Ramsey Quantifiers in Linear Arithmetics

Pascal Bergsträßer [1] Moses Ganardi [2] Anthony W. Lin [1,2]
Georg Zetzsche [2]

[1]Department of Computer Science, University of Kaiserslautern-Landau

[2]Max Planck Institute for Software Systems (MPI-SWS)

Theorietag 2023, Kaiserslautern

Linear Integer Arithmetic

LIA (a.k.a. Presburger arithmetic) is the first-order theory with the structure $\langle \mathbb{Z}; +, <, 1, 0 \rangle$.

Example

$\forall x \colon \exists y \colon 0 < x \to x < y \wedge y < 2x$ is not satisfiable

Proposition (Borosh,Treybig'76)

Satisfiability of existential formulas in LIA is NP*-complete.*

Proposition (Presburger'29)

LIA with the structure $\langle \mathbb{Z}; +, <, 1, 0, (\equiv_e)_{e>0} \rangle$ *admits quantifier elimination.*

Linear Real Arithmetic

LRA is the first-order theory with the structure $\langle \mathbb{R}; +, <, 1, 0 \rangle$.

Example

$\forall x \colon \exists y \colon 0 < x \to x < y \wedge y < 2x$ is satisfiable

Proposition (Sontag'85)

Satisfiability of existential formulas in LRA is NP*-complete.*

Proposition (Fourier 1826)

LRA with the structure $\langle \mathbb{R}; +, <, 1, 0 \rangle$ *admits quantifier elimination.*

Linear Integer Real Arithmetic

LIRA is the first-order theory with the structure $\langle \mathbb{R}; \lfloor \cdot \rfloor, +, <, 1, 0 \rangle$.

Linear Integer Real Arithmetic

LIRA is the first-order theory with the structure $\langle \mathbb{R}; \lfloor \cdot \rfloor, +, <, 1, 0 \rangle$.
The separation of $\exists \boldsymbol{x} \colon \varphi(\boldsymbol{x}, \boldsymbol{z})$ in LIRA is defined as

$$\exists \boldsymbol{x}^{\mathrm{i/r}} \colon \varphi(\boldsymbol{x}^{\mathrm{int}} + \boldsymbol{x}^{\mathrm{real}}, \boldsymbol{z}^{\mathrm{int}} + \boldsymbol{z}^{\mathrm{real}}) \wedge 0 \leq \boldsymbol{x}^{\mathrm{real}} < 1 \wedge 0 \leq \boldsymbol{z}^{\mathrm{real}} < 1.$$

Linear Integer Real Arithmetic

LIRA is the first-order theory with the structure $\langle \mathbb{R}; \lfloor \cdot \rfloor, +, <, 1, 0 \rangle$.
The separation of $\exists \boldsymbol{x} \colon \varphi(\boldsymbol{x}, \boldsymbol{z})$ in LIRA is defined as

$$\exists \boldsymbol{x}^{\mathrm{i/r}} \colon \varphi(\boldsymbol{x}^{\mathrm{int}} + \boldsymbol{x}^{\mathrm{real}}, \boldsymbol{z}^{\mathrm{int}} + \boldsymbol{z}^{\mathrm{real}}) \wedge 0 \leq \boldsymbol{x}^{\mathrm{real}} < 1 \wedge 0 \leq \boldsymbol{z}^{\mathrm{real}} < 1.$$

Existential formula in LIRA is decomposable if its separation can be written as an existentially quantified Boolean combination of Presburger and LRA formulas (called decomposition).

Linear Integer Real Arithmetic

LIRA is the first-order theory with the structure $\langle \mathbb{R}; \lfloor \cdot \rfloor, +, <, 1, 0 \rangle$.
The separation of $\exists \boldsymbol{x} \colon \varphi(\boldsymbol{x}, \boldsymbol{z})$ in LIRA is defined as

$$\exists \boldsymbol{x}^{\mathrm{i/r}} \colon \varphi(\boldsymbol{x}^{\mathrm{int}} + \boldsymbol{x}^{\mathrm{real}}, \boldsymbol{z}^{\mathrm{int}} + \boldsymbol{z}^{\mathrm{real}}) \wedge 0 \leq \boldsymbol{x}^{\mathrm{real}} < 1 \wedge 0 \leq \boldsymbol{z}^{\mathrm{real}} < 1.$$

Existential formula in LIRA is decomposable if its separation can be written as an existentially quantified Boolean combination of Presburger and LRA formulas (called decomposition).

Lemma

Every existential formula in LIRA is decomposable. Moreover, its decomposition is of linear size and can be computed in polynomial time.

Proposition

Satisfiability of existential formulas in LIRA is NP*-complete.*

Ramsey Quantifier

The formula

$$\exists^{\mathsf{ram}} \boldsymbol{x}, \boldsymbol{y} \colon \varphi(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$$

is fulfilled by valuation $\boldsymbol{c}$ of free variables $\boldsymbol{z}$ iff there exists $(\boldsymbol{a}_i)_{i \geq 1}$ of pairwise distinct valuations such that $\varphi(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c})$ for all $i < j$.
Such a sequence is called an infinite clique.

Example

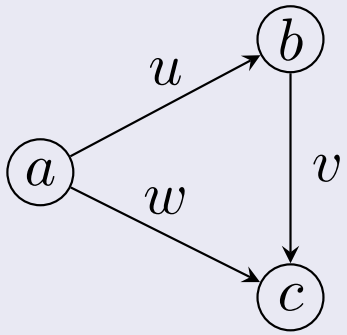
- $\exists^{\mathsf{ram}} x, y \colon x < y \wedge x \leq z$ is unsatisfiable over $\mathbb{Z}$ but satisfiable over $\mathbb{R}$
- $\exists^{\mathsf{ram}} x, y \colon \exists z \colon x < y \wedge x \leq z$ is satisfiable also over $\mathbb{Z}$

Eliminating Existential Quantifiers

Theorem

Let φ be an existential formula in LIRA. Then the following are equivalent:

- $\exists^{\mathsf{ram}} \boldsymbol{x}, \boldsymbol{y} \colon \exists \boldsymbol{w} \colon \varphi(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{w}, \boldsymbol{z})$

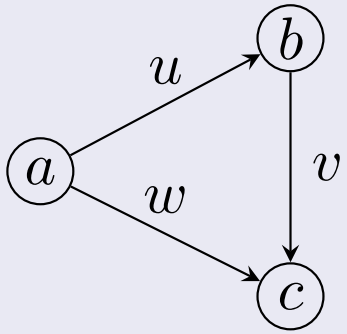


Eliminating Existential Quantifiers

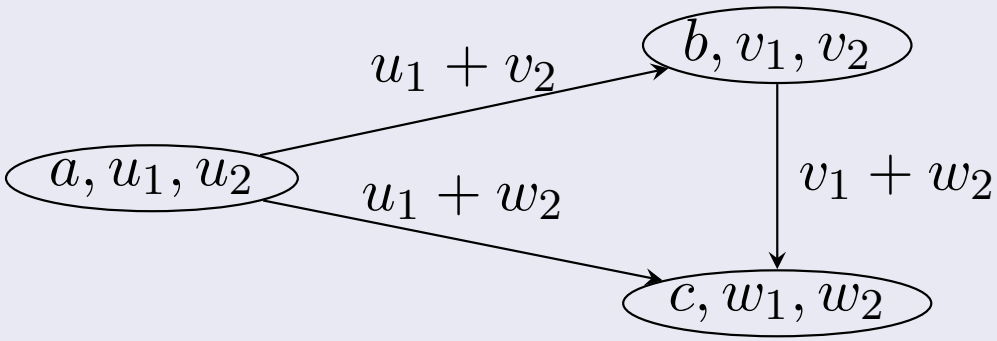
Theorem

Let φ be an existential formula in LIRA. Then the following are equivalent:

- $\exists^{\mathsf{ram}} \boldsymbol{x}, \boldsymbol{y} \colon \exists \boldsymbol{w} \colon \varphi(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{w}, \boldsymbol{z})$



- $\exists^{\mathsf{ram}} (\boldsymbol{x}, \boldsymbol{v}_1, \boldsymbol{v}_2), (\boldsymbol{y}, \boldsymbol{w}_1, \boldsymbol{w}_2) \colon \varphi(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{v}_1 + \boldsymbol{w}_2, \boldsymbol{z}) \wedge \boldsymbol{x} \neq \boldsymbol{y}$



Eliminating Existential Quantifiers in LIRA

- Bring decomposition of φ into DNF

$$\bigvee_{i=1}^{n} \alpha_i(\boldsymbol{x}^{\text{int}}, \boldsymbol{y}^{\text{int}}, \boldsymbol{w}^{\text{int}}, \boldsymbol{z}^{\text{int}}) \wedge \beta_i(\boldsymbol{x}^{\text{real}}, \boldsymbol{y}^{\text{real}}, \boldsymbol{w}^{\text{real}}, \boldsymbol{z}^{\text{real}})$$

where α_i are existential Presburger and β_i are existential LRA formulas.

Eliminating Existential Quantifiers in LIRA

- Bring decomposition of φ into DNF

$$\bigvee_{i=1}^{n} \alpha_i(\boldsymbol{x}^{\text{int}}, \boldsymbol{y}^{\text{int}}, \boldsymbol{w}^{\text{int}}, \boldsymbol{z}^{\text{int}}) \wedge \beta_i(\boldsymbol{x}^{\text{real}}, \boldsymbol{y}^{\text{real}}, \boldsymbol{w}^{\text{real}}, \boldsymbol{z}^{\text{real}})$$

  where α_i are existential Presburger and β_i are existential LRA formulas.

- By Ramsey's theorem, if there is a clique w.r.t. $\boldsymbol{c}$, then for some i

$$\begin{aligned} \exists^{\mathsf{ram}} \boldsymbol{x}^{\text{i/r}}, \boldsymbol{y}^{\text{i/r}} : \exists \boldsymbol{w}^{\text{int}} : \alpha_i(\boldsymbol{x}^{\text{int}}, \boldsymbol{y}^{\text{int}}, \boldsymbol{w}^{\text{int}}, \boldsymbol{c}^{\text{int}}) \wedge \\ \exists \boldsymbol{w}^{\text{real}} : \beta_i(\boldsymbol{x}^{\text{real}}, \boldsymbol{y}^{\text{real}}, \boldsymbol{w}^{\text{real}}, \boldsymbol{c}^{\text{real}}) \end{aligned}$$

Eliminating Existential Quantifiers in LIRA

- Bring decomposition of φ into DNF

$$\bigvee_{i=1}^{n} \alpha_i(\boldsymbol{x}^{\text{int}}, \boldsymbol{y}^{\text{int}}, \boldsymbol{w}^{\text{int}}, \boldsymbol{z}^{\text{int}}) \wedge \beta_i(\boldsymbol{x}^{\text{real}}, \boldsymbol{y}^{\text{real}}, \boldsymbol{w}^{\text{real}}, \boldsymbol{z}^{\text{real}})$$

  where α_i are existential Presburger and β_i are existential LRA formulas.

- By Ramsey's theorem, if there is a clique w.r.t. $\boldsymbol{c}$, then for some i

$$\begin{aligned}\exists^{\mathsf{ram}} \boldsymbol{x}^{\text{i/r}}, \boldsymbol{y}^{\text{i/r}} : \exists \boldsymbol{w}^{\text{int}} : \alpha_i(\boldsymbol{x}^{\text{int}}, \boldsymbol{y}^{\text{int}}, \boldsymbol{w}^{\text{int}}, \boldsymbol{c}^{\text{int}}) \wedge \\ \exists \boldsymbol{w}^{\text{real}} : \beta_i(\boldsymbol{x}^{\text{real}}, \boldsymbol{y}^{\text{real}}, \boldsymbol{w}^{\text{real}}, \boldsymbol{c}^{\text{real}})\end{aligned}$$

- Then (carefully) split $\exists^{\mathsf{ram}}$ into integer and real part and eliminate $\exists$ in Presburger and LRA.

Eliminating Existential Quantifiers in LIA

Assume $\exists^{\mathsf{ram}} \boldsymbol{x}, \boldsymbol{y} \colon \exists w \colon \varphi(\boldsymbol{x}, \boldsymbol{y}, w, \boldsymbol{z})$ and φ is a conjunction of inequalities

$$f_i(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) < w \qquad \text{and} \qquad w < f'_j(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$$

and modulo constraints

$$g_i(\boldsymbol{x}, \boldsymbol{y}, w, \boldsymbol{z}) \equiv_{e_i} d_i.$$

Eliminating Existential Quantifiers in LIA

Assume $\exists^{\mathsf{ram}} \boldsymbol{x}, \boldsymbol{y} \colon \exists w \colon \varphi(\boldsymbol{x}, \boldsymbol{y}, w, \boldsymbol{z})$ and φ is a conjunction of inequalities

$$f_i(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) < w \qquad \text{and} \qquad w < f'_j(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$$

and modulo constraints

$$g_i(\boldsymbol{x}, \boldsymbol{y}, w, \boldsymbol{z}) \equiv_{e_i} d_i.$$

Let $(\boldsymbol{a}_i)_{i \geq 1}$ be an infinite clique with $\varphi(\boldsymbol{a}_i, \boldsymbol{a}_j, b_{i,j}, \boldsymbol{c})$ for all $i < j$.
By Ramsey's theorem we can assume

$$f_1(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) \leq \cdots \leq f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) < b_{i,j} < f'_1(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) \leq \cdots \leq f'_m(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c})$$

Eliminating Existential Quantifiers in LIA

Suffices to consider greatest lower and smallest upper bound:

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) \quad < \quad b_{i,j} \quad < \quad f'_1(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c})$$

Eliminating Existential Quantifiers in LIA

Suffices to consider greatest lower and smallest upper bound:

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) \quad < \quad b_{i,j} \quad < \quad f'_1(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c})$$

To satisfy modulo constraints, we can always find

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) + 1 \quad \leq \quad b_{i,j} \quad \leq \quad f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) + N$$

where $N := e_1 \cdots e_k$.

Eliminating Existential Quantifiers in LIA

Suffices to consider greatest lower and smallest upper bound:

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) \quad < \quad b_{i,j} \quad < \quad f'_1(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c})$$

To satisfy modulo constraints, we can always find

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) + 1 \quad \leq \quad b_{i,j} \quad \leq \quad f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) + N$$

where $N := e_1 \cdots e_k$.
By Ramsey's theorem, we can assume that there is $r \in [1, N]$ s.t.

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) + r = b_{i,j}$$

Eliminating Existential Quantifiers in LIA

Suffices to consider greatest lower and smallest upper bound:

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) \quad < \quad b_{i,j} \quad < \quad f'_1(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c})$$

To satisfy modulo constraints, we can always find

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) + 1 \quad \leq \quad b_{i,j} \quad \leq \quad f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) + N$$

where $N := e_1 \cdots e_k$.
By Ramsey's theorem, we can assume that there is $r \in [1, N]$ s.t.

$$f_n(\boldsymbol{a}_i, \boldsymbol{a}_j, \boldsymbol{c}) + r = b_{i,j}$$

Thus, for additional components choose $\alpha(\boldsymbol{a}_i)$ and $\beta(\boldsymbol{a}_i, \boldsymbol{c}) + r$
where $f_n(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = \alpha(\boldsymbol{x}) + \beta(\boldsymbol{y}, \boldsymbol{z})$.

Eliminating Ramsey Quantifiers

Theorem

Given an existential formula $\varphi(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ in LIRA, we can construct in polynomial time an existential LIRA formula of linear size that is equivalent to $\exists^{\mathsf{ram}} \boldsymbol{x}, \boldsymbol{y} \colon \varphi(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$.

Idea for LIRA: Consider decomposition and handle integer and real part separately.

Eliminating Ramsey Quantifiers in LIA

Example

$$\exists^{\mathsf{ram}} x, y \colon y > 2 \cdot x \wedge \psi(x)$$

Clique is not Presburger definable but it exists iff there is $(a_i)_{i \geq 1}$ s.t. $\psi(a_i)$ and $a_1 < a_2 < \dots$

Eliminating Ramsey Quantifiers in LIA

Example

$$\exists^{\mathsf{ram}} x, y \colon y > 2 \cdot x \wedge \psi(x)$$

Clique is not Presburger definable but it exists iff there is $(a_i)_{i \geq 1}$ s.t. $\psi(a_i)$ and $a_1 < a_2 < \dots$

Assume φ is a conjunction

$$\bigwedge_{i=1}^{n} \boldsymbol{r}_i^\top \boldsymbol{x} < \boldsymbol{s}_i^\top \boldsymbol{y} + \boldsymbol{t}_i^\top \boldsymbol{z} + h_i \quad \wedge \quad \bigwedge_{j=1}^{m} \boldsymbol{u}_j^\top \boldsymbol{x} \approx^j_{e_j} \boldsymbol{v}_j^\top \boldsymbol{y} + \boldsymbol{w}_j^\top \boldsymbol{z} + d_j.$$

Eliminating Ramsey Quantifiers in LIA

Example

$$\exists^{\mathsf{ram}} x, y \colon y > 2 \cdot x \wedge \psi(x)$$

Clique is not Presburger definable but it exists iff there is $(a_i)_{i \geq 1}$ s.t. $\psi(a_i)$ and $a_1 < a_2 < \dots$

Assume φ is a conjunction

$$\bigwedge_{i=1}^{n} \boldsymbol{r}_i^\top \boldsymbol{x} < \boldsymbol{s}_i^\top \boldsymbol{y} + \boldsymbol{t}_i^\top \boldsymbol{z} + h_i \quad \wedge \quad \bigwedge_{j=1}^{m} \boldsymbol{u}_j^\top \boldsymbol{x} \approx_{e_j}^{j} \boldsymbol{v}_j^\top \boldsymbol{y} + \boldsymbol{w}_j^\top \boldsymbol{z} + d_j.$$

Describe the evolution of both sides of an inequality by

$$\sup\{\boldsymbol{r}_i^\top \boldsymbol{a}_k \mid k \geq 1\} \leq p_{2i-1}, \quad p_{2i} \leq \liminf\{\boldsymbol{s}_i^\top \boldsymbol{a}_k + \boldsymbol{t}_i^\top \boldsymbol{c} + h_i \mid k \geq 1\}.$$

The tuple $\boldsymbol{p} = (p_1, \dots, p_{2n}) \in \mathbb{Z}_\omega^{2n}$ is called profile.

Eliminating Ramsey Quantifiers in LIA

A sequence as above is called compatible with $\boldsymbol{p}$ for $\boldsymbol{c}$ if it additionally satisfies the modulo constraints.
A profile is admissible if $p_{2i-1} < p_{2i}$ or $p_{2i} = \omega$.

Lemma

$\exists^{\text{ram}} \boldsymbol{x}, \boldsymbol{y} \colon \varphi(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{c})$ if and only if there exists an admissible profile $\boldsymbol{p} \in \mathbb{Z}_{\omega}^{2n}$ such that there is a sequence compatible with $\boldsymbol{p}$ for $\boldsymbol{c}$.

Compatibility is Presburger expressible by restricting to sequences of the form $\boldsymbol{a}_0 + k \cdot \boldsymbol{a}$.

Applications

Corollary

Given a quantifier-free formula in LIA, LRA, or LIRA, deciding monadic decomposability is coNP*-complete.*

Corollary

Deciding whether a quantifier-free Presburger formula $\varphi(\boldsymbol{x}, \boldsymbol{y})$ defines a well-quasi-order is coNP*-complete.*

Corollary

Linear liveness is NP*-complete for continuous VASS, reversal-bounded counter machines, Praikh automata, and succinct one-counter automata.*