Linear Arithmetic Satisfiability via Strategy Improvement

Azadeh Farzan[1] Zachary Kincaid[1,2]

[1] University of Toronto

[2] Princeton University

July 13, 2016

- The problem: satisfiability modulo the theory of linear rational (& integer) arithmetic.
    - Applications in program analysis & synthesis

- The problem: satisfiability modulo the theory of linear rational (& integer) arithmetic.
  - Applications in program analysis & synthesis
- SMT solvers handle the ground fragment. Techniques for quantifiers:
  - Quantifier elimination (expensive)
  - Heuristic quantifier instantiation (incomplete)

- The problem: satisfiability modulo the theory of linear rational (& integer) arithmetic.
  - Applications in program analysis & synthesis
- SMT solvers handle the ground fragment. Techniques for quantifiers:
  - Quantifier elimination (expensive)
  - Heuristic quantifier instantiation (incomplete)
- Today: alternating quantifier satisfiability modulo linear rational (& integer) arithmetic via **strategy improvement**.

Game interpretation

$$\varphi \triangleq \underbrace{\exists w. \forall x. \exists y. \forall z.}_{\textit{quantifier prefix}} \underbrace{(y < 1 \vee 2w < y) \wedge (z < y \vee x < z)}_{\textit{matrix}}$$

- Two players: SAT and UNSAT
  - SAT wants to make the formula true
  - UNSAT wants to make the formula false

Game interpretation

$$\varphi \triangleq \underbrace{\exists w. \forall x. \exists y. \forall z.}_{\textit{quantifier prefix}} \underbrace{(y < 1 \vee 2w < y) \wedge (z < y \vee x < z)}_{\textit{matrix}}$$

- Two players: SAT and UNSAT
  - SAT wants to make the formula true
  - UNSAT wants to make the formula false
- A play of this game: SAT and UNSAT take turns picking elements of $\mathbb{Q}$.

$$[\qquad\qquad\qquad\qquad]$$

Game interpretation

$$\varphi \triangleq \underbrace{\exists w. \forall x. \exists y. \forall z.}_{\textit{quantifier prefix}} \underbrace{(y < 1 \lor 2w < y) \land (z < y \lor x < z)}_{\textit{matrix}}$$

- Two players: SAT and UNSAT
  - SAT wants to make the formula true
  - UNSAT wants to make the formula false
- A play of this game: SAT and UNSAT take turns picking elements of $\mathbb{Q}$.

$$[w \mapsto 1; \qquad\qquad\qquad\qquad\qquad\qquad]$$

Game interpretation

$$\varphi \triangleq \underbrace{\exists w. \forall x. \exists y. \forall z.}_{\textit{quantifier prefix}} \underbrace{(y < 1 \vee 2w < y) \wedge (z < y \vee x < z)}_{\textit{matrix}}$$

- Two players: SAT and UNSAT
  - SAT wants to make the formula true
  - UNSAT wants to make the formula false
- A play of this game: SAT and UNSAT take turns picking elements of $\mathbb{Q}$.

$$[w \mapsto 1; x \mapsto \frac{2}{3}; \qquad\qquad\qquad]$$

Game interpretation

$$\varphi \triangleq \underbrace{\exists w. \forall x. \exists y. \forall z.}_{\textit{quantifier prefix}} \underbrace{(y < 1 \lor 2w < y) \land (z < y \lor x < z)}_{\textit{matrix}}$$

- Two players: SAT and UNSAT
  - SAT wants to make the formula true
  - UNSAT wants to make the formula false
- A play of this game: SAT and UNSAT take turns picking elements of $\mathbb{Q}$.

$$[w \mapsto 1; x \mapsto \frac{2}{3}; y \mapsto -1; \qquad]$$

Game interpretation

$$\varphi \triangleq \underbrace{\exists w.\forall x.\exists y.\forall z.}_{\textit{quantifier prefix}} \underbrace{(y < 1 \vee 2w < y) \wedge (z < y \vee x < z)}_{\textit{matrix}}$$

- Two players: SAT and UNSAT
  - SAT wants to make the formula true
  - UNSAT wants to make the formula false
- A play of this game: SAT and UNSAT take turns picking elements of $\mathbb{Q}$.

$$[w \mapsto 1; x \mapsto \frac{2}{3}; y \mapsto -1; x \mapsto 1]$$

Game interpretation

$$\varphi \triangleq \underbrace{\exists w.\forall x.\exists y.\forall z.}_{\textit{quantifier prefix}} \underbrace{(y < 1 \vee 2w < y) \wedge (z < y \vee x < z)}_{\textit{matrix}}$$

- Two players: SAT and UNSAT
  - SAT wants to make the formula true
  - UNSAT wants to make the formula false
- A play of this game: SAT and UNSAT take turns picking elements of $\mathbb{Q}$.

$$[w \mapsto 1; x \mapsto \frac{2}{3}; y \mapsto -1; x \mapsto 1]$$

The SAT player wins if the corresponding structure is a model of the matrix.

Game interpretation

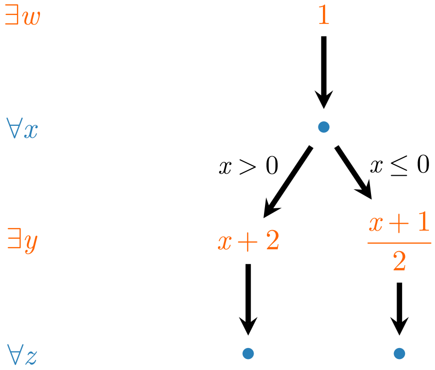
$$\varphi \triangleq \underbrace{\exists w. \forall x. \exists y. \forall z.}_{\textit{quantifier prefix}} \underbrace{(y < 1 \lor 2w < y) \land (z < y \lor x < z)}_{\textit{matrix}}$$

- Two players: SAT and UNSAT
  - SAT wants to make the formula true
  - UNSAT wants to make the formula false
- A play of this game: SAT and UNSAT take turns picking elements of $\mathbb{Q}$.

$$[w \mapsto 1; x \mapsto \frac{2}{3}; y \mapsto -1; x \mapsto 1]$$

  The SAT player wins if the corresponding structure is a model of the matrix.
- φ is satisfiable $\iff$ SAT has a winning strategy

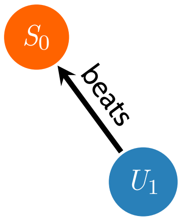
$$\varphi \triangleq \exists w. \forall x. \exists y. \forall z. (y < 1 \vee 2w < y) \wedge (z < y \vee x < z)$$



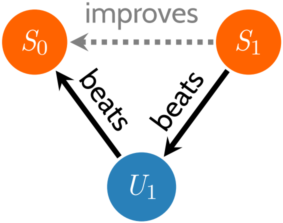
Mutual strategy improvement

S_0

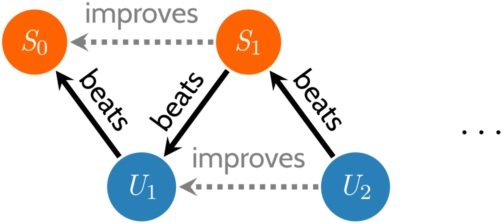
Mutual strategy improvement



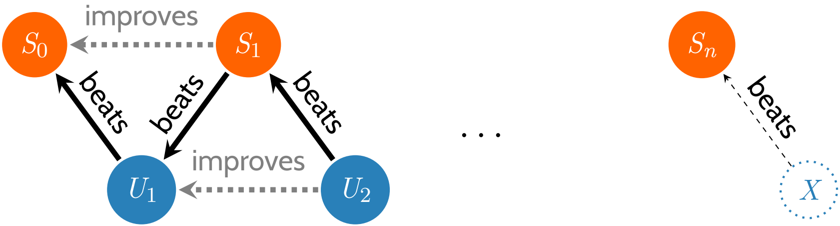
Mutual strategy improvement



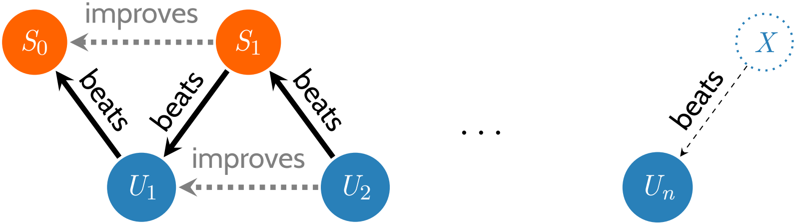
Mutual strategy improvement



Mutual strategy improvement



Mutual strategy improvement



Two questions:

- What does it mean to *improve* a strategy?
- How can we find counter-strategies?

Strategy skeletons

$$\varphi \triangleq \exists w.\forall x.\exists y.\forall z.(y < 1 \lor 2w < y) \land (z < y \lor x < z)$$

Strategy skeletons

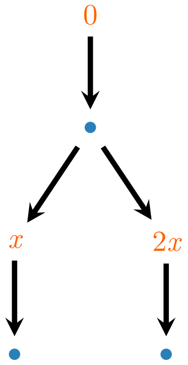
$$\varphi \triangleq \exists w. \forall x. \exists y. \forall z. (y < 1 \vee 2w < y) \wedge (z < y \vee x < z)$$

$\exists w$

$\forall x$

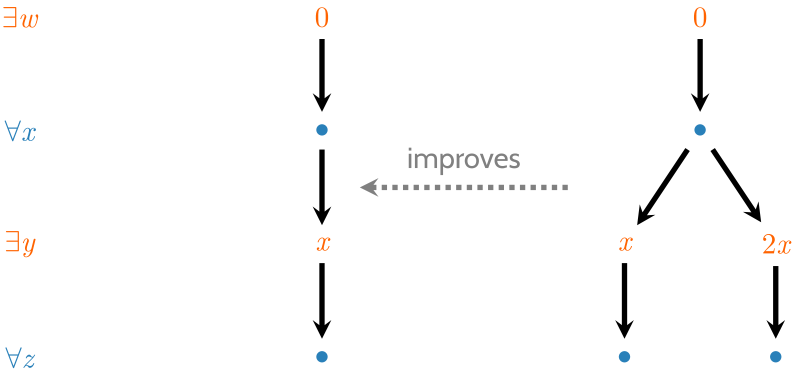
$\exists y$

$\forall z$



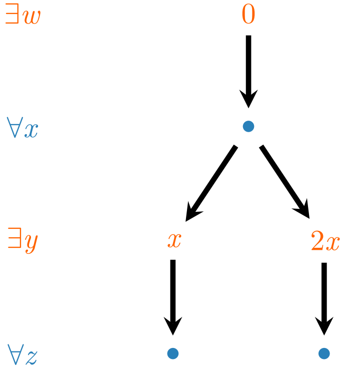
Strategy skeletons

$$\varphi \triangleq \exists w.\forall x.\exists y.\forall z.(y < 1 \vee 2w < y) \wedge (z < y \vee x < z)$$



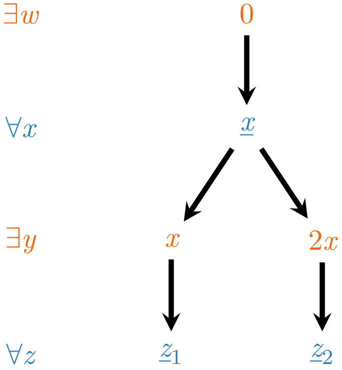
Counter strategy synthesis via ground satisfiability

$$\varphi \triangleq \exists w.\forall x.\exists y.\forall z.(y < 1 \vee 2w < y) \wedge (z < y \vee x < z)$$



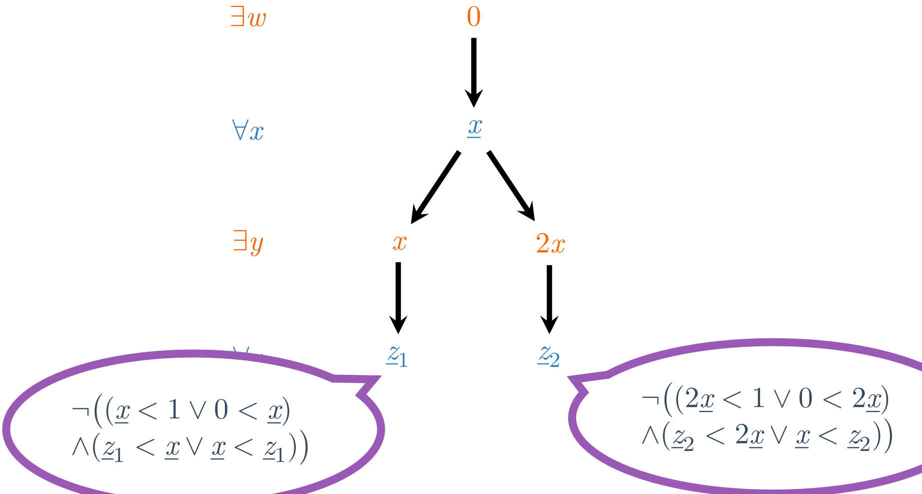
Counter strategy synthesis via ground satisfiability

$$\varphi \triangleq \exists w. \forall x. \exists y. \forall z. (y < 1 \vee 2w < y) \wedge (z < y \vee x < z)$$



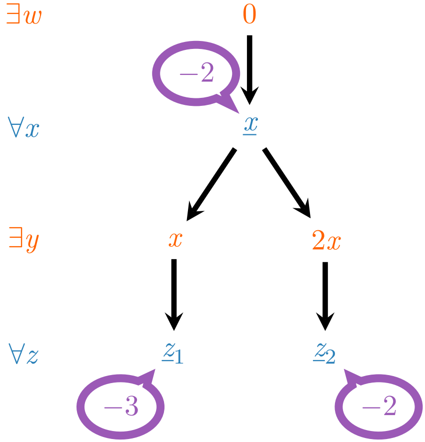
Counter strategy synthesis via ground satisfiability

$$\varphi \triangleq \exists w. \forall x. \exists y. \forall z. (y < 1 \lor 2w < y) \land (z < y \lor x < z)$$



Counter strategy synthesis via ground satisfiability

$$\varphi \triangleq \exists w.\forall x.\exists y.\forall z.(y < 1 \vee 2w < y) \wedge (z < y \vee x < z)$$

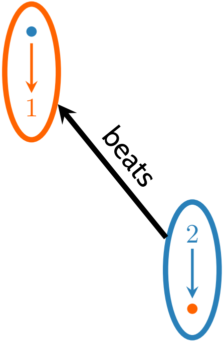


Selecting good strategies

$$\varphi \triangleq \forall x. \exists y. x < y$$

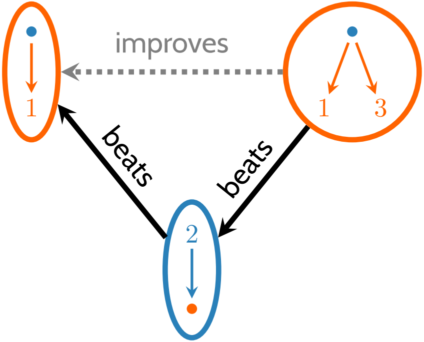
Selecting good strategies

$$\varphi \triangleq \forall x. \exists y. x < y$$



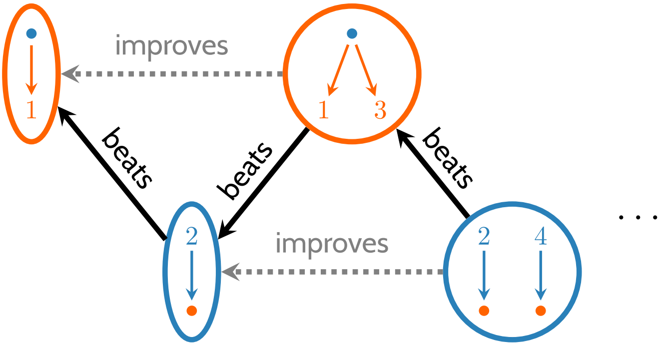
Selecting good strategies

$$\varphi \triangleq \forall x. \exists y. x < y$$



Selecting good strategies

$$\varphi \triangleq \forall x.\exists y.x < y$$



Model-guided term selection

Given:

- ground formula F
- model $m \models F$
- variable x

select(m, x, F) finds a term t such that:

Model-guided term selection

Given:

- ground formula F
- model $m \models F$
- variable x

select(m, x, F) finds a term t such that:

- *(Model preservation)* $m\{x \mapsto [\![t]\!]^m\} \models F$

Model-guided term selection

Given:

- ground formula F
- model $m \models F$
- variable x

select(m, x, F) finds a term t such that:

- *(Model preservation)* $m\{x \mapsto [\![t]\!]^m\} \models F$
- *(Finite image)* $\{\text{select}(m, x, F) : m \models F\}$ is finite

Model-guided term selection

Given:

- ground formula F
- model $m \models F$
- variable x

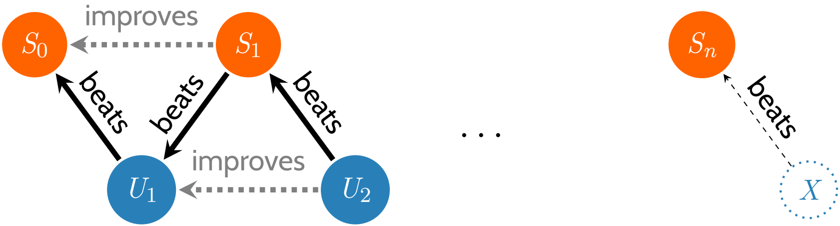
select(m, x, F) finds a term t such that:

- *(Model preservation)* $m\{x \mapsto [\![t]\!]^m\} \models F$
- *(Finite image)* $\{$select$(m, x, F) : m \models F\}$ is finite

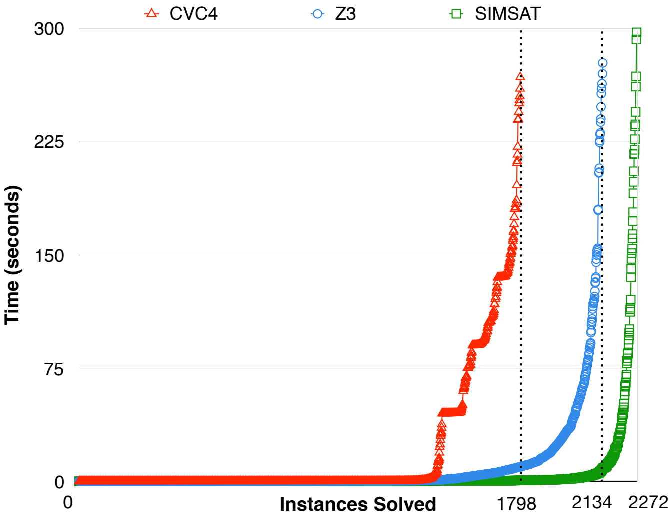
Idea: there is a set of terms T such that $\exists x. F$ is equivalent to $\bigvee_{t \in T} F[x \mapsto t]$.

Use model m to select the right disjunct.
(similar to model based projection - [Komuravelli, Gurfinkel, Chaki 2014]).

Mutual strategy improvement



Experimental results



2421 instances drawn from SMTLIB2 & Mjollnir benchmark suite, 300s time limit.

Thanks!