asserts that the entailment \( \bigwedge_{z \in \mathbb{Z}} z = 0 \land \bigwedge_{p \in P} p \geq 0 \models_{\text{NRA}} q \geq 0 \) holds exactly when \( q \in \text{the quadratic module generated by } Z \text{ and } P \) (provided that certain technical restrictions implying compactness are satisfied). The quadratic module generated by \( Z \) and \( P \) is \( \langle Z \rangle + \Sigma^2[X]\langle P \cup \{1\} \rangle \) (where \( \Sigma^2[X] \) is the set of sum-of-squares polynomials over \( X \)), mirroring the structure of algebraic cones, but with sum-of-squares polynomials in place of non-negative rationals. Every quadratic module over \( \mathbb{R}[X] \) is also regular algebraic cone (following from the fact that its additive units form an ideal [Marshall 2008, Prop 2.1.2]) (but not vice versa).

Integer Arithmetic. Unlike the case of the reals, the theory consisting of \( \sigma_{or} \)-sentences that hold over the integers is undecidable (in fact, not even recursively axiomatizable). However, a number of
effective heuristics have been proposed, including combining real relaxation with branch-and-bound [Jovanović 2017; Kremer et al. 2016], bit-blasting [Fuhs et al. 2007], and linearization [Borralleras et al. 2019, 2009]. Linearization shares the idea of using linear arithmetic to reason about non-linear formulas. However, our approaches are quite different: Borralleras et al. [2019, 2009] essentially restrict the domain of constant symbols to finite ranges (making the approach sound but incomplete for satisfiability), whereas our approach is sound but incomplete for validity.

Non-Linear Invariant Generation. There are several abstract domains that are capable of representing conjunction of polynomial inequalities [Bagnara et al. 2005; Colón 2004; Gulavani and Gulwani 2008; Kincaid et al. 2017]. Such domains incorporate “best effort” techniques for reasoning about non-linear arithmetic. Notably, Kincaid et al. [2017] and Bagnara et al. [2005] combine techniques from commutative algebra and polyhedral theory. Our approach differs in that we designed complete inference, albeit modulo a weak theory of arithmetic.

There is a line of work on complete algorithms for finding invariant polynomial equations of (restricted) loops [Hrushovski et al. 2018; Humenberger et al. 2018; Kovács 2008; Rodríguez-Carbonell and Kapur 2004]. Another approach is to reduce polynomial invariant generation to linear invariant generation by introducing new dimensions, which provides completeness up to a degree-bound [de Oliveira et al. 2016; Müller-Olm and Seidl 2004]. Chatterjee et al. [2020] obtains a completeness (up to technical parameters) result for template-based generation of invariant polynomial inequalities, based on a “bounded” version of Putinar’s Positivstellensatz. Lemma 13 is a kind of completeness result, which is relative to a class of recurrences, rather than an invariant “shape.”

Consequence-Finding. A key feature of the arithmetic theories introduced in this paper is that they enable complete methods for finding and manipulating the set of consequences of a formula (of a particular form). In the setting of abstract interpretation, this problem is known as symbolic abstraction [Reps et al. 2004; Thakur 2014], and is phrased as the problem of computing the (ideally, best) approximation of a formula within some abstract domain. Symbolic abstraction algorithms are known for predicate abstraction [Graf and Saidi 1997], equations [Berdine and Bjørner 2014], affine equations [Reps et al. 2004; Thakur et al. 2015], template constraint domains (intervals, octagons, etc) [Li et al. 2014], and convex polyhedra [Farzan and Kincaid 2015]. Kincaid et al. [2017] gives a symbolic abstraction procedure for the wedge domain (which can express polynomial inequalities); this procedure is “best effort,” whereas our consequence-finding algorithm offers completeness guarantees.

It is interesting to note that our lazy consequence-finding algorithm (Algorithm 2) can be seen as an instantiation of Reps et al. [2004]’s symbolic abstraction algorithm. The termination argument of this algorithm relies on the abstract domain satisfying the ascending chain condition, which algebraic cones do not; instead, we exploit the fact that we can compute minimal models of LRR / LIRR, and each formula has only finitely many.

DATA AVAILABILITY STATEMENT
The artifact for this work has passed the review by the POPL Artifact Evaluation Committee and is available online [Kincaid et al. 2022a].

ACKNOWLEDGMENTS
This work was supported in part by the NSF under grant number 1942537 and by ONR under grant N00014-19-1-2318. Opinions, findings, conclusions, or recommendations expressed herein are those of the authors and do not necessarily reflect the views of the sponsoring agencies.
REFERENCES


When Less Is More: Consequence-Finding in a Weak Theory of Arithmetic


Received 2022-07-07; accepted 2022-11-07